ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

2024-2025 Educational Webinar Series

Addressing the Expanding IoMT Attack Surface.

October 10, 2024

Eddie Myers
edward.myers@crothall.com

ACCE gratefully acknowledges the sponsorship of the 2024-2025 Educational Webinar series by

About the Moderator

Juuso Leinonen, BEng
Director of Medical Device Cybersecurity and Integration
Crothall Healthcare

Juuso Leinonen is currently the Director of Medical Device Cybersecurity and Integration at Crothall Healthcare where he leads a team of Cybersecurity and Integration Specialists.

Previously, Juuso served at the Device Evaluation group at ECRI where he led various medical technology projects from comparative medical device evaluations to complex medical device accident investigations. Juuso's research efforts led to over 100 ECRI publications, including some global medical device recalls.

In 2022, Juuso received the ACCE-HIMSS Excellence in Clinical Engineering and IT Synergies Award for his work in tackling challenges of managing medical device cybersecurity. Juuso has presented about the challenges of managing medical device cybersecurity at several international, national and local conferences, including at HIMSS and AAMI.

Juuso currently serves as the co-chair of ACCE Education Committee

Logistics

❖All attendees have their microphones muted during the presentation.

❖Questions to the panelists must be submitted via the "Q&A" feature in Zoom at any time. They will be addressed at the Q&A portion.

❖If there is any urgent issue, please use the "chat" feature to communicate with the host/moderator.

❖Please remember to complete the webinar evaluation after attending. A link will be provided at the end.

About the Speaker

Eddie Myers, HCISPP, CBET
National Director, Cybersecurity

crothall healthcare

Eddie Myers is the National Director of Cybersecurity for Crothall Healthcare and oversees Crothall's nation wide cybersecurity initiatives.

With over 20 years in the healthcare industry he brings knowledge not only around Cybersecurity but also PACS, Project Management, IT consulting and technical support.

Session Description

Managing the cybersecurity risks with IoMT devices is rapidly increasing in complexity. Healthcare organizations are facing expanding IoMT fleets with a dynamic threat landscape. In order for healthcare organizations to effectively address these cybersecurity risks with IoMT devices, we must move beyond the inventory and develop a robust medical device vulnerability management program. Join this webinar to learn about the recent trends and practical approaches to analyze cybersecurity risks to expedite your risk reduction efforts!

Agenda

- Emerging cybersecurity **trends** and **challenges**
- Moving **beyond Inventory** to Vulnerability Management, Risk Scores, Risk Simulations, Incident Response, Forensic Analysis, and accurate Utilization information
- Practical ways to **analyze security risk** before procurement
- Value of 3rd party services **to expedite risk reduction** efforts and get your network under control
- Q&A

Trends and Challenges

Healthcare Cybersecurity Trends

43
avg attacks per year
89% of the HDOs experienced an average of 43 attacks

$10M
avg HDO cost per incident
cyber attacks on hospitals cost an avg of $10.1M per incident

20%
increase in mortality from cyber incident
direct-line increase in mortality from cyber incident

1.4%
avg hospital operating margin
the average hospital operating margin is .4% in 2023

6.2
vulnerabilities per medical device
each device has an average of 6.2 vulnerabilities

40%
devices near end-of-life
more than 40% of medical devices in use are at EOL

64%
of HDOs had operational delays
64% of HDOs had delays in operations and 59% had longer patient stays due to incident

44%
breached by third party
of HDOs suffered a data breach caused by a third party in the last year

50%
of incidents caused by lack of talent
by 2025, lack of talent or human failure will be responsible for 50% of cyber incidents

An Ever Expanding Attack Surface

- In few industries is the growth of connected devices so rapid and widespread as it is in the healthcare industry. **Today, the average hospital room contains 15 to 20 connected medical devices.** In some hospitals, connected medical devices outnumber mobile devices, such as laptops and smartphones, 4 to 1.

