
January 18, 2022
ACCE gratefully acknowledges the sponsorship of this webinar by CyberMDX
About the moderator

Martin Poulin, P.Eng., FCMBES | Director, Biomedical Engineering

Director of Biomedical Engineering for Island Health, Victoria, BC, on the west coast of Canada.

23+ years health technology management.

5 years in the medical device development industry in Vancouver.

Master of Engineering in Clinical Engineering from UBC.

Past President of CMBES.

Member, 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 (not chat) in Zoom at any time.

• If there is any urgent issue, please use the “chat” feature to communicate with the panelists.

• We will try to ask Amir and Shannon to answer questions not addressed during the webinar and post them to ACCE website.

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

- Over 15+ years in IoT, cybersecurity, information security and enterprise software solutions.

- Holds a MBA, and BSc. Degree in Electrical and Computer Engineering and is working towards PhD in Organizational Leadership.
About the speaker

• Sodexo employee for 16+ years
• Bachelor degrees: Computer Science and Chemistry
• Healthcare experience 31+ years
• Medical Information Technology experience 26+ years
• Healthcare Technology experience 16+ years
• Medical device security over 6 years
Biomedical engineers responsible for healthcare technology management (HTM) make significant decisions that affect a hospital’s cyber security posture. Whether it's procuring new medical devices, managing device end-of-life, or connecting devices to the network, it’s critical that any decisions they make consider device security, data integrity, and patient safety.

In this webinar, we’ll discuss some of the challenges facing biomedical engineers – from procuring devices that have potential vulnerabilities to lack of device visibility and centralized management – and the security team should support their initiatives and integrate them into their overall cyber security strategy.

Attendees will learn:

- Best practices for managing hyper-connected environments.
- How a full discovery and profile of all the connected devices in the network (medical devices, IoT, Workstations, Mobile, servers) provide critical information for the entire organization.
- How to strategically improve the security posture of connected assets.
Agenda

• Understanding Both Worlds
• Best practices for managing hyper-connected environments
• Looking forward – a glimpse into the future
Agenda

• Understanding Both Worlds
• Best practices for managing hyper-connected environments
• Looking forward – a glimpse into the future
Typically, different organizations

Often, different objectives
**Biomedical Engineering: By Now, You Know This**

**HTM Lifecycle Management Must Include Medical Device Security**

<table>
<thead>
<tr>
<th>Challenges:</th>
</tr>
</thead>
</table>
| ❑ Time and resource required to manage assets  
| ❑ Lack of experience with security as part of lifecycle management  
| ❑ Not enough context/information for each asset  

<table>
<thead>
<tr>
<th>Seeks:</th>
</tr>
</thead>
</table>
| **Automate Inventory Management**  
Find what you need quickly - enriched with critical data, patching recommendations, and location info.  

**Maximize Device Utilization and Efficiency**  
Optimize usage across device, lifecycle, and allocation decisions (e.g., locate underutilized infusion pumps)  

**Lower TCO and Annual Maintenance Costs**  
Streamline maintenance schedules to avoid unplanned downtime and lost availability.  

---

Copyright © 2021 Cyber MDX
# CISO/IT Security

IT Security Teams Must Protect Critical Medical Assets

<table>
<thead>
<tr>
<th>Challenges:</th>
<th>Complexities and budget constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lack of security tools designed for medical devices</td>
</tr>
<tr>
<td></td>
<td>Escalating attacks on healthcare data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Seeks:</th>
<th>Scalable and Easy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Works across multiple network architectures (centralized, distributed, segmented) enabling scale, easy install, and optimal efficiency.</td>
</tr>
</tbody>
</table>

**End-to-End Risk Mitigation**

Zero-trust security model enables micro-segmentation based on asset visibility and trusted relationships.

**Leverages Existing Infrastructure**

CyberMDX integrates with diverse third-party products across IT systems and network solutions.
The Threats for Both Teams are the Same

- It’s a Patient Safety Imperative.
  - Medical devices can stop working or malfunction

- It’s a Threat to Data Security.
  - Healthcare data can be stolen and sold

- It’s a Huge Risk to Financials.
  - Hostile takeovers can hold you for ransom
1. Not automating inventory
2. Not protecting medical devices
3. Relying on patching as defense
4. Waiting vs preparing at install
5. Expecting compliance or insurance is a solution

Top 5 GAPs of Healthcare Security
Agenda

• Understanding Both Worlds
• Best practices for managing hyper-connected environments
• Looking forward – a glimpse into the future
1. Automated Asset Mgmt & Tracking
2. Intelligent Mitigation of Risks
3. New Vulnerability Insights with prioritization
4. Guidance & Reporting for onboarding new devices
5. Ongoing compliance alignment

How to Address the Gaps

5

BEST Practice Recommendations
Best Practice 1: Create a Live Inventory

**Enabler of Other Use Cases**
- On-going cyber risk management
- FDA compliance
- Software compliance
- Incident response
- Device tracking
- Daily service routines

- Live, Continuously up to date
- Complete
- Accurate and security-aware
- Provide Clinical Context
- Drive Cyber risk management
- Integrated
Without One, Manual Inventory Fails

Yesterday

Modern ICU ecosystem
Best Practice 2: Intelligently Mitigate Risks

Ongoing
Device-Centric
Risk Management

On-Device Remediation

- Configuration
- Patching
- AV/Agent

External Access Control

- Vendor Access Control
- Block Internet

Network-based Mitigation

Allowlist Policy
Blocklist Policy
Best Practice 3: Keep tabs on new vulnerabilities
Best Practice 4: Onboard With Compliance
Best Practice 5: Governance With Compliance
Agenda

- Understanding Both Worlds
- Best practices for managing hyper-connected environments
- Looking forward – a glimpse into the future
Major upcoming healthcare changes

Will Challenges Stay the Same?

Hospital EMRs & Personal Medical Device Data Interoperability

- Inventory
- Risk Management
- Compliance
- Operational Efficiency

Copyright © 2021 Cyber MDX
Strategy: Create Layers of Protection

- Asset Management and Inventory
- Concise Risk Assessment and Security Insights
- Network Segmentation
- Threat Detection
- Incident Response Playbook
BioMed and Cyber Security Together

A single source of truth that breaks down siloes
Get in touch!

Amir Vashkover
VP, Business Development & Strategic Alliances
amir_v@cybermdx.com

Shannon P. Lavack
Senior Project Manager, HTM IT
shannon.lavack@sodexo.com
Questions
Thank You

Please complete the online evaluation at
https://www.surveymonkey.com/r/01-18-22_evaluation

Or scan this QR code to complete survey: