ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

The Changing Landscape of Connected Medical Devices

Ty Greenhalgh
Industry Principal, Healthcare
Medigate by Claroty
Ty.g@claroty.com

Nick Sturgeon, MS, ITIL, eJPT
Executive Director, Information
IU Health & IU School of Medicine
nsturgeon@iuhealth.org

MEDIGATE
by Claroty

October 20, 2022

ACCE gratefully acknowledges the sponsorship of this webinar by

About the moderator

Martin Poulin, P.Eng., FCMBES

Director of Biomedical Engineering for Island Health, Victoria, BC, on the west coast of Canada.

23+ years health technology management

5 years in the medical device development industry in Vancouver.

Master of Engineering in Clinical Engineering from UBC

Past President of CMBES

Logistics

- All attendees have their microphones muted during the presentation.
- Questions to the panelists must be submitted via the “Q&A” feature (not chat) in Zoom at any time.
- If there is any urgent issue, please use the “chat” feature to communicate with the panelists.
- We will try to ask Nick & Ty to answer questions not addressed during the webinar and distribute them to participants via email or post them to ACCE website.
- Please remember to complete the webinar evaluation after attending. A link will be provided at the end.

About the speaker

Ty Greenhalgh, HCISPP
Industry Principal, Healthcare

MEDIGATE by Claroty

Ty Greenhalgh was an early pioneer of the electronic medical record (EMR). The Henry Ford Health System awarded the "Most Innovative Technology of the Year" to Mr. Greenhalgh, in conjunction with the AHIMA, for groundbreaking work in developing one of the first EMR systems to contain automated HIM workflow, electronic signature and integration into the AHIMA FORE library in Chicago.
He was employed with 3M Health Information Systems for over 25 years. He helped introduce disruptive technologies to include Remote Transcription, Digital Dictation and Speech Recognition, Document Scanning, Computer Assisted Coding and Computer Assisted Clinical Documentation Improvement.
Ty is currently an ambassador with the HHS 405(d) Program and Task Group which was responsible for the recognized security practices referenced in the new HITECH amendment more commonly known as the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.*

Ty is currently the Healthcare Industry Principal with Medigate by Claroty. Claroty, a worldwide leader in cybersecurity, empowers organizations around the world to secure all their cyber-physical systems. Claroty recently purchased Medigate, the Best in KLAS healthcare solution, integrating the tools required for cybersecurity of medical devices to become the dominant leader for healthcare device cybersecurity. Ty has authored dozens of articles and is a frequent speaker for AHIMA, HCCA, HIMSS and AAMI.

ACCE AMERICAN COLLEGE OF CLINICAL ENGINEERING

About the speaker

Nick Sturgeon, MS, ITIL, eJPT
Executive Director, Information Security
IU Health & IU School of Medicine

Nick Sturgeon currently serves as an Executive Director in Information Security for IU Health and IU School of Medicine. His responsibilities include supporting the IU School of Medicine's cyber risk management program and leading the IU Health's Offensive Security Team. Nick is also the founder of the IU Health Medical Device Security Lab located at 16Tech. Nick has worked in Information Technology for nearly 20 years, with 10 years in Cybersecurity, nine years in Law Enforcement, and 10 years in State Government. Nick is also a PhD student and graduate research assistant at Purdue University Polytechnic Institute. His PhD research is focusing on medical device security. Nick has extensive experience in incident response, digital investigations, e-discovery, criminal investigations, digital media recovery, cyber risk management, and criminal law. Nick serves on the board of the Cyber Threat Intelligence Network, Sports-ISAO, and the Indiana HIMSS Chapter.

Session Description

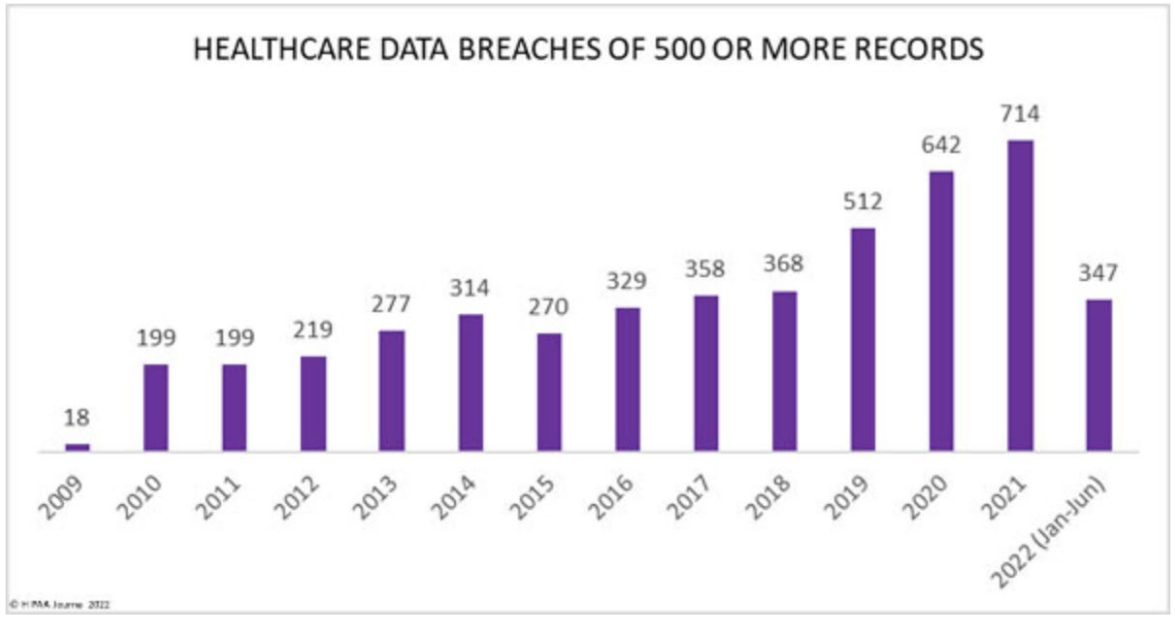
Within the last year, organizations like the Congress, FDA, CMS, OCR, Joint Commission, HSCC, and CISA have been proactive in their efforts to align the health industry's cybersecurity efforts in support of networked connected medical devices. In this webinar, we will discuss the basics that are driving this activity and what is being done to help secure healthcare operational technology.

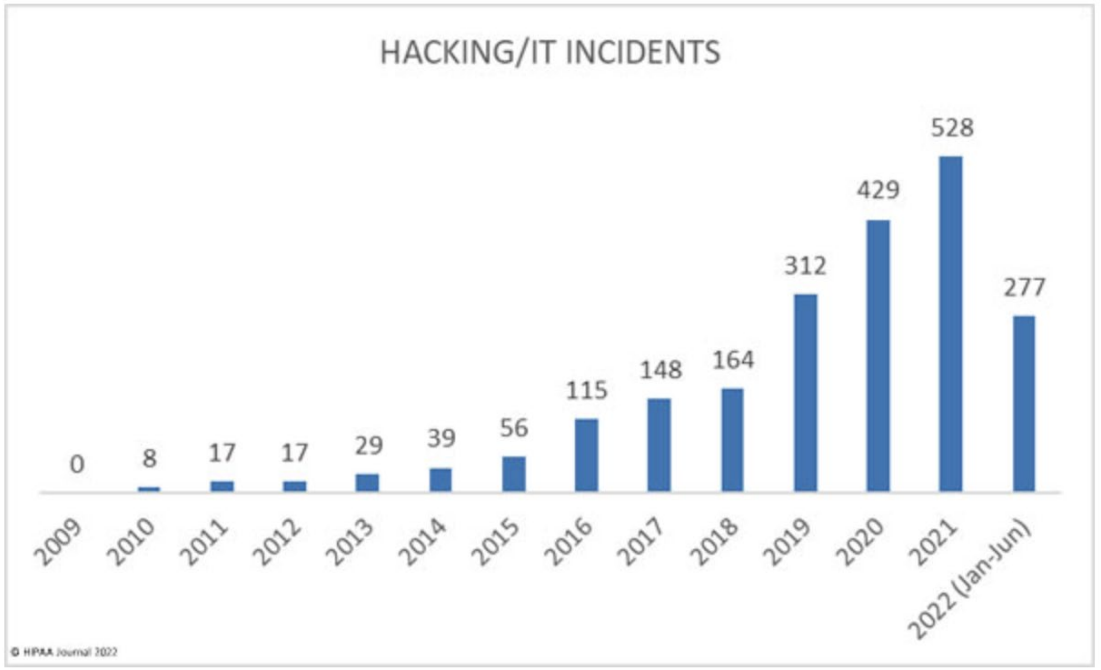
Nick Sturgeon is the Executive Director of Information Security at IU Health leading their Offensive Security Team. Ty Greenhalgh is the Industry Principal from Medigate, the Best in KLAS solution for connected medical device cybersecurity. Together they will touch on a myriad of topics.

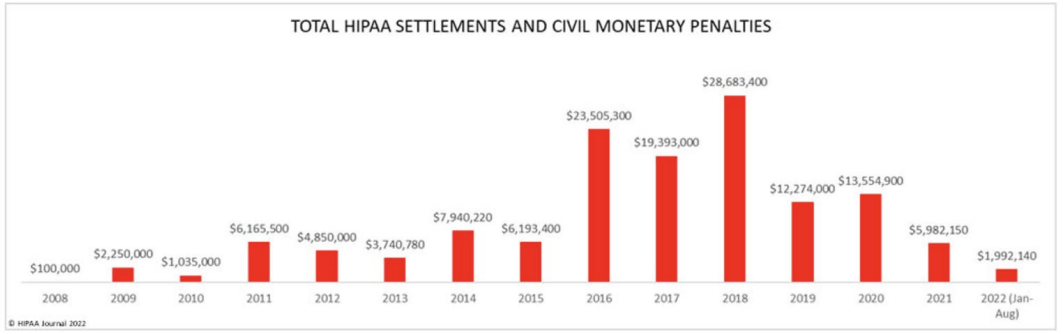
- Why is the Healthcare Industry the #1 Target for Hackers
- What are the challenges for securing connected medical devices
- Review the Initiatives:
  - IU Health Medical Device Security Lab
  - University of Minnesota Center for Medical Device Cybersecurity
  - Legislation & Regulations
  - New HITECH Amendment – Recognized Security Practices
  - The Joint Commission – New Audits
- Where should Healthcare Delivery Organizations look to for solution.

Join us while we discuss the challenges and initiatives that are in motion for the healthcare industry to protect these devices. Attendees will be brought up to speed on the current landscape, how it's changing and what they can do to position their organizations for the coming changes.

Healthcare Breach Statistics - 2022







HIPAA Journal: June 2022 Healthcare Data Breach Report

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

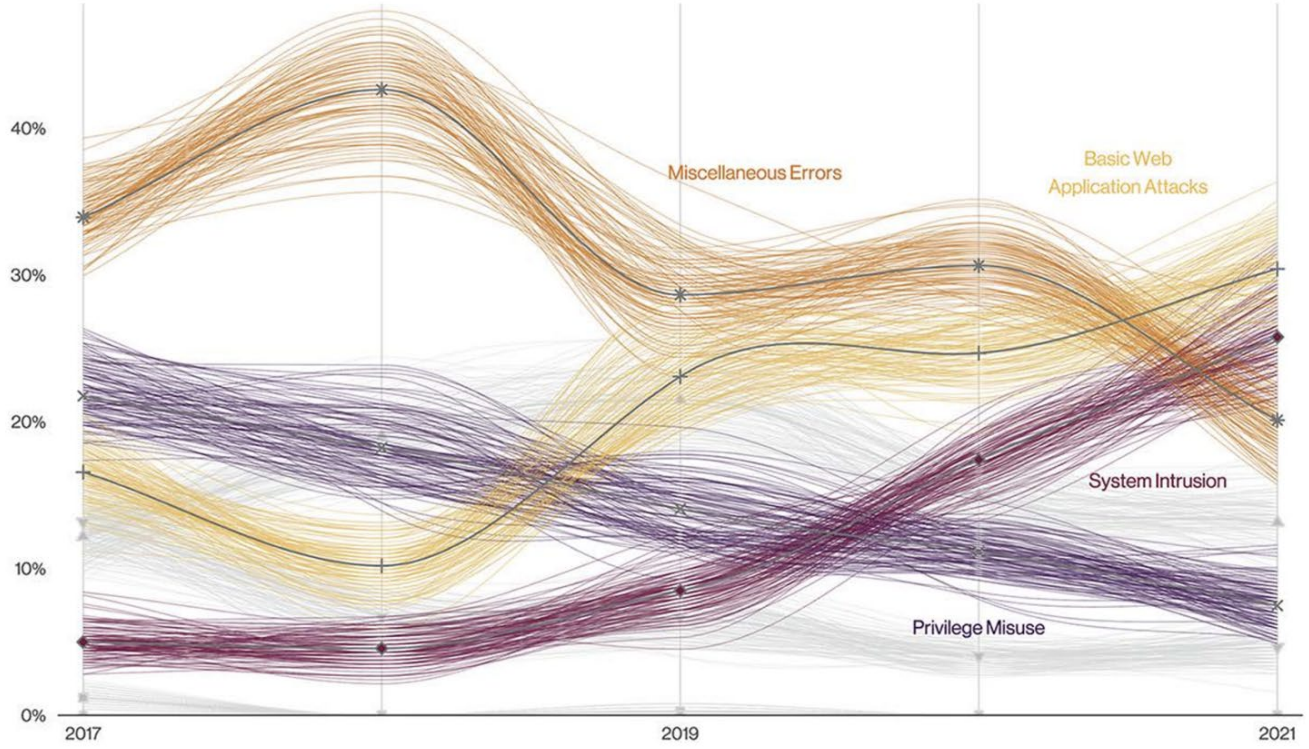
Verizon Data Breach Investigation Report 2022 Healthcare Industry

Frequency	849 incidents, 571 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion 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.

Patterns over time for Healthcare Industry Breaches - VDBIR



https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

Cyber Attacks on Healthcare Orgs - 2022

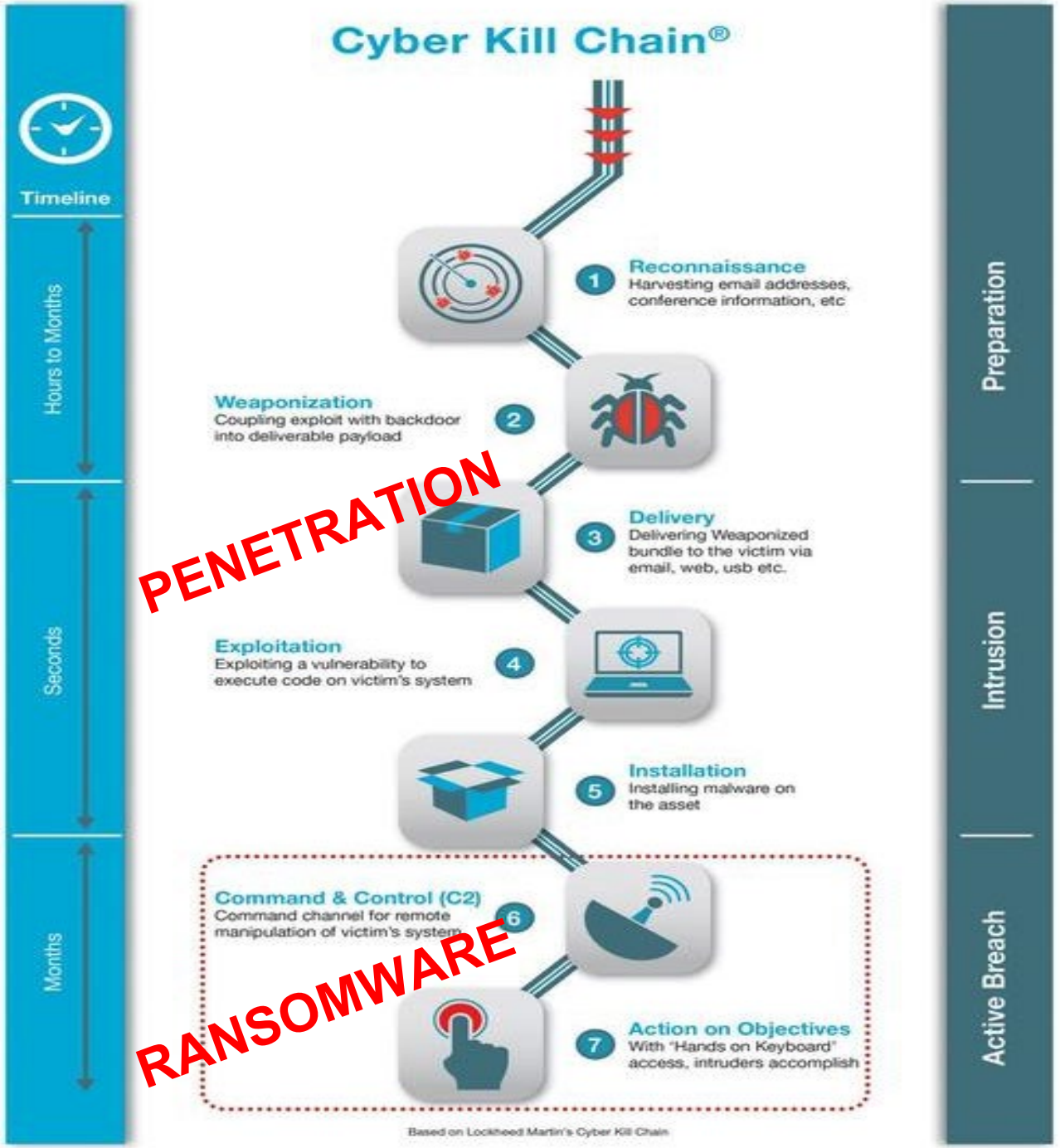
- Broward Health – FL, 1.3 million people affected[2]
  - Third-party provider
- Monongalia Health System – WV, almost 500k people affected[2]
- Norwood Clinic – Alabama healthcare system, 228k people affected[1]
- Yuma Regional Medical Center – AZ, 700k people affected[3]
  - Ransomware
- MCG Health – WA, PHI & PII was accessed by unauthorized actors[3]
- Goodman Campbell – IN, compromised network and data[4]

1. https://www.heraldtimesonline.com/story/news/healthcare/2022/06/22/indiana-university-health-mcg-data-breach-what-should-patients-do/7686747001/
2. https://www.ibj.com/articles/goodman-campbell-computer-network-attacked-by-hackers
3. https://www.heraldtimesonline.com/story/news/healthcare/2022/06/22/indiana-university-health-mcg-data-breach-what-should-patients-do/7686747001/
4. https://www.ibj.com/articles/goodman-campbell-computer-network-attacked-by-hackers

Patient Safety – Food & Drug Administration (FDA)

- Diversion Death – ER down
  - Dusseldorf Hospital Germany
- Child Death – lack of fetal monitor
  - Springhill Memorial, Alabama
- Ransomware
  - Delays & Obstacles in Treatment
- Ponemon Study
  - Longer Stay 71%, Delayed Testing 70%, Transfers 65%, 36% Increased Complications, 22% Increased Mortality Rates

https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate



Systematic Attack Steps

1. **RECONNAISSANCE**

   - Find gap in the security

2. **WEPONIZATION**

   - Build malicious attachment

3. **DELIVERY**

   - Hacking or Email targeting employee

4. **EXPLOITATION**

   - Employee opens the file. Vulnerability exposed.

5. **INSTALLATION**

   - Malware installs on client immediately

6. **COMMAND AND CONTROL**

   - Attacker gains control and backdoor

7. **ACTION ON OBJECTIVE**

   - Able to pinpoint and access to critical data

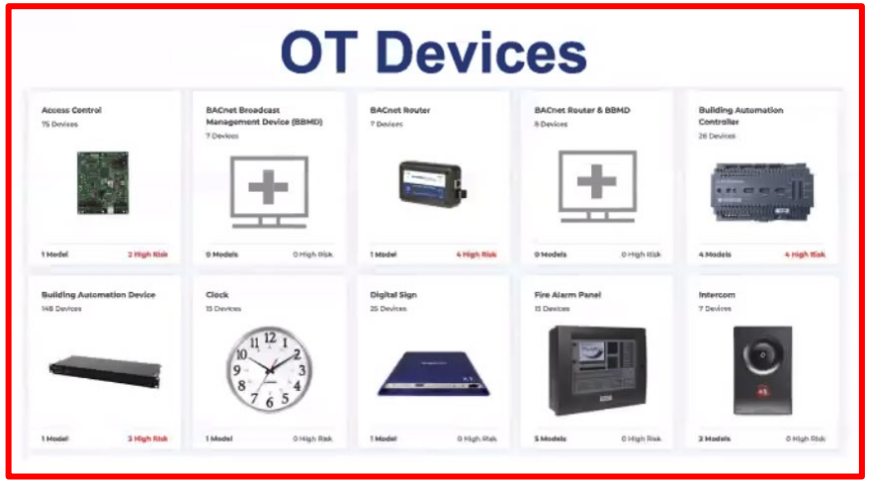
IT vs. Extended Internet of Things (XIoT)

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



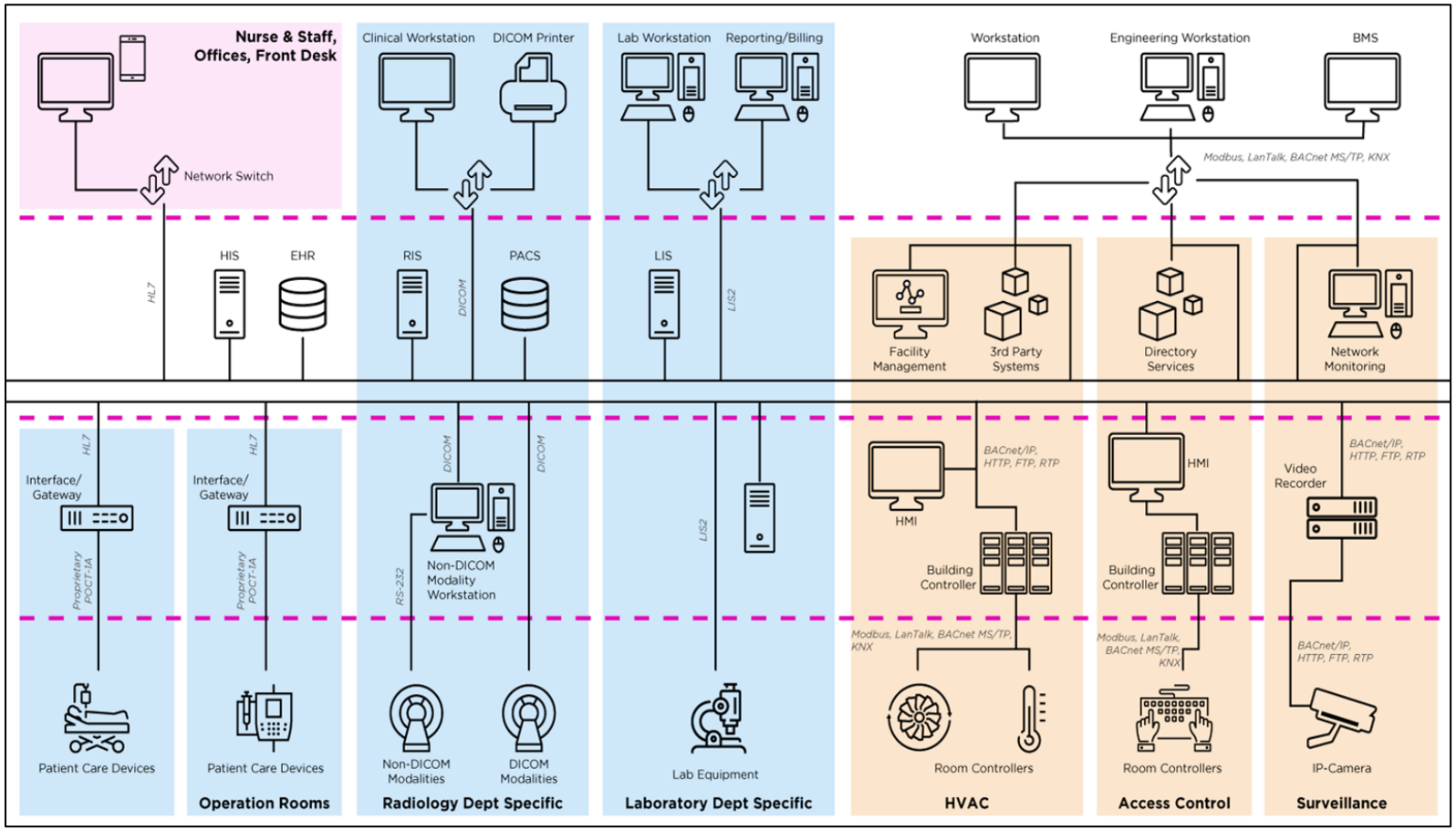
ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

THE MODERN HEALTHCARE NETWORK

The Idea!!

- To combat these threats security researchers, experts, manufacturers, academic institutions, and health systems must be constantly vigilant and proactive in their efforts.

- The cybersecurity, med-tech, and bioresearch ecosystems in Indiana presents a prime opportunity to bridge a major gap that exists in medical device security.



