An 8-Year Journey to Medical Device Security… Lessons Learned

Building & Maturing a Medical Device Cybersecurity Program

Kevin A. McDonald
Principle Healthcare Cybersecurity Advisor
MedSec

The Challenges that Hospitals Face

Demographics

- 6090 US hospitals (200 less than in 2019)
- 60% of these are 200 beds or less
- Median income down 16% in 2020 (including aid & relief)
- 1 of 4 rural hospitals in danger of closing

Threat

- Increasing number of healthcare providers are being targeted
- Cybersecurity disruptions of healthcare facilities across the U.S.

Challenges

- Millions of medical devices on hospital networks, many with unsupported OS & software
- HDO's have difficulty finding & retaining security professionals
- Most hospitals lack resources & experience to build a medical device security program

MedSec

Kevin McDonald

Professional Background

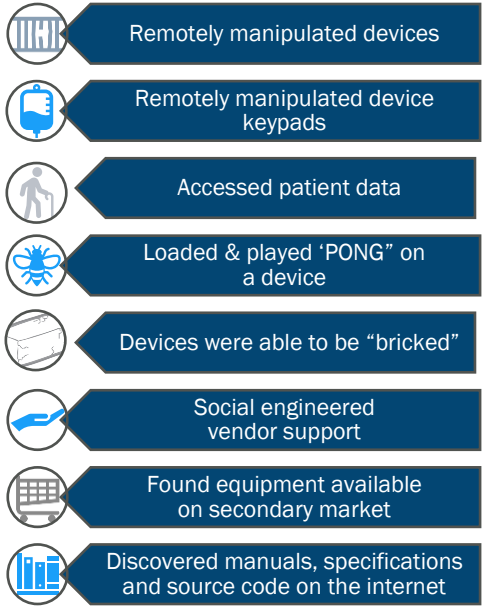
- 40+ years of experience in healthcare
- He began his hospital career as a clinical practitioner
  - Critical Care and ER nurse
  - Nursing Director of Critical Care, Telemetry and PACU
- Transitioned into a broad number of IT leadership roles
  - EMR implementations
  - Project Coordination, BCM, Account Management
  - SOX, security controls, security tool selections
- Frequent speaker at HIMSS, FDA and other national conferences
- Built, lead and matured Mayo Clinic's medical device security program
- In 2019, Kevin joined MedSec. He began advising hospitals on developing and maturing their own unique medical device security initiatives

MedSec

Changing the Culture

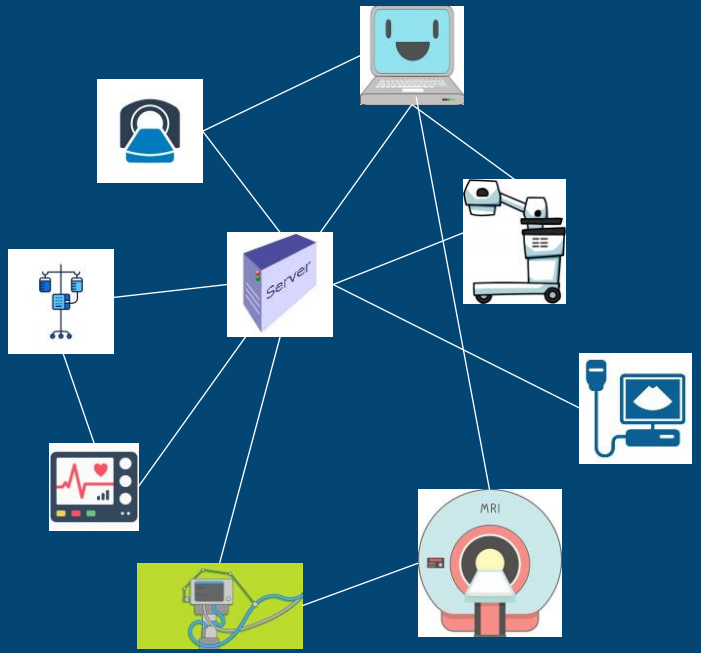
- Security became a board and institutional issue
- Demonstrated the vulnerabilities in medical devices. Assembled several pen testing companies to test 40+ devices with all devices being compromised
- Early engagement of clinical equipment staff, clinical area staff and physicians
- With management and clinical assistance, brought patient care issues and concerns to practice groups
- Formed physician lead governance for medical device security

Testing Outcomes:



MedSec

Medical Devices Represent 15-20% of Hospital Endpoints



Millions of medical devices are in use that run non-supported operating systems and software

Too many HDOs don't have a complete inventory of their medical devices, much less what risk they present

Medical devices are different than IT devices. They have unique maintenance/upgrade requirements, operational responsibility, threats & vulnerabilities, complexity, and impact of failure

The challenge for hospitals is not how to create a medical device security program. It is ultimately how to embed security awareness & processes into all the existing strategic day-to-day operational activities in the hospital.

MedSec

Outcomes of a Medical Device Program

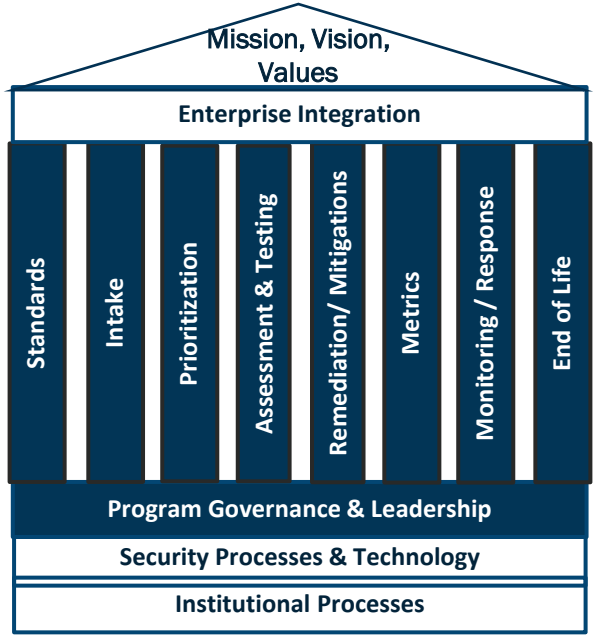
Medical Device Risks are Visible and Conscious and Deliberate Decisions are Made on Accepting the Risk

- You can identify your cybersecurity risks for individual medical devices and the fleet
- Your program is integrated into involved department workflows
- Defined steps, templates, that can drive efficiency and shift work to less skilled staff
- You have a dashboard for communication to leadership of current state and risks
- Leadership is engaged and involved in risk decisions

MedSec

The Foundation for a Successful Program

- Articulate impacts of cybersecurity risks on your institution's mission, vision and values
- Focus on patient harm and impact to patient care workflow
- Put in place a clinically lead governance organization
- Integrate work into institutional processes
- Tailor your program to your risk appetite, available resources and inherent institutional risk
- Inventory of devices with estimation of risk based on technical vulnerabilities and patient care impacts
- Show your work… (metrics, dashboards, presentations, etc.)



MedSec

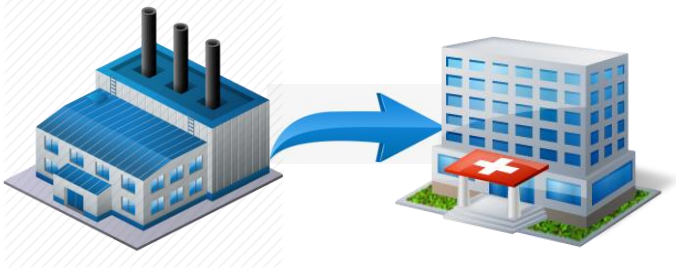
Changing the Hospital & Medical Device Industry

- Include security requirements in your contracts
- Drive cybersecurity product updates with the vendors
- Push current vendors to:
  - Partner for clinical and use case input
  - Fix/mitigate egregious issues
  - Implement internal security programs
  - Form client security advisory groups

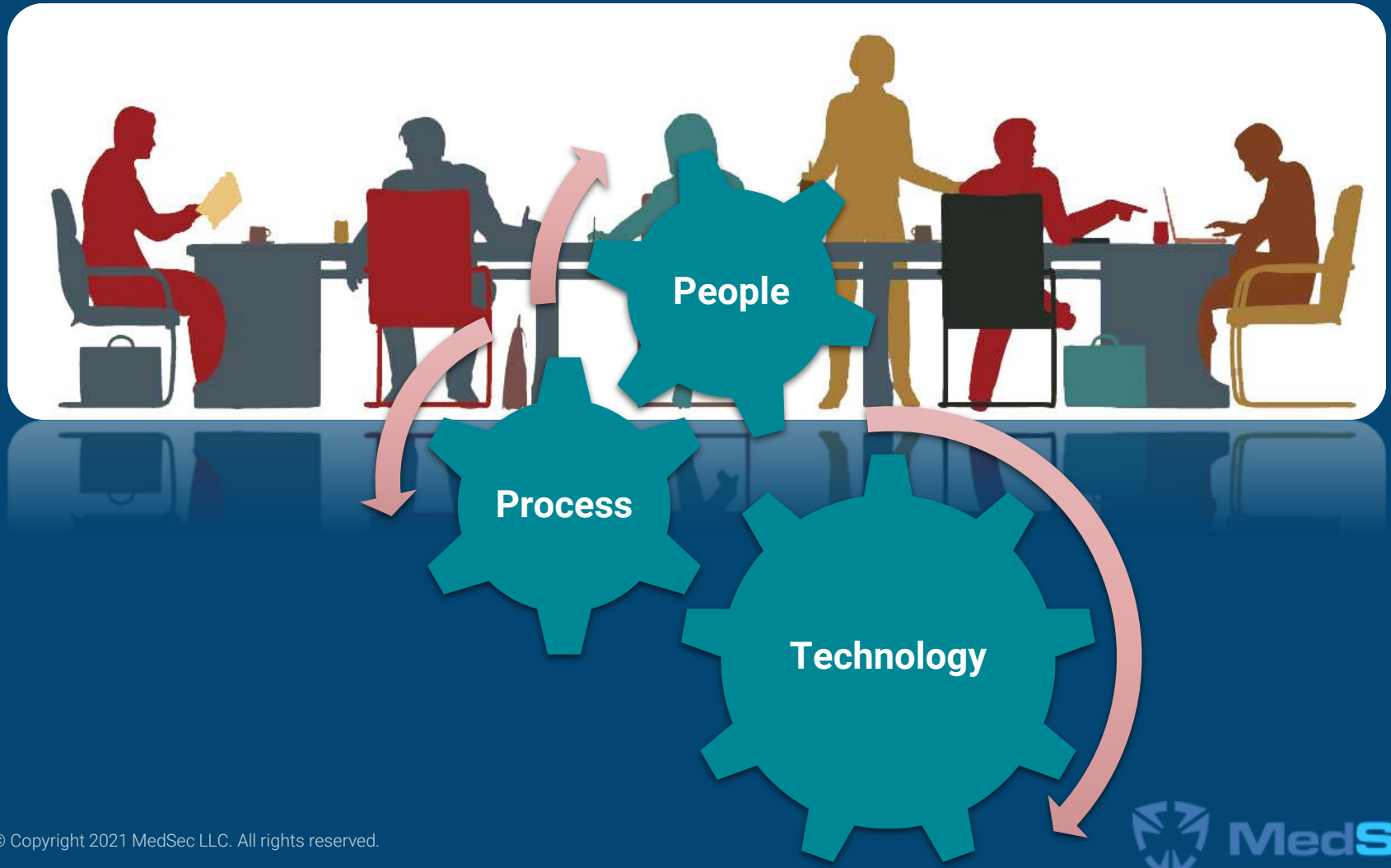
Focus with vendors on:

- ***"If you want to sell to us, you must meet our standards"***
- ***"It is just the right thing to do"***
- ***"You an be a market differentiator"***
- ***"There will be a business impact if no action is taken after being warned and your device is compromised"***

- Participate in industry groups such as H-ISAC, Archimedes, HIMSS, etc.
- Provide experienced input for development of industry standards
- Share assistance, site visits and materials with other HDOs



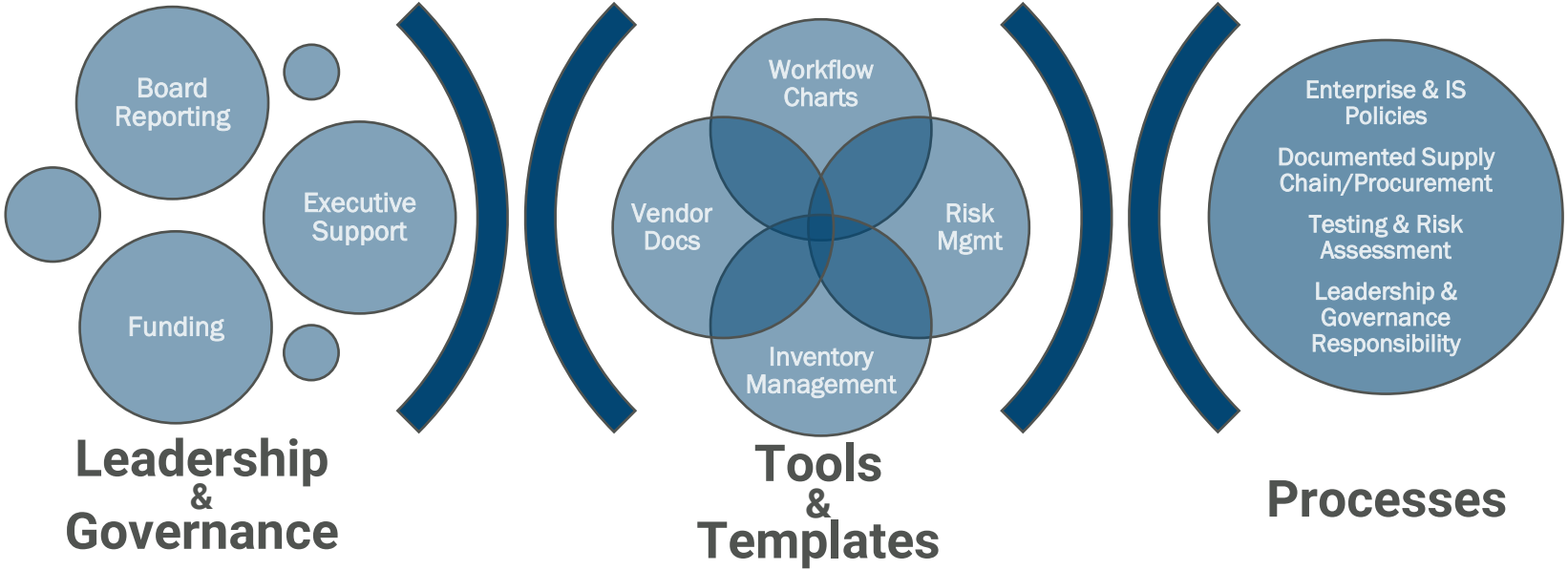
MedSec



MedSec

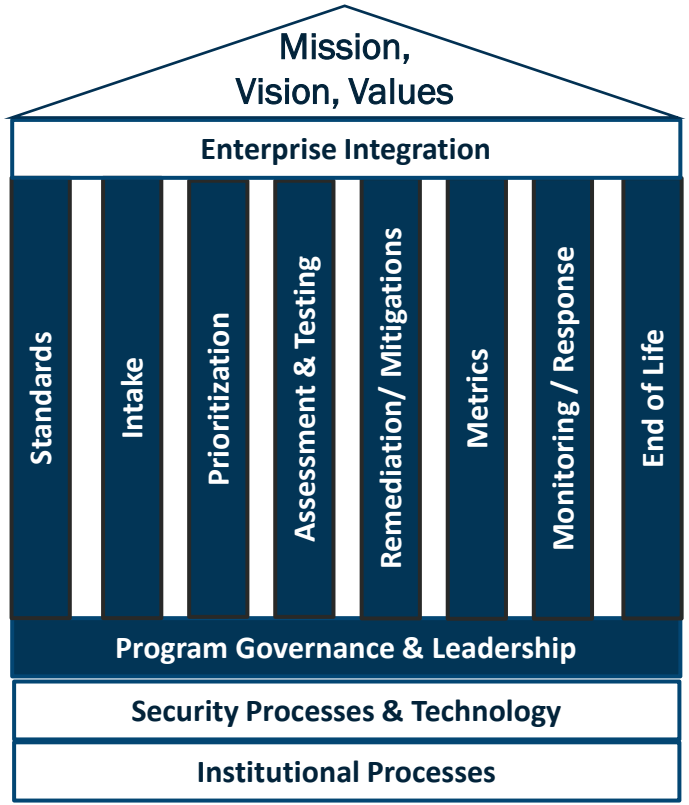
The Approach

To efficiently & effectively execute a program, you must develop and document a systematic, repeatable program and processes



MedSec

Your Program Needs “A Book” & Repeatable Processes



Example* Documents included in the ”Book” :

- ❑ Leadership & Governance responsibility
  - ✓ Governance reporting structure
  - ✓ Group charge
  - ✓ Members involved
  - ✓ Escalation/“break the glass”/exception criteria
- ❑ Documented supply chain/procurement processes
- ❑ Enterprise & IS policies/procedures
- ❑ Vendor data collection elements

Example* Templates” included in the “Book”:

- ❑ Workflow flow charts
- ❑ Email communication templates
- ❑ Medical device cybersecurity contract language &addendums
- ❑ Vendor data collection forms
- ❑ Risk matrix

*Note: These represent some of the tools that fall under the first two “Pillars” (Standards & Intake)

MedSec

MedSec Areas of Proficiency that can be Leveraged

- Maturity assessment
- Guidance for engaging executive support and governance
- Predefined “Book” of templates, contract language, risk formulas, processes, etc.
- Guidance on ”Best Practices”– from design to maturity
- Budget, planning and peer reviews
- Technology Integration
- Workshops
- Monitoring Trends in Medical Device Security
- *Emotional support when things aren’t going well…*

MedSec

MedSec

Questions?

Kevin McDonald

KevinMcDonald@MedSec.com

www.MedSec.com