IoMT Risk Remediation: How Context-rich Assessments Rationalize Response Effectiveness

Drew Ganther - Presenter
Regional Director of Sales – WEST
Medigate

Matt Dimino - Presenter
Connected Asset Program Manager
First Health Advisory

July 22, 2021
ACCE gratefully acknowledges the sponsorship of this webinar by MEDIGATE
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.
22+ years management
5 years in the medical device development industry in Vancouver.
Master of Engineering in Clinical Engineering from UBC
Past President of CMBES
About the speaker

Drew Ganther, Regional Director at Medigate

Drew Ganther is Regional Director at Medigate. Before joining Medigate as the first sales leader in the western US, Drew spent 7 years with an IT systems reseller and professional services organization where he helped create a cyber security consulting practice (later acquired by Insight). Drew’s career started in IT training after he moved from Virginia Beach, VA to San Diego, CA with his Bachelors Degree from James Madison University in Harrisonburg, VA.
About the speaker

Matt Dimino, Connected Asset Program Manager at First Health Advisory

Matt comes to First Health as a Connected Asset Program Manager. He brings a wide range of technical, security, academic and HTM knowledge to this team. Matt has over 15 years’ experience in various roles from associate faculty teaching Infosec, IT, HTM courses, and HTM leadership roles, many of those years as a practitioner in medical device security. Through his career he has developed multiple security programs, integrated complex architectures, performed security consulting, as well as developed risk assessment methodologies coupled with hands on device hardening experience. A major focus for Matt is to expand on IoMT risk management strategies and prepare First’s customers and partners for the future of IoMT.
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 Drew and Matt to answer questions not addressed during the webinar and distribute them to participants via email or post them to ACCE website.

• Please remember to complete the webinar evaluation after attending. A link will be provided at the end.
IoMT risk is constant and ever evolving as the threat landscape changes and our ecosystem of disparate systems continues to grow and intertwine. IoMT systems have numerous dependencies and factors that create not only inherent risk, but aggregated and cascading risk which can have significant impacts on how and what IoMT risks to remediate. The process behind risk remediation is to characterize the systems and contextualize the risks to understand what they mean to the organization faced with them before trying to remediate them. Today, to properly remediate IoMT risks, healthcare organizations must understand the environment of the risks and learn how to prioritize by evaluating and ranking risks that are most credible.

Medigate’s Drew Ganther and Matt Dimino from First Health Advisory will host a conversation about the IoMT risk identification and remediation. Webinar attendees will be treated to an open, candid discussion.
IoMT Risk

Your Challenge

• CVE’s / CISA notifications, industry alerts, and IoMT passive scanning tools are revealing more vulnerabilities, increasing risk, and it’s unclear how to manage and prioritize.

• Organizations are struggling to not only understand IoMT risk but also how to prioritize vulnerabilities for remediation, as there are many factors to consider, including the threat of the vulnerability, the exposure, and the potential remediation option.

Common Obstacles

• Patches are often seen as an answer to vulnerabilities, but these are rarely an applicable solution as many IoMT systems cannot be patched.

• Many don’t understand that vulnerabilities for IoMT devices exist beyond CVE’s and CVSS scores.

• Organizations are unaware of the risk implications and lack insight to remediation options.

Approach

• Design and implement a risk management program that identifies, prioritizes, and remediates vulnerabilities, anomalies and risk.

• Understand what needs to be considered when implementing remediation options, including patches, configuration changes, and defense-in-depth controls.

• Build a strategy from a framework that includes a risk management lifecycle approach that allows you to identify risk, assess risk, apply risk response and mitigation efforts and risk monitoring.
IoMT Risk is a Business Risk

• The business risk associated with the use, ownership, operation, involvement, influence and adoption of IoMT within an enterprise.

• We are failing to grasp the security risks of our IoMT assets.
  • Risk is constant and ever evolving as the threat landscape changes and our ecosystem of disparate systems grows.
  • IoMT has dependencies and factors that create not only inherent risk but aggregated and cascading risk.
  • Understand the environment of the risks and learn how to prioritize by evaluating and ranking risks that are most credible.

• Process behind risk remediation is to characterize the systems and contextualize the risks to understand what they mean to the organization.
What is Risk?

- **Risk** is a combination of the probability of an event and its consequences.
- The probability of an event is the likelihood that a given threat will exploit an exposed vulnerability.
- If there are no consequences or impact, there is considered to be no risk.
- Conversely, the greater the consequences or impact, the greater the risk.