- **A large hospital could be home to as many as 85,000 connected devices.** While each of these devices has a significant role in the delivery of care and operational efficiency, each connected device can also open the door to a malicious cyberattack.

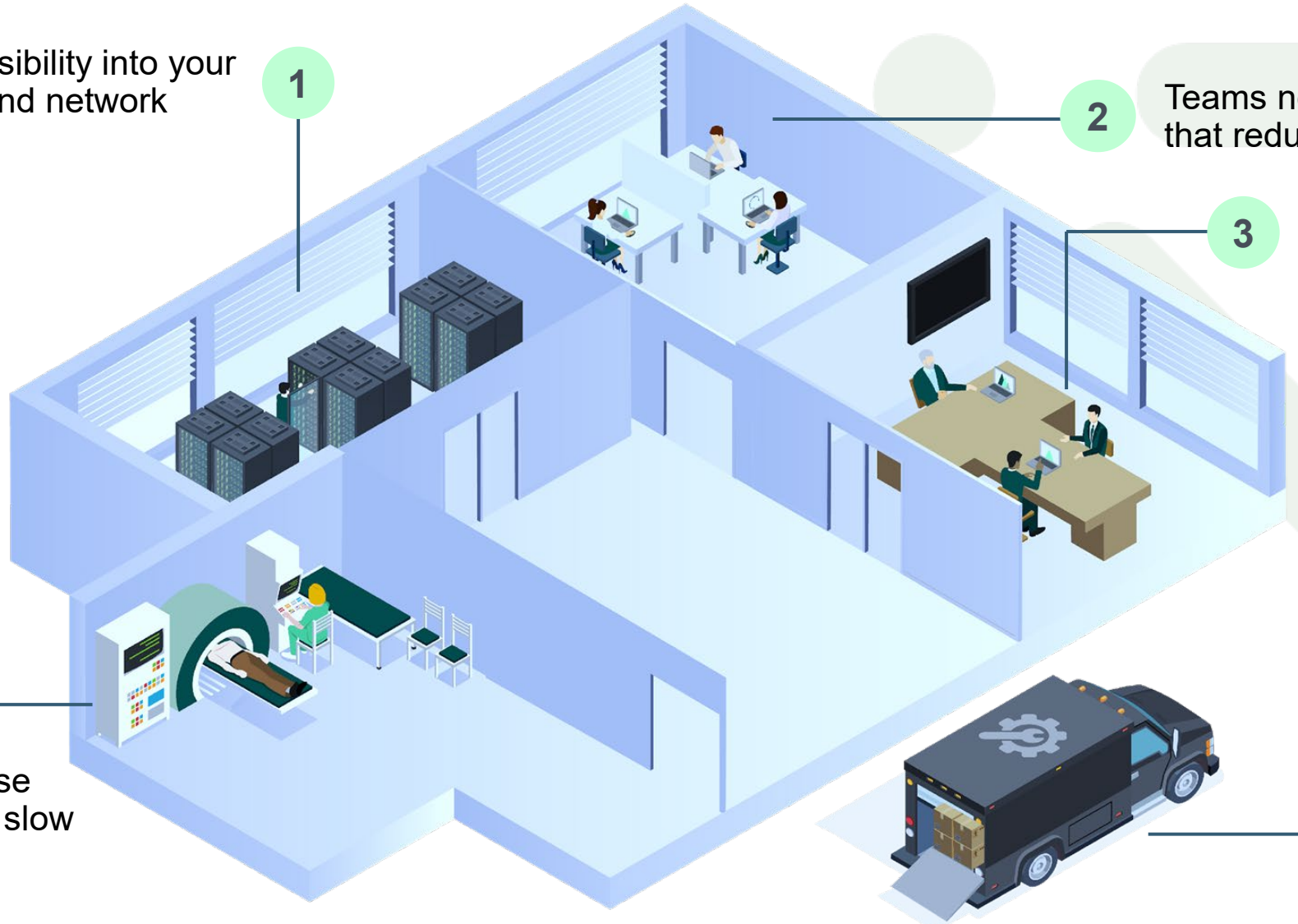
www.businessnewsdaily.com/15031-connected-medical-devices-healthcare-cybersecurity.html

Challenges Hospitals Face With Device Risk

1 Lack of visibility into your devices and network

2 Teams need help prioritizing the work that reduces risk the most

3 Risk is difficult to define, measure, and reduce



4 Incident Response is disruptive and slow

5 Third-party risks are concerning

How Should This Work?

