Mayo Clinic Efforts to Secure Connected Medical Devices and HIoT

August 27, 2020
Keith Whitby, MBA, CHTM

Keith has worked at Mayo Clinic for over 22 years in several different support and leadership roles. He is currently the Section Head of Healthcare Technology Management Cybersecurity and Operations. Keith has also had several other positions in HTM, starting as a Unit Manager of the X-Ray equipment service group and most recently as the Section Head for Enterprise Lab, Research, and Ophthalmology Service. Prior to his roles in HTM, he worked in Surgical Services as a Core and Prosthesis Supervisor, and as a Surgical Process/Systems Analyst.

During his time at Mayo, Keith has had extensive experience collaborating on several multidisciplinary teams. He has demonstrated a commitment to customer service, strong leadership skills, and experience with process analysis, project management, and technical support. During his tenure in Surgical Services and HTM, he has been exposed to the depth and breadth of medical equipment in a large healthcare organization. This includes the use of, service and support on, and the operationalization of cybersecurity for a wide range of medical equipment and HIoT technology.
Pandian Gnanaprakasam currently serves as Chief Product Officer at ORDR Inc., an agentless devices security startup company, that he co-founded. Before the current role, he was the Chief Development Officer at Aruba, responsible for all of engineering and product management functions. Aruba, is an enterprise mobile wireless company, which got acquired by HPE for $3 Billion in March 2015.

With 20 years of engineering and product management experience, Pandian has held various engineering management roles in Cisco Systems, a computer networking company. During his long career at Cisco, Pandian worked on various networking products, that includes routers, switches, WiFi, security and others. Before departing for Aruba, Pandian served as the head of engineering for Cisco’s WiFi product line taking the business unit to multi-billion dollar run rate. Before that, he was also the vice president of engineering for the low-end switching, a very successful product line, that has also reached several billion dollars’ annual run rate.

Pandian graduated with a Master's degree in Electrical Engineering from IIT, Chennai, India and holds several patents to his credit in various networking technologies.
Mayo Clinic – At a Glance
Mission:

To inspire hope and contribute to health and well-being by providing the best care to every patient through integrated clinical practice, education and research

Primary value:

The needs of the patient come first.
HTM Organizational Structure

• ~280 HTM Staff: ~220 Biomed technicians, ~20 Managers & ~40 Support staff
• 26 Shops providing services in over 66 communities, and spanning 5 states
• Over 130,000 medical devices and systems inventoried, and valued at approximately $2B
• Heavy focus on in-house service and support, contract reduction/elimination, cost avoidance
Historical Gaps and Challenges Related to Medical Device Cybersecurity
GAPS

- OIS--Industry leading intake and assessment process
- Excellent security knowledge, but limited operational resources or expertise
- Asset specific security assessment with findings:
  - Mitigating control requirements
  - Many were vendor dependent
  - Many could never happen
  - Asset by asset approach had very limited impact on fleet risk
  - Who should be “doing the new work”? 
  - No standard operational framework or processes
Unique Nature of Medical Devices/Systems and HIoT

- Regulatory guidelines (FDA, CAP, JCAHO)
- Complex systems
- Critical to patient care
- Research and testing
- Vendor validation prior to Mayo action
- Manual, resource intensive patching process
- Access to devices
- Lack of “IT” like deployment options
- Specialized skills required
- Lack of vendor urgency
- Outdated/Unsupported Devices
- Largely unable to scan with standard tools
- Service keys required
- Unable to load agents
Security Challenges
HDO Size and Scope

- Significant geographical implications—5 States, 26 Shops, Over 300 Buildings
- Roughly 50,000+ Network Connected Medical, Lab, Research, and HIoT Devices
  - Hundreds of Vendors
  - Thousands of Models
- Inventory discrepancies
  - Determining ownership: Who’s responsible for capturing, verifying, and maintaining critical attributes? Who’s responsible for tracking, documenting, and applying controls/patches?
  - Mismatched data—CMMS vs. Cisco ISE
  - Are all network connected medical devices inventoried?
The Cybersecurity Team Within HTM
Organizational Fit

- Healthcare Technology Management (HTM)
  - HTM Cybersecurity
- Office of Information Security (OIS)
  - CIS-R
HTM Role in Cybersecurity

• Operationalize Security on Medical Equipment and Systems
  – Structured
  – Standardized approach
  – Economies of Scale

• Also....Facilities Operations and HIoT

• Ensure that equipment is functional and optimized in order to meet organizational--patient safety, business continuity, regulatory, and cybersecurity requirements.