- **Exposure**, the extent to which a vulnerability is exposed, to a threat factors into the risk equation.
- Exposure is also known as the attack surface.
- Exposure is affected by the extent and effectiveness of controls and where a particular device is within the network.
What is a Vulnerability?

Any kind of exploitable weak spot in your defense that threatens your organization:

- Unpatched Software
- Misconfiguration
- Weak Credentials
- Phishing
- Trust Relationships
- Compromised Credentials
- Malicious Insider
- Missing Encryption
- Zero-days and Unknown Methods
Elements of IoMT Risk

- Consequences associated with specific assets
- A threat to those assets, requiring both intent (motivation) and capability
- Vulnerability specific to the threat
The Risk Management Approach

- Develop a Risk Management Strategy
  - Define scope and charter
  - Define risk appetite
- Begin by identifying risk
- Frame and analyze risk
- Evaluate Risk

Risk Management Lifecycle:
- Risk Identification
- Risk Assessment
- Risk Response and Mitigation
- Risk and Control Monitoring and Reporting
The Risk Management Approach

Risk Management Process

- Context Establishment
- Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment

Risk Management Lifecycle

- Risk Identification
- Risk Assessment
- Risk Response and Mitigation
- Risk and Control Monitoring and Reporting
Assessing Risk

- A comprehensive risk assessment includes:
  - System Characterization
  - Threat Identification
  - Vulnerability Identification
  - Control Analysis
  - Likelihood Determination
  - Impact Analysis
  - Risk Determination
  - Control Recommendations
  - Results Documentation
- Define asset criticality and sensitivity
- Creation of a fully connected asset inventory

A risk matrix is useful in calculating a risk rating for vulnerabilities.
Contextualizing Risk

• Creating a risk profile:
  • Data (Impact)
  • Patient (Impact)
  • Business (Impact)
  • Active Vulnerabilities (likelihood)
  • Security Capabilities (likelihood)
  • Technical/Administrative / Physical controls (likelihood)
• Develop scoring metrics / Risk Ranking
Assessing Risk - System Characterization - Threat ID

2.3.1 Security / Vulnerabilities / Top 10 Clinical Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability Name</th>
<th>Affected Models</th>
<th>Affected Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICSMA-17-250-02A</td>
<td>1</td>
<td>799</td>
</tr>
<tr>
<td>ICSMA-20-317-01</td>
<td>2</td>
<td>577</td>
</tr>
<tr>
<td>ICSMA-17-017-02A</td>
<td>1</td>
<td>575</td>
</tr>
<tr>
<td>ICSMA-18-128-01</td>
<td>4</td>
<td>38</td>
</tr>
<tr>
<td>ICSMA-19-248-01</td>
<td>1</td>
<td>36</td>
</tr>
<tr>
<td>ICSMA-20-049-02</td>
<td>6</td>
<td>19</td>
</tr>
<tr>
<td>ICSMA-20-343-01</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>ICSMA-20-777-01</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>ICSMA-20-170-01</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ICSMA-18-226-01</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

N / M / L Risk Score Distribution

Risk Score Distribution

- % Devices
- Risk Score
  - Critical
  - High
  - Medium
  - Low
  - Very Low
Assessing Risk - Vulnerability Identification

<table>
<thead>
<tr>
<th>Vulnerability Name</th>
<th>Affected Models</th>
<th>Affected Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICSMA-17-250-02A</td>
<td>1</td>
<td>799</td>
</tr>
<tr>
<td>ICSMA-20-317-01</td>
<td>2</td>
<td>577</td>
</tr>
<tr>
<td>ICSMA-17-017-02A</td>
<td>1</td>
<td>575</td>
</tr>
<tr>
<td>ICSMA-18-128-01</td>
<td>4</td>
<td>38</td>
</tr>
<tr>
<td>ICSMA-19-248-01</td>
<td>1</td>
<td>36</td>
</tr>
<tr>
<td>ICSMA-20-049-02</td>
<td>6</td>
<td>19</td>
</tr>
<tr>
<td>ICSMA-20-343-01</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>ICSMA-20-777-01</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>ICSMA-20-170-01</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ICSMA-18-226-01</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

2.3.1 Security / Vulnerabilities / Top 10 Clinical Vulnerabilities

<table>
<thead>
<tr>
<th>Device Inventory</th>
<th>Visio Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>44,483 Corporate</td>
<td>119 Guest</td>
</tr>
<tr>
<td>5,944 Medical</td>
<td>15,963 IoT</td>
</tr>
<tr>
<td>44,602 Devices</td>
<td>22,695 IT</td>
</tr>
<tr>
<td>14,733 Online</td>
<td>29,869 Offline</td>
</tr>
<tr>
<td>3,587 High Risk</td>
<td>4,202 New This Week</td>
</tr>
</tbody>
</table>