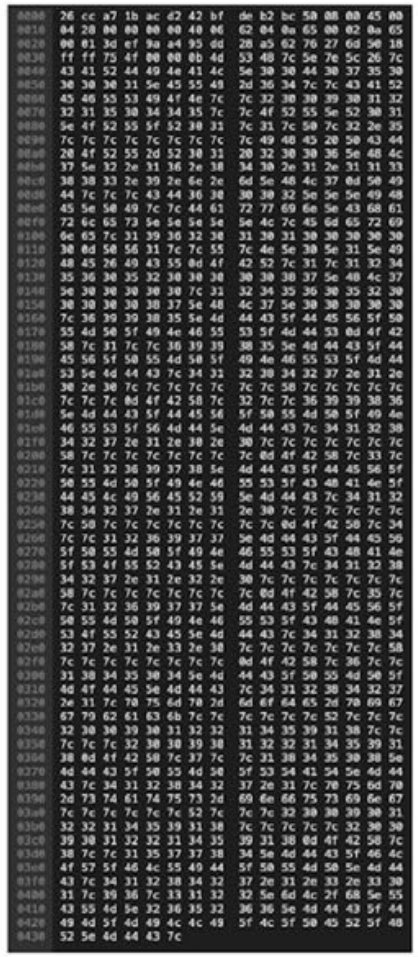
IoMT ⟷ **BMS**

Passive Network Packet Analysis

Parsing Protocol Packets for Unmatched Depth of Visibility

Packet Header

Medigate DPI



Infusion pump communicating with DCMP

Device IDs	IP 10.13.15.190	MAC 00:10:7A:68:5A:05	MAC OUI Ambicom (was Tandy?)	CATEGORY Medical
	SUB CATEGORY Patient Devices	MANUFACTURER Alaris	TYPE Infusion Pump	MODEL 8015 PC Unit
	MACHINE TYPE Physical	MOBILITY Portable	SERIAL NUMBER 1201410868	FDA CLASS 2
Versions & Names	OS Proprietary Enea OSE	OS NAME Proprietary	OS VERSION Enea OSE	APP VERSION 9.19.1.2
Network	NETWORK Corporate	NETWORK SCOPE Default	VLAN 902	VLAN NAME WIFI_902
	VLAN DESCRIPTION WIFI_902	CONNECTION TYPE Wireless	IP ASSIGNMENT DHCP	WIRELESS ENCRYPTION WPA2
	FIRST SEEN 1/31/22, 1:39 AM	LAST SEEN 4/20/22, 10:54 AM		
Network Security	AUTHENTICATION USER 00-0C-C6-01-37-B0	ENFORCEMENT/AUTH. PROFILES 8015_PC_Unit_Wireless_Access	APPLIED WIRELESS AC... 8015_PC_Unit_Wireless_Access	ISE AUTHENTICATION METHOD mab
	ISE SECURITY GROUP NAME Infusion_Pumps_sgt	ISE SECURITY GROUP TAG 1	ISE SECURITY GROUP DESC. Infusion Pumps Group - Exported fro...	TRUSTSEC RES. GROUP Infusion Pumps
Location	SITE NAME Clinton	LOCATION (PROTOCOL) PCU	AP BSSID 00:C0:58:27:31:20	SSID MEDNET
	AP NAME CO02010034	AP LOCATION columbia > Building 3 > Floor 2	LAST SEEN ON AP 9/13/22, 1:19 PM	

CLAROTY

Healthcare Cybersecurity

In need of collaboration

IT & Security

- Device Visibility
- Patching Process

Biomed & Clinical Engineering

- Safety Delays Operations
- Specialized Patching

Operations & Finance

- Procurement & Onboarding
- Risk Assessments

Facilities Management

- Device Visibility
- Broad Impact

Cyber Resilience

Operational Resilience

- Vulnerability Disclosure
- SBOM

Medical Device Manufacturer

- Right to Repair
- Operationalization

Independent Service Organization

- The Joint Commission Audits
- FDA Guidance
- New Laws

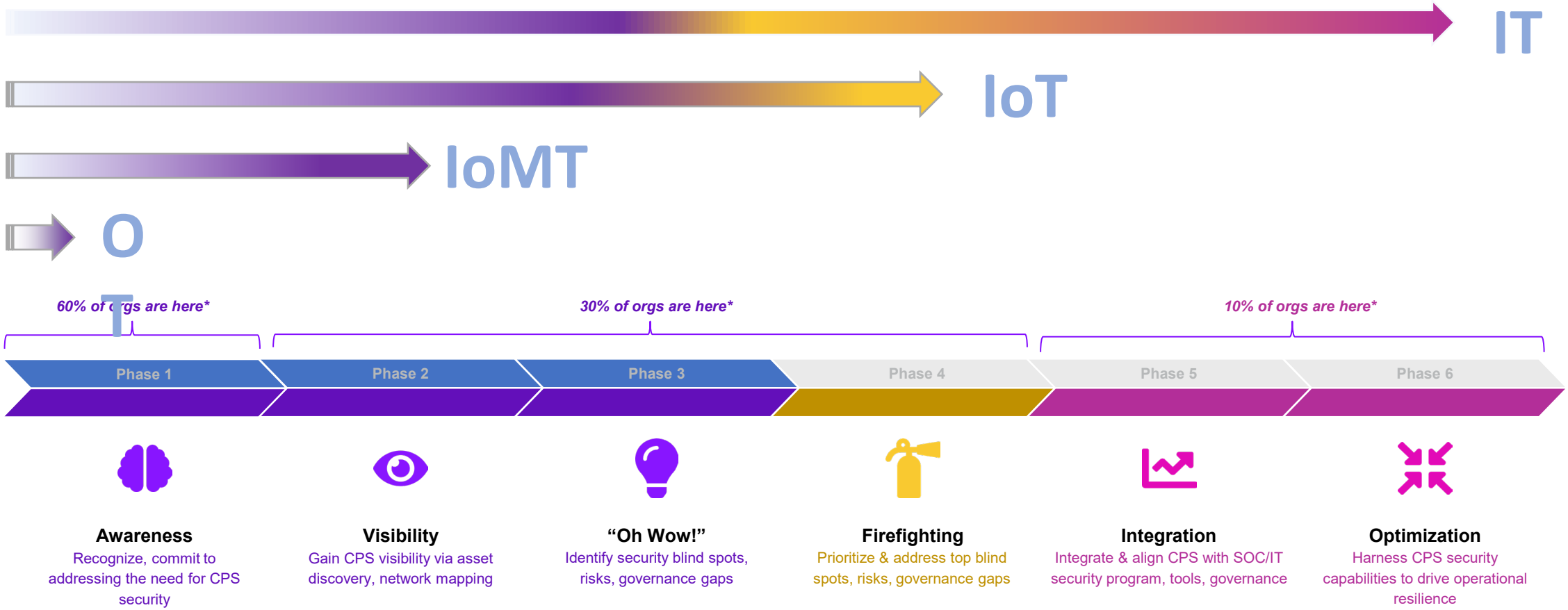
Government Oversight

- Device Visibility
- Broad Impact

Compliance

The Cyber-Physical Systems (CPS) Security Journey

Gartner's 6-phase approach to achieving CPS Security Maturity



Gartner®

*Source: Market Guide for Operational Technology Security, Gartner, 2021

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Regulatory Considerations

- President Biden Executive Order – Improving Nations Cybersecurity[1]
- FDA Guidance - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions[2]
- Protecting And Transforming Cyber Health Act – HR 7084[3]
- Strengthening Cybersecurity for Medical Devices Act – S 4336[4]
- HHS OIG Report – cybersecurity for connected medical devices[5]
- New OCR Director Ranier – doubling investigators
- FDA Reauthorization Bill – User Fees & Medical Device Security[6]
- New Healthcare Cyber Law
  - Recognized Security Practices – PL 116-321 or HR 7898[7]

1. https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity
2. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
3. https://www.congress.gov/bill/117th-congress/house-bill/7084/text?r=1&s=1
4. https://www.congress.gov/bill/117th-congress/senate-bill/4336?q=%7B%22search%22%3A%5B%22S+4336%22%2C%22S%22%2C%224336%22%5D%7D&s=1&r=1
5. https://www.oig.hhs.gov/oei/reports/OEI-01-20-00220.asp
6. https://www.hipaajournal.com/medical-device-cybersecurity-requirements-stripped-from-fda-reauthorization-bill/
7. https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf

Medical Device Security Research Organizations

Agile Research, Scientific Procedures & Peer Reviewed Articles

- This research needs to be agile to adapt to the everchanging threat landscape.
- Scientific based procedures to ensure quality and integrity of the data.
- Publish findings in peer reviewed articles and industry related publications.

Indiana University Health
https://iuhealth.org/iu-health-medical-device-security-testing-lab

https://mdiss.org/

https://www.villageb.io/

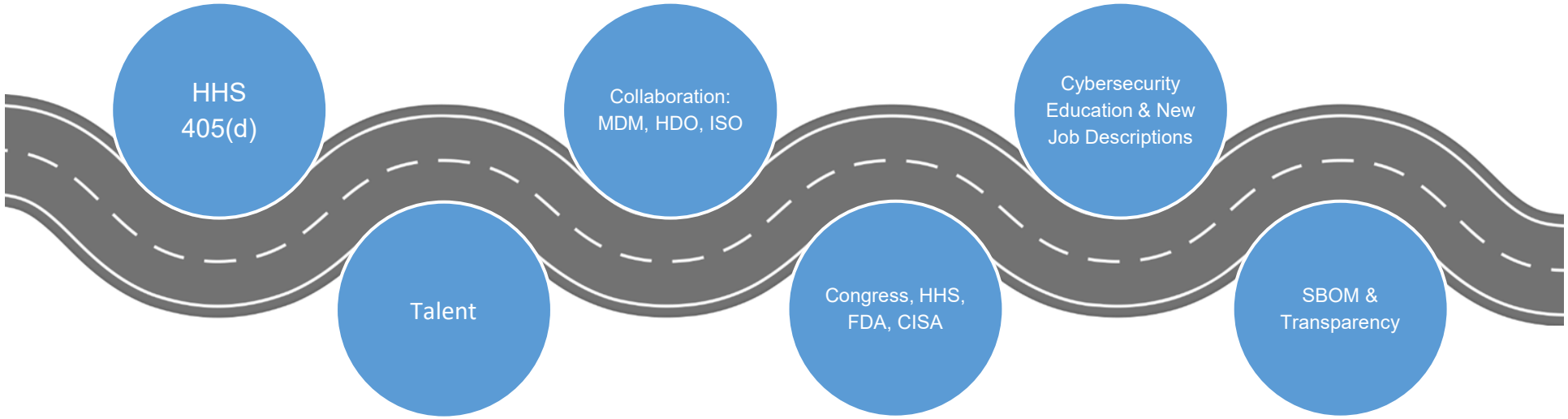
https://www.secure-medicine.org/

https://cse.umn.edu/cmdc

https://mdpnp.org/

Photo from Hackers Conference

Navigating the Changing Environment



Thank You

Please complete the online evaluation/attendance form at https://www.surveymonkey.com/r/ACCE_Medigate_10-20-22

Nick Sturgeon - nsturgeon@iuhealth.org

Ty Greenhalgh – ty.g@claroty.com

Happy Clinical Engineering Day!

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING