Qualified DATA SYSTEMS

Medical Device Cybersecurity – ***A Marriage of Safety and Security***

121st AFDO Annual Education Conference
Medical Devices Track
June 20th, 2017
By: Armin Torres, Principal Consultant

Cyber Security Overview

Cybersecurity – is the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.

Requires Medical Device Manufacturers to consider appropriate Information Security Controls for:

- Physical and Logical Access
- Data and Record Controls
- Secure Communications
- **Protection for Essential Clinical Performance**

Medical Device Cybersecurity

- Device Cybersecurity is a Life Cycle process which starts with initial design and ends with decommissioning and disposal of devices.
- **Key QMS areas impacted include Design Controls, Production & Process Controls, and Supply Chain elements.**
- Robust Security is not something that can be bolted on but must be designed into medical products from inception
- Cybersecurity Risks are different than Patient Safety Risks but some Cyber risks may impact patient safety
- Threats and Vulnerabilities for Cyber Risk much broader in scope than typical Safety Hazard, Harm, and device failure mode assessment processes.
- Impacts to Business environment substantial including potential for:
  - Degradation or Disruption of Customer Business
  - Increase costs due to breaches and non-compliance to regulatory requirements
  - Brand Recognition

The New Cyber Attack Landscape

Medical Data and the Cyber Physical Ecosystem

Implantable Medical Devices

Robotic Surgery

Sensor & Monitoring System

Personal Health Devices

Wearables

Telemedicine

Cloud Computing

Body Area Networks

Health Social Networks

Digital “Smart” devices

Connected Health and Mobile

EHR Ecosystems

Medical Devices

US FDA definition of Medical Devices: An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animal, …

Medical Devices – Can be Software only product, Hardware based, SW/HW combination, or a Medical Device Data System.

- Scope includes devices which are networked and standalone which include software
- Software can be Firmware, Applications, Algorithms, Mobile APPs, and/or Machine code

Medical Devices

- Increasingly rely upon computers, software, and networking (Health TECH)
- Often incorporate third-party components
- Are subject to regulation, which can impact patching and re-configuration
- Traditionally focused on Product performance and Safety not Security
- Are often developed without secure development techniques
- Manufactured with minimal product security controls

Qualified DATA SYSTEMS

Medical Devices and the IOT

Medical Devices are increasingly part of our connected world:

- Embedded systems
- Wireless Sensors
- Decision Support Software
- Therapy Delivery Systems
- Diagnostic Devices
- Cloud Computing Infrastructure
- Remote Patient Monitoring
- Cyber-Physical Systems
- Mobile Medical Apps
- Image Management Systems
- Connected autonomous systems
- Interoperable Devices

The Internet of things is changing the world quickly:

Changing Ecosystem:

- Lower costs and improve efficiency
- Aging Population
- Government stimulated digitization (HITECH)
- Oversight and legal (HIPAA)
- Back-end systems in cloud (EHR, PACS)
- Care models (home-based, mHealth)
- Design complexity vs. skillset

Changing Threat Landscape:

- Targeted and sophisticated attacks
- Motivations and threat agent skillsets
- Single-point -> systems-of-systems
- Applications and data migrating to cloud
- Fragmented and distributed information

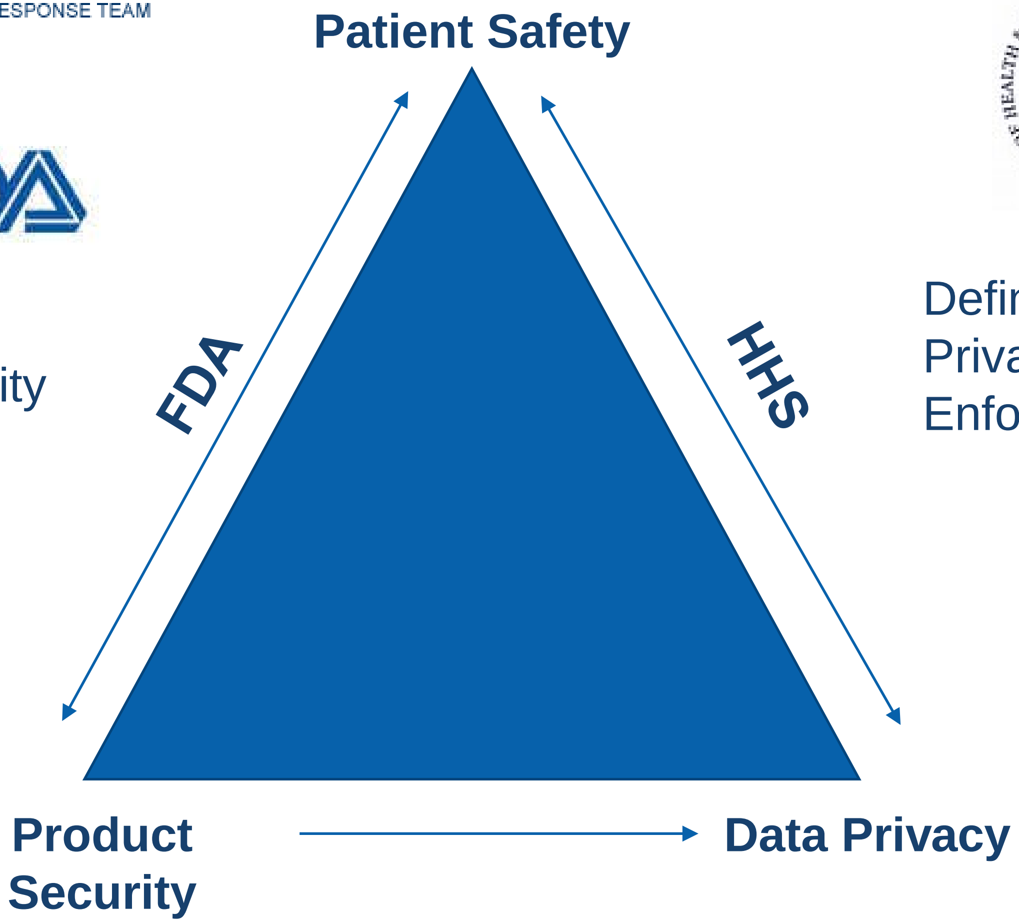
Cornerstones of Cyber Risk

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

FDA

Guidance from FDA, NIST, and Department of Homeland Security

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Defined by HIPAA Security and Privacy Rules.
Enforcement via Office of Civil Rights

Example Threats & Vulnerabilities

- Device Defects (SW/FW)
- Unauthorized access & exposure
- Physical tampering
- Unauthorized modifications or manipulations (e.g., devices, settings, data, event triggers)
- Eavesdropping
- Denial-of-service
- Intentional Malware exploitation
- Operational gaps (human error, lack of incident response, contingency planning)
- After sales value-added services

- Ubiquitous and pervasive connectivity
- Legacy systems
- Use of Obsolete technology
- Weak or missing security controls
- Inability to patch or retrofit security
- Exposed (Unencrypted) data
- Remote Access
- Lack of environmental awareness and anomaly detection
- Lack of full life-cycle assurance practices
- Uncontrolled servicing
- Misconfigurations & Installation defects

Medical Device Security

Life Enhancing to Life Threatening….

Evolving Industry Trends

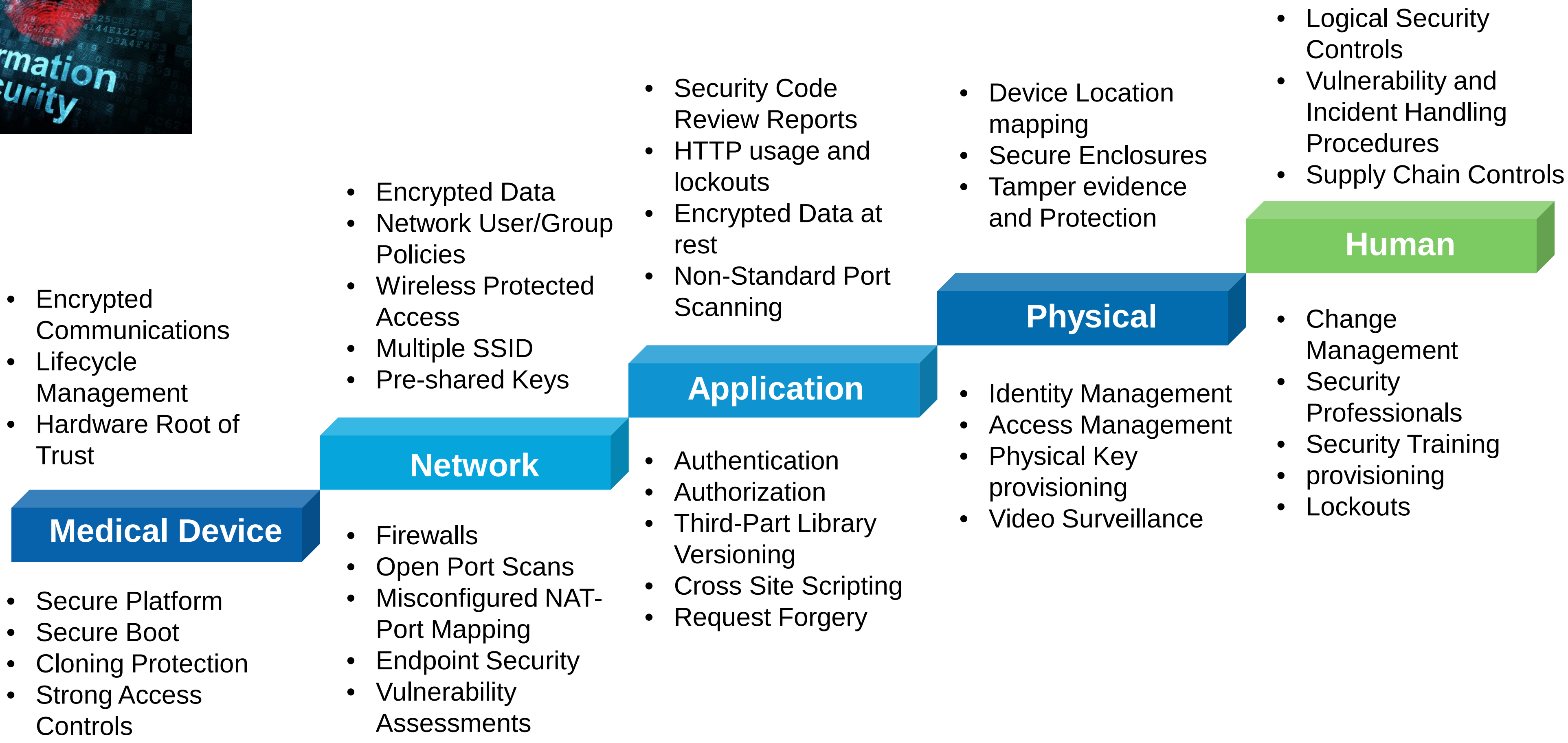
- Less reliance on human decision-making
- More reliance on computational intelligence, analytics, prognosis predictions, and automation
- Demands for greater environmental awareness and automated response & recovery

What do you think?

Evolving Device Trends

- Connectivity driven by IOT and demonstration of meaningful use for Health IT
- More Software only devices
- Expansion of Services
- Remote Control highly desired
- Cloud Integration everywhere
- Increased Interoperability (MTM)
- Global Supply Chains for cost optimization

IOT Security Landscape



Medical Device

- Encrypted Communications
- Lifecycle Management
- Hardware Root of Trust

- Secure Platform
- Secure Boot
- Cloning Protection
- Strong Access Controls

Network

- Encrypted Data
- Network User/Group Policies
- Wireless Protected Access
- Multiple SSID
- Pre-shared Keys

- Firewalls
- Open Port Scans
- Misconfigured NAT-Port Mapping
- Endpoint Security
- Vulnerability Assessments

Application

- Security Code Review Reports
- HTTP usage and lockouts
- Encrypted Data at rest
- Non-Standard Port Scanning

- Authentication
- Authorization
- Third-Part Library Versioning
- Cross Site Scripting
- Request Forgery

Physical

- Device Location mapping
- Secure Enclosures
- Tamper evidence and Protection

- Identity Management
- Access Management
- Physical Key provisioning
- Video Surveillance

Human

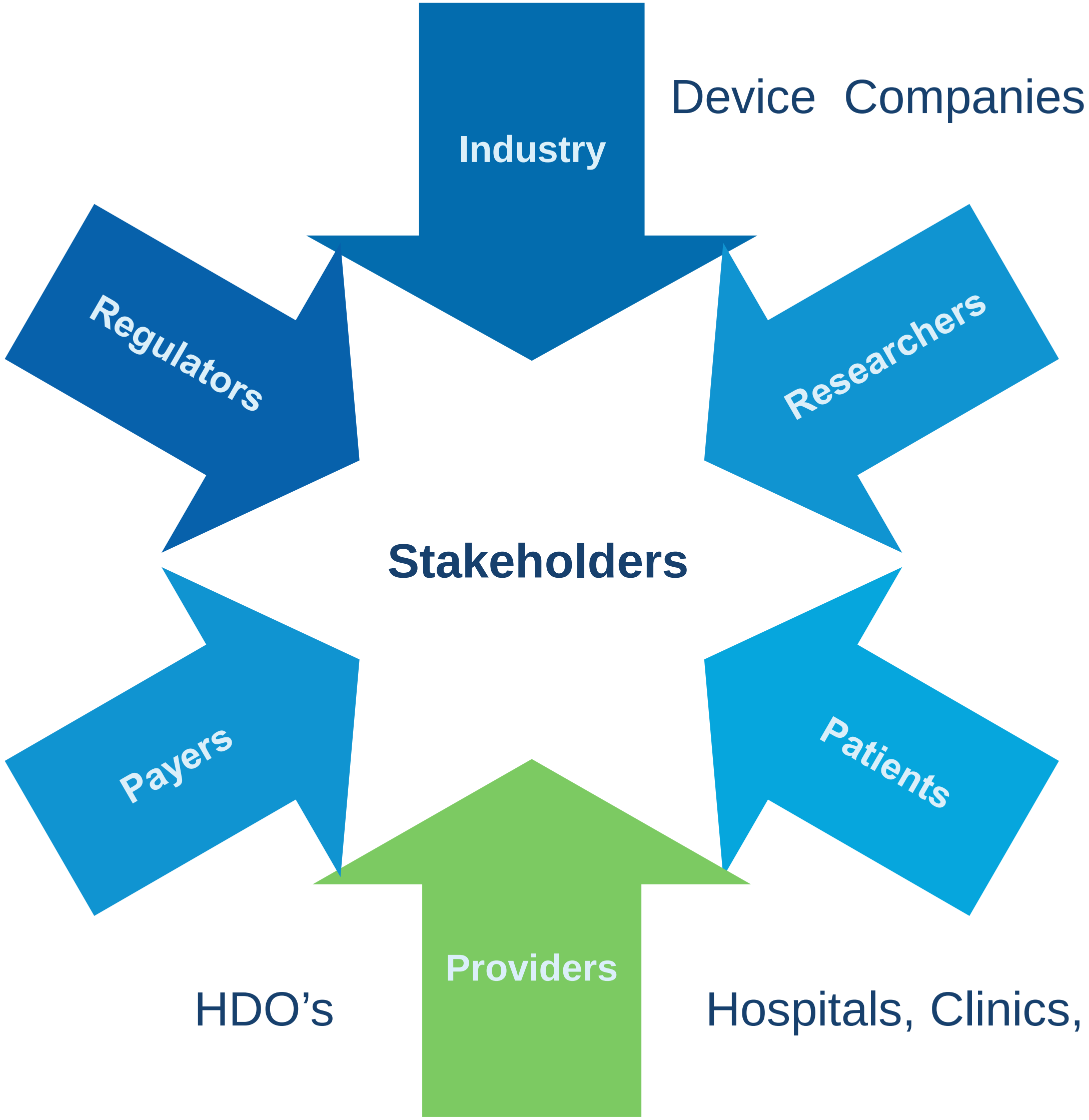
- Logical Security Controls
- Vulnerability and Incident Handling Procedures
- Supply Chain Controls