• Accountability through the entire technology lifecycle
  – Visibility
  – Monitoring
  – Action
Align Efforts to Industry Standards

Mapping of HTM Activities to NIST and AAMI Guidelines

- Matching will not always be explicit
- Identify unmatched activities
- Reverse map to close gaps
- Identify lines of responsibility (OIS, HTM)

Many of the Mayo activities leverage automated asset, flow identification and security tools (Ordr)

One-to-One mapping
MAYO/HTM Information Security Team
Core Team

• Develop NIST and AAMI based security framework for HTM and HIoT
• Develop standardized security processes and procedures
• Assist with projects (NAC and Segmentation Efforts, med device security tool testing)
• High End Resource for Associate Eng, Technicians, and Clinical Groups
• Develop and guide HTM vulnerability management program
• Construct and maintain fleet-level comprehensive cyber risk scoring
• Engage with industry groups and participate in initiatives (FDA, SBOM, CISA)
• Ordr Implementation and Administration
• Automate security workflows
HTM Associate Info Sec Engineers

- Embedded within the local HTM shops
- Security SME for Biomed Techs
- Security point of contact for vendors
- Create procedures for:
  - Compensating Control application
  - Vulnerability mitigation/remediation
- Apply controls to medical devices (as possible)
- Network connectivity SME (NAC, Segmentation, Onboarding)
- Training and education for HTM shops
- Local incident response SME
SPAD (Security, Privacy, Architecture, Data)—”Security Assessment”

• Initial intake triage of all capital and non-capital medical device purchases (~1500 per year)
  – Hardware
  – Software

• Route through the appropriate level of intake assessment

• “White glove” service for purchase proponents
  – Guide proponents through the purchase assessment process
  – Work with vendors to acquire review deliverables

• Collaborate with OIS and the proponent to determine mitigating controls

• Construct Security Lifecycle Profiles (Model Specific Roadmap/Template)
Execution
Proactive Security

**Strategic Approach**

- Leverage Known Security Incidents (e.g. Malware attack, Ransomware, etc.)
- Leverage Zero Day Vulnerabilities (BlueKeep, DejaBlue, Ripple20)
- Leverage Regulatory Compliance and other Business Opportunities
- Internal Audit Observations
- Next Level of Security Operations
- Governance

**Thought:** What do we want to do better?
Proactive Security

Security Operations within the Equipment Lifecycle

- Perform security risk assessment on device using Mayo’s **six baseline security criteria** prior to making purchase decisions. Know what is in the device if to be connected to the network (**sBoM**)  
- Work with the vendors to address **device weakness** prior to use  
- Deploy, track and apply security mitigations using **device Security Lifecycle Profile** (SLP)  
- Address ongoing security issues through a **vulnerability management process** (patching, mitigating controls, etc.)  
- Sanitize device after use to prevent unintentional disclosure. Adopt a robust disposition policy and procedure
Proactive Security

Device Security Standard – Pre-Purchase

- Mayo’s Six Baseline Security Standard for connectable new device purchases
  - Runs supported OS
  - Receives routine OS patches
  - Has AV applied and updated
  - Receives routine 3rd - party software patches
  - Contains no default hardcoded passwords
  - Complies with Mayo work Account standards

- Test/Assess new device before purchase
- Document security weakness and work with vendors to address the weaknesses
Proactive Security

Security Lifecycle Profile (SLP) – Deployment

- Document the device onboarding procedure
- Include pre-determined security controls as part of the deployment
- Assign ownership
- Address device risk by type and by model
- Reduce deployment variation- standardize and centralize the process
- Work Orders are tied to remediation tasks
- Remediation ties back to the findings
- Support risk model and quantification

Proactive Security

Adopt Fleet Approach to Security Remediation Efforts

Vendor: ABC Manufacturer
Make: ABCD-123-EXY-Patient-Station
Model: 200/WXseries/Win10SP1
Proactive Security

Vulnerability Management & Remediation Program - Maintenance

- Enhance CMMS asset inventory with attributes for VM activities (e.g. OS, 3rd software, firmware, protocol, etc.)
- Track software vulnerabilities from various sources (Internal or external)
- Prioritize remediation in the context of impacted asset and patient impact, exploitability, exposure, etc.
- Standardize patching procedure; by model, by type; creating work order for tracking completion and status
- Monitor and track status of all remediation
- FDA Post Market Guidance for Patching
Tools
Key Tools

Operational Tools to Execute and Automate Security Operations

- Robust CMMS Solution (Lifecycle Maintenance)
  - Enterprise Asset Management Solution
  - Flexible and robust Work Orders
  - Support Risk scoring and modeling
  - Support vulnerability management module
  - Create device SLPP approach for mitigations efforts
  - Integrate with CMDB and other Enterprise Security tools
Key Tools

Operational tools to execute and automate security operations

• Modern Asset Discovery (Foundational)
  - Improves quality of data for Asset inventory
  - Capability to detect networked medical devices (including legacy)
  - Robust medical device asset classification
  - Provides insight into connected device actions
  - Supports device security operations
  - Integrates with other Enterprise Security tools
  - Micro-Segmentation
Progress
Two Years...

Program is adding “Security Value”.....

- Significantly Improved Device “Repeat” and “New” Purchase Turn-around time
- Established an algorithm for calculating and determining security risks across the fleet.
- Established a mechanism for tracking and applying security mitigation during device onboarding
- Operationalized the medical device vulnerability management program
- Recently launched a medical device patch installation automation utility tool
- Active participation in the Industry workgroups to contribute to medical device security
- Leveraging Ordr for asset identification and reconciliation, security analysis, VM, and micro-segmentation
Two Years…
About Ordr Inc.

- Founded in 2015 by Cisco and Aruba Networks veterans
- $50M raised from top investors
- Customers in North America, Europe and APJ
- 95%+ customer retention rate
- Ordr is IoT device security made simple….
  - Zero agents, zero touch provisioning
  - One comprehensive platform to
    - secure all unmanaged devices (IoT, IoMT, OT)
    - enable the entire device security workflow
    - address the needs of security, networking and device owners

Venture Partners

Kaiser Permanente Ventures and Mayo Clinic Invest in Ordr

Ordr Proven In Large Networks, Many Verticals
One Network One Team

Internet

Data Center

Campus Network

WCL

Access Switch
360 Degree Enforcement – Complete Accurate Inventory

Inventory augmented with vulnerability and security threats to do detailed risk assessment for patient safety
Foundation - Detailed Info on Med Devices
### Assess Vulnerabilities - Patches, Hotfixes, AV Updates

**Criticality:** LEVEL_1
**Alarm Count:** 5
**Risk Score:** 93
**Vulnerability:** normal

---

#### 25 vulnerabilities

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDA-165969</td>
<td>DigitalDiagnost, Single-Detect (stitching Patient Support) 712062…</td>
</tr>
</tbody>
</table>

#### Operating System Patches/Updates (10)

<table>
<thead>
<tr>
<th>No.</th>
<th>Hotfix Id</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>KB4100347</td>
<td>Update</td>
</tr>
</tbody>
</table>

#### Third Party Software (7)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AVG AntiVirus FREE</td>
</tr>
</tbody>
</table>

#### Anti-Virus Software (2)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Up-to-date</th>
<th>Last Updated</th>
<th>Protection State</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Windows Defender</td>
<td>Yes</td>
<td>Mon June 3rd 2019</td>
<td>Inactive</td>
<td>windowsdefender://</td>
</tr>
</tbody>
</table>
Medical Device Behavior Monitoring and Analytics
360 Degree Enforcement – Disconnect Attackers

- Non-compliant wireless laptop trying to access to the network, spreading malware laterally.
- Indicator of compromise observed in the network through this laptop and immediate prevention needed.

Action = Disconnect
360 Degree Enforcement – Regulate Internet Traffic

• Firewall allowing specific site and operation based on device type
• Disallow usage of MRI to browse internet for bitcoin mining, and allow legitimate traffic to imaging servers in the data center using firewall
360 Degree Enforcement - MicroSegment Med Devices

- Prevent traffic going in and out of MRI – only legitimate devices can communicate with MRI
- Microsegmentation policy to permit specific action to protect line of business and its critical devices
360 Degree Enforcement – Close the Loop

Proactive Protection Methods
- Border Gateway – Firewall rules
- Wireless Controllers - Role Based Access
- Wired switches – Access Control Lists
- Server Access control – VMware/NSX
- Remote user access control - VPN
- Application tracking - Load Balancers
- User Tracking - Active Directory/local users

Endpoint agent not possible
### Medical Device Protection: Best Practices

<table>
<thead>
<tr>
<th><strong>DEVICE INVENTORY, UPDATES &amp; ALLOWLISTING</strong></th>
<th><strong>GROUP BY DEV MODEL AND SEGMENTATION</strong></th>
<th><strong>HYGIENE ON NETWORK ENVIRONMENT</strong></th>
<th><strong>SWITCH/WIRELESS POLICY FOR MICROSEGMENTATION</strong></th>
<th><strong>FIREWALL POLICY FOR EXT. COMMUNICATION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Allowlist medical devices reconciling with CMDB/CMMS</td>
<td>• Create network segments for medical vs facilities vs contractor vs ER vs pharmacy vs guest</td>
<td>• Plug open ethernet ports on the walls, Patient waiting areas</td>
<td>• Stop Malware spreads - Restrict internal traffic from devices in the same segment reaching out to medical or facility devices</td>
<td>• Block any device reaching out to bad IP/URL to prevent phishing attacks</td>
</tr>
<tr>
<td>• Patch(OS/AV) vulnerable medical Devices; Identify older OS like XP</td>
<td>• Selectively allow group-to-group access</td>
<td>• Disconnect rogue APs</td>
<td>• AllowList internal flows for medical devices with for imaging and EMR/HER servers</td>
<td>• Block unwanted users accessing medical devices – zero trust model with admin access</td>
</tr>
<tr>
<td>• Identify facility devices – elevator, phones to understand the interactions</td>
<td>• Identify facility devices – elevator, phones to understand the interactions</td>
<td>• Prevent devices from guest network accessing clinical resources</td>
<td>• Ransomware - Prevent Medical workstations used to reach social sites</td>
<td>• Ransomware - Prevent Medical workstations used to reach social sites</td>
</tr>
<tr>
<td>• Update password, close open ports, vulnerability scan if possible</td>
<td>• Update password, close open ports, vulnerability scan if possible</td>
<td>• Identify and remove move outlier devices from wrong segments</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

ACCE Membership

Apply Now!

https://accenet.org/Membership/Pages/ApplicationForms.aspx

Benefits

• Bi-monthly ACCE newsletter with timely updates and articles
• Complimentary ACCE receptions
• Volunteer opportunities
• Complimentary educational webinar

Discounts

• AAMI, HIMSS, IFMBE conference registration
• JCE Journal
• ACCE educational content
• Free access to IFMBE/Springer publications
Thank you

Keith Whitby
Section Head of Healthcare Technology Management
Cybersecurity and Operations
Mayo Clinic

Pandian Gnanaprakasam
Chief Product Officer
Ordr Inc.
Please complete the online survey at