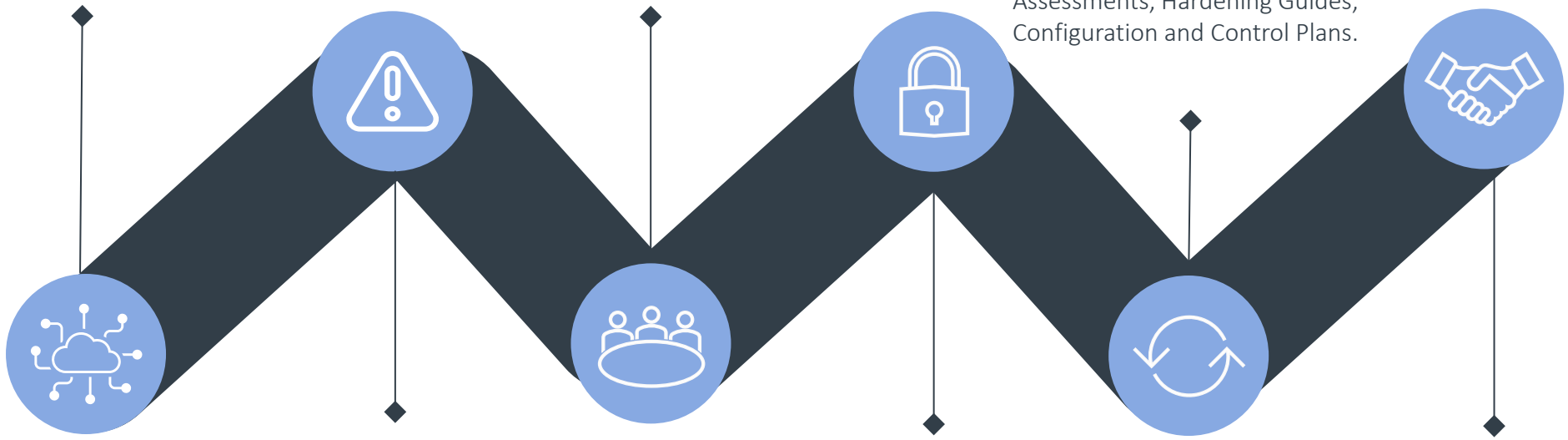
What does Good Look Like?

Addressing the Problem in 6 Easy Steps

Complete Visibility
All Sites, All Devices,
All Connections, in Real-time

Collaborating for Remediation
It is critical that the different teams work together to remediate risk

Manage Across the Lifecycle
Pre-Procurement Risk Assessments, Hardening Guides, Configuration and Control Plans.



Understand Your Risk
What is vulnerable, Why is it at risk, and what do you need to do to Remediate

Protect from Real-Time Threats
Identify real-time threats to devices quickly and have a tested plan for Incident Response

Leveraging Vendors
Use Vendors to fill in the gaps where your missing skills, manpower, etc.

Moving Beyond Inventory

Accurate Classification

- ✓ Tools should use AI-based classification and support multiple sources for Asset Identification.
- ✓ Configurable classification is important to support

AI & Deep Packet Inspection

- ✓ Purchase tools that use both DPI and AI.
- ✓ Some tools only use DPI and this creates a shadow IT problem, AI and DPI is best.

Beyond the Basics

- ✓ Tools should provide data beyond the basics of IP, MAC, OS.
- ✓ All Sites, All Devices, All Connections in real-time. This includes IoT, IoMT, IoLT, and OT.

Understanding Attack Paths

Stay away from tools that just give you a big list of vulnerabilities but don't do anything to reduce false positives or validate that a CVE is attackable.

An industry **standard exploit analysis such as MITRE ATT&CK should be completed** and must take into consideration the following:

- Device and Network Configuration
- MDS2's/SBOMs
- Network Neighbors

Key to Mitigating Vulnerabilities

Is it feasible/cost effective to patch?

▶ Then Apply patches

Can we mitigate the exploit vector?

▶ Then Apply Mitigation

Apply Full segmentation

Not all vulnerabilities are attackable within your network, and if they can't be exploited then their risk is minimal

Collaborating for Success

Effective collaboration is key to remediation. Organizing around a process with clear roles and responsibilities

Forming a committee comprised of HTM, Information Security, and Network Engineering, and Vendors

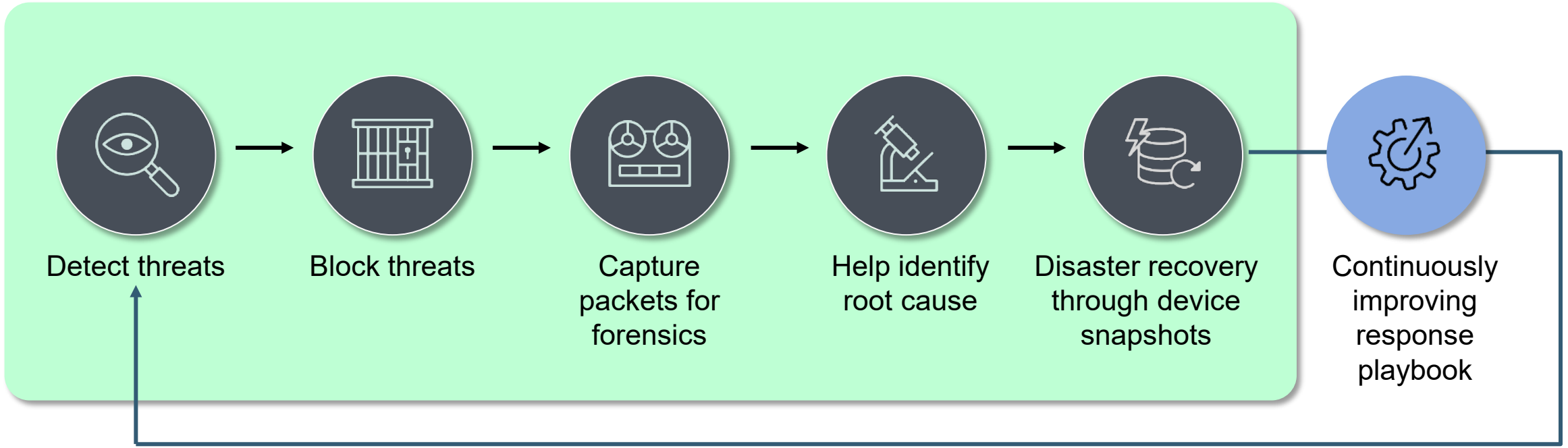
Another critical success factor is an **effective Change Management** process

Leveraging your vendors for help as well

Threat Detection & Integrated Response

BENEFITS

- Minimize Incidents
- Accelerate Investigations
- Recover Rapidly



Keys to Success for Medical Device Risk Management

Having a well-defined, staffed and implemented program means **you must manage across the lifecycle**. We recommend the following phases.

1. Pre-Procurement
2. Hardening and Deployment
3. Operations
4. Disposition/Retirement

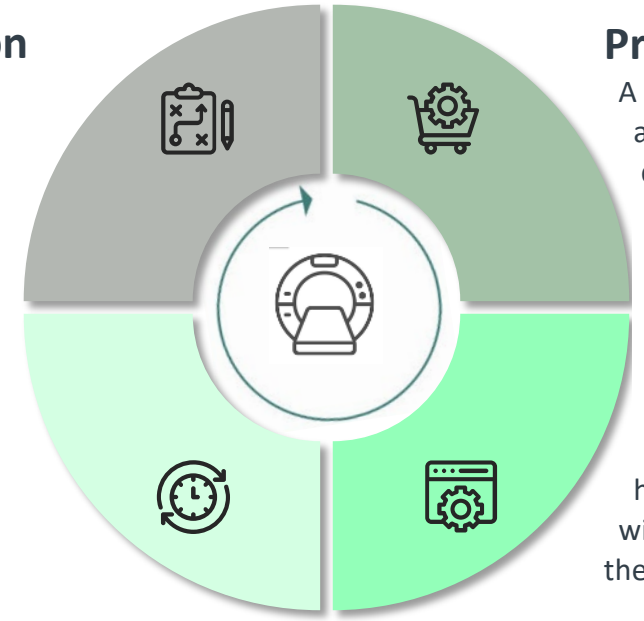
These are typically not managed by the same team but usually involve, IS, Networking, HTM, and Procurement or Capital Planning. It is not uncommon for one or many of these to be outsourced.

Managing across the lifecycle of the device

It is critical that you have an integrated process for managing a device from Pre-Procurement to Disposition.

Disposition

Before being retired the device should be sanitized and properly decommissioned



Pre-Procurement

A pre-procurement risk assessment should be done to determine the best medical device to buy with the lowest risk

Operations

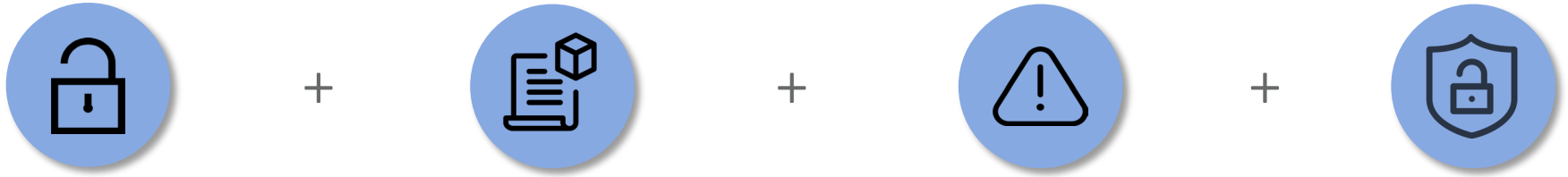
Once placed into operation the device should be monitored for anomalies and changes in its risk profile

Deployment

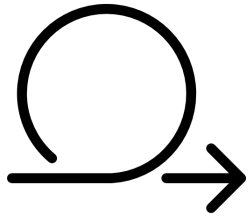
The device should be hardened in accordance with a plan for all similar devices and then deployed

Risk Assessments: Functional/Valuable

A valuable risk assessment must accomplish the following:



Inputs
- MDS2's
- SBOM's
- Clinical Workflow
- Service & Operator Manuals
- Device Deployment Plan



Outputs
- Documented Exploitable vulnerabilities
- Hardening Guide
- Configuration Plan
- Documented Exceptions

Value of Managed Solutions

Why are Cybersecurity Managed Solutions Critical?

Investment In Resources/Staffing

Access to a variable workforce and flexible technology, supporting your dynamic cybersecurity needs when and where you want it.

Concentrate On Your Core Mission: Patient Care Services

Navigating the ever-evolving threat and regulatory landscapes can be a challenge, consuming the time clients spend on patient care.

Threats are Constantly Growing in Sophistication

By relying on managed solutions, hospitals can access cutting-edge capabilities not available in-house.

Thank You

Any question?

Please type your questions to the Zoom Q&A window

Please complete the online evaluation form at
https://www.surveymonkey.com/r/2024-2025_web2