Cybersecurity
Center of Excellence

OT Cybersecurity and Impact on Patient Care in Health Care Facilities

October 15th, 2019

Anthony Ciccozzi, PE, GICSP, PMP

EATON
Powering Business Worldwide

IP 1 Public

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

Healthcare Sector as a Target

NEWS

Medical data of 33,000 BJC HealthCare patients exposed online for 8 months

by Jessica Davis | March 14, 2018

An internal scan by the St. Louis-based health system found a misconfigured server could be easily accessed without authentication.

NEWS

134,512 patient records breached in malware attack

by Jessica Davis | March 12, 2018

St. Peter's Surgery and Endoscopy Center was hit with the second-largest healthcare breach of 2018.

NEWS

VA OIG finds cybersecurity flaws at Orlando VA Medical Center

by Jessica Davis | February 09, 2018

The Florida VA provider set-up its Wi-Fi network without coordinating with the VA's IT office.

NEWS

205,000 patient records exposed on misconfigured FTP server

by Jessica Davis | May 18, 2018

MedEvolve, a practice management software vendor, left its FTP server open to the public without the need for a login.

NEWS

417,000 Augusta University Health patient records breached nearly one year ago

by Jessica Davis | August 17, 2018

The Georgia provider was hit by two cyberattacks in September 2017, but did not explain when the breach was discovered.

DDoS Attacks: In the Healthcare Sector

Distributed denial of service (DDoS) attacks are a popular tactic, technique, and procedure (TTP) used by hacktivists and cybercriminals to overwhelm a network to the point of inoperability. This can cause a serious problem for healthcare providers who need access to the network to provide proper patient care or need access to the Internet to send and receive emails, prescriptions, records, and information. While some DDoS attacks are opportunistic or even accidental, many target victims for a social, political, ideological or financial cause related to a situation that angers the cyber threat actors.

Example

This was the case with Boston Children's Hospital in 2014. Anonymous (a well-known hacktivist group) targeted the Boston's Children's Hospital with a DDoS attack after the hospital recommended one of their patients, a 14-year-old girl, be admitted as a ward of the state and their custody be withdrawn from her parents. The doctors believed the child's ailment was actually a psychological disorder and that her parents were pushing for unnecessary treatments for a disorder the child did not have. The custody debate put Boston Children's Hospital in the middle of this controversial case, and some, including members of Anonymous, viewed this as an infringement on the girl's rights. Anonymous took action by conducting DDoS attacks against the hospital's network, which resulted in others on their network, including Harvard University and all its hospitals, to lose Internet access as well. The ransoms experienced outages for almost a week, and some medical patients and medical personnel could not use their online accounts to check appointments, test results, and other case information, according to the Boston Globe. As a result, the hospital spent more than $300,000 responding to and mitigating the damage from this attack, according to the attacker's arrest affidavit.

Recommendations

DDoS attacks occur in a variety of ways, and understanding which type of attack is occurring is an important part of being able to properly mitigate the attack. In the MS-ISAC Guide to DDoS Attacks you will find an explanation of the different types of attacks (including the multiple types of standard and reflection DDoS attacks), followed by specific recommendations unique to each type of attack. General recommendations for defense against DDoS attacks include maintaining an effective partnership with your upstream network service provider as well as partnering with companies that provide DDoS mitigation services.

CISA
CYBER+INFRASTRUCTURE

HOME | ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING | FAQ

Control Systems
- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.
[change view]: Advisories by Vendor | Advisories by Vendor - sorted by Last Revised Date

- ICSA-19-050-01 : Intel Data Center Manager SDK
- ICSA-19-050-02 : Delta Industrial Automation CNCSoft
- ICSA-19-050-03 : Horner Automation Cscape
- ICSA-19-050-04 : Rockwell Automation Allen-Bradley PowerMonitor 1000
- ICSA-19-045-01 : Pangea Communications Internet FAX ATA
- ICSA-18-310-01 : gpsd Open Source Project
- ICSA-19-043-01 : OSIsoft PI Vision
- ICSA-19-043-02 : Siemens EN100 Ethernet Communication Module and SIPROTEC 5 Relays
- ICSA-19-043-03 : Siemens Licensing Software for SICAM 230 (Update A)
- ICSA-19-043-04 : Siemens SIMATIC S7-300 CPU
- ICSA-19-043-05 : Siemens Intel Active Management Technology of SIMATIC IPCs
- ICSA-19-043-06 : Siemens CP1604 and CP1616
- ICSA-19-038-01 : Siemens SICAM A8000 RTU Series
- ICSA-19-038-02 : Siemens EN100 Ethernet Module
- ICSA-19-036-01 : AVEVA InduSoft Web Studio and InTouch Edge HMI
- ICSA-19-036-02 : Rockwell Automation EtherNet/IP Web Server Modules
- ICSA-19-036-03 : WECON LeviStudioU
- ICSA-19-036-04 : Siemens SIMATIC S7-1500 CPU
- ICSA-19-036-05 : Kunbus PR100088 Modbus Gateway (Update A)
- ICSA-19-031-02 : IDenticard PremiSys
- ICSA-19-031-01 : Schneider Electric EVLink Parking
- ICSMA-19-029-01 : Stryker Medical Beds
- ICSMA-19-029-02 : BD FACSLyric (Update A)
- ICSA-19-029-01 : Yokogawa License Manager Service
- ICSA-19-029-02 : Mitsubishi Electric MELSEC-Q Series PLCs

1 2 3 4 5 6 7 8 9 ... next › last »

Multiple motives… impact patient healthcare delivery, patient health/financial data, ransomware, terror/societal disruption, infant abduction, drug theft

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

1. Brian Krebs, *Sources: Target Investigating Data Breach*, KrebsOnSecurity (Dec. 18, 2013) (online at http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/)
2. https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf

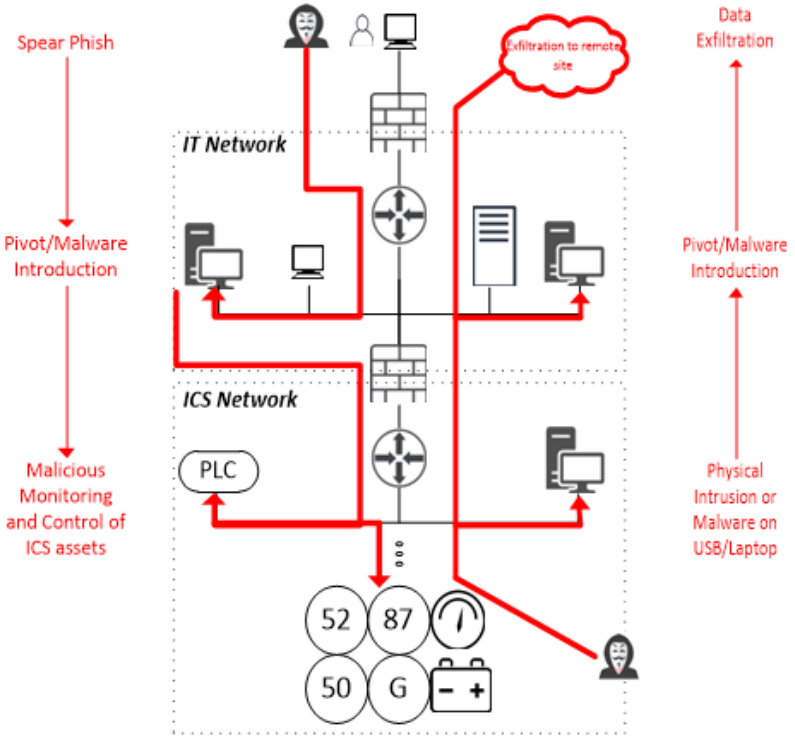
Attacks can originate:

- 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

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

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

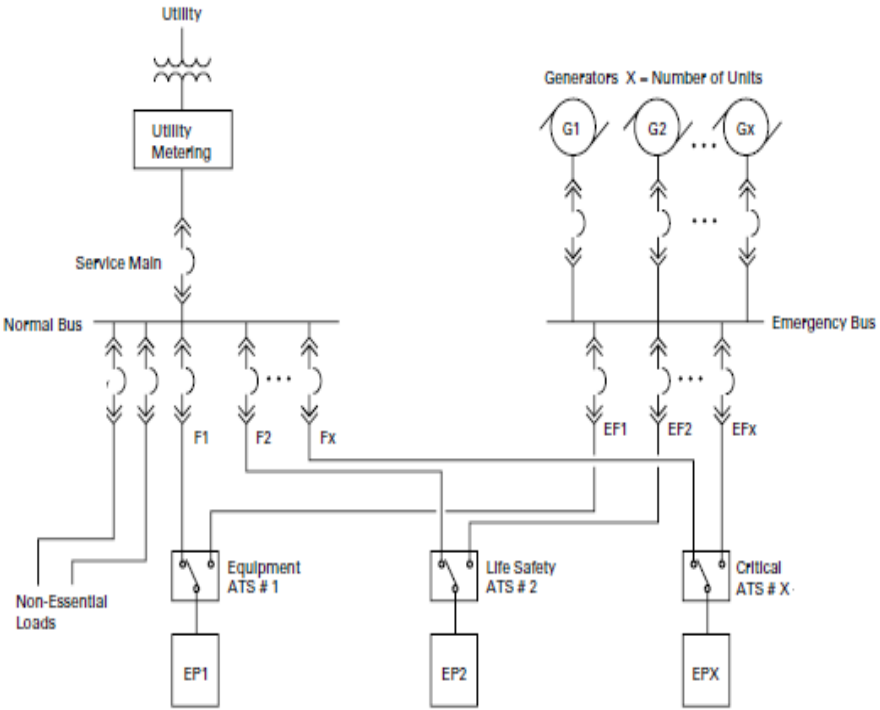
Healthcare Facility OT: Electrical Infrastructure Overview

Power System

- Protection
- Breakers
- Relays
- Meters
- UPS
- PLC/Real-Time Controller

Automation System

- Network Switches
- Routers
- Firewalls
- Comm Gateways
- HMI
- Server



Power System Functions

- Transfer Switching
- Generator Paralleling
- Generator Control
- Ground Fault Protection
- Surge Protection
- Battery Monitoring

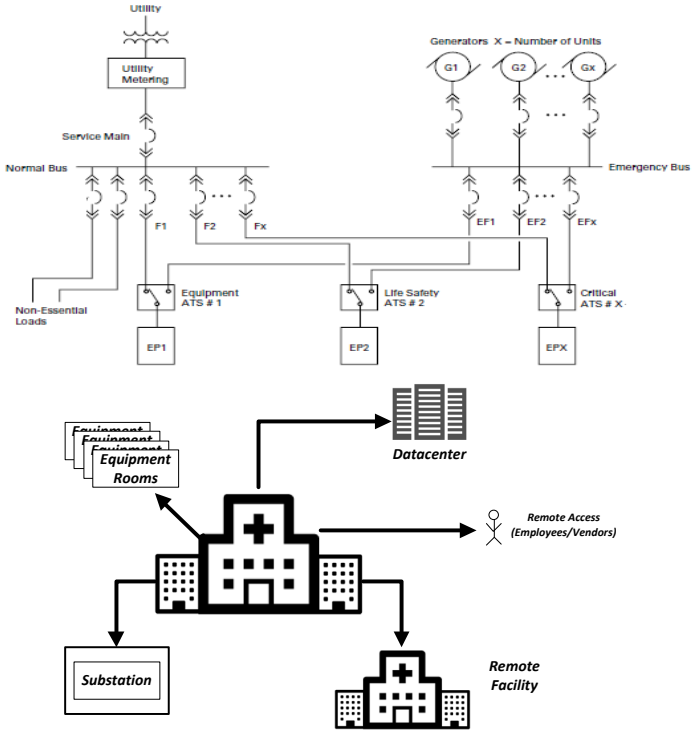
Time-sensitive and critical applications… *like* ***Transfer Switching****, require fast response and high availability often leading to the use of specialized controllers to provide* ***Hot Standby*** *redundancy.*

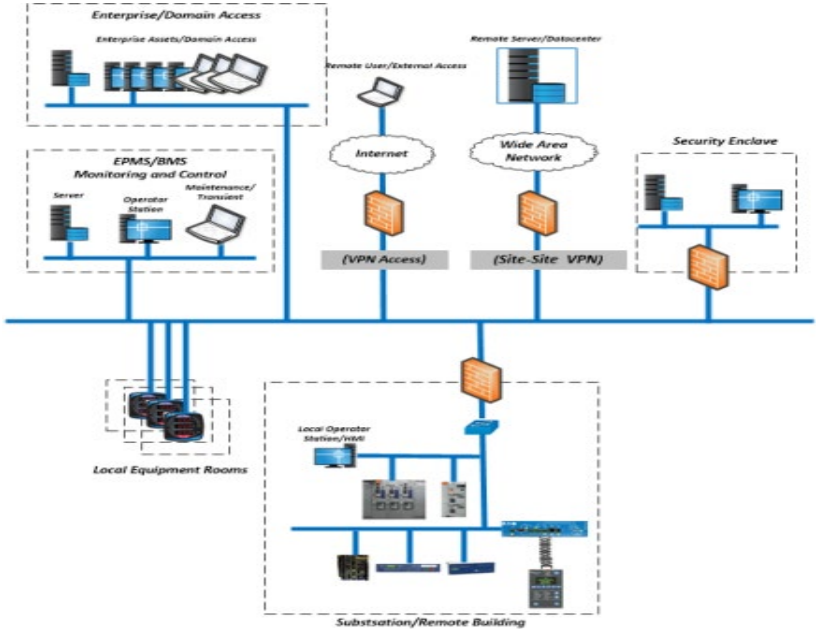
*Controller A fails over to Controller B that is fully synchronized and can provide no disruption (****bump-less transfer****).*