Vulnerability Score Distribution

- Critical: <0.1%
- High: 7.9%
- Medium: 72.3%
- Low: 13.1%
- Very Low: 6.6%
Remediation recommendations:

- Assign static IP addresses to the Medfusion 4000 Wireless Syringe Infusion Pump.
- Monitor network activity for rogue DNS and DHCP servers.
- Ensure network segments which the Medfusion 4000 medical infusion pumps are installed are segmented from other hospital and clinical information technology infrastructure.
- Consider network micro segmentation.
- Consider use of network virtual local area networks (VLANs) for the segmentation of the Medfusion 4000 medical infusion pumps.
- Apply proper password hygiene standards across systems (i.e., use uppercase, lowercase, special characters, and a minimum character length of eight).
- Do not re-use passwords.
Assessing Risk - Likelihood Determination

Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump:

- Syringe infusion pumps used to deliver small doses of medication in acute care setting
- No known public exploits specifically target these vulnerabilities
- Only an attacker with high skill would be able to exploit these vulnerabilities.

Remediation recommendations:

- Assign static IP addresses to the Medfusion 4000 Wireless Syringe Infusion Pump.
- Monitor network activity for rogue DNS and DHCP servers.
- Ensure network segments which the Medfusion 4000 medical infusion pumps are installed are segmented from other hospital and clinical information technology infrastructure.
- Consider network micro segmentation.
- Consider use of network virtual local area networks (VLANs) for the segmentation of the Medfusion 4000 medical infusion pumps.
- Apply proper password hygiene standards across systems (i.e., use uppercase, lowercase, special characters, and a minimum character length of eight).
- Do not re-use passwords.
Assessing Risk - Risk Determination

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Total Score (Impact + Likelihood)</th>
<th>Category Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>0-7</td>
<td>Medical devices with no active technical vulnerabilities, a low impact on patient care, little to no ePHI storage or transmission, and little to no organizational impact if disabled. Likely an acceptable risk level without additional review.</td>
</tr>
<tr>
<td>Moderate</td>
<td>8-13</td>
<td>Medical devices with no active technical vulnerabilities but may have non-technical vulnerabilities and few or no technical security controls currently implemented. These devices have a lower impact on patient care, data, and the overall business operations of the organization.</td>
</tr>
<tr>
<td>High</td>
<td>14-18</td>
<td>Medical devices that likely have at least one active technical vulnerability requiring remediation activities or extremely robust compensating controls to be implemented - causing a very high likelihood of threat occurrence. These devices usually have non-technical vulnerabilities, do not have any technical security controls currently implemented, will impact care delivery if affected, and store and/or transmit large amounts of ePHI. It is not suggested to proceed at this risk level.</td>
</tr>
<tr>
<td>Critical</td>
<td>19-21</td>
<td>Medical devices with more than one active technical vulnerability requiring specific remediation activities to mitigate, such as, security updates or system upgrades which causes a very high likelihood of threat occurrence. These devices also directly impact patient care and pose a risk to patient safety if affected, store and/or transmit large amounts of ePHI, and have a high level of asset utilization causing a higher level of impact to the organization if disabled.</td>
</tr>
</tbody>
</table>
Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump:

- Syringe infusion pumps used to deliver small doses of medication in acute care setting
- No known public exploits specifically target these vulnerabilities
- Only an attacker with high skill would be able to exploit these vulnerabilities.

Remediation recommendations:

- Assign static IP addresses to the Medfusion 4000 Wireless Syringe Infusion Pump.
- Monitor network activity for rogue DNS and DHCP servers.
- Ensure network segments which the Medfusion 4000 medical infusion pumps are installed are segmented from other hospital and clinical information technology infrastructure.
- Consider network micro segmentation.
- Consider use of network virtual local area networks (VLANs) for the segmentation of the Medfusion 4000 medical infusion pumps.
- Apply proper password hygiene standards across systems (i.e., use uppercase, lowercase, special characters, and a minimum character length of eight).
- Do not re-use passwords.
Prioritizing Remediation Response

- Triage vulnerabilities, filter out the noise
- Evaluate vulnerabilities for urgency (verified exploit, CVSS base of 7+, lateral movement)
- Determine business criticality
- Use patient safety factors to help determine urgency
- Review current security posture
  - What does your network look like? (Flat, ACL’s, VLANS, )
  - Defense-in-depth controls
Prioritize Remediation Based on Risk

- Identify remediation options
  - Patch or update
  - Configuration change
  - Compensating controls
  - Accept the risk
- Assess the options and identify how to implement
  - Task force
  - Operationally (PM’s & CM’s)
- Implement or select another option
Remediation Response Effectiveness

- Based on a Risk Management Strategy
  - List of controls
  - Risk appetite
- Create a risk register / risk treatment plan
- Input assessment and response activities into CMMS as work orders
- Properly code and track work orders and progress
  - Establish a baseline
- Heavily consider IoMT passive scanning solution and CMMS integration

<table>
<thead>
<tr>
<th>Rank</th>
<th>HTM Risk Treatment Plan Description</th>
<th>% Complete</th>
<th>Estimated Completion Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Address CVE-2020-1350 – Patch</td>
<td>50%</td>
<td>8/14/2021</td>
<td>48 Devices initially affected, Current: 24</td>
</tr>
<tr>
<td>7</td>
<td>Non-medical device in medical device VLANS</td>
<td>28%</td>
<td>6/1/2022</td>
<td>Risk Management Program Related</td>
</tr>
<tr>
<td>6</td>
<td>Medical devices communicating externally with unsecure protocols</td>
<td>85%</td>
<td>8/1/2021</td>
<td>Risk Management Program Related</td>
</tr>
<tr>
<td>7</td>
<td>Address medical device inventory deficiencies</td>
<td>94%</td>
<td>8/1/2021</td>
<td>Initial: 462, Current: 97</td>
</tr>
<tr>
<td>3</td>
<td>Change of default passwords on infusion pumps</td>
<td>100%</td>
<td>12/1/2020</td>
<td>Complete</td>
</tr>
<tr>
<td>2</td>
<td>Determine enterprise and IoMT risk appetite</td>
<td>100%</td>
<td>1/1/2021</td>
<td>Complete</td>
</tr>
<tr>
<td>3</td>
<td>Medical device security strategy, and executive engagement and ownership</td>
<td>100%</td>
<td>3/1/2021</td>
<td>Complete</td>
</tr>
<tr>
<td>4</td>
<td>Address medical device alert workflows</td>
<td>100%</td>
<td>3/1/2021</td>
<td>Complete</td>
</tr>
<tr>
<td>4</td>
<td>Ad hoc threat intelligence and profiling</td>
<td>100%</td>
<td>4/1/2021</td>
<td>Complete</td>
</tr>
<tr>
<td>3</td>
<td>Instances of unmanaged privileged access</td>
<td>100%</td>
<td>4/1/2021</td>
<td>Complete</td>
</tr>
<tr>
<td>5</td>
<td>Limited protective technologies deployment</td>
<td>100%</td>
<td>5/1/2021</td>
<td>Complete</td>
</tr>
<tr>
<td>3</td>
<td>Med devices at clinics not centrally managed.</td>
<td>100%</td>
<td>6/1/2021</td>
<td>Complete</td>
</tr>
</tbody>
</table>
Metrics, KPI’s, and CSF’s

• Without metrics, you lack the visibility to manage or improve your processes.
• KPIs are the specific metrics that help you track performance. KPIs tell the story of “how are we doing?”
• CSFs are the specific KPIs that track the activities that are necessary to accomplish for the organization to be successful.

<table>
<thead>
<tr>
<th>Business Goal</th>
<th>Critical Success Factor</th>
<th>Key Performance Indicator</th>
<th>Metric to track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimize overall risk exposure</td>
<td>Reduction of overall risk due to vulnerabilities</td>
<td>Decrease in the number of vulnerabilities</td>
<td>The number of vulnerabilities year after year.</td>
</tr>
<tr>
<td>Appropriate allocation of resources</td>
<td>Proper prioritization of mitigation activities</td>
<td>Decrease of critical and high vulnerabilities</td>
<td>The number of critical and high vulnerabilities.</td>
</tr>
<tr>
<td>Consistent &amp; measurable remediation of threats to</td>
<td>Minimize risk when vulnerabilities are detected</td>
<td>Remediate vulnerabilities more quickly</td>
<td>The average time between the identification to remediation.</td>
</tr>
<tr>
<td>the organization</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Questions
Thank You

Please complete the online evaluation at
https://www.surveymonkey.com/r/ACCE_07-22-21

Or scan the QR code: