

HIMSS[®]19

CHAMPIONS OF HEALTH UNITE

Global Conference & Exhibition
FEB 11-15, 2019 | ORLANDO



Mitigating the Next Generation of Risk - Connected Medical Devices

Session 72, February 12, 2019

Matt Broomhall, BDE & CTO, Healthcare Solutions North America, IBM TSS

Donald Kneitel, Global Healthcare BLE, IBM TSS

Conflict of Interest

Matt Broomhall, MSA, CPHIMS

Has no real or apparent conflicts of interest to report.

Donald Kneitel, MBA

Has no real or apparent conflicts of interest to report.

Agenda

- Issues & Challenges
 - What are the industry perspectives
 - How are we viewing it
 - What are the issues we're trying to address
- Solution approach
 - Discovery
 - Analysis
 - Remediation
 - Integration
 - Governance
- Call to action and next steps



Hackers managed to steal \$80m from Bangladesh's central bank because it skimmed on network hardware and security software, reports Reuters.

Hackers managed to steal \$80m (£56m) from Bangladesh's central bank because it skimmed on network hardware and security software, reports Reuters.

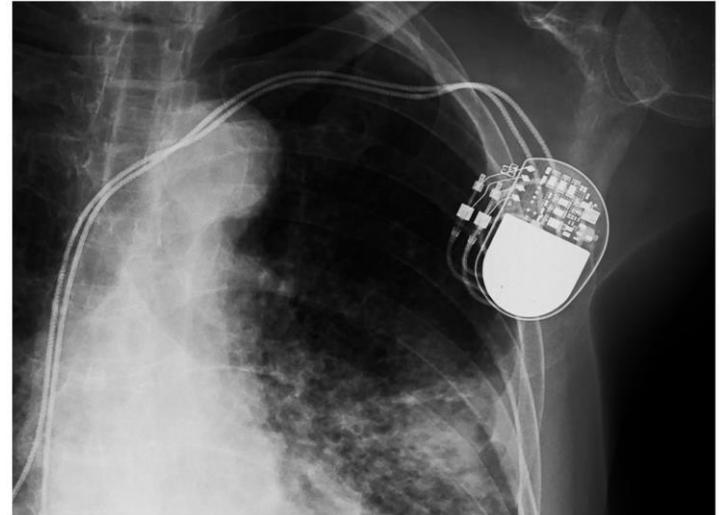
Learning Objectives

- **Contrast** practices in management of IT assets to that of connected medical devices
- **Identify** opportunities to improve the management and security of connected medical devices
- **Describe** a programmatic approach to managing the safety and security of connected medical devices
- **Describe** the benefits of an end to end approach of managing and securing IT assets in conjunction with connected medical devices



LILY HAY NEWMAN SECURITY 08.09.18 12:30 PM

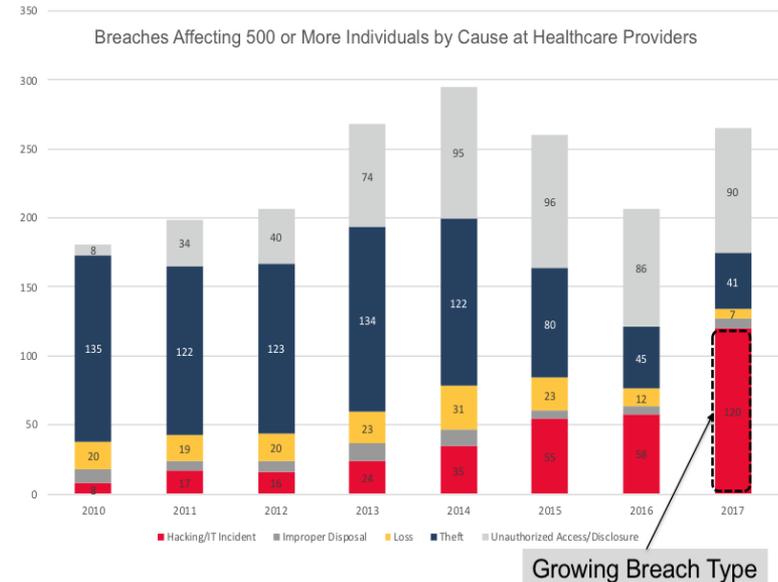
A NEW PACEMAKER HACK PUTS MALWARE DIRECTLY ON THE DEVICE



Supporting the embedded IT in Medical Devices (IoMT), and across all connected devices (IoT & IT) is a challenge

- Healthcare organizations typically have 300-400% more medical equipment than IT devices
- Only 51% of medical device manufacturers follow FDA guidance to mitigate risks
- As of January 2013, patient privacy noncompliance penalties total \$1.5 million annually for each violation category
- IoMT device hacking is the fastest growing breach type for connected medical devices and follows the trend of malicious IoT hacking
- Nearly 4 out of 10 medical devices are networked or networkable
- Many devices can be compromised by non-network connections – such as USB port

The healthcare industry is experiencing a decrease in theft, while hacking/IT incidents are increasing.



Source: U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal

The **growth** in medical devices is exponential with 10-15 device ratio per bed

Examples include:

- Defibrillators
- Patient beds
- EKG machines
- Ventilators
- Infusion pumps
- Vital sign monitoring systems
- CT scanners
- MRI
- Lab equipment - analyzers



The growth in medical devices has increased the **data** that can be compromised

Examples include:

- Drug types and dosages
- Patient information (PII)
- Control information for devices – anesthesia delivery
- Diagnostic images
- Lab results
- Vital signs of all types
- Continuous output from EKG and EEG and similar systems



Issues & Challenges



Hijacking software updates to infiltrate even the most well-guarded networks

- FDA Guidance

- Content of Premarket Submissions for Software Contained in Medical Devices
- Not covered
 - software designed for manufacturing not intended for use as a device.
- Guidance is based “Level of Concern”
 - related to potential harm to a patient
- FDA is modernizing this guidance

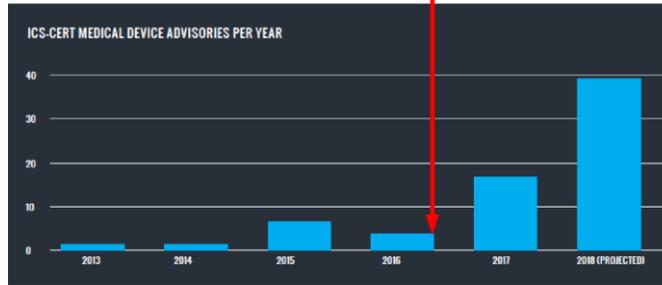
<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf>

<http://www.24x7mag.com/2018/09/fda-boost-medical-device-cybersecurity/>

<https://www.symantec.com/security-center/threat-report>



Issues & Challenges



Steady increase in discovered & disclosed vulnerabilities.

- FDA Guidance

- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software
- Includes recommendations for medical device manufacturers that incorporate off-the-shelf software and that can be intranet or internet connected
- The device manufacturer bear responsibility for the continued safe performance of the medical device
- FDA recommends users of medical devices potentially subject to vulnerability contact the OEM
- FDA recognizes medical device security is shared responsibility between stakeholders

<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf>

<https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf> 9

<https://www.medcrypt.co/medcrypt-vulnerability-analysis-whitepaper-1.pdf>



Issues & Challenges

- Cyberattacks on medical devices on the rise
 - FDA , leveraging ethical hackers to find vulnerabilities on machines that could put patients' lives at risk.
 - Manufacturers have pushed back with this
 - FDA embracing the “white hat” hacking community — and are stepping up efforts.



The Washington Post

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/10/17/the-cybersecurity-202-the-fda-is-embracing-ethical-hackers-in-its-push-to-secure-medical-devices/5bc6156b1b326b7c8a8d1a01/?noredirect=on&utm_term=.0e32b6b1ea77



Issues & Challenges

- HIPAA and Medical Device Security

- Device manufacturers historically have overlooked the possibility that their devices may be subject to compliance with the [Health Insurance Portability and Accountability Act \(HIPAA\)](#),
- Information is considered protected if it is individually identifiable, such as a name or date of birth that may identify the individual and it consists of data regarding that individual's health.

- Covered Entities and Business Associates

- Most information generated or transmitted by medical devices is protected health information.
- There are two types of “entities’ that are subject to compliance with [HIPAA](#):
 - Covered entities - healthcare providers, clearinghouses, or insurers
 - Business Associates - a third-party that receives, transmits, maintains, or creates protected health information on behalf of a covered entity.

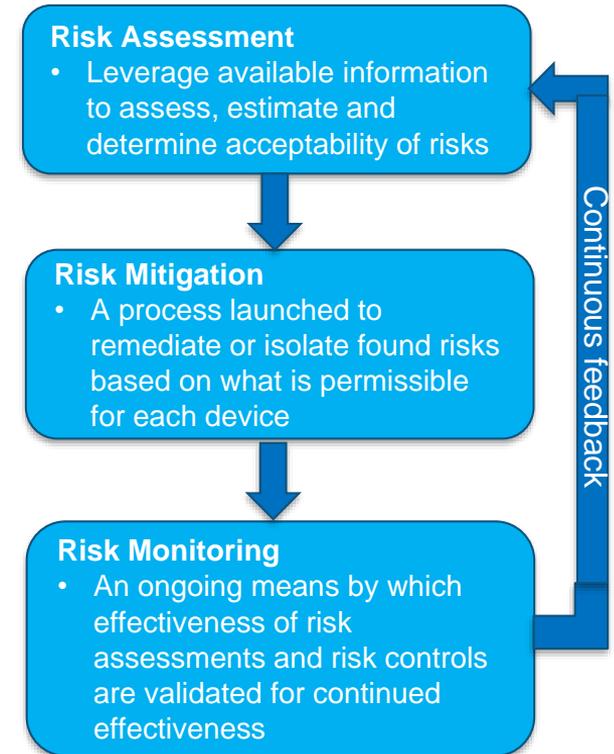


The law has emerged into greater prominence in recent years with the proliferation of health [data breaches](#) caused by cyberattacks and [ransomware](#) attacks on health insurers and providers.

Under the HIPAA Privacy Rule, falling victim to a healthcare data breach, as well as failing to give patients access to their PHI, could result in a fine

Issues & Challenges

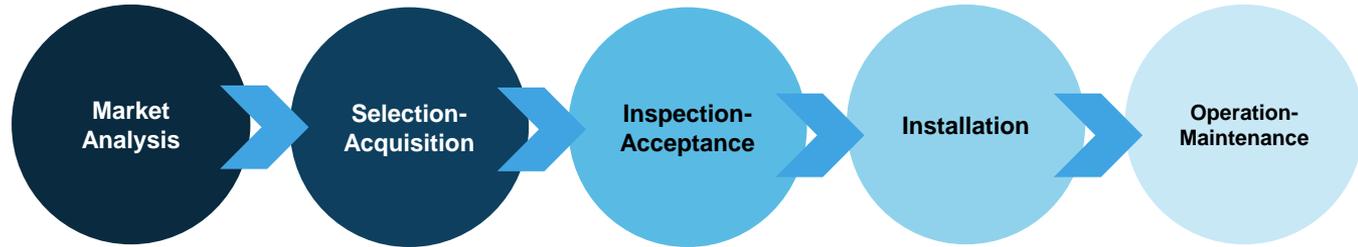
- “Medical device users should also conduct frequent risk assessments of all their internet-connected devices” Richard Staynings, Chief Security and Trust Officer at Nashville, Tenn.-based Clearwater Compliance, told Bloomberg Law.
 - Medical devices take about five or six years to go through testing and clinical trials before they receive FDA approval
 - New devices arriving in hospitals today were designed using technology that may already be out of date, Staynings indicated.
 - “Anyone connecting their 2012 Windows computer to the internet without any security software or updates would more than likely be compromised inside 10 minutes, yet that’s what we do with medical devices,” Staynings also said in the same interview.



Bloomberg Law <https://www.bna.com/device-makers-combating-n73014482033/>
<http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=6489>

Issues & Challenges

Asset Management



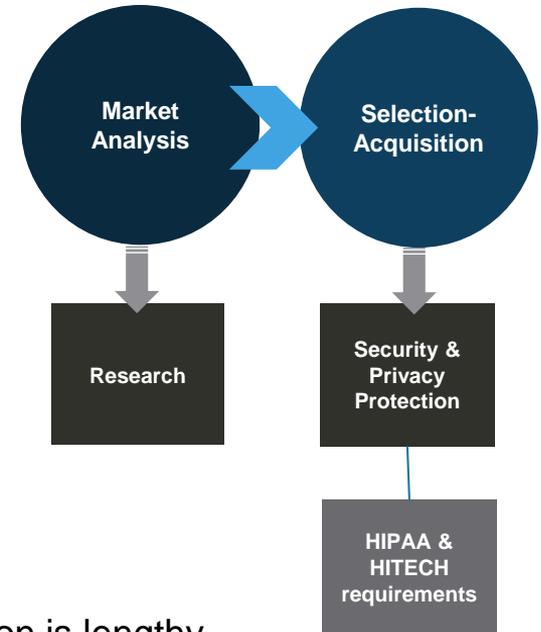
1. Continuous security monitoring to ensure the medical device is up-to-date with patches and updates
2. Good rapport with the manufacturer for patch-management process
3. Decide on an automated patch-management process or manual process, and implement
4. Apply the patch or update, then test for functionality and safety

**It should be noted that under the HIPAA Omnibus Rule, device manufacturers or servicers may now be considered as business associates of the health care organizations, which makes them responsible for the patch management.

Issues & Challenges

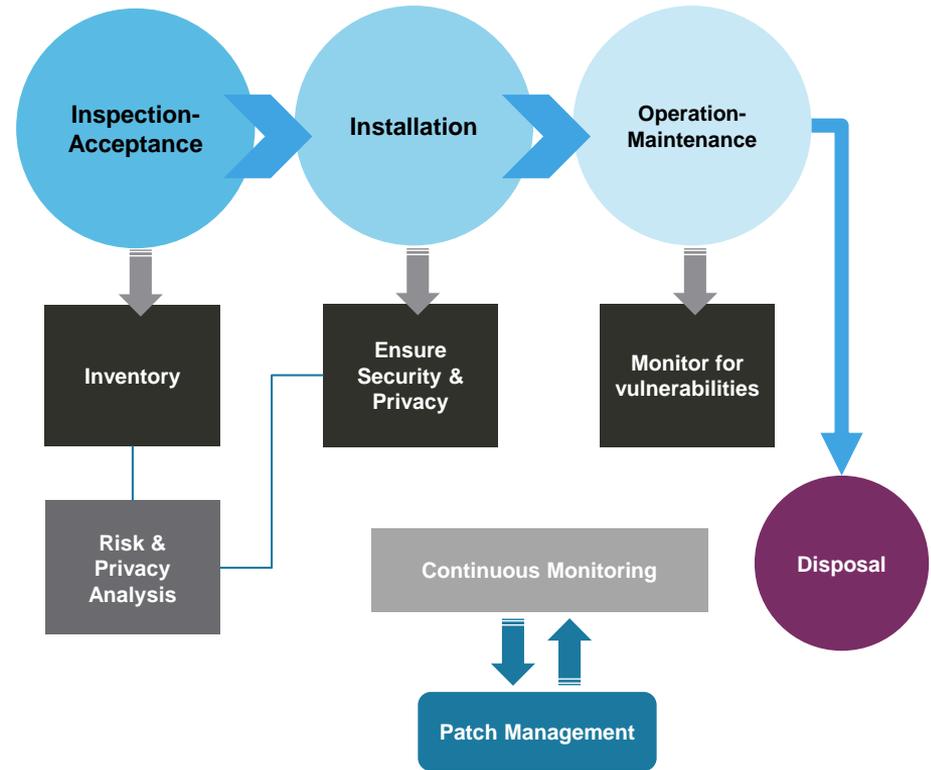
- Internet of Medical Device Lifecycle

- Product Design
- Product Test
 - Functionality and FDA certification prep
- FDA Certification
- Market Entry
- Product Purchase
 - The time span from design to FDA certification is lengthy
 - By the time device enters clinical use, multiple threat vectors may exist with device



Issues & Challenges

- Internet of Medical Device Lifecycle
 - Clinical Use – device active in continuum of patient care
 - Integration into clinical environment:
 - Network, HIT Systems, EHR, PAC, CMMS, governance
 - Maintenance/Repair
 - Patient safety
 - Cyber threat protection
 - Patient care and safety
 - End of Life
 - Removal from service



Issues & Challenges

Risks

- Patient Safety
- Data breaches
- Revenue impact

Vulnerability

- Poorly protected
- No alerting or detection
- Long useful product life
- Network connected

Threats

- Theft
- Compliance violations
- Collateral damage

Considerations for Medical Device Security



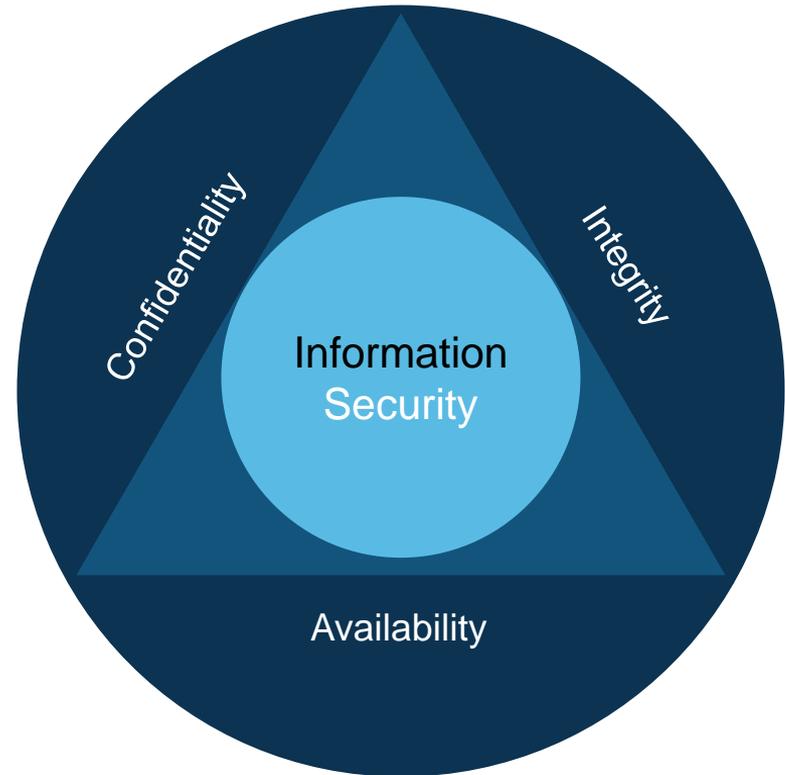
Risk Management and Patient Safety

CIA – Cybersecurity

- Confidentiality
- Integrity
- Availability

Information Security

Risk Management



Issues & Challenges

Confidentiality

- Theft of patient information results in HIPAA violations and liability for HDO

Integrity of data resources

- Compromise of data used to make clinical and treatment decisions impacts patient care and patient safety

Availability

- Systems that are unavailable can compromise patient care and safety

Considerations for Patient Safety



Issues & Challenges

- Sampling of Security Vulnerabilities
 - Employee understanding of cybersecurity
 - Patches not applied as required
 - Lack of encryption
 - Connectivity to internet or intranet
 - Weak or no authentication
 - Admin privileges not contained to clinical engineering
 - Open ports
 - Communications not secured or monitored
 - Devices used past reasonable EOL



Discovery

- What and where to focus
- OEM data available
- Published Vulnerabilities & Scans
- Tooling to discover network connected medical devices, IT, IoT
- Physical collection of additional medical device attributes
- Network Visibility & Optimization

Analysis

- Comprehensive medical device risk analysis, and Security gaps
- Security Frameworks
- Operational Governance as applicable to assessment
- Compensating controls (e.g firewalls, IDS/IPS, micro-segmentation)

Remediation

- Medical Device Risk by CIA (Confidentiality, Integrity, Availability)
- Security Risk Planning & Mitigation
- Reporting & Communication
- Patient care & Utilization review
- Remediation activities
 - Patching, Testing, Compensating Controls, Policies, Technical

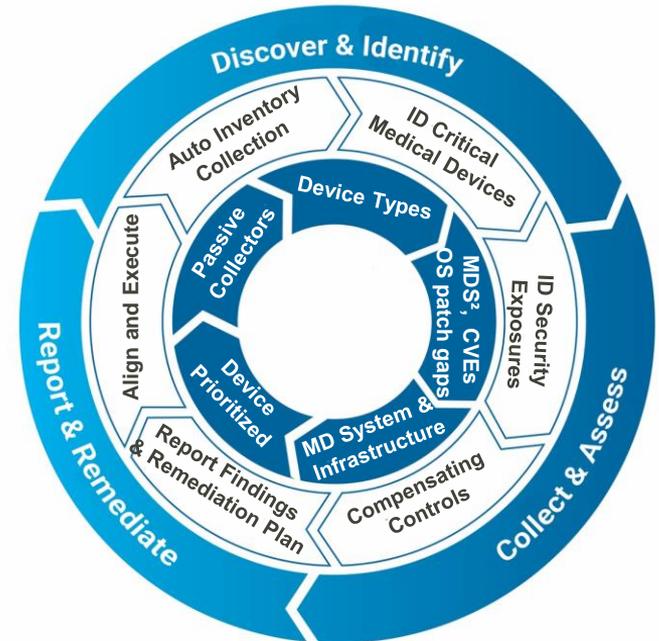
Integration

- Integration to Security – SIEM, Logs
- Integration to CMMS, Service Mgmt
- Network Integration – Network Segmentation
- IDPS and Firewall integration
- Process, Technical, control integration

Governance

- Management of lifecycle processes and on going remediation
- SPOC in place to help manage real time breaches / exploits
- Linkage to TPM's and IT capabilities to improve process flows
- Integration with mgmt. approaches

By focusing on a lifecycle set of activities we can define a Holistic & Proactive IoMT & IoT Management Approach



No one tool does it all, but by integrating capabilities the organization can have a broad understanding of all connected devices

Discovering and maintaining accurate and up to date inventory of the IoMT, IoT, IT devices is the first step – there are several ways to execute this:

Approach	Execution	Pro's	Con's	Ongoing
Physical Inventory	By facility - selected sampling	Detailed data	Time consuming	Hard to maintain
Network Deep Packet Inspection	Several tools developed for IoMT	Automated fingerprint & network mapping, utilization	Can be expensive to deploy, have to touch all data flows	Real time capability, industry focus
CMMS & Service Management systems	Database of managed systems and ticketing	Can drive automated workflows	Automated feeds vary, may not be complete	Integrate with real time feed engine
Multiple related systems (security & Network)	Leverage SIEM, Scanners, Network Flow data	Full picture on several attributes	Several tools to integrate and refine	Important to have multiple capabilities
System Interrogation	Tools that do authenticated scan	Additional details, Utilization, AI, Predictive	Can't interrogate IoMT devices	Leverage for IT tools
RFID, Asset Tags	Tagging and tracking	Real time inventory and location data	Can be costly	Provides utilization/ location data
Blockchain	Distributed Ledger	Lifecycle history of device	Developing technology	Provides lifecycle record

Inventory & **Discovery** Planning – Before undertaking these projects we recommend the organization consider these key issues

Scope & Planning Questions	Recommended Initial approach	Approach/Comments
Number of locations & timing/dates to analyze/install	Would recommend one to three facilities	Best to start with a couple core facilities and refine, also need to be able to capture network traffic across appropriate span ports
Size and address of each location	Recommend one large and up to one or two medium/small	Large > 400 beds or 1500 employees per site, Med = 100 to 400 beds or 500 – 1500 employees, small < 100 beds or 500 employees
What devices to capture during Inventory & Discovery	Start with IoMT devices leveraging tooling, add IT and IoT devices	Need to understand if want to capture IT, IoT, IoMT devices and next steps with those devices
What network and utilization data is needed	Review tool data and determine how best to leverage	Do we need to map traffic and look at utilization or vulnerability data of devices
Network segmentation, taps, and installation of collectors	Try to place device in core span port to capture all traffic	Appliance, Cloud based, collectors required, PHI/data sensitivity, change management
Any Physical Inventory needed	May want to collect additional parameters by device type	Recommend doing a sampling of high risk devices working with Clinical Engineering or TPM
Desired Analysis and control mapping	Review control frameworks and dashboarding approach	Recommend focusing on IEC TR 80001-2-2 and one or two other inter related frameworks
Desired integration to other data	CMMS, Vulnerability scans, Network data	How best to integrate for holistic view



As the team conducts an automated inventory & **discovery** of the IoMT - Medical Devices, they need to determine what the tool can collect and what information needs to be collected by other means

INTEGRATED DISCOVERY & INVENTORY DATA COLLECTION

Basic device type Info*	Automated NW data collection**	Software Info***	Security Info***
<ul style="list-style-type: none"> • Serial Number • Manufacturer • Model • Category • Department • Location • If Network Capable • PHI/SEI Contained • Repair History 	<ul style="list-style-type: none"> • Host Name • VLAN • IP Address • MAC Address • Network Interfaces • Utilization of device • Device characteristics • CVE/Vulnerability rating • Wireless Security Protocol 	<ul style="list-style-type: none"> • Operating System • OS Version • Firmware or Application Software Version • OS Patch Level • Date of Last Update • Device Storage Capability • COTS Middleware • Application details & Dependencies 	<ul style="list-style-type: none"> • Authentication Controls • Credential Management • Anti-Malware or Other Security Technologies • Encryption • Event Alerts and Logging • Remote Access Management • I/O Port Management

* As available – typically from CMMS system

** Automated leveraging packet inspection tooling

*** Manual data collection typically on high risk device types





Performing a security **analysis** leveraging control frameworks – UCF, 80001, 800-53 (examples below) allows the organization to determine control and technical gaps

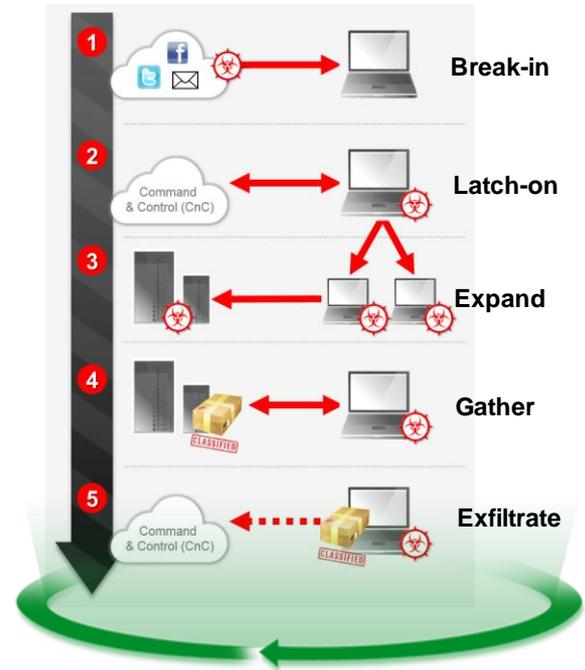
Common Control Title	Control ID	The International Organization for Standardization	IEC 60001-1	US Federal Government	NIST SP 800-53	HIPAA	Impact Zone	Control Requirement	Control Type	Control Classification
Establish and maintain a network configuration standard.	00530	1	§ 4.3.2	1			Technical security	mandated	Establish/Maintain Documentation	Preventive
Establish and maintain information flow procedures.	04542			1	App F §		Technical security	mandated	Establish/Maintain Documentation	Preventive
<i>Establish and maintain a network security policy.</i>	06440						Technical security	implied	Establish/Maintain Documentation	Preventive
Establish and maintain a wireless networking policy.	06732	1		1	App F §		Technical security	mandated	Establish/Maintain Documentation	Preventive
<i>Establish and maintain information exchange procedures.</i>	11782						Technical security	implied	Establish/Maintain Documentation	Preventive
Enable encryption of a protected distribution system if sending restricted data or restricted information.	01749			1	App F §		Technical security	mandated	Configuration	Preventive
Protect data from unauthorized disclosure while transmitting between separate parts of the system.	11859			1	App F §		Technical security	mandated	Data and Information Management	Preventive
Establish and maintain whitelists and blacklists of software.	11780			1	App F §		Technical security	mandated	Establish/Maintain Documentation	Preventive
<i>Manage all internal network connections.</i>	06329						Technical security	implied	Technical Security	Preventive
Plan for and approve all network changes.	00534	1	§ 4.5.2.3				Technical security	mandated	Technical Security	Preventive
Manage all external network connections.	11842	1		1	App F §		Technical security	mandated	Technical Security	Preventive

Security Control Information				Control Assessment Information							
NIST Security Control Number	Security Control Name	Priority / Baseline Allocation	Security Control and Enhancements	Security Control Type (verify this type)	Last Date Security Control Assessed	Assessor Information	Assessed Security Control Effectiveness (select one of the following)	Findings / Deficiencies Found	Scoping Guidance/ Risk -Based Decision Justification (must be completed if Assessed Security Control Effectiveness is Not Applicable or Risk-based decision not to implement)	NIST 800-53A Assessment Steps Used	Assessment Evidence
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	P1 MOD AT-1	Control: The organization: a. Develops documents and disseminates to [ASSIGNMENT: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose scope roles responsibilities management commitment coordination among organizational entities and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [ASSIGNMENT: organization-defined frequency]; and 2. Security awareness and training procedures [ASSIGNMENT: organization-defined frequency]	Common If additional system/application policy/procedures are in place this is a hybrid control.			Satisfied Partially satisfied Not satisfied Not applicable Risk-based decision not to implement			AT-1.1 Examine organizational records or documents to determine if security awareness and training policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated when organizational review indicates updates are required. AT-1.2 Examine the security awareness and training policy to determine if the policy adequately addresses purpose scope roles responsibilities management commitment coordination among organizational entities and compliance. AT-1.3 Examine the security awareness and training procedures to determine if the procedures are sufficient to address all areas identified in the security awareness and training policy and all associated security awareness and training controls. AT-1.4 Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness and training policy and procedures control is implemented.	

While designing key Network and Security technical controls and architectures that can limit the attack surface

Implementing security and network controls that can be placed throughout the attack chain.

- The network must be designed in a way which:
 1. **Limits the attack surface** in an attempt to prevent a compromise, or at least make it difficult.
 2. **Contains a compromise** and limits lateral movement in the environment.
 3. **Controls outbound connections** and provides visibility into possible Command and Control (C&C) channels and data exfiltration.
- Additionally organizations must build capabilities for rapid detection of, and rapid response to, suspicious activity so that the damage associated with a breach can be minimized.



Properly **analyzing** the appropriate approach to network segmentation for the organization

#	Approach	Examples	Typically managed by	Differentiators	Technical limitations or dependencies
1	Traditional network segmentation	Firewalls & NGFWs (routed and transparent modes), ACLs, VLANs, PVLANS	<ul style="list-style-type: none"> Network / firewall team 	<ul style="list-style-type: none"> Leverages existing technologies 	<ul style="list-style-type: none"> May require IP address changes Not scalable for extensive microsegmentation
2	Identity based segmentation	Cisco Firepower Identity Policy, Checkpoint Identity Awareness, Palo Alto User-ID	<ul style="list-style-type: none"> Network / firewall team 	<ul style="list-style-type: none"> Focuses on user access to resources rather than IP addresses 	<ul style="list-style-type: none"> Requires integration with identity sources May require endpoint agents
3	OS level and cryptographic “microsegmentation”	Illumio ASP, Certes Networks, Unisys Stealth	<ul style="list-style-type: none"> Information security team 	<ul style="list-style-type: none"> Coverage for all workload types (physical, virtual, cloud) May include good application flow visualization Process level and identity based granularity may be possible Use of IPSec to protect flows built in 	<ul style="list-style-type: none"> Coverage depends on operating system May require endpoint agents
4	Hypervisor based “microsegmentation”	VMWare NSX distributed firewall	<ul style="list-style-type: none"> OS / Virtualization team 	<ul style="list-style-type: none"> Hypervisor based – does not impact network or operating system Not constrained to network level constructs for firewall rules 	<ul style="list-style-type: none"> Virtual machine coverage only
5	Network based “microsegmentation”	Cisco TrustSec / ISE / ACI	<ul style="list-style-type: none"> Network team 	<ul style="list-style-type: none"> Coverage for all workloads Enforcement throughout the network infrastructure 	<ul style="list-style-type: none"> Dependent on networking hardware



MANAGEMENT OF PRIVATE DATA

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		Yes, No, N/A, or See Note	Note #
A	Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])?	Yes	—
B	Types of private data elements that can be maintained by the device :		
B.1	Demographic (e.g., name, address, location, unique identification number)?	Yes	—
B.2	Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	Yes	—
B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes	—
B.4	Open, unstructured text entered by device user/operator ?	Yes	—
B.5	Biometric data ?	Yes	—
B.6	Personal financial information?	No	—
C	Maintaining private data - Can the device :		
C.1	Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	—
C.2	Store private data persistently on local media?	Yes	—
C.3	Import/export private data with other systems?	Yes	—
C.4	Maintain private data during power service interruptions?	Yes	—
D	Mechanisms used for the transmitting, importing/exporting of private data – Can the device :		
D.1	Display private data (e.g., video display, etc.)?	Yes	—
D.2	Generate hardcopy reports or images containing private data ?	Yes	—
D.3	Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	Yes	Y
D.4	Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	Yes	Y
D.5	Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	Yes	Y
D.6	Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	No	Y
D.7	Import private data via scanning?	No	—
D.8	Other?	—	—

D4: : USB is active for clinicians to export clinical data to desktop for presentations. Scanner OS will boot, but the CT clinical scan applications will not.

Management of Private Data notes: D.5: The system can import/ export patient data from locally configured trusted DICOM network nodes. The system is disabled from general browsing the Internet.

D.6: Wireless networking is not implemented.

D.7: Document scanning is not implemented.

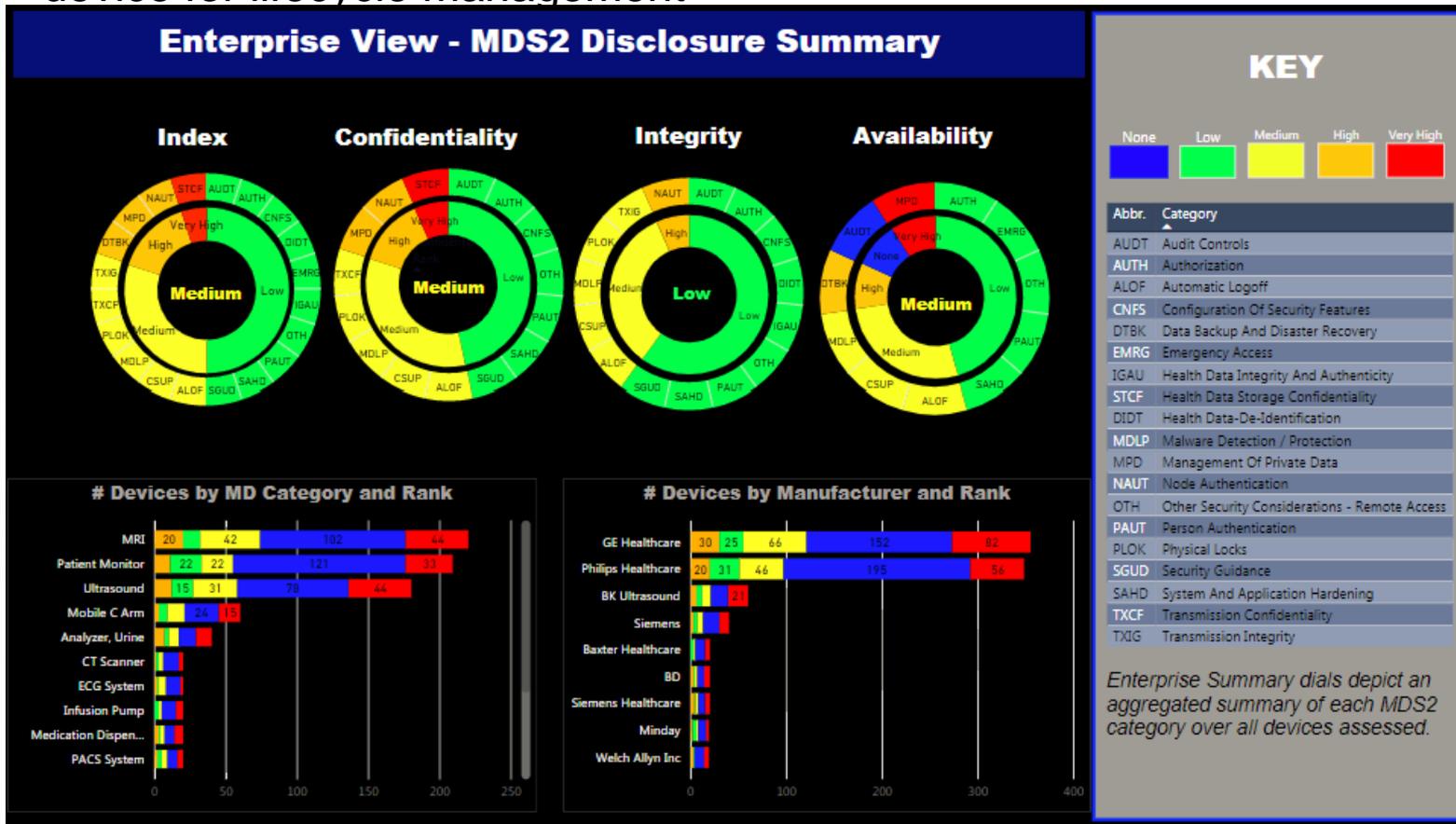
Leveraging the manufacturer data via the MDS2 and OEM details we can **analyze** and determine the risk and approach to patch/maintain the device or implement compensating controls



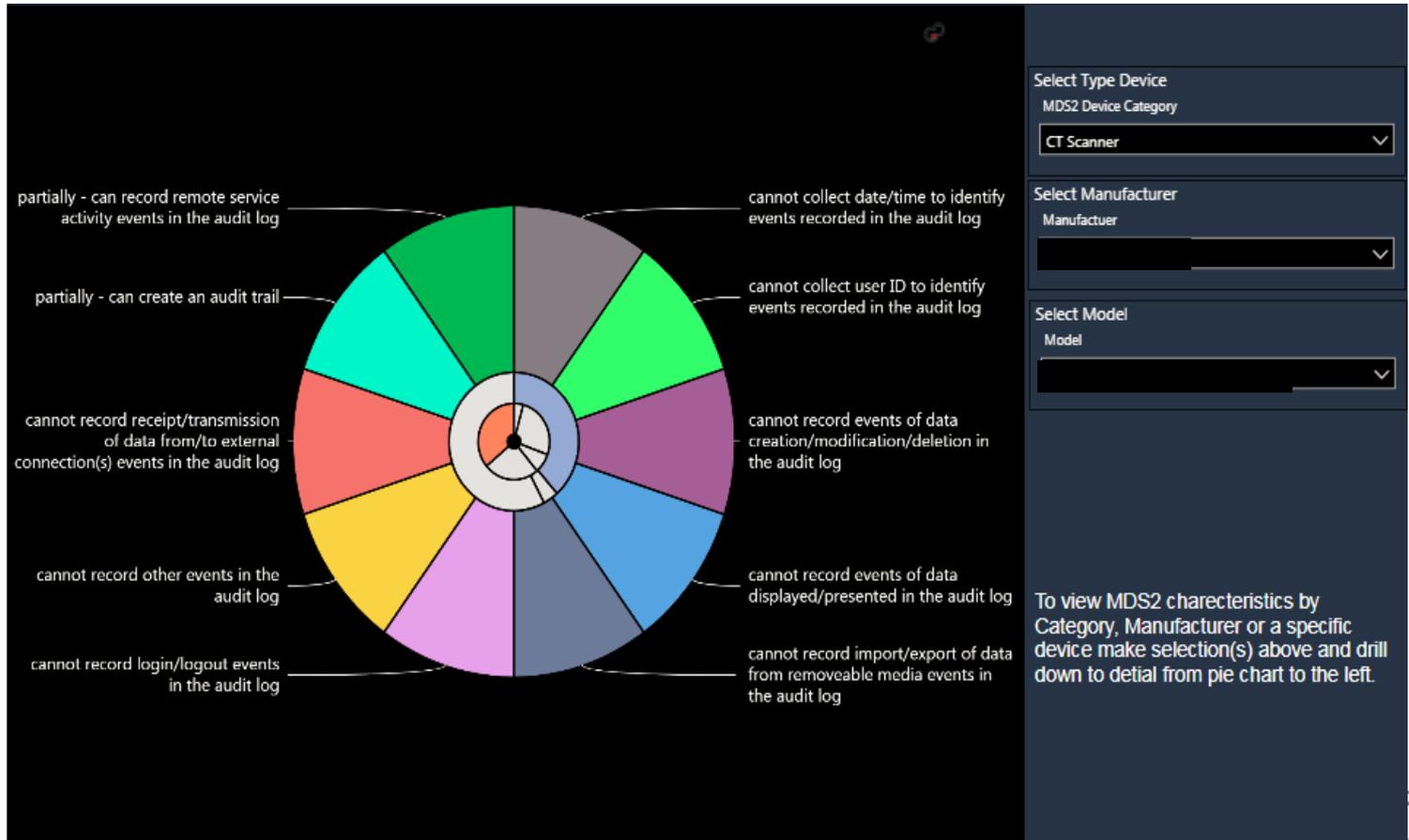
Analyzing this MDS2 data allows us to visualize and dashboard risk by device for lifecycle management

Aggregated Rating at an enterprise level of all assessed medical devices broken out by Index (all categories), and CIA.

Count of MDS2 questions by rank



With the ability to drill down into details such as capabilities and security exposures under the MDS2 category selected.



Remediation - The inventory & analysis should lead to an initial Medical Device plan that drives actionable items for Hospital Leadership & ongoing lifecycle management

Inventory Summary:

- ✓ Medical Device Operating System stats (i.e. supported to unsupported ratio)
- ✓ Statistics on newly found devices

Medical Device Analysis Findings and Recommendations:

- Security Vulnerabilities by device make/model including but not limited to:
 - ✓ Security patches
 - ✓ Published known CVEs
 - ✓ Vulnerability rating per tool findings
 - ✓ Controls and Policies such as physical access, User Credentials, Authentication, Encryption
 - ✓ Dataflow map and analysis

Network Infrastructure and Security Findings and Recommendations (if added to assessment)

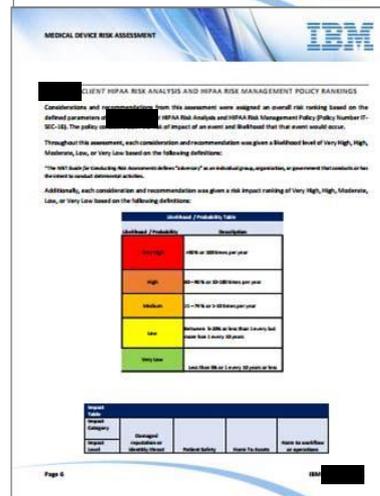
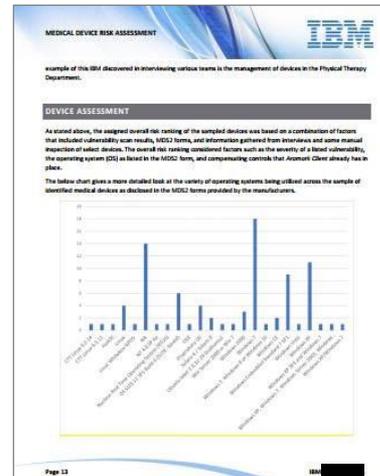
- ✓ Findings and Recommendations on Security Assessment using NIST or other framework best practices
- ✓ Network design Security components that are protecting the network/infrastructure (**compensating controls**) including Firewalls, IDS/IPS, Web Proxy & Content Filtering, DLP (network/email/device), Segmentation

Medical Device Patch Plan

- ✓ Medical Devices with recommended patches prioritized by Risk Index

Followup Capabilities

- ✓ Patching and Remediation (with Clinical Engineering or Medical Device TPM)
- ✓ OnGoing patch lifecycle review and management
- ✓ Ongoing inventory of IT/IoT/Medical Devices and Presentation Portal to track
- ✓ Integration into broader Support, Maintenance & Service capabilities
- ✓ Technical integration with Networking, Security, Service Management systems



Remediation activities should commence once the analysis and planning activities are completed and typically over a 2 to 4 month timeline to integrate into a lifecycle management approach

	Month 1	Month 2	Month 3	Month 4	
Planning					<ul style="list-style-type: none"> • Agree on scope and number of facilities • Finalize agreements & Statement of Work • Pre Install planning and change management requests (i.e. Network) • Install and Run Tool on core Network • Review existing inventory and analysis data
Discovery					<ul style="list-style-type: none"> • Gather data from tool • Review individual device data & correlate to device type data • Review Network and Flow data – data flow mapping • Review utilization and other relevant device details • Possibly integrate with other sources of record (i.e. CMMS or Inventory system) • Possibly perform some manual device inventory data collection & testing
Analysis					<ul style="list-style-type: none"> • Gather Security approach and tie back to 80001-2-2 Medical Device Framework • Input and Capture MDS2 data by Device type • Analyze Medical Device Dataflow, Software / Security Patch levels • Analyze Medical Device Network & Infrastructure • Review existing Medical Device security controls and policies, • Assessment and prioritization of captured vulnerability data
Remediation					<ul style="list-style-type: none"> • Develop dashboard on risk and potential remediation options • Review supporting Network and infrastructure device configuration analysis (Data center, core layer, wireless) integration with medical devices • Develop roadmap report for medical device specific issues around Confidentiality, Integrity, Availability and other general risks/IT issues • Possibly complete a clinical device dataflow analysis & network flow mapping • Patch devices via clinical engineering (or Third Party Maintenance organization) • Implement technical and compensating controls
Integration & Governance					<ul style="list-style-type: none"> • Determine long term approach to manage • Integrate with other maintenance and support activities • Develop long term solution – Monitoring, Inventory, Scanning, Patching, Compliance • Review IoT and IT data – devices to address across healthcare system • Integrate with core systems – NAC, SIEM, Service Management, FW/Networking, IDPS • Bring together a lifecycle governance approach for IoMT, IoT, IT across all facilities



Remediation and patching can be completed through a set of implementation activities



Analysis – What can be patched by device type, how to apply the patch (automated/manual), how to test, backout, change management



Deploy – Actual deployment of patch, testing, backout and recovery, help desk support, issue resolution, integration with other physical device activities (i.e. inventory)



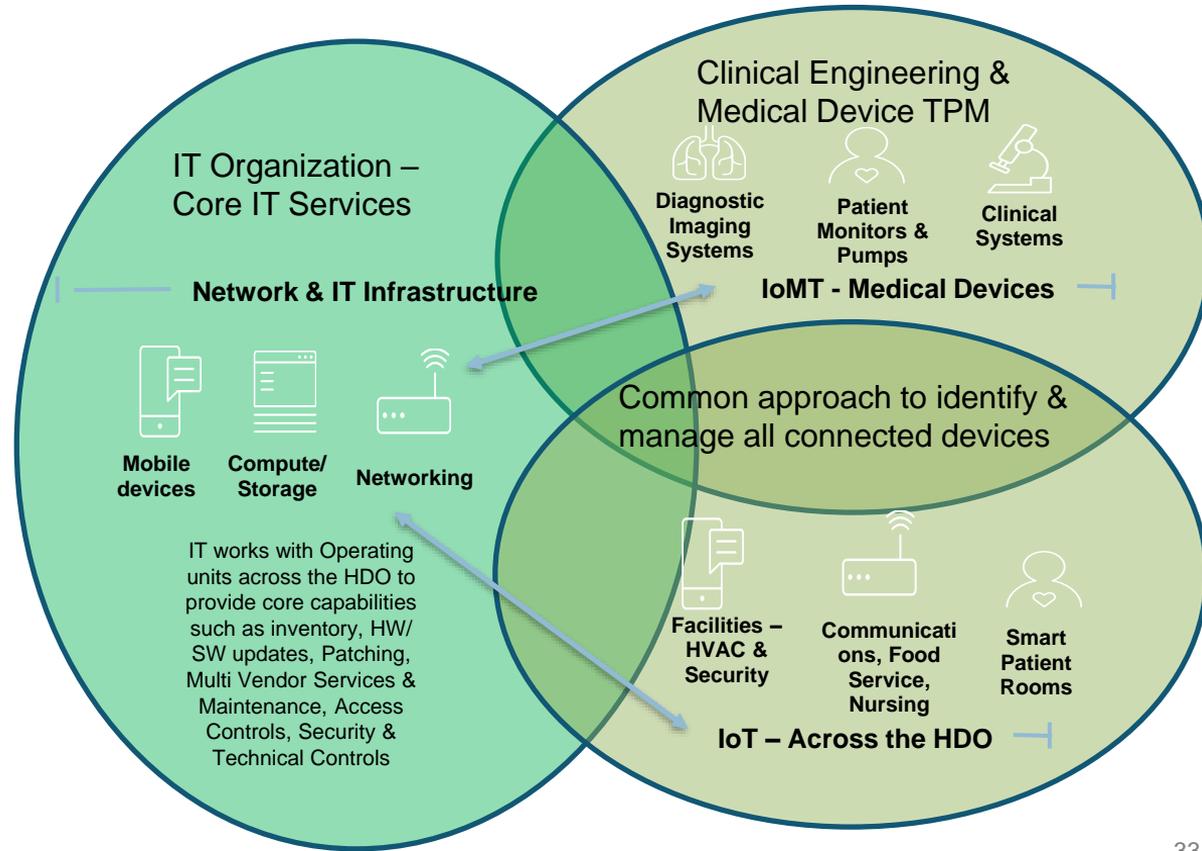
Manage – Continued monitoring leveraging internal and external sources for new threats or infections on devices and endpoints



Monitor – Continue to analyze IoMT and IoT traffic combined with increased focus on patching, remediation, compensating controls to decrease time to investigate and resolution

The IT/Security teams need to equip the organization with capabilities to address various IoMT/IoT systems and applications across the Hospital

- Implement a lifecycle proactive approach to address inventory/discovery, device analysis & risk management, patching, technical and compensating controls and maintenance & support for IT/IoT/IoMT devices
- A holistic end to end approach via integrating with core IT systems should address key goals of improving confidentiality, availability, integrity and patient care



System integration & automation can greatly increase core capabilities

By leveraging discovery tooling capabilities, an **integrated** approach to IoMT management can be automated to greatly increase risk management capabilities

Integration area	Approach	Cost	Benefit	Activities
Threat & Security Intel & Scanning	Active threat and CVE feeds	Low to Med	Real time analysis of threat data correlation	Determine core feeds and integrate to Discovery tool
Security/NW – Firewall, IDPS, Web Filtering	Clinical device specific security rules/controls	Low to implement, may be time consuming to refine	Increased Security rule sets to protect IoMT/IoT	Leverage potential rules advice to set control parameters
Network Access Control	Enforce access control to Medical Devices	Med to High if NAC solution in place, integration tuning	Isolation and potential segmentation	Develop NAC approach and integrate for IoMT
Security Information Event Management (SIEM)	Feed logs and additional intel data to Security Ops	Med if SIEM in place – need parsers and use cases built	Security Ops can react to alerts generated via SIEM	API or Parser and use cases to be built
Maintenance & Support - CMMS & Ticketing systems	Capture device information, open tickets for patching	Med - Bi Directional interfaces to systems for ticketing	Capture information and avoid swivel chair	Leverage available interfaces and customize
Advanced capabilities – RFID, Blockchain	Additional location and history/ maintenance data	Med to High, custom approach	Integration of core information and intelligence	Determine broader RFID & blockchain approach

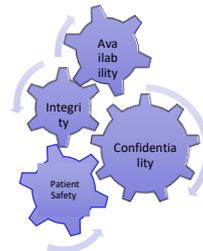
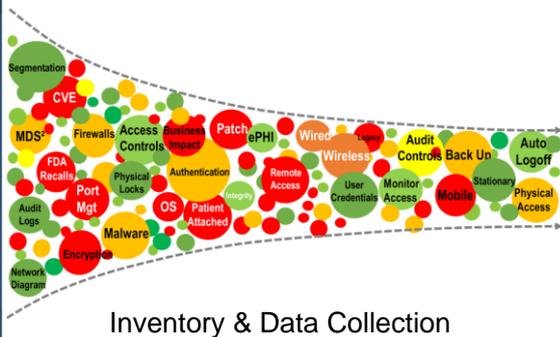


The explosion of connected medical and smart devices (IoT/IoMT) required to deliver patient care impacts all parts of the HDO



It is critical for the healthcare system to take a holistic approach to managing medical & smart devices across the enterprise

The organizations dependence on the IT team to coordinate a lifecycle management approach across the organization to ensure success



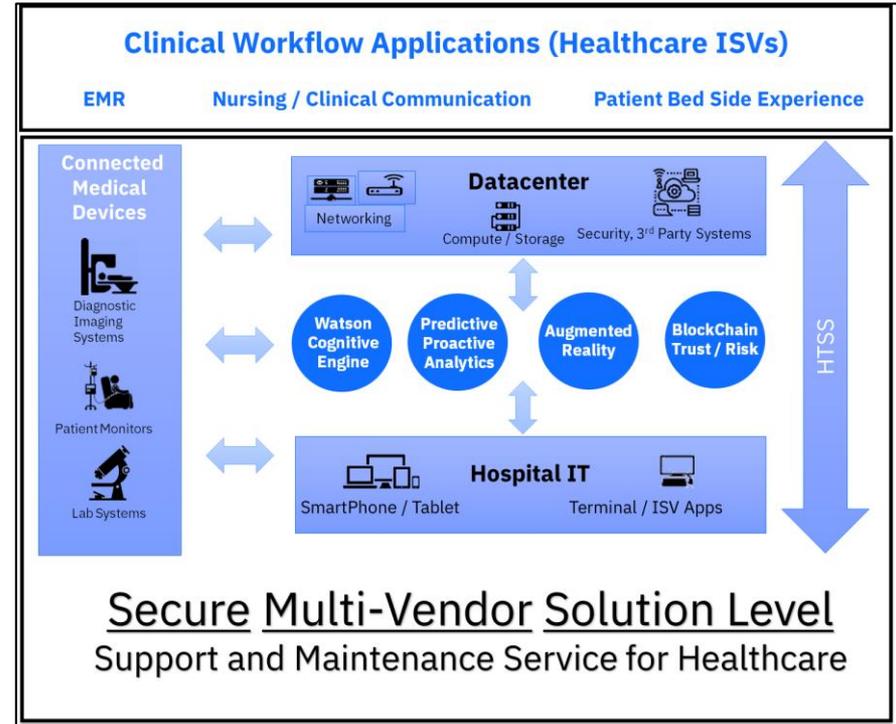
Patching, Remediation, Maintenance & Compensating Controls
 Governance & Reporting – Dashboarding & Lifecycle Management

Key Issues that Healthcare organizations need to address:

- Can the HDO identify through automated inventory and device attribute information what is connected to the Network
- Can they in turn use this information to understand risks, critical devices to patch, or implement compensating controls
- Is Availability and Security optimized through pro-active maintenance and remediation of risk exposures
- How do you minimize disruption to clinical workflow, ensure the best confidentiality, integrity, availability and patient safety
- How should the IT and IoT/loMT systems be maintained and supported – Vendors, OEM's, TPM's
- How does the organization protect it's reputation and minimize financial impact
- What is the governance and approach to manage loMT and IT/IoT lifecycle patch and maintenance management
- How do we create solutions across the ecosystem of capabilities to minimize spend and maximize results

Ultimately the IT organization should look at how best to integrate their IoMT lifecycle management to key technologies and processes core to Healthcare IT Support:

- Integrated Technical and Multi Vendor Support across the Data Center, Hospital IT and Connected Medical Device Embedded IT
- **Security, Compliance and Resiliency** throughout the Network and Infrastructure
- **Improve Operational Efficiencies** and Lower TCO Single Point of Contact to Managing Multiple Vendors
- **Medical Device and IT/IoT Inventory, Analysis & Remediation planning** to address patching and Security & Risk
- **Improved hospital IT workflows and end user experience** through automation and analytics
- **Support of Infrastructure HW/SW** used to deliver critical applications across the Healthcare system



Next Step & Call to action

- What is your organization currently doing?
- Are you prepared to address the explosion of IoMT & IoT devices from an IT perspective?
- How do you approach this, and what steps should you take?
- Please feel free to contact us further to discuss:
 - Matt Broomhall, mattb@us.ibm.com, 802-734-1863
 - Donald Kneitel, kneiteld@us.ibm.com, 561-302-1196