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

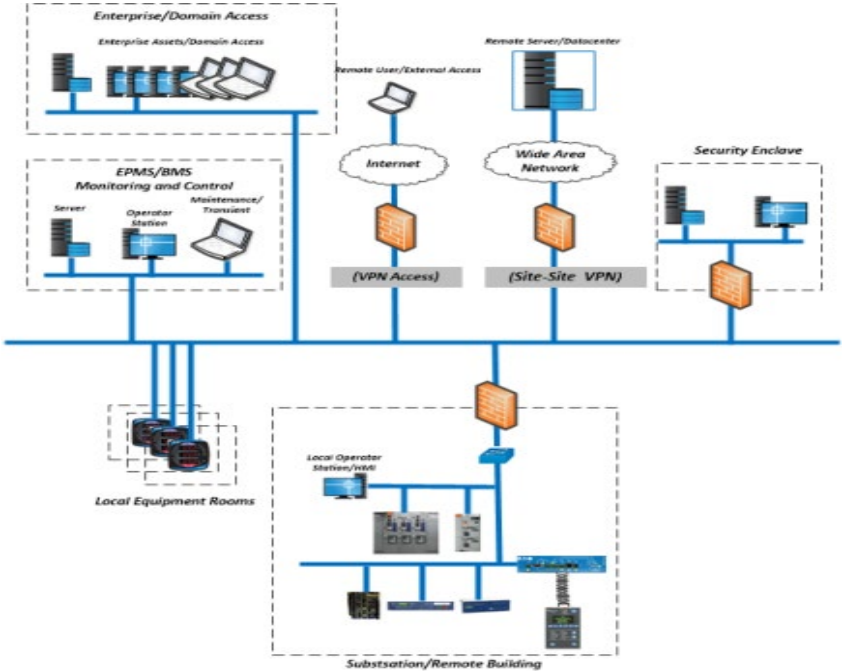
Electrical infrastructure, physical asset distribution, and monitoring and control requirements…

Determine the overall architecture and attack surface….





Healthcare Facility OT Characteristics

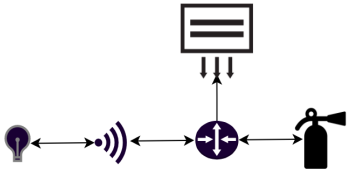


OT cybersecurity risks are not typically fully considered by IT!

- ✓ *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:*

(OT/EPMS/BAS)	(IT)
1. Availability	1. Confidentiality
2. Integrity	2. Integrity
3. Confidentiality	3. Availability

- ✓ *Several adjacent systems tied together by common infrastructure*

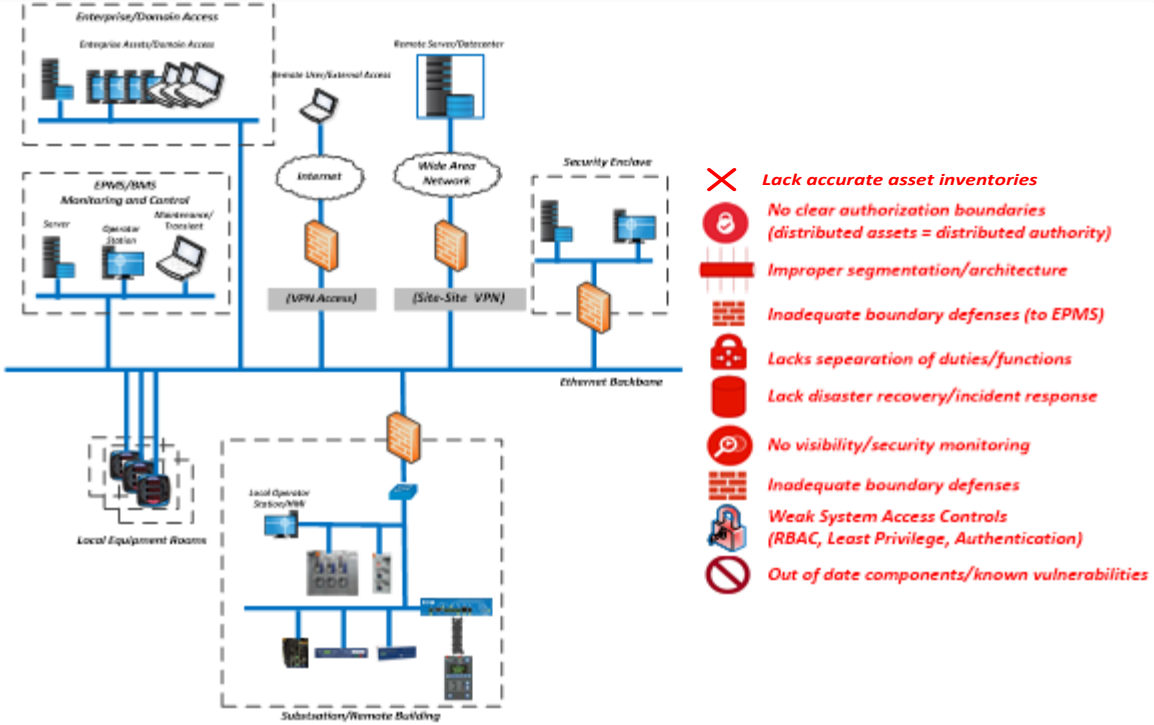


- ✓ *Lighting control systems*
- ✓ *HVAC*
- ✓ *Fire Detection/Suppression*
- ✓ *Public Address*

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***

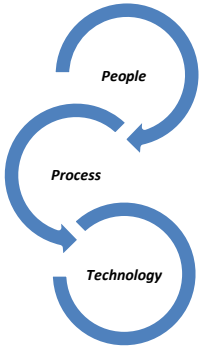
Collaborate… with vendors and internal stakeholders to review roles & responsibilities and identify gaps in governance (e.g. disaster recovery and incident response)

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

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

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]

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***

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 an indicate no malicious activity
- ❑ Verify disaster recovery and incident response plans consider Facility OT

Yearly (Every 15 Months)

- Asset inventory and baseline generation
- Network topology and drawing review
- Vulnerability Assessment

Monthly (Every 35 days)

- Pre-update configuration baseline
- Backup system assets
- Vulnerability review (vendor and public)
- Deploy patches and firmware updates
- Deploy "security" updates (e.g. AV definitions)
- Review access control lists
- Review user accounts and controls
- Post-update configuration baseline

Bi-weekly

- Logging review and analysis
- Time synchronization verification

Additional Activities

- *System health assessment*
- *Redundancy testing*
- *Configuration management update*
- *Disaster recovery tabletop exercises*
- *Incident response tabletop exercises*

Evaluating Facility OT Cybersecurity Evaluation

Perform this basic evaluation for Facility OT… *No* and *Partial* response indicates gaps and potential risks

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

Eaton Cybersecurity Services

- **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 Cybersecurity Service Offerings

Our services are designed to be minimally disruptive to your staff & performed on operational equipment

	What is it?	What you get out of it.
Eaton Audit	An assessment of the maturity and implementation of your overall Cybersecurity program with a focus on your **people, processes & technology.**	You will receive an overall **Eaton fitness score** and report on your cybersecurity program derived from industry standards and best practices. Your will **gain visibility** to your strengths and weaknesses with improvement recommendations.
Eaton Assessment	Builds upon the Audit by performing an in-depth **connected device architecture analysis** to determine your threat model. **Passive data collection** on your operational system will enable a vulnerability analysis and device configuration security review.	An Eaton **cybersecurity leader** will walk you through your identified **attack surface profile** and associated vulnerabilities and weaknesses. A **prioritized lists** of all findings with recommendations on how to address each will be delivered, along with a **corrective action proposal.**
Eaton Life-Cycle Management *Never one and done.*	Provides **ongoing services** to ensure your cybersecurity measures remain sufficient, comprehensive and integrated into your lifecycle management.	Reoccurring assessment of your people, processes and technology to ensure you are **keeping pace with the evolving threat space** and existing practices do not erode over time.

Eaton offers **training**, **consulting** and **remediation** services to address identified vulnerabilities to help you maximize patient safety and well being.

Eaton cybersecurity services initiative

"We'll focus on your power system... you focus on your business"

Installation and commissioning

Cybersecurity hardening and security updates

Governance and compliance

Cybersecurity assessment

Training and situation awareness

Secure architecture and design

Questions?

Cybersecurity

Center of Excellence

OT Cybersecurity and Impact on Patient Care in Health Care Facilities

October 15th, 2019

Anthony Ciccozzi, PE, GICSP, PMP

AnthonyCiccozzi@eaton.com

EATON Powering Business Worldwide

IP 1 Public