

405(d) Mitigation #9 – Medical Device Cybersecurity

Left To Our Own Devices

Will We Follow Best Practices



Ty Greenhalgh
Industry Principal, Healthcare
Medigate by Claroty



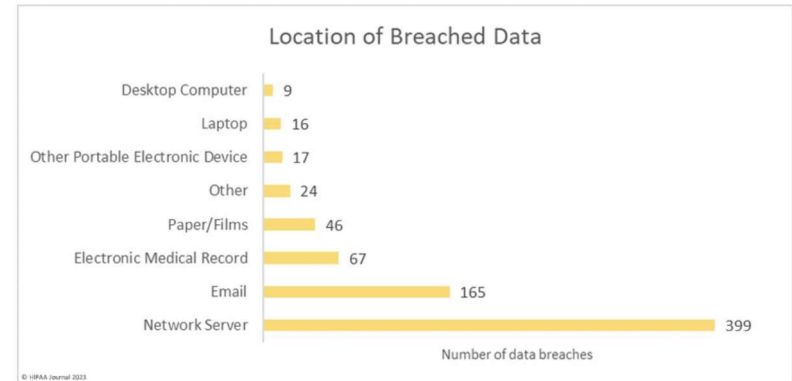
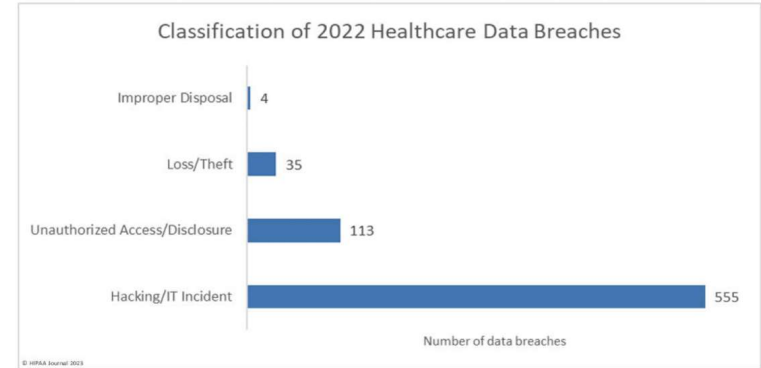
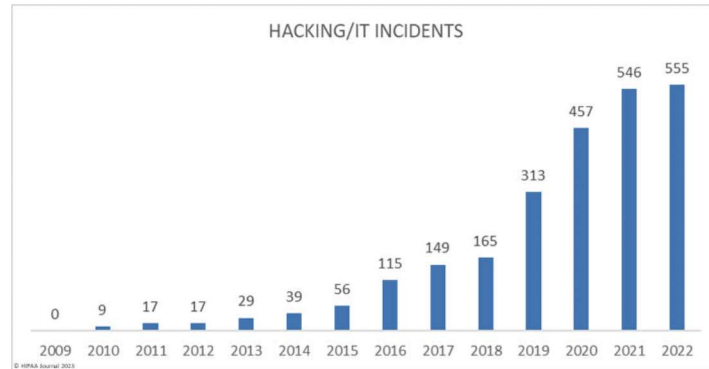
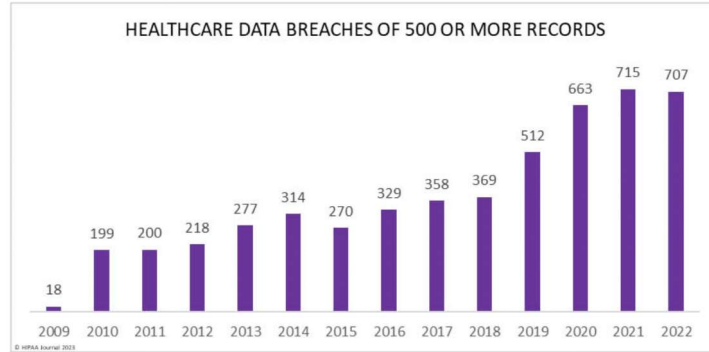
**Ambassador for
HHS 405(d)**
Aligning Health Care
Industry Security Approaches

A Brief History of Time

- American Recovery & Reinvestment Act (ARRA)
 - EHR Meaningful Use
- Cyber Security Act 2015
- WannaCry 2017
- HICP 2018
- HITECH Amendment 2020
- EO Improving Nations Cybersecurity 2021
- Omnibus Bill - 2022



Healthcare Breach Statistics - 2022



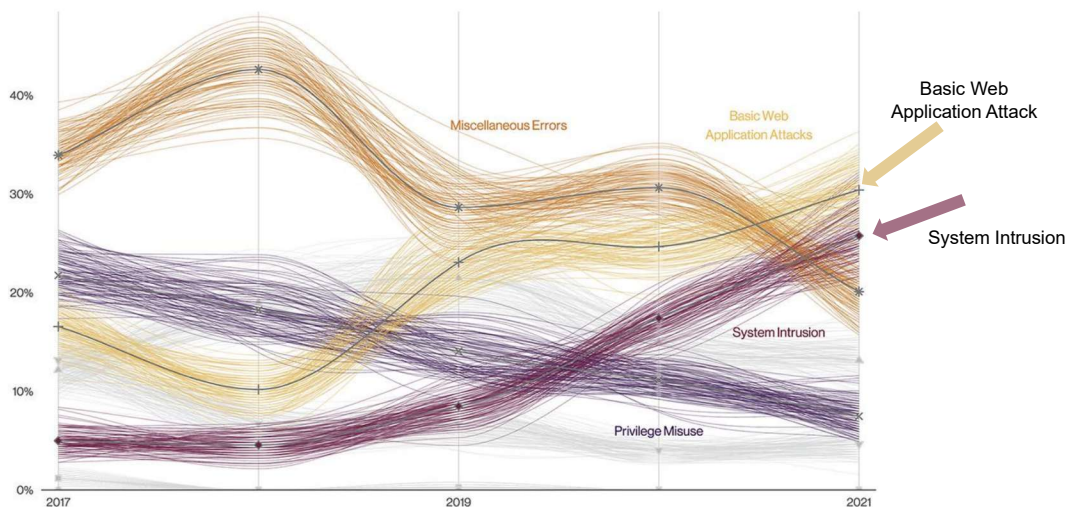
Verizon Data Breach Investigation – Report 2022

Healthcare Industry

Frequency	849 incidents, 571 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, <u>Miscellaneous Errors</u> and <u>System Intrusion</u> represent 76% of breaches
Threat actors	External (61%), Internal (39%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Personal (58%), Medical (46%), Credentials (29%), Other (29%) (breaches)

Summary

The Basic Web Application Attacks have overtaken the Miscellaneous Errors in causing breaches in this sector. Errors are still a significant problem.



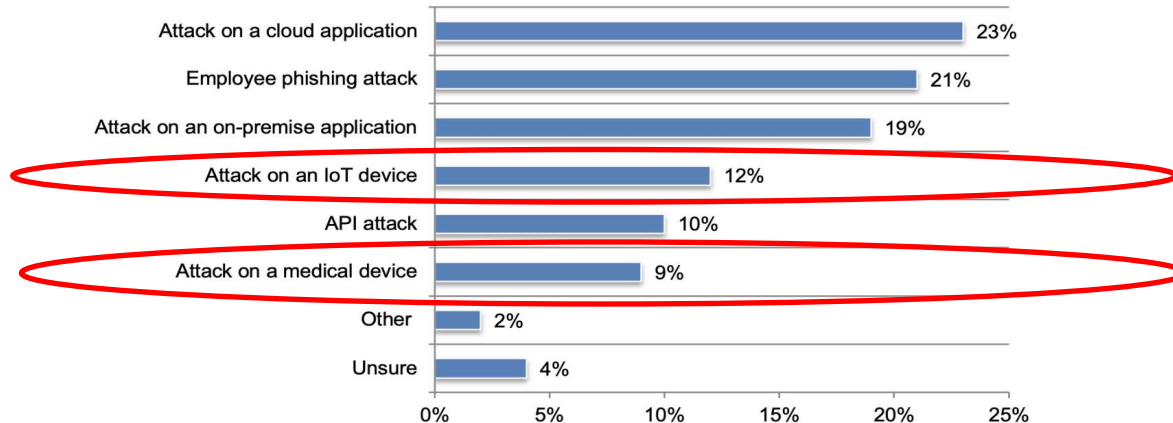
21% of Ransomware Attacks – Medical & IoT Devices



The majority of respondents (60 percent) say their HDOs had a data breach in the past two years involving 28,505 records and costing an average of \$837,750. As shown in Figure 11, cloud application and employee phishing attacks were the primary root causes of these breaches.

Figure 11. What was the root cause of the data breach?

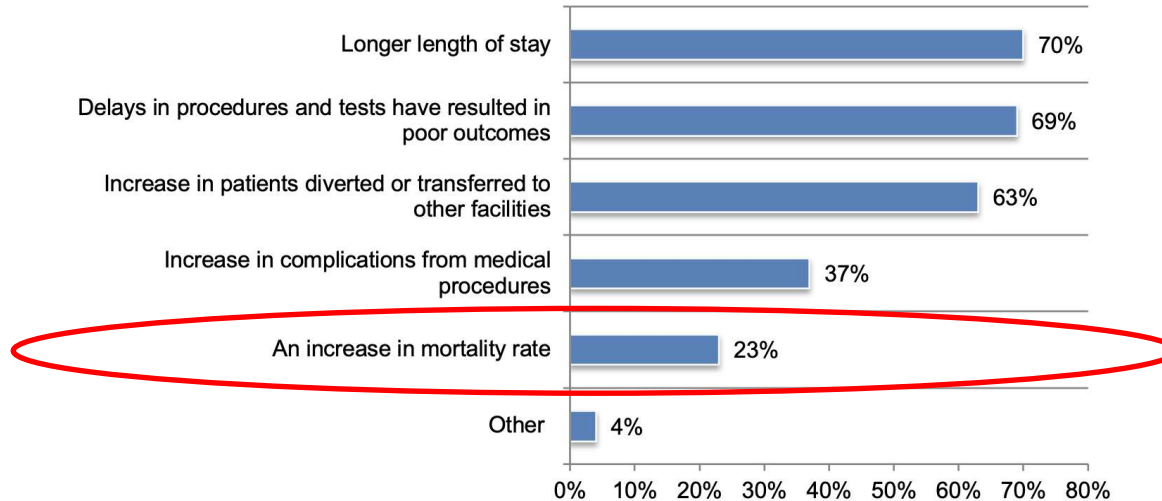
Only one choice permitted



Negatively Impacting Patient Outcomes

Figure 13. The consequences of cyberattacks on patient care

More than one response permitted



IT vs Extended Internet of Things (XIOT)

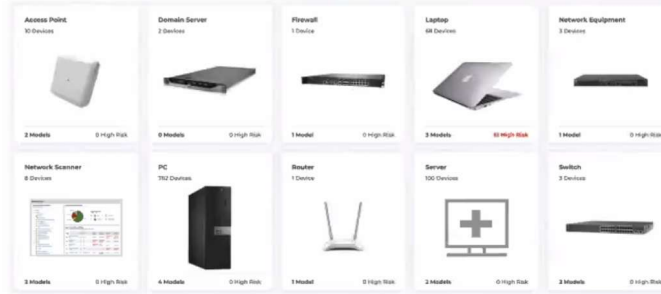
Complexity

Unique Protocols
Proprietary OS
No Anti-virus
Remote Access
Patient Safety
Patching Process
Traditional Security Tools

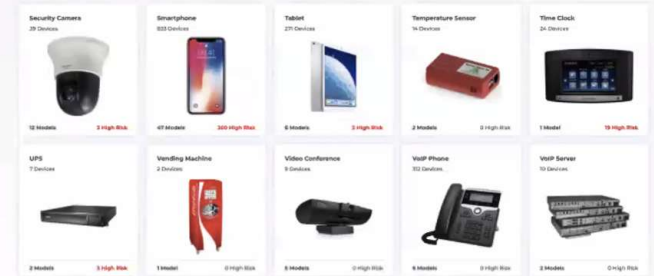
Visibility Needed

- Modality – type, make and model
- Version – OS type & patch
- Software – embedded software and utilized protocols
- Unique Identifiers – serial number, hostname, MAC address, Location – SSID, access point (AP), AP location

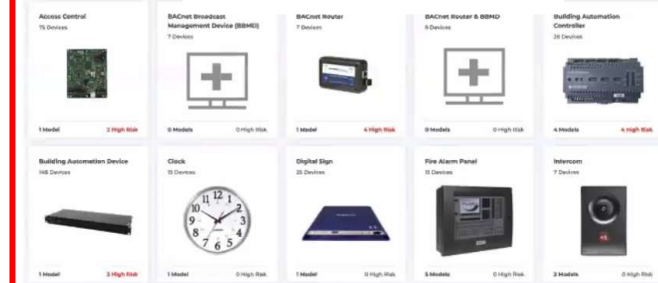
IT Devices



IoT Devices



BMS Devices

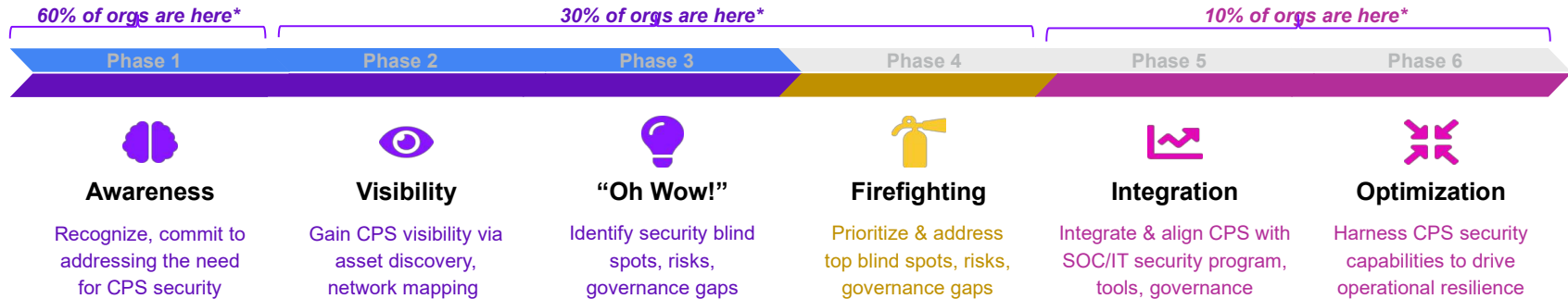


IoMT Devices



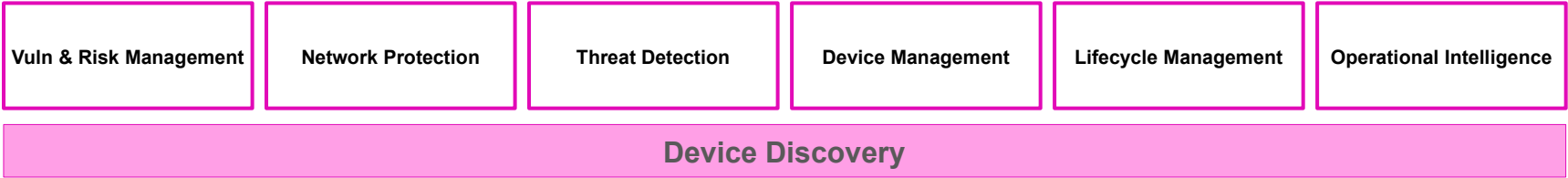
Cyber-Physical Systems (CPS) Security Journey

Gartner's 6-Phase approach to Achieving CPS Security Maturity



Medical Technology Security

Areas of Attention



Regulation and Legislation

Aligning Security Function with Basic Cyber Hygiene for Connected Medical Devices

Vuln & Risk Management

Network Protection

Threat Detection

Device Management

Lifecycle Management

Operational Intelligence

Device Discovery



Regulation and Legislation

Aligning Security Function with Basic Cyber Hygiene for Connected Medical Devices

SECURITY FUNCTIONALITY	405(d)	Warner CIPS	HIC MaLTS	FDA Post Market	Section 3305 (PATCH)	NIST CSF Healthcare
Device Discovery	9MA, 9MD	2.3, 3.1, 3.4	Visibility, Technical Investigation, MDS2, SBOM/VEX, Assessment Surge	Monitor for Identification & Detection of Vuln. & Risk over Lifecycle; Intack & Handling.	524B.(b).1	ID.AM-1, ID.AM-2, ID.AM-3
Vuln & Risk Management	9ME	2.1, 2.2, 3.4, 4.4, 5.1, 5.4, 5.5, 6.1	Disclosure, Patching Lifecycle, Updates, Risk Mgmt.	Detecting Presence and Impact of Vuln. Deploy Mitigations & Remediations	524B.(b).2, 524B.(b).2.(A), 524B.(b).2.(B)	ID.AM-5, ID.RA-1, PR.AC-1, PR.AC-4, PR.AC-5, DE.CM-8
Network Protection	9MG	2.1, 2.3, 3.4, 8.1	Connectivity & Technical Exposure Reduction	Traffic Monitoring using Deep Packet Inspection, Automated Network Segmentation/Zero Trust.		PR.PT-3, PR.PT-4
Threat Detection	9MD	1.1, 1.2, 1.3, 1.4, 2.1, 3.4, 5.4	HDO Cybersecurity Signals	Analyze Detect and Assess Threat Sources.	524B.(b).2.(A)	ID.RA-1, ID.RA-5, DE.AE-1, DE.AE-3
Device Management	9MA, 9MD	2.1, 2.2, 2.4, 2.5, 3.1	CMMS Unified Asset Mgmt.	Integration with CMMS for single source inventory & automated workflow		ID.GV-4
Lifecycle Management	9LC	2.1, 2.2, 3.4, 4.5, 6.2	EOG, EOS, EOL, Technology Stages	Maintain Safety & Essential Performance: CVSS 3.0, Manufacturer CVSS	524B.(b).2	PR.DS-1, PR.DS-5, PR.IP-2
Operational Intelligence	9MB	2.1, 2.5, 3.4, 3.5, 7.4	Communications	Assess Severity of Patient Harm	524B.(b).2, 524B.(b).2.(A), 524B.(b).2.(B)	DE.CM-1, DE.CM-7

In The News.....

March 27th Politico reported.....

“The **Biden administration** will pursue new policies to further **secure the health care sector and medical devices against cyberattacks in 2023**, and is considering using either executive orders or support legislative efforts to accomplish these goals, an administration official says.

Big picture: The effort comes after two years of escalating cyberattacks on hospitals and health care organizations that have made it even more difficult for them to cope with both the Covid-19 pandemic and complicated efforts to tackle ongoing IT security vulnerabilities.

A senior administration said that the White House is “**working closely**” with the Department **of Health and Human Services** on the agency’s effort to identify the most critical hospitals and health care groups, and to then **develop “minimum standards” for cybersecurity**. This is similar to what the Transportation Security Administration did for critical pipeline groups in the wake of last year’s crippling ransomware attack on Colonial Pipeline.

More to come: The official noted that the White House will be carefully assessing the HHS program and “based on that, determining how that scales” across the wider health care sector. Further, the administration is **considering federal grants for hospitals to adopt certain minimum cybersecurity requirements for medical devices**, and the Cybersecurity and Infrastructure Security Agency is working to produce security products for the healthcare.”



HHS 405(d) HICP 2023

Aligning Health Care Industry
Security Approaches

- Congressionally Mandated
- Public/Private
- Convened by HHS in 2017
- Comprised of over **230 +**
 - information security officers
 - medical professionals
 - privacy experts
 - industry leaders



HITECH Amendment

H.R.7898 — 116th Congress (2019-2020)

Signed January 5, 2021 | Public Law No: 116-321



Public Law 116-321
116th Congress

An Act

To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. RECOGNITION OF SECURITY PRACTICES.

Part 1 of subtitle D of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.) is amended by adding at the end the following:

42 USC 17941.

“SEC. 13412. RECOGNITION OF SECURITY PRACTICES.

“(a) IN GENERAL.—Consistent with the authority of the Secretary under sections 1176 and 1177 of the Social Security Act, when making determinations relating to fines under such section 1176 (as amended by section 13410) or such section 1177, decreasing the length and extent of an audit under section 13411, or remedies otherwise agreed to by the Secretary, the Secretary shall consider whether the covered entity or business associate has accurately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place that may—

“(1) mitigate fines under section 1176 of the Social Security Act, as amended by section 13410;

“(2) result in the early, favorable termination of an audit under section 13411; and

“(3) mitigate the remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title) between the covered entity or business associate and the Department of Health and Human Services.

“(b) DEFINITION AND MISCELLANEOUS PROVISIONS.—

“(1) RECOGNIZED SECURITY PRACTICES.—The term ‘recognized security practices’ means the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with

Amend HITECH Act - consider **certain recognized security practices**

HHS must consider it when making decisions for things like audits and enforcement

Demonstrate recognized security practices for at least the previous 12 months

HHS can take **Recognized Security Practices** into consideration to:

1. Reduce fines
2. Decrease length of audits/increased favorable result
3. Mitigate remedies during Settlement negotiations (CAP's, etc.)

Recognized Security Practices

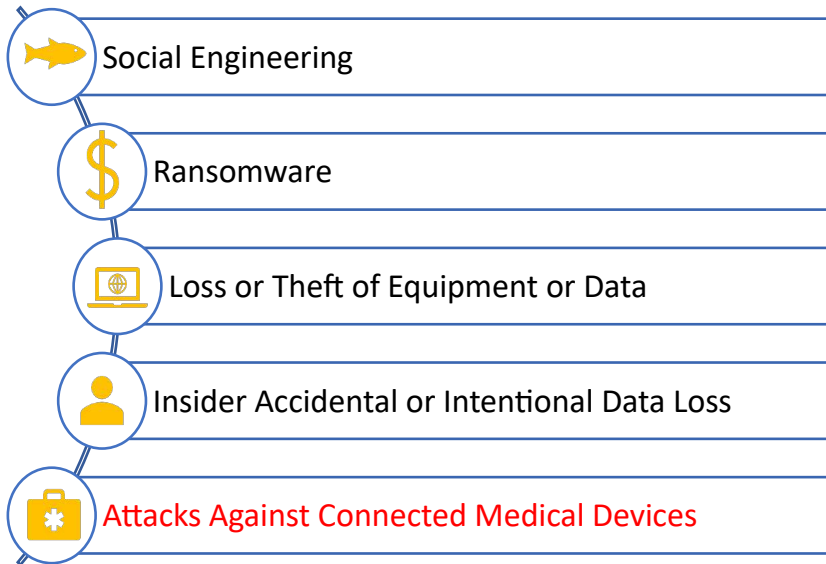
1. NIST
2. **405(d) – Cybersecurity Act of 2015**

<https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf>

<https://journal.ahima.org/page/navigating-the-new-hipaa-safe-harbor>



Top 5 Most Impactful Cybersecurity Threats



- ## Top 10 Most Impactful Mitigations
1. Email Protection Systems
 2. Endpoint Protection Systems
 3. Access Management
 4. Data Protection and Loss Prevention
 5. Asset management
 6. Network Management
 7. Vulnerability Management
 8. Incident Response
 9. **Medical Device Security**
 10. Cybersecurity Oversight & Governance

Medical Device Security – Mitigation #9

What are the changes?

- Medical Device Security - Sub Practices

- Asset Management – Asset Discovery & Security (ADS)
- Endpoint Protection – agents & OT
- Identity and Access Mgmt. – MAC authentication bypass
- Network Management - scaling ZTA with clinical workflows
- Vulnerability Management – maximizing visibility
- Security Operations & Incident Response – reduce false positives
- Procurement & Security Evaluation – don't onboard more risk

Areas of Impact

PHI

Medium Sub-Practices

9.M.A Asset Management

9.M.B Endpoint Protections

9.M.C Identity and Access Mgmt.

9.M.D Network Management

9.M.E Vulnerability Management

9.M.F Contacting the FDA

Large Sub-Practices

9.L.A Security Operations and Incident Response

9.L.B Procurement and Security Evaluations

Key Threats Addressed

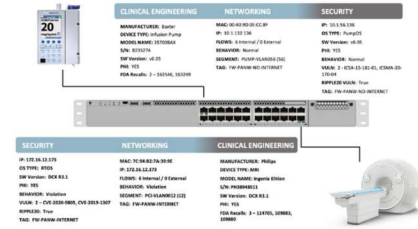
Attacks against network connected medical devices that can affect patient safety

405(d) Resources

Prescription Poster: [Network Connected Medical Devices](#)

Within the medical technology discipline, it is recommended to store the results of these inventories into CMMS. These systems are like ITAM systems for IT assets but contain specialized fields for the tracking of maintenance, recalls, and other key attributes specific to medical devices.

It is common for an HDO to have hundreds to thousands of medical devices deployed throughout the system. As such, conducting these hardware and software inventories manually is likely to be inefficient. Automated tools, called ADS monitoring systems, exist to assist with this issue. These ADS tools can automate many control implementation tasks while collecting device specific and network ecosystem



Asset Management – 9:M:A

- Automated - Asset Discovery & Security (ADS) aka Medigate
 - AI/ML vs DPI
 - Hardware & Software Inventory
 - Baseline Network Communications
- Computerized Maintenance Management System (CMMS)
 - Single Central Repository – Source of Truth
 - Automated Workflow – service ticketing & mitigations

Packet Header

Medigate DPI

CLAROTY

Infusion pump communicating with DCMP

Device IDs	ID	HW	HW Desc	SOFTWARE
	10.13.13.190	00102A685A.05	Ambicom (was Tandy?)	Medical
	MANUFACTURER	Alaris	Infusion Pump	8015 PC Unit
	MACADDR TYPE	MOBILE	GENERAL BUSINESS	PCB CLASS
	Physical	Portable	120140868	2
Versions & Names	OS	OS NAME	OS VERSION	APP VERSION
	Proprietary Enea OSE	Proprietary	Enea OSE	9/912
Network	NETWORK SCOPE	Default	VLAN	VLAN NAME
	Corporate	Default	902	WIFI_902
	VLAN DESCRIPTION	CONNECTION TYPE	IP ASSIGNMENT	WIRELESS ENCIPHERMENT
	WIFI_902	Wireless	DHCP	WPA2
	IP/PORT SCEN	LAST SEEN		
	1/3/22, 1:39 AM	4/20/22, 10:54 AM		
Network Security	AUTHENTICATION USER	8015_PC_Unit_Wireless_Access	APPLIED WIRELESS ACL	8015_PC_Unit_Wireless_Access
	8015_PC_Unit_Wireless_Access	Infusion_Pumps.sgt	8015_PC_Unit_Wireless_Access	Infusion Pumps
Location	WIFI NAME	LOCATION (PROVIDING)	AP GROUP	WIFI
	Clinton	PCU	00C05B273120	MEDNET
	AP NAME	AP LOCATION	LAST SEEN ON AIR	
	C002010034	columbia > Building 3 > Floor 2	9/13/22, 1:19 PM	

Endpoint Protection – 9:M:B

- Zero Trust/Least Privilege
- Passive traffic collection - Validation
- Integration
 - Medigate imports IT data
 - Agent – Is there an Agent; Falcon
 - High level OS, application list
 - Patch level – Remove vulnerability off device
 - Reduce alert fatigue
 - Medigate exports
 - Risk report
 - Can the medical device support EDR but not loaded
- Presence of Agent/Falcon reduces risk scores



Identity & Access Management – 9:M:C

- MAC Authentication Bypass
- Device ID plus Policy Management
 - Manufacturer
 - Device Type
 - MAC Address
 - Serial Number
 - Policy Creation - Group Management



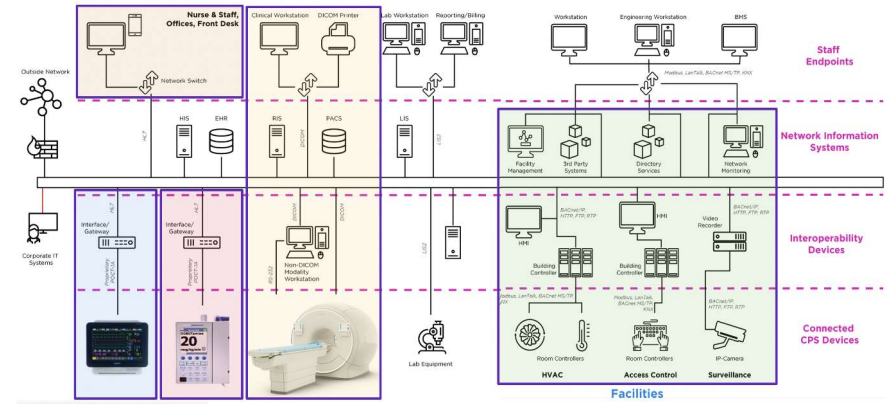
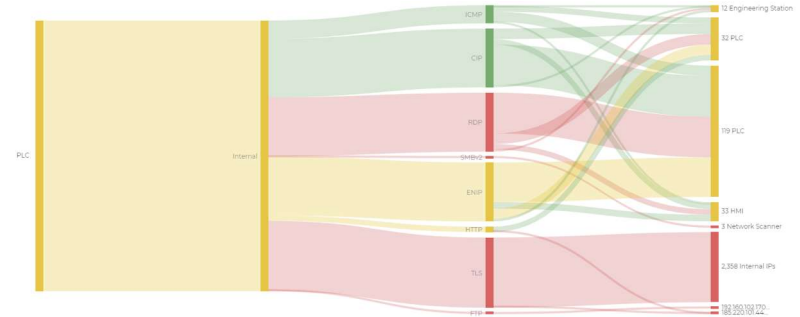
Network Management – 9:M:D

- Challenges of NAC

- Visibility
- Resource Costs
- Resilience/Speed
- Scale
- Clinical Workflow

- Zero Trust – Least Privilege

- Device Identification – Visibility
- Baseline Behavior – Clinical Workflow
- Integration
 - Access Control Lists/SGTs
 - Cisco/Fortinet/Aruba – imports ACL and enforces policy



Vulnerability Management – 9:M:E

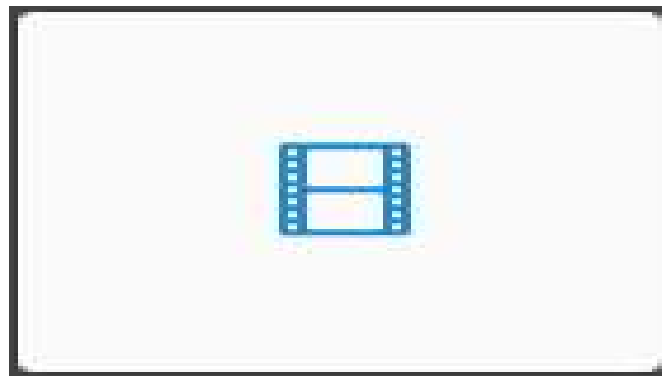
- Scanning of Devices
 - Ingest into ADS from Vuln Scanner
 - List of vuln in their environment
 - Change Vuln Status - “Indication” to “Confirmed” increase accuracy
 - Decrease noise – alert fatigue
 - Safe Scan Targets
 - Export medical device IP’s to Vuln Scanner
 - Scan areas that contain medical devices - subnet but avoid devices w/ these IP addresses
 - Exclusion lists – all infusion pumps, patient monitors, printers, cameras, etc.
- Risk Categorization

Table 13. ADS Use Cases

Use Cases	Monitor	Analyze	Secure
Undesired Traffic	Watch risky ports (e.g., 3389)	Assess appropriateness	Block ports or segment
Vulnerabilities	Correlate known vulnerabilities with existing assets (e.g., Ripple 20, Deja Blue)	Evaluate, discuss with vendors, and determine mitigation	Patch, block ports or segment
Unsupported OS	Identify risky devices	Assess traffic—necessary and unnecessary	Upgrade OS, replace device or segment
Device Behavior	Determine “normal activity” baseline	Assess traffic—necessary and unnecessary	Block unnecessary traffic

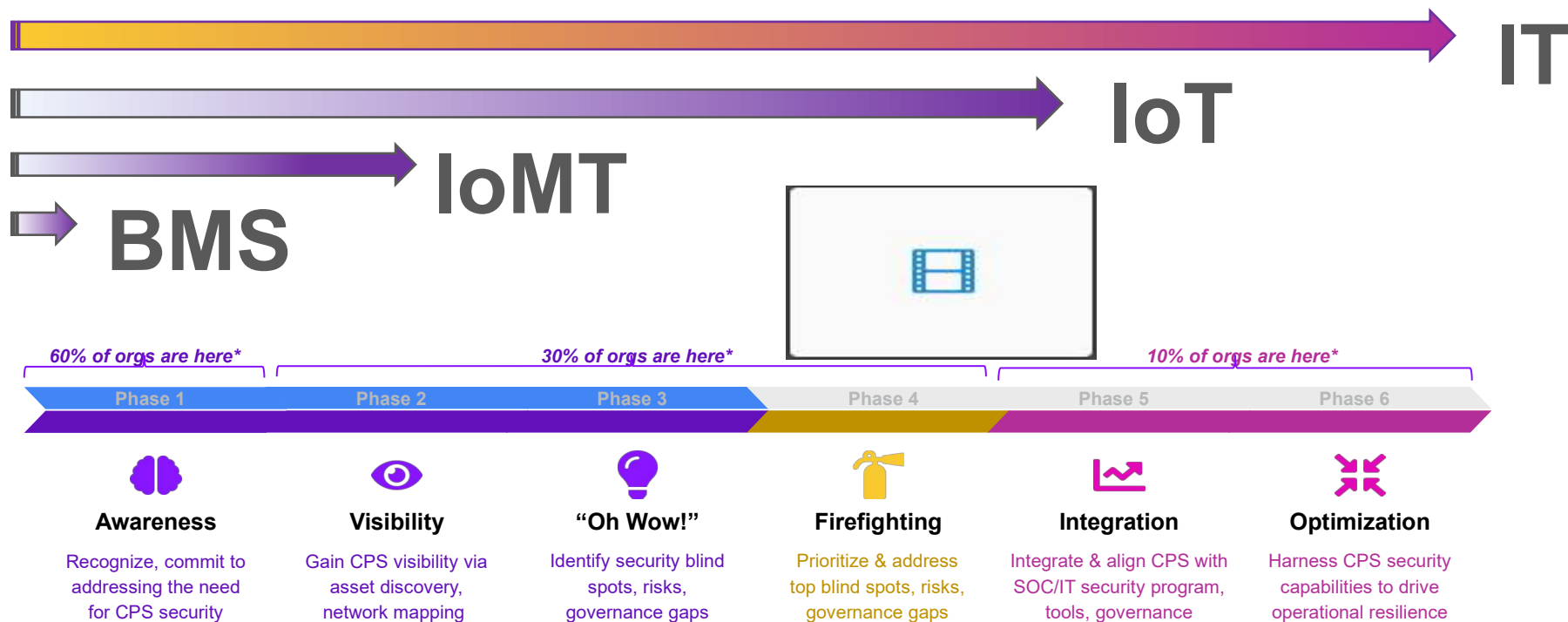
Procurement & Security Evaluations – 9:L:B

- MDS² - Manufacturer Disclosure Statement for Medical Device Security
 - Import & Index data to the device
 - Similar to upcoming SBOM processes
- SBOM – Omnibus Bill/Patch Act
- Intake Triage
 - Risk Assessment – Compare Risk of New Device Types
- Contract Negotiation
 - MC² - Model Contract Language for MedTech Cybersecurity
- End of Life Support (EOS)
 - HIC – MaLTS
 - Healthcare Industry Cybersecurity MedTech Legacy Technology Security



Cyber-Physical Systems (CPS) Security Journey

Gartner's 6-Phase approach to Achieving CPS Security Maturity



Summary

- Ransomware Attacks are Increasing
- IT Security vs. OT Security
- Government is Considering Best Practices & Minimum Requirements
- HICP will be foundational
- Cybersecurity Framework Basics – Visibility
- ROI - Leverage Security Data for Asset Management

Resources

- Health Sector Coordinating Council ([HSCC](#))
- Healthcare Cyber - Managing Legacy Technology & Security [HIC-MaLTS](#)
- Cyber Risk Mgmt. for MDMs [Joint Security Plan](#)
- Senator Warner – Cybersecurity Is Patient Safety ([CIPS](#))
- White House Cybersecurity [Strategy](#)
- 405(d) Healthcare Industry Cybersecurity Practices ([HICP](#))
- NIST CSF Healthcare Implementation [Guide](#)



Thank you

Ty Greenhalgh
Industry Principal, Healthcare
Ty.G@Claroty.com

Connect on LinkedIn