OT Cybersecurity and Impact on Patient Care in Health Care Facilities

October 15th, 2019
Anthony Ciccozzi, PE, GICSP, PMP
Learning Objectives

• Learn what facility managers can do to protect healthcare facilities/patients from cybersecurity threats

• Understand differences between Information Technology (IT) and Operations Technology (OT) networks

• Learn how OT vulnerabilities could negatively impact patient care

• Review common security vulnerabilities Healthcare facilities (through the presentation of a case study)

• Learn how facility managers can evaluate the cybersecurity state of their Healthcare system through a simple framework of questions

The term OT will be used when referring to the Healthcare Facility networks (Electrical Infrastructure, Building Automation, etc.)

Other terms used (depending on the specific context and vendor):

ICS = Industrial Control System
BAS = Building Automation System
BMS = Building Management System
EPMS = Electrical Power Monitoring System
SCADA = Supervisory Control and Data Acquisition

© 2019 Eaton. All Rights Reserved
Multiple motives... impact patient healthcare delivery, patient health/financial data, ransomware, terror/societal disruption, infant abduction, drug theft
Cybersecurity Incident Review and Takeaways

December 2013: up to 110 million Target Corporation customer financial and personal exfiltrated to external server.

- Spear Phishing to steal remotes access credentials from an HVAC and refrigeration company

- Gained remote access to the network, exploited known vulnerabilities, pivoted around network (exploiting weak segmentation/boundary defenses), installed malware on Point of Sale (POS), exfiltrated data to external server

- Target had the Technology (an expensive IDS and malware prevention tools) – but the People and Process were lacking:

  “Target’s FireEye malware intrusion detection system triggered urgent alerts with each installation of the data exfiltration malware... Target’s security team neither reacted to the alarms nor allowed the FireEye software to automatically delete the malware in question. Target’s Symantec antivirus software also detected malicious behavior around November 28, implicating the same server flagged by FireEye’s software.”

Analysis of the attacks found weaknesses in overall vulnerability management, cybersecurity maintenance and supply chain cybersecurity


© 2019 Eaton. All Rights Reserved
Attacks can originate:
- From the Outside into OT
- From OT into larger IT infrastructure

**Attack Surface:** Sum of the points where an attacker can interact with the system (input, output, manipulate control, elevate privilege, etc.)

**Attacker Objectives**
- Primary attack (e.g. disconnect power)
- Supporting attack (e.g. UPS disconnect)
- Establish remote access/exfiltration point
- Loss of View/Control
- Manipulation of View/Control
Healthcare Facility OT Lacks Direct Cybersecurity Standards

Additional action is needed to protect patients and staff from cybersecurity threats - there is not one size fits all certification or standard!

**Health Insurance Portability and Accountability Act (HIPAA)**
Privacy Rule and Security Rule govern Protected Health Information (PHI) electronic Protected Health Information (ePHI)

**NFPA 99: Health Care Facilities Code** provides risk-based approach to facility Safety and Availability.

**U.S. FDA** issues pre-market and post-market guidance and approval for medical devices

**OT focused industry standards and best practices exist that give specific consideration to availability and real-time needs**
Healthcare Facility OT: Electrical Infrastructure Overview

**Power System**
- Protection
- Breakers
- Relays
- Meters
- UPS
- PLC/Real-Time Controller

**Automation System**
- Network Switches
- Routers
- Firewalls
- Comm Gateways
- HMI
- Server

Electrical infrastructure is part of overall **Attack Surface**. Consider other adjacent systems: medical gas, HVAC, lighting, fire and, public address, etc.

Time-sensitive and critical applications... like Transfer Switching, require fast response and high availability often leading to the use of specialized controllers to provide **Hot Standby** redundancy.

Controller A fails over to Controller B that is fully synchronized and can provide no disruption (**bump-less transfer**).
Electrical infrastructure, physical asset distribution, and monitoring and control requirements...

Determine the overall architecture and attack surface....
Healthcare Facility OT Characteristics

- Distributed network of vendor specific and Commercial Off the Shelf (COTS) components
- Distributed authority for assets and network (Facilities/OT vs. IT)
- Industrial equipment and protocols (e.g. Modbus TCP, BACNet, etc.)
- Static, real-time, deterministic traffic/data flows
- Patching/updating devices not possible/practical
- Remote accessibility (for maintenance and troubleshooting)
- Differing security objectives from standard IT:
  1. Availability
  2. Integrity
  3. Confidentiality
- Several adjacent systems tied together by common infrastructure
  - Lighting control systems
  - HVAC
  - Fire Detection/Suppression
  - Public Address

OT cybersecurity risks are not typically fully considered by IT!
Case Study: U.S. Healthcare Facility

• **Relatively minor investment can make big improvements:**
  • Updating asset inventories
  • Patching/updating devices
  • Updating access controls
  • Adding a few (OT) firewalls
  • Extending IT monitoring to OT assets
  • Integrating security maintenance

• Several devices were used that supported capability to integrate into overall IT security monitoring

Example: OT specific network switch was installed without any of the necessary features configured

**Takeaway:** Otherwise “secure” organizations have serious gaps in Facility OT cybersecurity
Actions for Facility OT Leaders

**Inventory**... all connected hardware, software, dataflows and correlate **Reality, Monitoring**, and **Drawings**

**Collaborate**... with vendors and internal stakeholders to review roles & responsibilities and identify gaps in governance (e.g. disaster recovery and incident response)

**Integrate**... cybersecurity into overall lifecycle maintenance (look for overlap in activities, skillsets, and competencies)

**Train**... staff on OT specific cybersecurity considerations including best practices and policies around USB and maintenance laptops

**Assess**... facility OT networks and assets to evaluate the attack surface and discover known vulnerabilities and weaknesses

**Effective Cybersecurity for Facility OT** a full lifecycle risk management activity requiring comprehensive consideration of **People**, **Process**, and **Technology**

**Perform an OT focused Assessment!**

Done properly can be executed on running systems using **Passive Scanning** and OT specific tools and techniques

© 2019 Eaton. All Rights Reserved
Assessing Facility OT: Focus Areas

**Asset Inventory** - Know what you have, know how it is connected, know how (if) it is monitored

**Vulnerability Management** – Discover and address (mitigate/remediate) vulnerabilities (patch, configuration, etc.)

**Architecture and Boundary Defenses** – Verify segmentation, remote access, traffic restriction, intrusion detection, functional isolation

**Log Review and Analysis** - Verify all devices are monitored and review all alerts and logs for malicious/unauthorized activity

**Access Controls** - Verify default usernames and passwords have been changed

**Backup and Recovery** - Verify all assets have recent backups (or at least documented configurations)

**Secure Configuration** – Verify configurations per vendor guidance, disable unnecessary ports and services

---

1. As an example a mapping to ID.BE-4 Dependencies and critical functions for delivery of critical services are established in the CSF could be added

---

**Technical Framework**

- Base on NIST Cybersecurity Framework (CSF)
- Customize for OT: e.g. use mappings to IEC-62443, Center for Internet Security (CIS) Critical Security Controls (CSC)
- Add consideration to real-time and critical functions\(^1\)
Assessing Facility OT: Cybersecurity Maintenance

- Industry standards and best practices specify bi-weekly, monthly, and yearly activities

- Comprehensive vulnerability assessments effectively serve as a review of cybersecurity maintenance activities

---

**Verify it...**

- Verify no unauthorized devices or software are on Facility OT networks
- Verify no known vulnerabilities
- Verify all devices are monitored for malicious/unauthorized activity
- Verify no insecure/unauthorized remote access exists
- Verify logs and alerts have been reviewed and indicate no malicious activity
- Verify disaster recovery and incident response plans consider Facility OT
## Evaluating Facility OT Cybersecurity Evaluation

