Building a security management plan for your networked medical devices

INHEL REKIK MS, DIRECTOR OF HEALTH TECHNOLOGY SECURITY, MEDSTAR HEATH

JON MCKEEBY D.SC MBA CPHIMS CPHI, CHIEF INFORMATION OFFICER, NIH

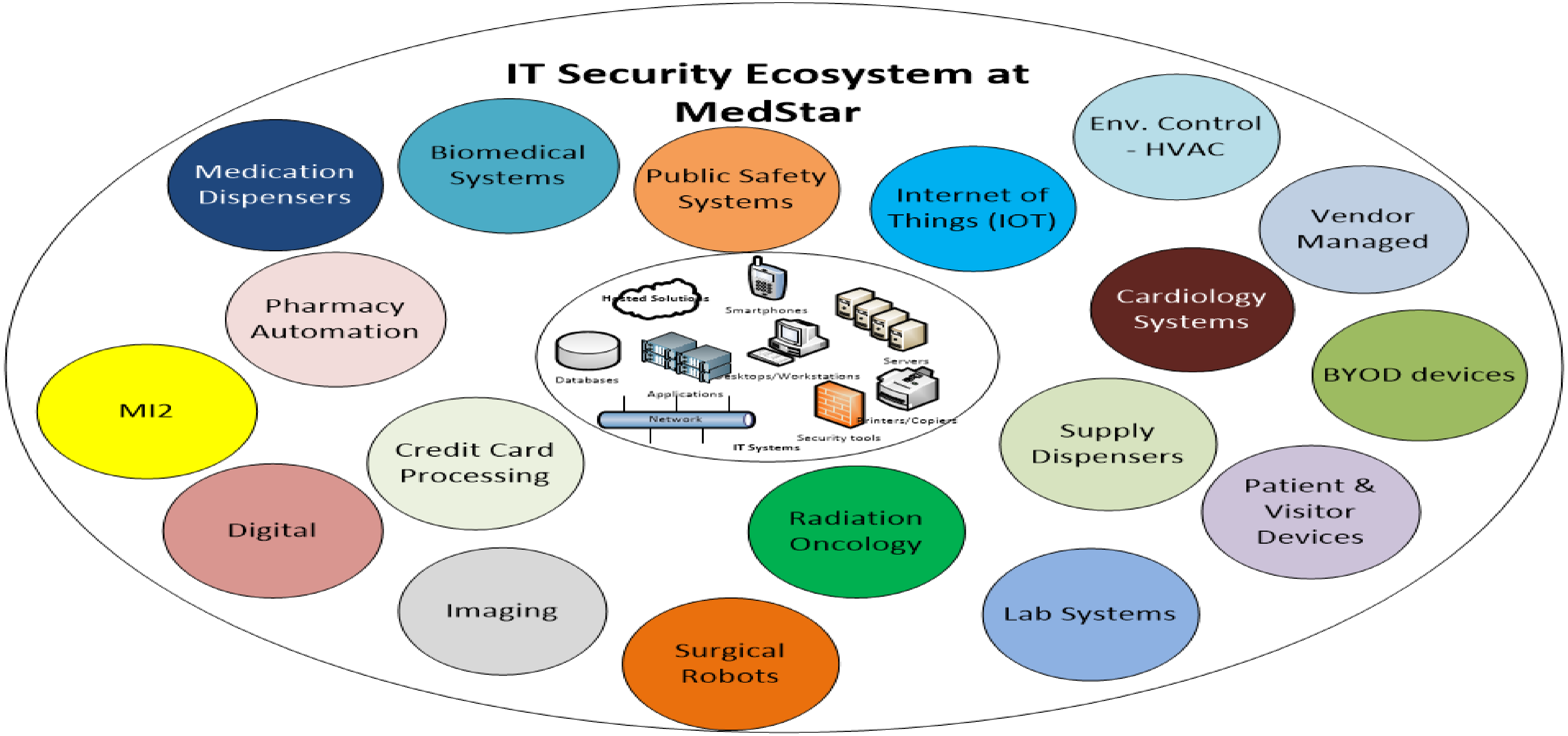
Jon Mckeeby & Inhel Rekik

Have no real or apparent conflicts of interest to report.

Building a security management plan for your networked medical devices

- What constitute a connected medical device?
- Regulatory aspects around medical device security
- Roles and responsibilities as it pertains to medical device security
- How clinicians contribute to an efficient medical device security program
- How can you build security into the life cycle of a medical device at a health system?
- Network monitoring tool for medical devices.
- Securing OT devices that patients use to collect PGHD (patient generated health data) and incorporation of those into EHRs

Connected medical device



IT Security Ecosystem at MedStar

Medication Dispensers

Biomedical Systems

Public Safety Systems

Internet of Things (IOT)

Env. Control - HVAC

Vendor Managed

Pharmacy Automation

Cardiology Systems

BYOD devices

MI2

Credit Card Processing

Supply Dispensers

Patient & Visitor Devices

Digital

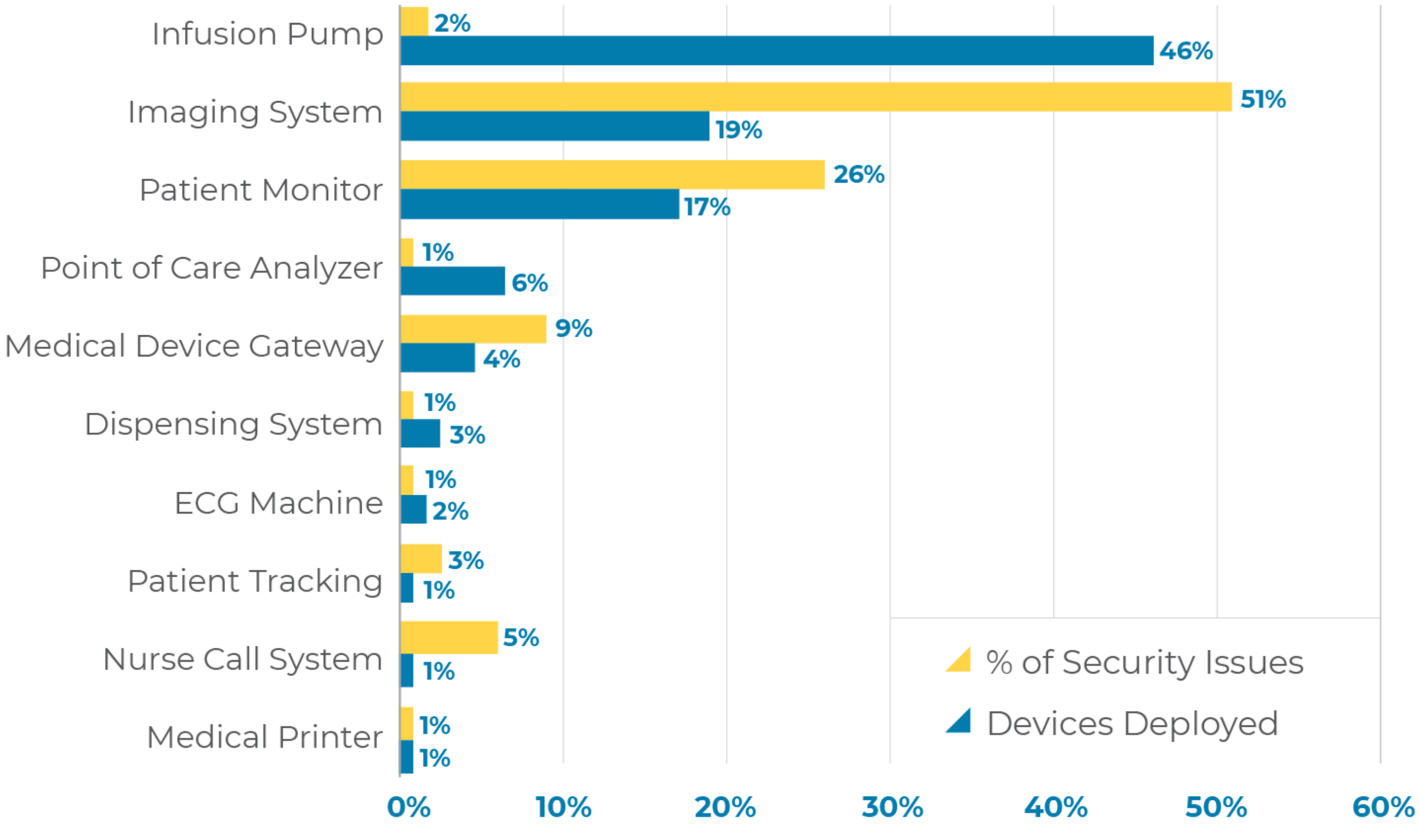
Radiation Oncology

Imaging

Lab Systems

Surgical Robots

Medical devices with most security issues



Top three device types account for **86%** of security issues.

Practical guide for medical device security by Xu Zou from Zingbox

Background

- Director of Health Technology Security at MedStar Health
- Oversees the security program for medical devices and IoT
- Clinical engineer with over 10 years of HTM experience and most recent role being the CE manager at MedStar Georgetown University Hospital
- Bachelor's degree in Computer Engineering from Laval University and Master's degree in Biomedical Engineering from Polytechnic School of Montreal
- Active member of AAMI Healthcare Technology Leadership committee, AAMI Next Generation Task Force and author of Tech Tips column in TechNation magazine

Background

- Chief Information Office, NIH Clinical Center
- Oversees EHR with 5,000 users
- Oversees Clinical Center IT with over 2,200 Employees, Contractors and Volunteers
- Doctorate in Computer Science from George Washington University
- Member HIMSS, AHIMA, CHIME

Safe and Reliable Patient Care should be our top Priority

- Integrity
- Availability
- Confidentiality

Regulatory aspects for medical device security

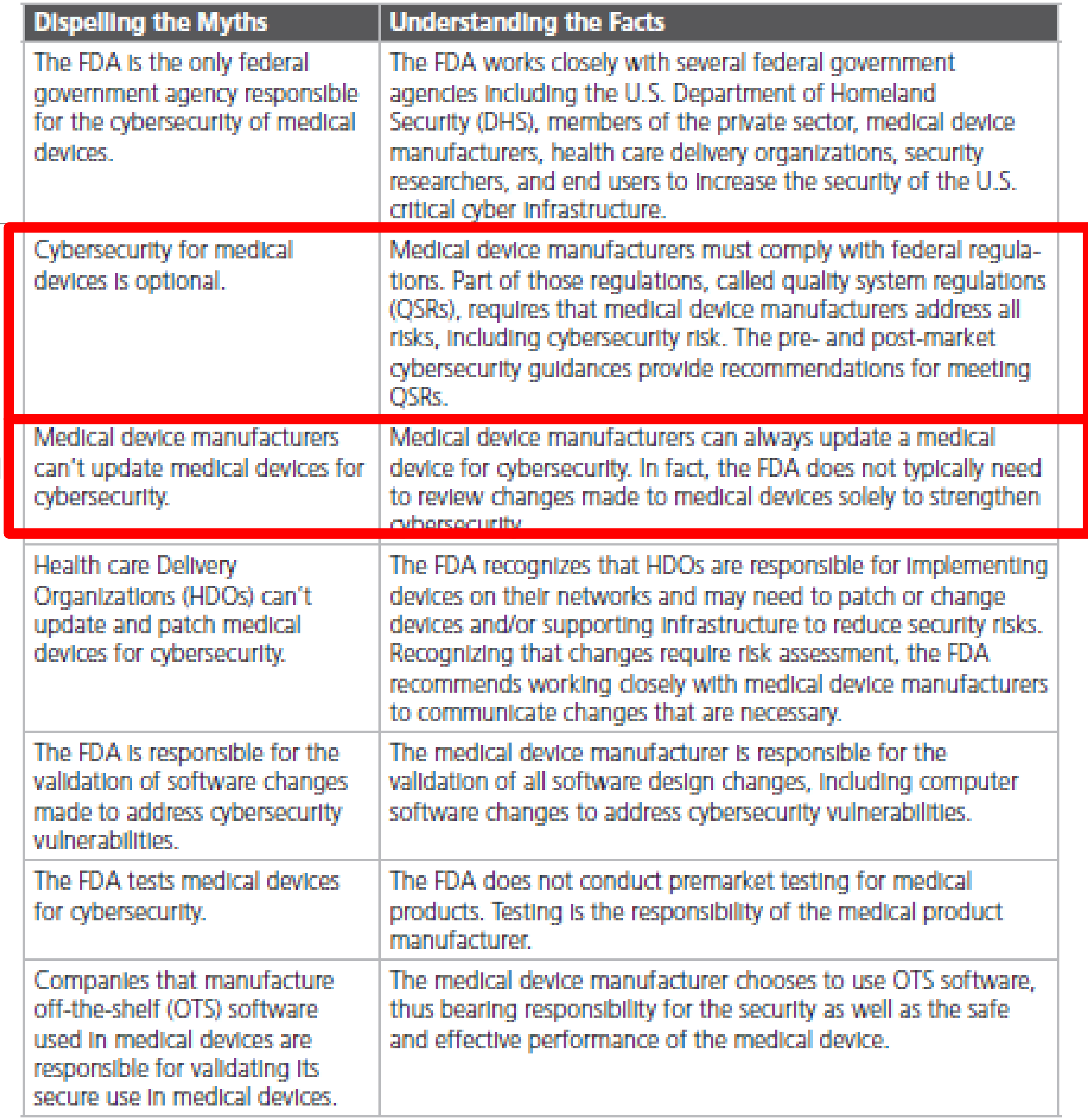
- The FDA’s Center for Devices and Radiological Health (CDRH) is responsible for regulating medical devices
  - Class I (lowest risk): no premarket submission
  - Class II (medium risk): premarket notification (510(k))
  - Class III (highest risk): premarket approval (PMA) application (more in depth submission which includes clinical trials).
- A device needs to meet all relevant special guidance in addition to the basic content of submission
- Manufacturers are expected to report adverse events to the FDA
- Manufacturers are expected to communicate the need to correct or remove devices to the FDA

Regulatory aspects for medical device security

- FDA Premarket Guidance for Management of Cybersecurity in Medical devices
- FDA Postmarket Guidance for Management of Cybersecurity in Medical devices
  - Controlled risk
  - Uncontrolled risk
- Security updates are considered device enhancement. However, If a cybersecurity fix modifies the function of the device or if it's released to address a security vulnerabilities that poses a significant risk to health than manufacturer must report it to the agency

