Building a Case for Medical Device Security

Session 131, August 11, 2021

David Finn, CISA, CISM, CRISC, CDPSE

EVP, External Affairs, Information Services and Security, CynergisTek

Priyanka Upendra, BSBME, MSE, CHTM, AAMIF

Senior Director, Customer Success, Asimily

HIMSS21

Meet the Speakers

Priyanka Upendra
Senior Director, Asimily

David Finn
EVP, CynergisTek

Conflict of Interest

David Finn, CISA, CISM, CRISC, CDPSE

Priyanka Upendra, BSBME, MSE, CHTM, AAMIF

Have no real or apparent conflicts of interest to report.

Agenda

1. Why Medical Device Security?
2. Three stages of Medical Device Security
3. Risk Analysis Methodology
4. Risk Categorization
5. Governance Model
6. Q & A

Learning Objectives

- Identify and understand the 3 stages of building a medical device security program
- Appreciate how risks related to medical devices are not just technical risks but can impact quality of care and clinical operations
- Recognize that the same device models may require different remediation strategies and be able to identify relevant risk vectors
- Understand that medical device management may cross multiple functional lines in a healthcare setting
- Realize that security and device management require a life-cycle approach and long-term strategies rather than a “once and done” approach

Our Business Philosophy

Mission

To reform health globally through information and technology.

Vision

To realize the full health potential of every human, everywhere.

When you're in health care, if people can't do the right thing, how can they trust you with their lives? Health care has to be run at a different standard.

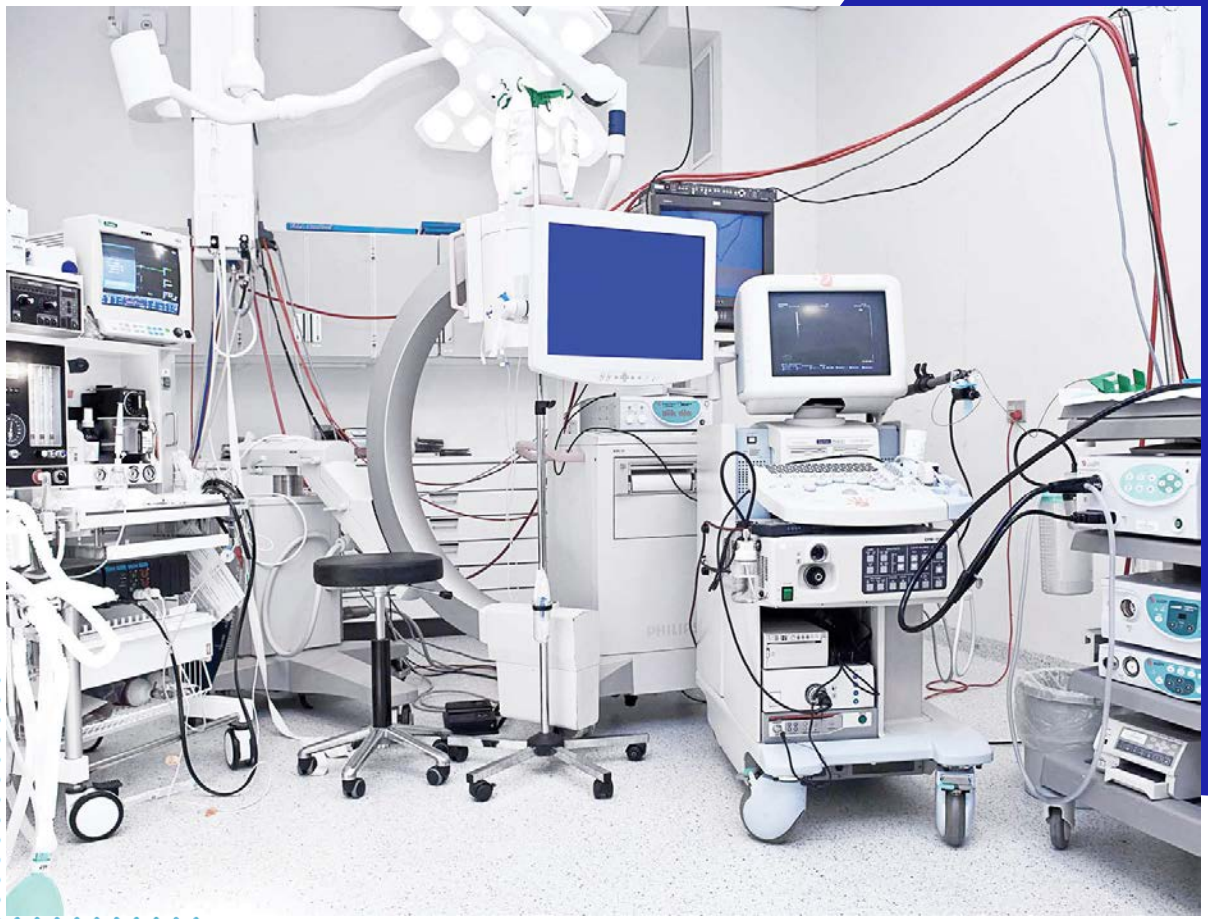
Dr. Charles Sorenson

Former CEO of Intermountain Healthcare, Salt Lake City, Utah

1 Why Medical Device Security?

Why Medical Device Security?

- Increasing number of Internet-connected medical devices
- Device Vulnerabilities
- Security
  - Device level
  - Network
- Who does it belong to?
  - Who is responsible?
  - How is it governed?
- The Risks

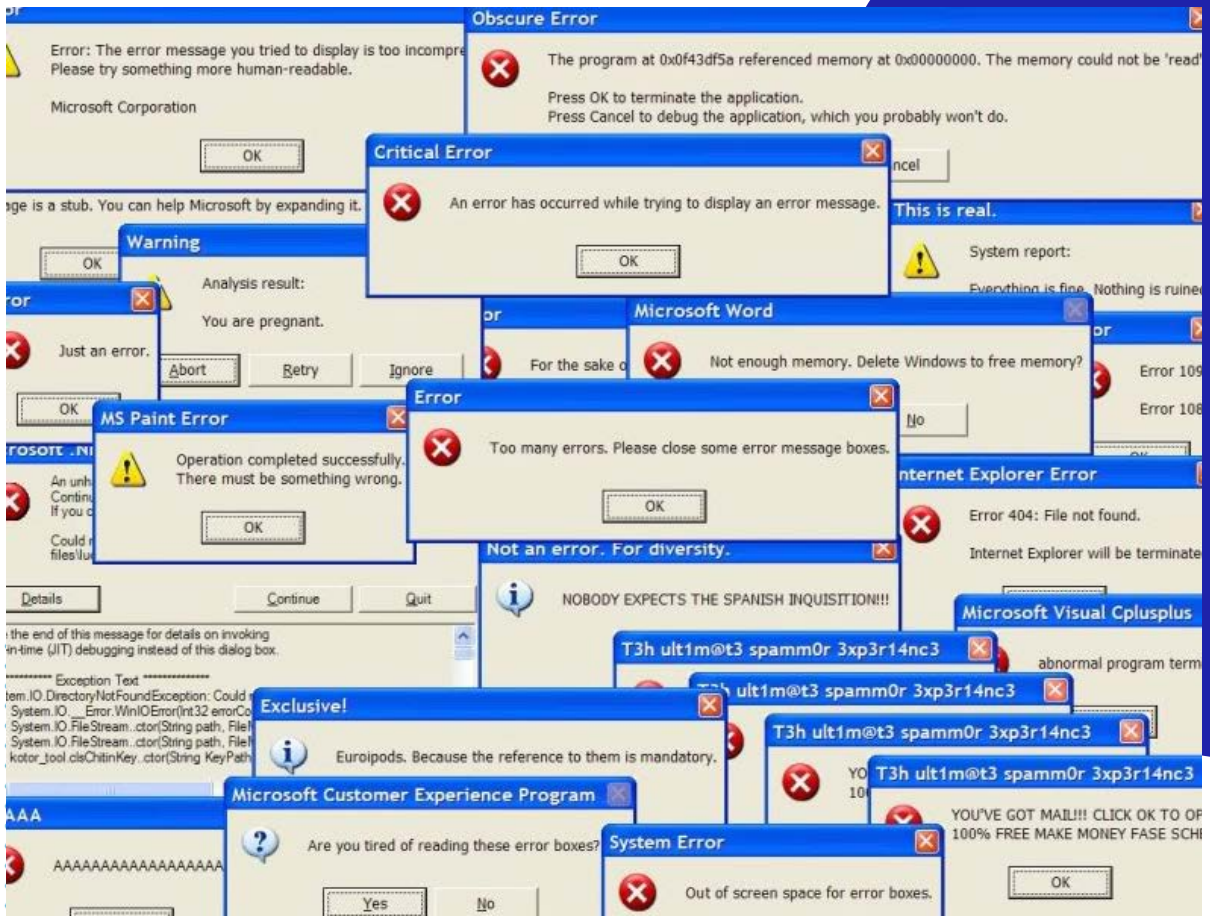


And why now?

Connected medical devices are crucial to supporting patient care, but cybersecurity mitigations and processes are needed to protect patient safety.

Four key risk areas:

- Clinical
- Organizational
- Regulatory
- Financial



2 Three Stages of Medical Device Security?

Three stages of Medical Device Security

- Like Security overall this is a journey, not a destination
  - You don't ever stop doing it
  - That is why you begin with governance, Roles & Responsibilities, and addressing processes
- Like security overall, choose a framework from which objectives, tactics and metrics will evolve
  - NIST CSF: Identify, Detect, Protect, Respond, Recover
  - Example: Identify: Inventory: devices, data, parameters
- Like security overall, identify every objective and what is needed to achieve it
- Like security overall, inventory and management of that inventory is the first step
  - You cannot protect what you don't know is there (data and devices)
  - If you don't know how, what, when, where, and why it is used, you may not protect it adequately (or overprotect it)

Stage 0: Before you Begin . . .

- Establish and define Objectives
  - What are you trying to accomplish
  - Use a Standard Framework (NIST CSF)
- Objectives should align with the Framework you are using and what you are trying to accomplish
  - IDENTIFY: Inventory
  - DETECT: Vulnerability Management (Scoring, Risk Assessment) and Intrusion Detection
  - PROTECT: Contain Attacks, Micro-segmentation at the device level
- List other requirements (non-security goals)
- Identify metrics
- Identify resources (internal & external)
- This is likely a multi-year plan - - create a map

Stage I: Risk Assessment

- Inventory Management will be the first step to any program
- Detection through Vulnerability Management and Intrusion Detection
- Protecting through Segmentation, Quarantining and Blocking
- Responding through Forensic Analysis
- Identify Key Program Metrics
- Identify resources (internal and external) to achieve objectives
- Build and follow the roadmap

Stage 2: Program Assessment (Security/Network IT)

- On-boarding processes
- Policy and policy management
- Inventory gap analysis and baseline configuration
- Network tool monitoring and reporting
- Incident response management
- Disposition and sanitization practices (don't forget the data)

Stage 3: Program Assessment (Clinical Engineering)

- This is where it gets hard.
  - On-boarding processes
  - Inventory gap analysis and baseline configuration
  - Network tool monitoring and reporting
  - Incident response management
  - Disposition and sanitization practices (don't forget the data)

- It is not just about devices.
  - Procurement management
  - Inventory Management
  - Vulnerability management
  - Intrusion detection with forensics
  - Containment and micro-segmentation

3 Risk Analysis Methodology

Risk Analysis Methodology

- Risk analysis must be **robust** and **factor in increasing trends** in technology
  - Increasing integration
  - Increasing complexity
  - Increasing capability
  - Increasingly diverse care delivery modes
- Risk analysis must **incorporate a multi-disciplinary approach**
  - Evaluate patient, clinical workflow and clinician risks
  - Evaluate supply chain risks
  - Evaluate healthcare technology management risks
  - Evaluate information technology risks
  - Evaluate financial, legal, and other business risks

Risks with Mission-Critical Assets

- Patient Safety Risks
  - Intentional or unintentional changes to asset functionality, availability, or integrity
- Care Delivery Risks
  - Patient care diversion or delay or downtime due to asset unavailability

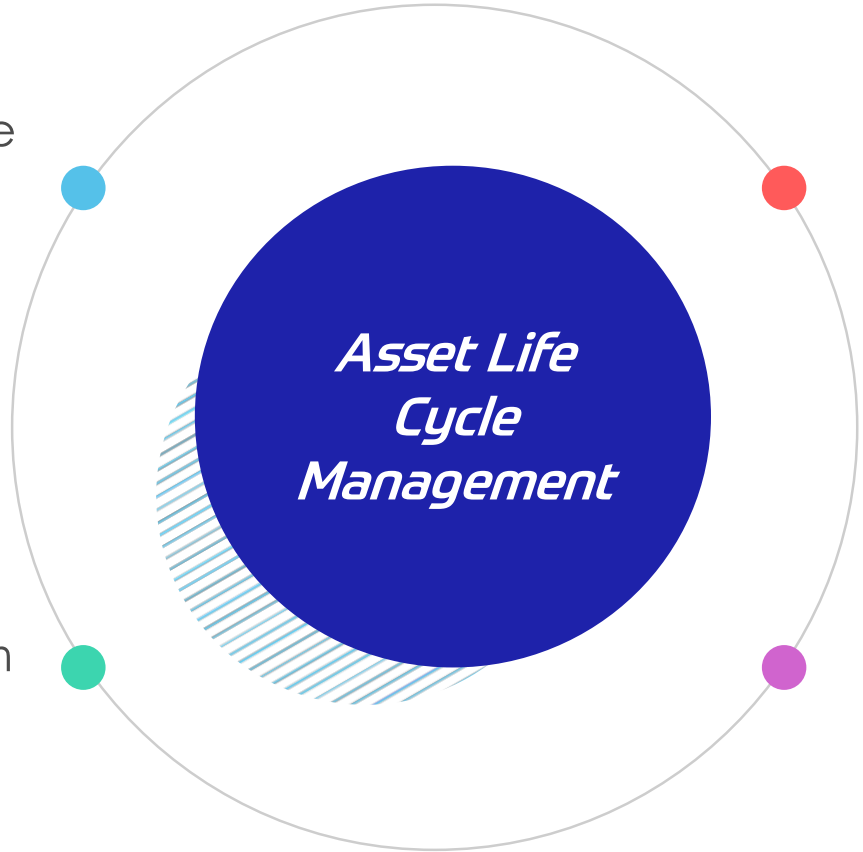
- Privacy Risks
  - Loss of patient health information, patient identifiable information, sensitive data, credentials, business intellectual property, etc.
- Cybersecurity Risks
  - Asset used as a backdoor to the network, delay of critical alarms, delay in transmission of diagnostic or treatment information, denial of service, etc.
- Business Risks
  - Lawsuits, financial loss, reputational damage, patient diversion, etc.

Selection & Acquisition

- Evaluate obtained cybersecurity documents with key stakeholders and the multi-disciplinary team
- Evaluate deployment and ongoing support & maintenance processes
- Ensure cybersecurity related contracts are in place before purchase

Pre-Procurement

- Engage a multi-disciplinary team
- Obtain relevant cybersecurity documents from the vendor
  - MDS2
  - CBOM/SBOM
  - Network architecture



Ongoing Support & Maintenance

- Ensure vendor support is available prior and during cyber events and incidents
- Ensure software keys, licenses, and support documents are available
- Ensure ground level resources are trained to handle cyber events and incidents
- Ensure asset management practices align with key stakeholders
- Ensure continuous and real-time vulnerability management processes are implemented

Decommissioning & Disposal

- DoD data sanitization methods are implemented prior to decommissioning or disposing devices
- All sensitive data is removed
- Documentation is completed and retained for auditing

Challenges with Current Risk Analysis Techniques

- Lack of security monitoring tools to analyze clinical assets real-time
- Lack of visibility on clinical asset performance due to stand-alone deployments or lack of integration with security monitoring tools
- Lack of access to proprietary or asset-specific data solely managed by vendors
- Lack of skilled staff that have working knowledge of clinical assets and cybersecurity
- Budget constraints related to dedicated staffing and asset replacement
- Cybersecurity practices are not clinician and clinical workflow friendly

4 Risk Categorization

Risk Categorization

- Evaluate and categorize program and device specific risks using the NIST Cybersecurity Framework (NIST CSF)

National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF)

Consists of standards, guidelines, and best practices to manage cybersecurity-related risk

ID	Function	Category
ID.AM	IDENTIFY (ID)	Asset Management
ID.BE		Business Environment
ID.GV		Governance
ID.RA		Risk Assessment
ID.RM		Risk Management Strategy
PR.AC	PROTECT (PR)	Access Control
PR.AT		Awareness and Training
PR.DS		Data Security
PR.IP		Information Protection Processes and Procedures
PR.MA		Maintenance
PR.PT		Protective Technology
DE.AE	DETECT (DE)	Anomalies and Events
DE.CM		Security Continuous Monitoring
DE.DP		Detection Processes
RS.RP	RESPOND (RS)	Response Planning
RS.CO		Communications
RS.AN		Analysis
RS.MI		Mitigation
RS.IM		Improvements
RC.RP	RECOVER (RC)	Recovery Planning
RC.IM		Improvements
RC.CO		Communications

Function	Category	Subcategory
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-4:** Potential business impacts and likelihoods are identified
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed

- Five (5) "**Functions**"
- Twenty-three (23) "**Categories**"
- One hundred Eight (108) "**Subcategories**"
- Subcategories define expected **outcomes and security controls**

Risk Categorization

Patient Safety

- Evaluate and categorize risk based on the clinical workflow
- Align NIST risk categorization with CMS and TJC risk categorization for clinical assets

Operational Safety

- Ensure compensating controls are configured and designed to ensure safe and reliable operation of clinical assets
- Test controls to prevent functional hazards of clinical assets

Data Safety

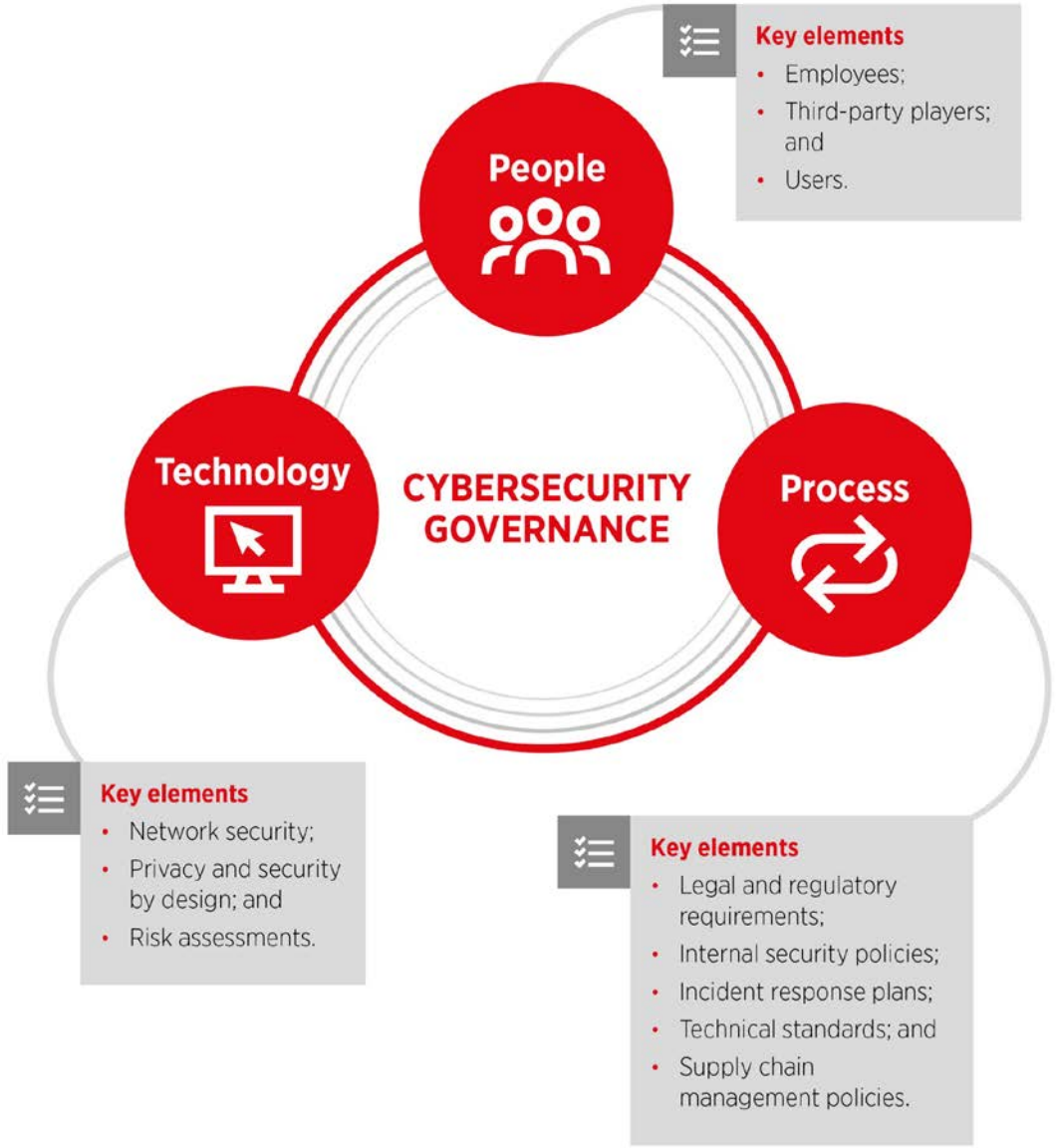
- Identify clinical assets that store, transmit, or display sensitive data
- Ensure data is protected from unauthorized users or unwanted actions

5 Governance Model

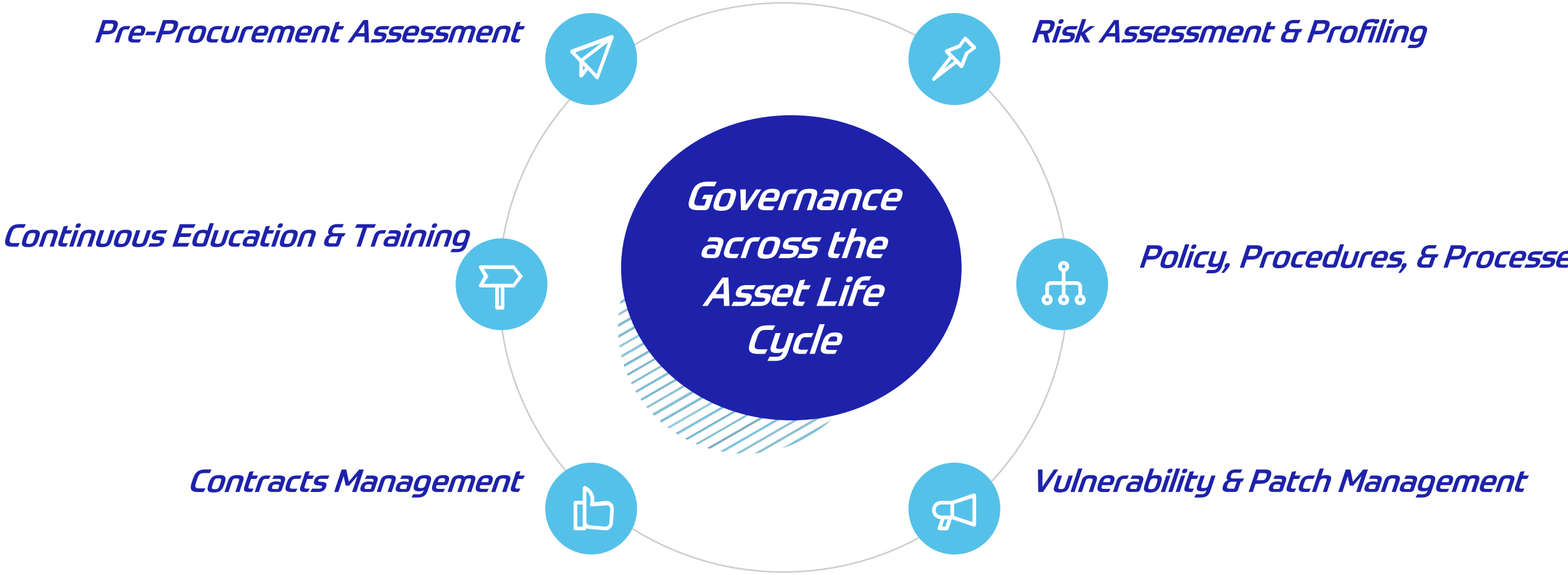
Technical and Operational Dependencies

1. Establishment of Governance
2. Dedicated Staff and Budget
3. Integrated Architecture
4. Ongoing Training, Education, and Awareness
5. Develop specific policies, procedures, and processes
6. Establish key performance metrics with vendors and other support entities

Governance Model



- Establish formal oversight of medical device cybersecurity with a clinical champion
- Identify and assign specific roles and responsibilities to key stakeholders
- Adopt and implement the NIST CSF for program implementation


Pre-Procurement Assessment
Risk Assessment & Profiling
Continuous Education & Training
Governance across the Asset Life Cycle
Policy, Procedures, & Processes
Contracts Management
Vulnerability & Patch Management

Bridging Healthcare Technology Management and Information Technology Gaps

Stakeholder Commitment & Stewardship

Leverage Cross-Functional Skillsets

Skill-Specific Roles & Responsibilities

Summary

- Clinical assets' cybersecurity management comes with unique challenges
- Its management requires the establishment of a cross-functional team
- A clinical champion will provide the necessary visibility to the efforts, including support for budget and staffing needs
- Automating device identification, risk profiling, and vulnerability management will optimize use of ground level resources and balance cost
- Industry engagement will expand education, awareness, and the overall knowledge base
- Utilizing existing resources from AAMI, ACCE, ECRI, NIST, HSCC, and HIMSS will ensure processes are implemented in a timely manner without reinventing the wheel

6 Q&A

Thank you!

Priyanka Upendra
Priya@asimily.com

David Finn
David.Finn@cynergistek.com