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Partial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are only authorized devices communicating on the network?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is remote access to system assets secure (strong access controls, boundary defenses, etc.)?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are unaddressed vulnerabilities present on any system assets?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is network traffic monitored for unauthorized, anomalous, and malicious behavior?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are strong system access controls in place and least privilege applied (e.g. no default passwords)?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are asset owners, authorization boundaries, and responsibilities clearly defined?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do accurate inventories of authorized hardware, software, and dataflows exist?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do accurate network/topology drawings exist showing all connected devices?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are secure configurations for all assets defined and deployed (no default credentials, only necessary ports and services running/open, disable unused physical ports, etc.)?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does an asset (device) qualification and decommissioning program exist?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are trust boundaries identified and segmentation/boundary defenses deployed?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are malicious code detection/prevention mechanisms deployed and up to date?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are assets included in a security monitoring and protection program?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all assets synchronized to the same (accurate) time and time zone?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does a vulnerability management program exist?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are vulnerability assessments performed on the system (at least yearly)?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does an incident response program exist?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does a backup and disaster recovery program exist?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does a cybersecurity awareness program exist (for employees and vendors)?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does a transient asset/removable media cybersecurity hygiene program exist?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **No** and **Partial** response indicates gaps and potential risks.
• **Eaton’s Cybersecurity Services** can help you maximize patient safety and hospital uptime by focusing on all 3 tenants:
  - **People**: Ensure your staff is trained on best practices and awareness
  - **Process**: Put a system in place - know what to measure & how to respond
  - **Technology**: Analyze attack surface, risks, and help address vulnerabilities and gaps

• **Eaton’s Cybersecurity Services** team is uniquely positioned as your most qualified partner
  - Cross-functional team of **Power management** and **OT Cybersecurity Experts**
  - Services Team is well versed on the latest cybersecurity industry standards and best practices
  - Eaton runs the first certified lab under UL2900
Eaton offers **training**, **consulting** and **remediation** services to address identified vulnerabilities to help you **maximize patient safety and well being**.

<table>
<thead>
<tr>
<th>Eaton Audit</th>
<th>An assessment of the maturity and implementation of your overall Cybersecurity program with a focus on your <strong>people, processes &amp; technology</strong>.</th>
<th>You will receive an overall <strong>Eaton fitness score</strong> and report on your cybersecurity program derived from industry standards and best practices. Your will <strong>gain visibility</strong> to your strengths and weaknesses with improvement recommendations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eaton Assessment</td>
<td>Builds upon the Audit by performing an in-depth <strong>connected device architecture analysis</strong> to determine your threat model. <strong>Passive data collection</strong> on your operational system will enable a vulnerability analysis and device configuration security review.</td>
<td>An Eaton <strong>cybersecurity leader</strong> will walk you through your identified <strong>attack surface profile</strong> and associated vulnerabilities and weaknesses. A <strong>prioritized lists</strong> of all findings with recommendations on how to address each will be delivered, along with a <strong>corrective action proposal</strong>.</td>
</tr>
<tr>
<td>Eaton Life-Cycle Management</td>
<td>Provides <strong>ongoing services</strong> to ensure your cybersecurity measures remain sufficient, comprehensive and integrated into your lifecycle management.</td>
<td>Reoccurring assessment of your people, processes and technology to ensure you are <strong>keeping pace with the evolving threat space</strong> and existing practices do not erode over time.</td>
</tr>
</tbody>
</table>
Eaton cybersecurity services initiative

“We’ll focus on your power system... you focus on your business”

Installation and commissioning

Cybersecurity assessment

Cybersecurity hardening and security updates

Training and situation awareness

Governance and compliance

Secure architecture and design

Questions?
OT Cybersecurity and Impact on Patient Care in Health Care Facilities

October 15th, 2019
Anthony Ciccozzi, PE, GICSP, PMP
AnthonyCiccozzi@eaton.com