- Change Management
- Security Professionals
- Security Training
- provisioning
- Lockouts

Medical Device Ecosystem

Eco System:

- Complex
- Rapidly Evolving
- Collaboration is Key
- Security is Personal
- Shared Responsibility



Device Companies (MDM)

FDA
HHS

Academic, Independent,
and Consultants

Insurance Companies

HDO’s

Hospitals, Clinics, Diagnostic Centers, etc.

Qualified DATA SYSTEMS

HDO Perspective

- Highly diverse: “If you’ve seen one hospital, you’ve seen one hospital”
- No standardization across HDOs
- On the front lines to ensure patient safety, and ultimately responsible
- Medical device security is important, but one of many problems
- Management of medical devices different than IT devices (i.e. Biomed Eng. vs Enterprise IT)
- Boards, C-suite, and doctors do not consider security a priority
- Difficult to convince manufacturers to fix discovered issues in existing products
- Uncoordinated vulnerability disclosures are disruptive
- Vague and unclear Disclosure Reporting from MDM’s
- Limited resources to validate security controls from MDM products, especially proprietary features
- Improvements often one User Facility at a time.

Source: The MITRE Corporation

MDM Perspective

- Manufacturers Driven by:
  - Speed to Market
  - Cost
  - Regulatory Emphasis on Safety and Privacy
- Manufacturers do not have sufficient knowledge of contested hospital environments
- HDOs do not provide security requirements in a consistent way
- Manufacturers view cybersecurity vulnerability researchers as disruptive
- Manufacturer size is a factor:
  - Smaller manufacturers can be more agile but have fewer resources to apply to security
  - Larger manufacturers have adopted better practices but struggle with larger code bases

Source: The MITRE Corporation

Researcher Perspective

- Cybersecurity researchers may include individuals, patients, and consultants
- Varying motivations and experience levels
- Not understood by MDMs
- Many vendors are unprepared to receive vulnerability reports
- Lack of awareness about the clinical environment
- Often new to operating within a regulatory environment
- Find it difficult and/or expensive to gain access to devices
- Are typically not TRUSTED by MDM and/or HDOs

Source: The MITRE Corporation

Stakeholder Common Ground

- Patient safety is the highest priority
- Lack of trust across stakeholders
- NDAs between stakeholders reduces information sharing across the community:
    - HDOs can’t share internal evaluations with other HDOs
    - Researchers can’t share information learned when under contract with an HDO/MDM
- Lack of tools to assess clinical impact and risk of vulnerabilities
- Fear that real change might not occur until there is reported patient deaths or injuries

Source: The MITRE Corporation

Cross Stakeholder Challenges

- Lack of alignment of goals between stakeholders
- Limited information sharing of threats, vulnerabilities, and best practices
- Lack of cybersecurity baselines for medical device classes
- Need cybersecurity solutions for large and small organizations
- Lack of clear association of technical impact of cybersecurity vulnerabilities to patient safety
- Lack of cybersecurity testing/certification of medical devices
- Lack of a systems engineering view across the lifecycle
- Need to develop incentives and business cases

Source: The MITRE Corporation

Cybersecurity Timeline

- **1996:** HIPAA….2009 HITECH Act – Both emphasize Security and Privacy of Data
- **August 4, 2011:** Jerome Radcliff hacks his own insulin pump at Black Hat Security Conference in Las Vegas
- **August 23, 2011:** Legislators launch congressional inquiry into medical device security and safety
- **September 27, 2012:** GAO recommends FDA develop a plan to address security
- **February 12, 2013:** Executive Order 13636 is issued by President Obama mandating improved Cyber Security through implementation of risk-based standards and security frameworks
- **October 2, 2014:** FDA releases Final guidance for "Content of Pre-Market Submissions for Management of Cyber Security in Medical Devices"
- **January 22, 2016:** FDA releases draft guidance for "Post-market Management of Cyber Security in Medical Devices"
- **December 28, 2016:** FDA releases Final guidance for "Post-market Management of Cyber Security in Medical Devices"
- **May 11, 2017:** Executive Order is issued by President Donald Trump mandating review of federal systems and critical national infrastructure to strengthen cybersecurity efforts.

FDA Pre-Market Cyber Security Guidance

- Draft Guidance June 2013
- Final Guidance October 2014
- Key Principals:
  - Shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices
  - Address cybersecurity during the design and development of the medical device
  - Establish design inputs for device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g)

FDA Pre-Market Submission Requirements

Manufacturers should address cybersecurity during the design and development of the medical device, as this can result in more robust and efficient mitigation of patient risks.

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Assessment of residual risk and risk acceptance criteria.

FDA Pre-Market Submission Documentation

In the premarket submission, manufacturers should provide the following information related to the cybersecurity of their medical device:

- **Hazard analysis**, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with your device, including:
  - A specific list of all cybersecurity risks that were considered in the design of your device;
  - A specific list and justification for all cybersecurity controls that were established for your device.
- A **traceability matrix** that links your actual cybersecurity controls to the cybersecurity risks that were considered;
- A summary describing the **plan for providing validated software updates** and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness. The FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity.
- A **summary describing controls** that are in place to assure that the medical device software will maintain its integrity (e.g. remain free of malware) from the point of origin to the point at which that device leaves the control of the manufacturer; and
- **Device instructions for use** and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g. anti-virus software, use of firewall).

FDA Post-Market Cyber Security Guidance

- Collaborative approach to information sharing and risk assessment
- Articulate manufacturer responsibilities by leveraging existing Quality System Regulation and post-market authorities
- Align with Presidential EOs and NIST Framework
- Incentivize the “right” behavior
- Risk-based approach to assuring risks to public health are addressed in a timely fashion

Post-Market Risk Management

Guidance follows NIST Cybersecurity Framework’s 5 core functions:

- Identify
- Protect and Detect
  - Vulnerability assessment and risk analysis
- Respond and Recover
  - Compensating controls, risk mitigation and remediation

FDA Post-Market Guidance

Cybersecurity risk management programs should include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation

Information Sharing and Analysis Organizations (ISAO)

The ISAO best practice models are intended to be:

- Inclusive - groups from any and all sectors, both non-profit and for-profit, expert or novice, should be able to participate in an ISAO;
- Actionable - groups will receive useful and practical cybersecurity risk, threat indicator, and incident information via automated, real-time mechanisms if they choose to participate in an ISAO;
- Transparent - groups interested in an ISAO model will have adequate understanding of how that model operates and if it meets their needs; and
- Trusted - participants in an ISAO can request that their information be treated as Protected Critical Infrastructure Information. Such information is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is exempt from regulatory use and civil litigation.
- FDA recommends NH-ISAC (ISAO) http://www.nhisac.org/

Device Manufacturer Program Elements

Design & Development Activities:

- Integration of Product Security into SDLC
- Enhance Software Development Planning with Product Security Requirements
- Augment existing Safety Risk Management Program with Product Security
- Upgrade existing V&V activities with Product Security Testing
- Develop security operations and maintenance plans (i.e. patches, upgrades)

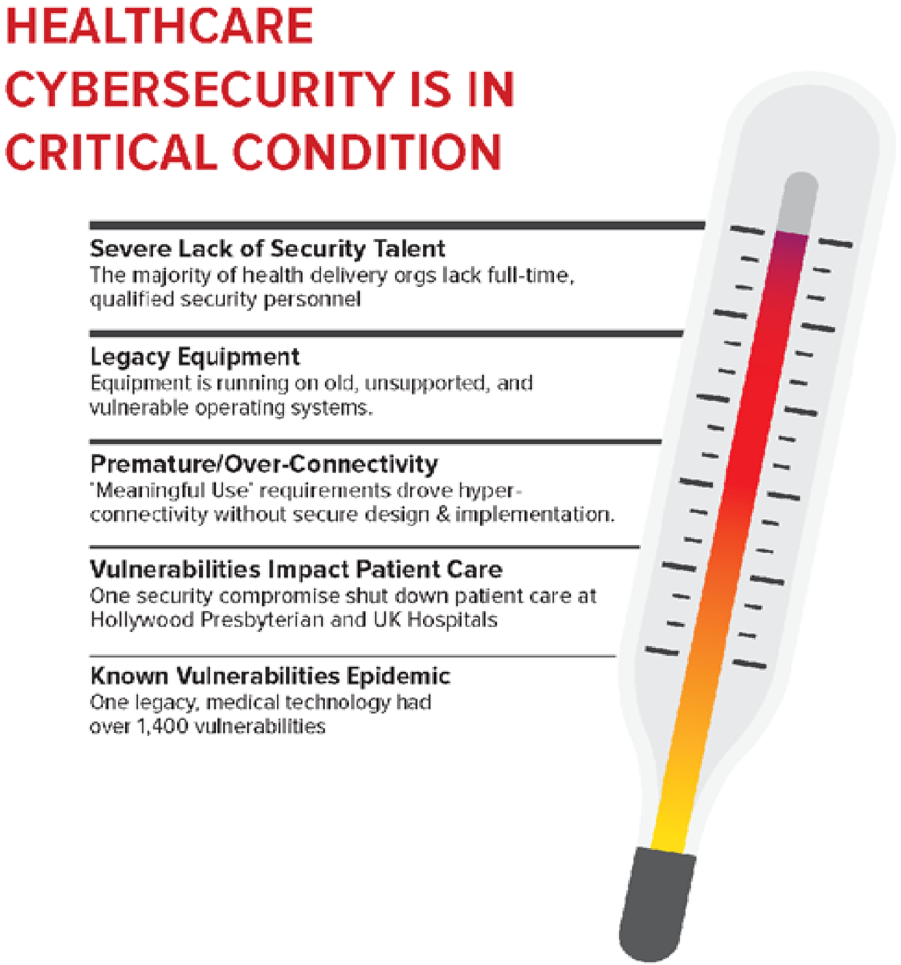
Production & Process Controls:

- Incorporate Secure Manufacturing Techniques

Supply Chain:

- Address Procurement and Supplier Controls
- Develop Incident and Vulnerability Handling Procedures including coordinated disclosure

State of the Industry



HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

- Education & Training on Product Security still lacking
- Industry has not addressed Legacy Systems
- Cyber Risk Management activities not managed using a Life Cycle approach
- Lack of resources to address vulnerabilities and risks
- Most Medical Devices Manufacturers have just begun to address product security

Source: **REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY**
Healthcare Industry Cybersecurity Task Force June 2, 2017

Existing Challenges

- Both device makers and users have little confidence that patients and clinicians are protected
- Medical devices are very difficult to secure
- In many cases, budget increases to improve the security of medical devices would occur only after a serious hacking incident occurred
- Medical device security practices in place are not the most effective
- Medical devices contain vulnerable code because of a lack of quality assurance and testing procedures as well as the rush to release
- Testing of medical devices rarely occurs
- Accountability for the security of medical devices manufactured or used is lacking
- Manufacturers and users of medical devices are not in alignment about current risks to medical devices
- Most device makers and users do not disclose privacy and security risks of their medical devices

Source: Ponemon Institute, May 2017 Research Report

Recommendations

- Continue to Educate and Train Stakeholders!
- Adopt a unified Cybersecurity Management Framework specific to Healthcare. Use NIST Cybersecurity and HIPAA Security Rules as a starting point for minimum requirements.
- Focus Cybersecurity activities using a Life Cycle approach with keen attention to Design Controls implementation for new products.
- Verification needs to be commensurate with Cyber Risk profiles for devices. Product Security needs to be engrained into the V&V process.
- Simulate Product Security incidents, exploitation, and response in order to be prepared. Integrate Cybersecurity into Disaster and/or Business Continuity Planning efforts.
- Establish a strategy for dealing with legacy devices
- Participate in Information Sharing via ISAO’s. For Healthcare this is NH-ISAC.