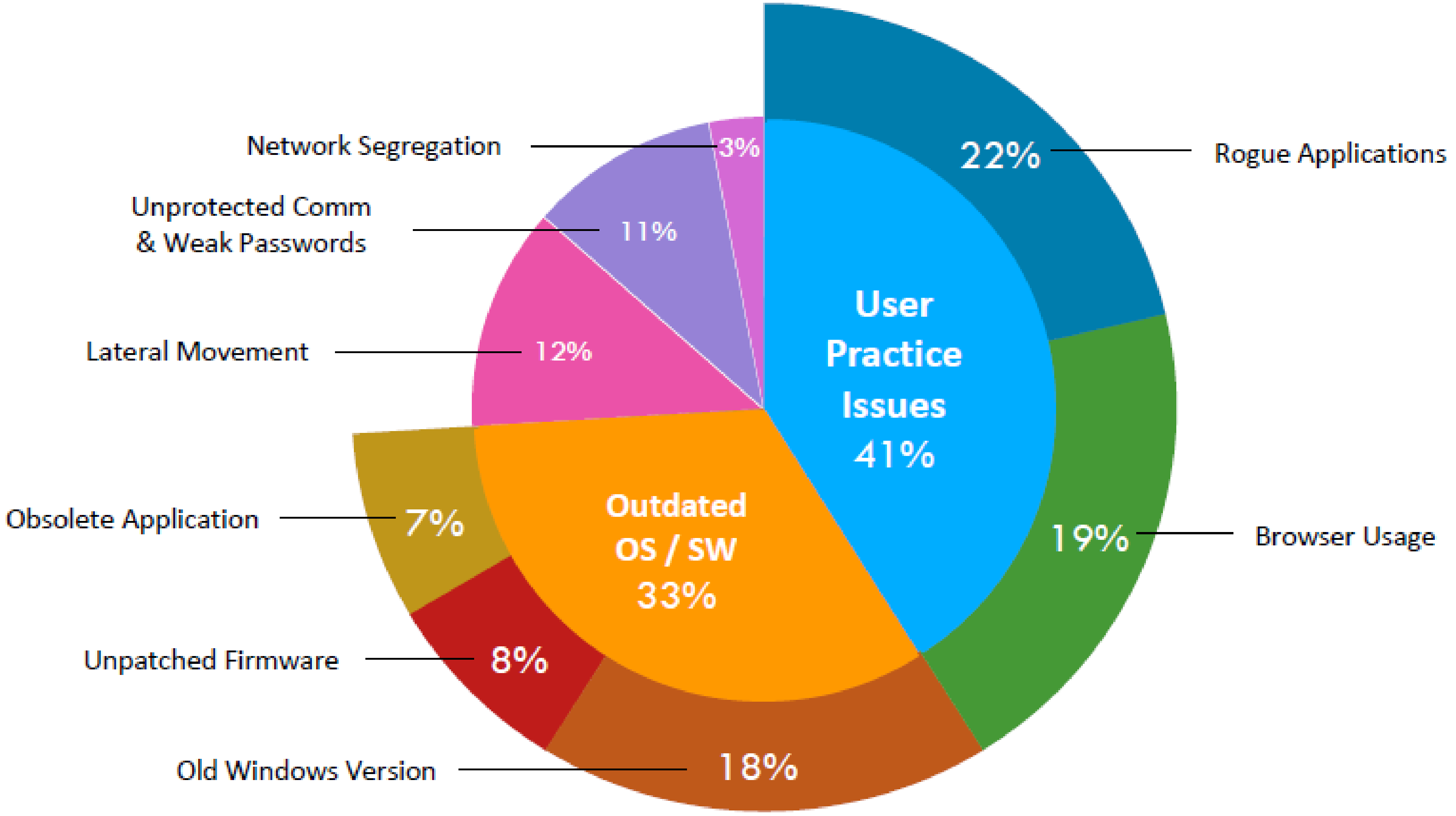
FDA’s Role in Cybersecurity Fact Sheet

https://www.fda.gov/downloads/Medica
4.pdf



Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Cybersecurity for medical devices is optional.	Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post-market cybersecurity guidances provide recommendations for meeting QSRs.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.
Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.	The FDA recognizes that HDOs are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.
The FDA is responsible for the validation of software changes made to address cybersecurity vulnerabilities.	The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.
The FDA tests medical devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.
Companies that manufacture off-the-shelf (OTS) software used in medical devices are responsible for validating its secure use in medical devices.	The medical device manufacturer chooses to use OTS software, thus bearing responsibility for the security as well as the safe and effective performance of the medical device.

What are the main security issues?



Practical guide for medical device security by Xu Zou from Zingbox

Roles: Organizational Executive Leadership

- **Support a culture of security.**
- **Understand business and legal implications of cybersecurity risks.**
- **Identifies security expectations as part of business needs.**
- **Review security direction, incidents and metrics regularly with Information Security and Information Technology.**
- **Complete security training.**
- **Includes C-Suite.**

Roles: Information Security Steering Committee

- Approves the security plan to align with business needs, system and data assets.
- Review security direction, incidents and metrics regularly.
- Sets the direction for cybersecurity for the organization.
- Approves all cybersecurity policies for the organization.
- Membership: Business owners, Chief Information Officer, Chief Information Security Officer (CISO), Information System Security Officer (ISSO), Privacy Act Officer, Enterprise Architect, Chief Technology Officer (CTO), Data Center Manager, Information Technology, Clinical Engineering/Health Technology Management/Biomed.

Roles: Information Security

- Develops and maintains security plan to align with business needs, system and data assets.
- Develops, implements and enforces organizational processes and policies (documentation processes, remote access, hardening, incident reporting, access and authentication).
- Partners with Information Technology, Enterprise Architecture, Clinical Engineering/Health Technology Management/Biomed to develop an organizational security plan.
- Identifies security requirements for all systems.
- Provides contractual language for all procurements.
- Provides cybersecurity risk management structure.
- Develops and delivers security awareness and training based on roles.
- Evaluates, selects, provide tools and technologies to manage security risks.
- Provides continuous monitoring of system vulnerabilities.
- Works with Information Technology to resolve security vulnerabilities and incidents.
- Reviews security posture to Organizational Leadership.
- Chief Information Security Officer (CISO), Information System Security Officer (ISSO), Security Team

Roles: Information Technology

- Partners with Information Security, Enterprise Architecture, Clinical Engineering/Health Technology Management/Biomed to develop an organizational security plan.
- Works with business owners to understand business requirements with security requirements.
- Develops appropriate network infrastructure based on system (firewall, dmz, network segregation, network access controls).
- Hardens systems based on organizational system policies.
- Follow organizational configuration management process for all system and security updates.
- Defines, develops and executes patch management processes for all systems.
- Monitors all logs for security, access, authentication, application errors.
- Performs vulnerability scans on servers.
- Remediates server vulnerabilities and incidents.
- Completes security training based on roles.
- Reports potential and actual security risks to Information Security.
- Works with vendors to maintain security posture.
- Chief Technology Officer (CTO), Data Center Manager, System Administrators, User Support, Database Administrators, Clinical informaticists, Network Administrators.

Roles: Clinical Engineering/Health Technology Management/Biomed

- Partners with Information Security, Enterprise Architecture, and Information Technology to develop an organizational security plan.
- Maintains an accurate inventory of medical devices (Network attributes, OS, SW, PHI)
- Collaborate with IT Security to make sure that risk management strategies are developed, documented, and practiced
  - Secure configurations are deployed and maintained
- Defines, develops and executes patch management processes for all medical devices.
- Makes sure that Data Security Addendum is included in contracts prior to execution.
- Factoring cybersecurity in lifecycle management of medical devices.
- Remediates medical devices vulnerabilities and incidents.
- Completes security training based on roles.
- Reports security incidents to Information Security and facilitates investigation.
- Works with vendors to maintain a security posture.

Roles: Business Owners/Clinicians/Users

- **Follow security based procurement strategies.**
- **Follow security policies and procedures.**
- **Works with Information Security to complete security documentation from business owner perspective.**
- **Report security issues and incidents to Information Security, Information Technology, Clinical Engineering/Health Technology Management/Biomed.**
- **Completes security training based on roles.**

Roles: vendors

- Design and implement industry standard controls.
- Follow System Development Life Cycle approach for updates including security controls.
- Provide complete documentation at time of procurement and for all updates.
- Provide timely patches based on operating system and software vulnerabilities.
- Communicate known vulnerabilities to customers in a timely manner.
- Update system to ensure no end of life or unsupported software.
- Provide remote access approach to meet customer remote access policy.
- Work with organization to meet security requirements over time.
- Stay current with all trends related to cybersecurity to ensure proper measures of security are maintained to protect the medical device and organization.
- Identify all ports, services, third party software used by medical device to allow whitelisting.

NIST CYBERSECURITY FRAMEWORK (CSF)

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

- Identify
  - Manual and automated identification via network scanning, device discovery tools, etc
  - Understanding and identifying data flows, architectural diagrams, and support requirements

- Protect
  - Determine controls available and not available on the medical devices
  - Create implementation plans for securely deploying devices
  - Determine and applying compensating controls and appropriate network segmentation methods as necessary

- Detect
  - Establish behavior baselines and monitor for abnormal behavior

- Respond
  - Establish response plans when controls fail and develop communication plans for control failures, breaches, theft, loss, etc.

- Recover
  - BCDR plans for redeploying medical device following an incident and to restore data

Build security into the lifecyle of the device

- Incorporate security in the procurement process
  - Cybersecurity documentation (AV, encryption, patch management, data destruction technique..)
  - MDS2 document
  - Who will maintain the operating system?
  - Add data security addendum to Master Service Agreement
- Inventory standard/procedure/policy
  - Obtain and document network information; OS; SW version; ePHI/ PII/ PCI; local data storage capability
  - Risk assessment is performed
  - Document security requirements issued by IS security and mitigation strategies recommended in the CMMS
  - Before deploying the device, perform vulnerability scanning and check security configurations (AV, patch level, firmware version) and apply mitigation strategies
  - Patch strategies are documented

Build security into the lifecyle of the medical device

➢Preventive maintenance procedure

Periodic review of security controls for the device or systems

- Default password
- AV updates
- Encryption of sensitive data
- Last patch update/ Do we need to update?
- Document the validated controls in the preventive maintenance action plan

Build security into the lifecyle of the medical device

- Disposition procedure
  - Delete any PHI and any proprietary information such as network credentials, domains and user accounts…
  - Use secure wipe techniques as described in *NIST 800-88 or DoD 5220.22M*
  - Equipment control number, date of secure wipe, technician performing the secure wipe, reason for wipe, method and outcome of secure wipe

Role of clinicians: Before returning the medical device (case of trial), disposing or transferring the device, contact clinical engineering.

Build security into the lifecyle of the medical device

Vulnerability management

- National Health Information Sharing and Analysis Center (NH_ISAC)
  - Security alerts shared daily
  - MDSISC and PSIC list serves
- ICS-CERT advisories
  - Partnership with manufacturers
  - Resources for HDOs

Build security into the lifecyle of the medical device

Patch management

- HDOs should ensure medical device receive cybersecurity routine updates and patches

Role of clinicians: Restart the device so it can receive security updates (medication cabinets, lab analyzers, EEG workstations)

Build security into the lifecyle of the medical device

Patch management

- HDOs should ensure medical devices receive cybersecurity routine updates

Role of clinicians: Restart the device so it can receive security updates (medication cabinets, lab analyzers, EEG workstations)

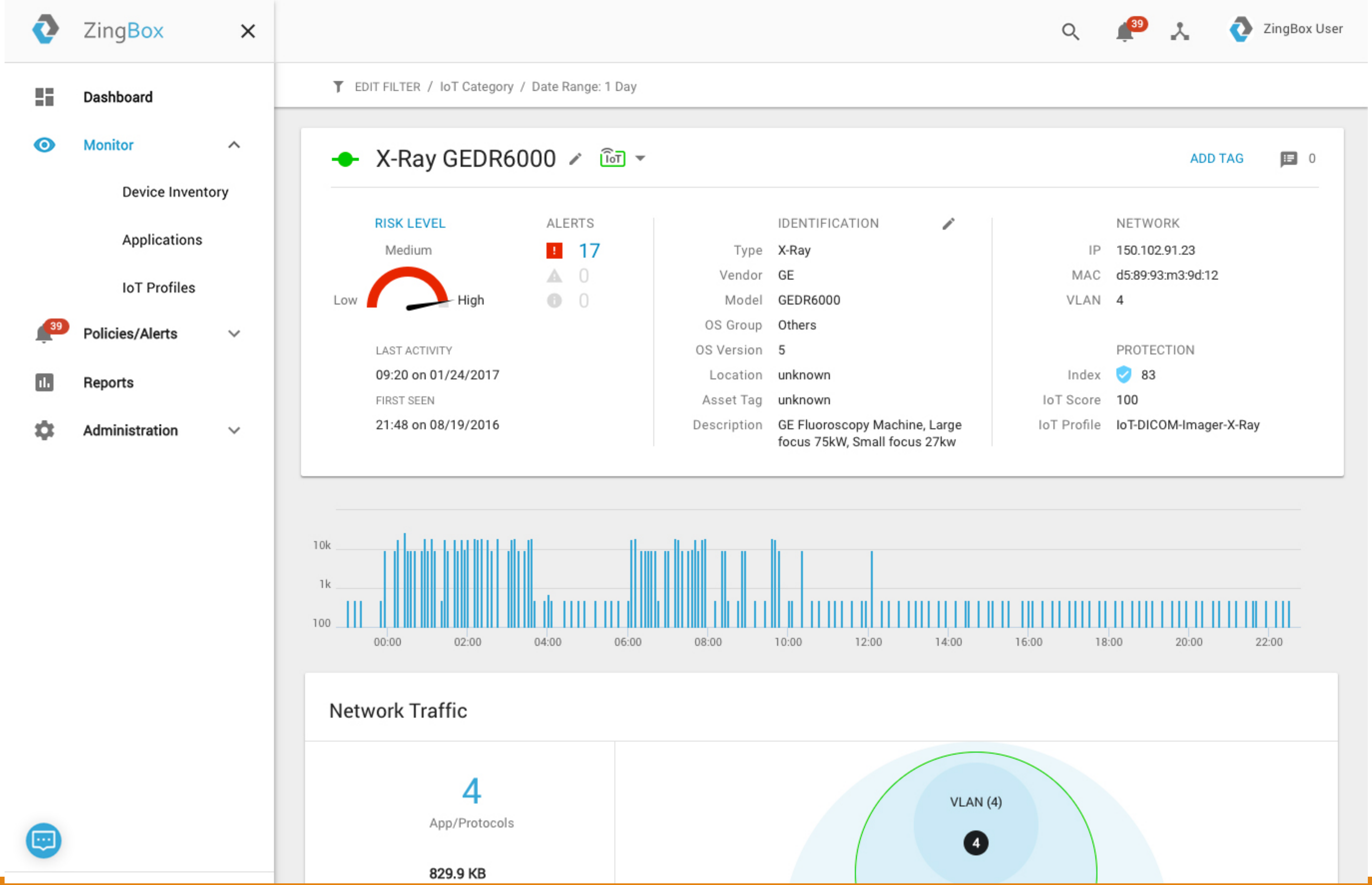
Do you have a Business Continuity and Disaster Recovery plan (BCDR)?

- ➢ Work with key stakeholders to vet the incident response process
- ➢ Establish your downtime procedure and practice
  - Include education and training on a routine basis, if necessary
- ➢ Identify DR resources – do you have contracts to bring in additional help?
- ➢ What plans are in place for vendor support for recovery if multiple devices need to be reimaged?
- ➢ Practice – tabletop exercises?

Network monitoring tool for medical devices: Threat detection

- Automatic discovery and risk assessment of biomedical devices on the network
- Analysis of medical device behavior through machine learning for baselining and anomaly detection
- Medical device relationship and data flow and identification of devices communicating outside the organization
- Proactive security and real-time protection with immediate policy enforcement

Network monitoring tool for medical devices: Threat detection



X-Ray GEDR6000

RISK LEVEL
Medium
Low High

ALERTS
17
0
0

LAST ACTIVITY
09:20 on 01/24/2017

FIRST SEEN
21:48 on 08/19/2016

IDENTIFICATION

Type	X-Ray
Vendor	GE
Model	GEDR6000
OS Group	Others
OS Version	5
Location	unknown
Asset Tag	unknown
Description	GE Fluoroscopy Machine, Large focus 75kW, Small focus 27kw

NETWORK

IP	150.102.91.23
MAC	d5:89:93:m3:9d:12
VLAN	4

PROTECTION

Index	83
IoT Score	100
IoT Profile	IoT-DICOM-Imager-X-Ray

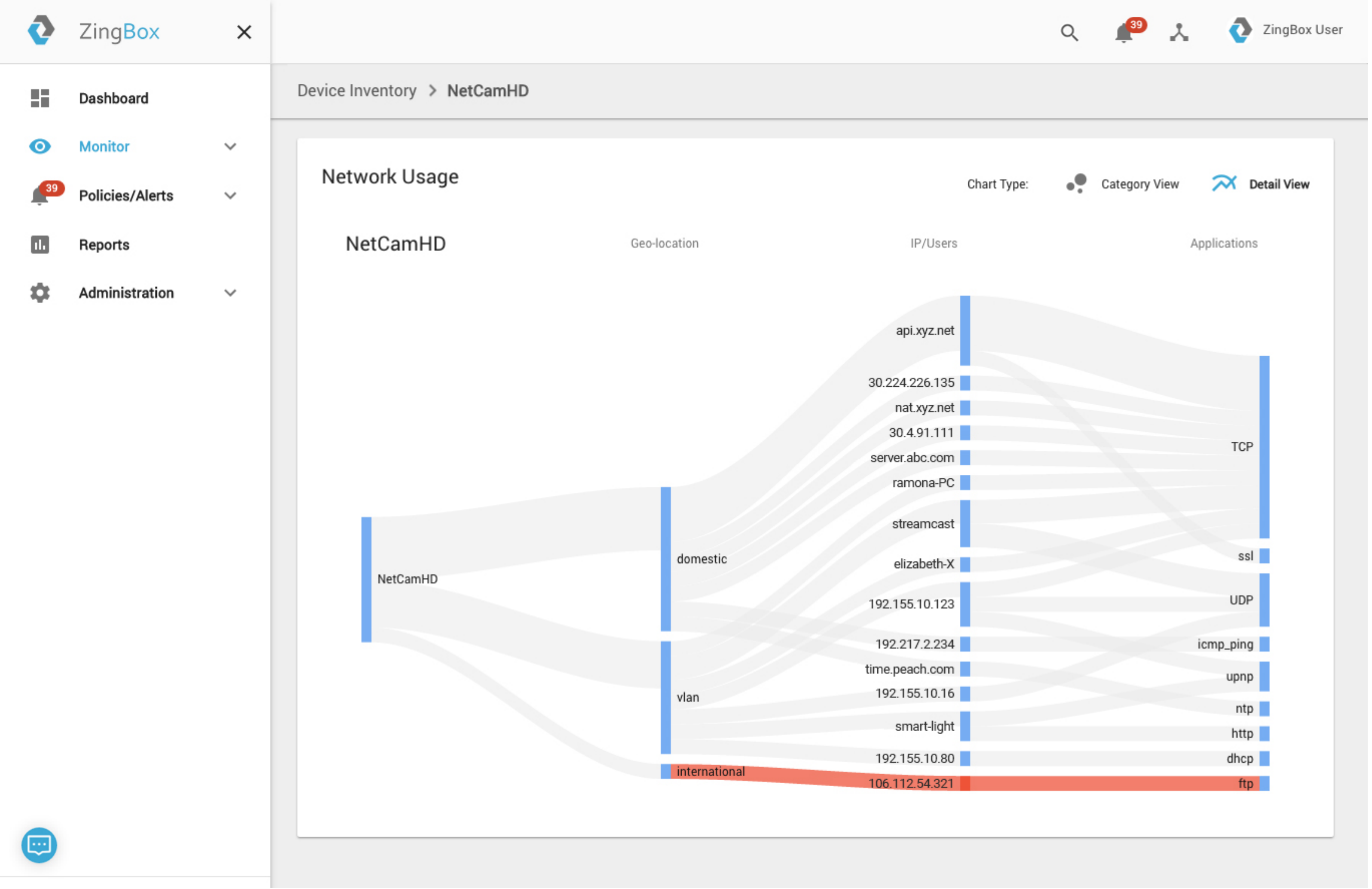
Network Traffic

4
App/Protocols

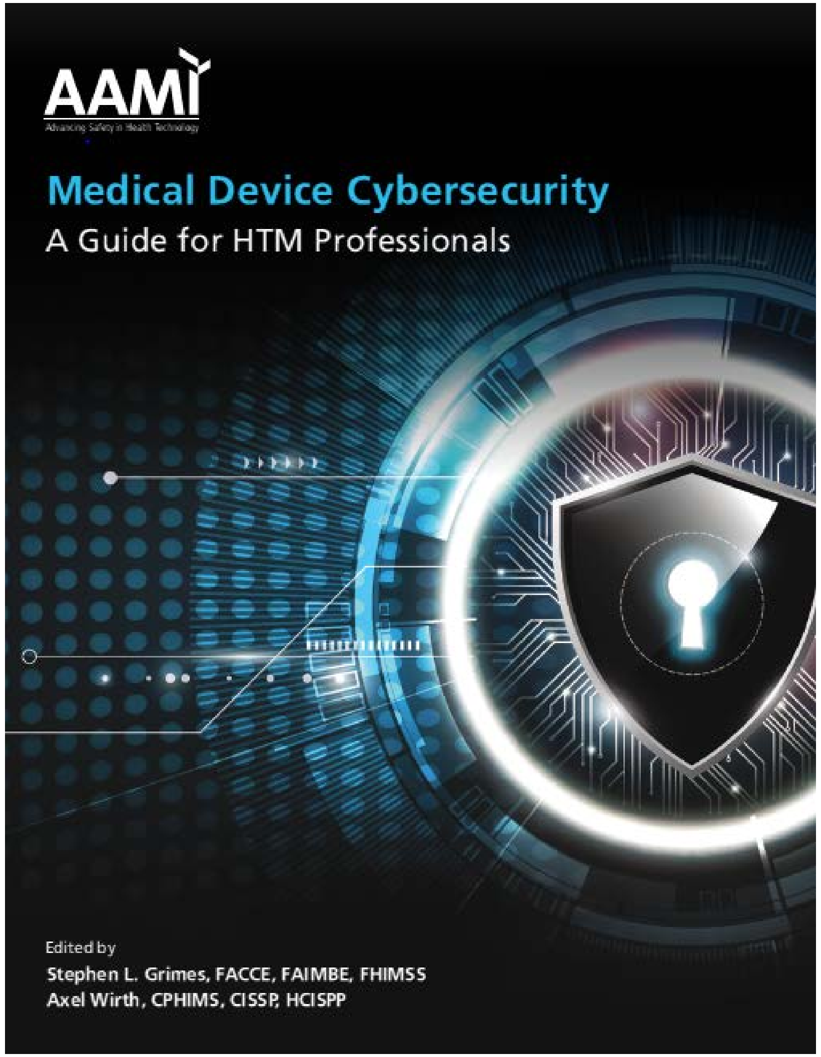
829.9 KB

VLAN (4)
4

Network monitoring tool for medical devices: Threat detection



AAMI’s Medical Device Cybersecurity Practice Guide for HTMs



AAMI

Advancing Safety in Health Technology

Medical Device Cybersecurity

A Guide for HTM Professionals

Edited by

Stephen L. Grimes, FACCE, FAIMBE, FHIMSS

Axel Wirth, CPHIMS, CISSP, HCISPP

Securing OT devices that patients use to collect PGHD (Patient Generated Health Data) and download into EHRs

- What’s the main security concern?

Confidentiality and Integrity

- How do you guarantee integrity and confidentiality of PGHD?

Containerized app that clears the cache on exit

- What integrity check are in place to guarantee that data is accurate in transit?

SHA-2, MD5

Securing OT devices that patients use to collect PGHD (Patient Generated Health Data) and download into EHRs

- How is the data uploaded to the records?

21st Century Cures requires vendors, healthcare providers, or HIS system providers to accept apps for downloading from EHR but where does it falls for uploading data?

- To what extend the diagnosis and treatment is based on this data provided by patients?

US Gov Cyber & ISE References

a) Presidential Policy Directive/PPD-21 Critical Infrastructure Security and Resilience issued February 12, 2013.

b) Executive Order (EO) 13636 Improving Critical Infrastructure Security, Federal Register issued February 19, 2013.

c) Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices, U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Office of Compliance, Office of Device Evaluation issued September 9, 1999.

d) Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software issued January 14, 2005.

e) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff issued October 2, 2014.

f) Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff issued December 2, 2014.

g) Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff issued on January 22, 2016.

h) Updated recommendations on submitting a new 510(k) for device modifications August 5, 2016.

i) Deciding When to Submit a 510 K for a software change to an existing device issued August 8, 2016.

j) Post Market Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff Document issued on December 28, 2016.

Credits: Bill Hagestad, Cybersecurity Expert

US Gov Cyber & ISE References

a) AAMI TIR57/Ed. 1, Principles for Medical Device Information Security Risk Management dated June 9, 2016.

b) IEC 80001-1:2010 Application of Risk Management for IT-Networks Incorporating Medical Devices -- Part 1: Roles, Responsibilities and Activities.

c) AAMI's Health IT Risk Management: A Practical Tool to Help Hospitals and Medical Devices Stay Secure in a Complex World

d) ISO/IEC 27005:2011 provides guidelines for Information Security Risk Management.

e) ISO/IEC 15408-3 1999-12-01 Information Technology — Security Techniques — Evaluation Criteria for IT Security — Part 3: Security Assurance Requirements.

f) ISO/IEC 14971 Risk Management for Medical Device Manufacturers.

g) ISO/IEC 29147 Vulnerability Disclosure Process.

h) ISO/IEC 30111 Vulnerability Handling Processes.

i) RFC 2196 Site Security Handbook September 1994.

j) IEC TS 62443-1-1:2009 Industrial Communication Networks - Network and System Security - Part 1-1: Terminology, Concepts and Models.

k) IEC TS 62443-2-1:2009 NIST Cybersecurity Framework Core: Informative Reference Standards.

l) IEC TR 62443-2-3:2015 Security for Industrial Automation and Control Systems - Part 2-3: Patch Management in the IACS Environment.

Credits: Bill Hagestad, Cybersecurity Expert