Medical Device Cybersecurity Workforce Development

Julie Connolly
Eileen Division
The MITRE Corporation

NICE Conference

November 19, 2019

MITRE

Agenda

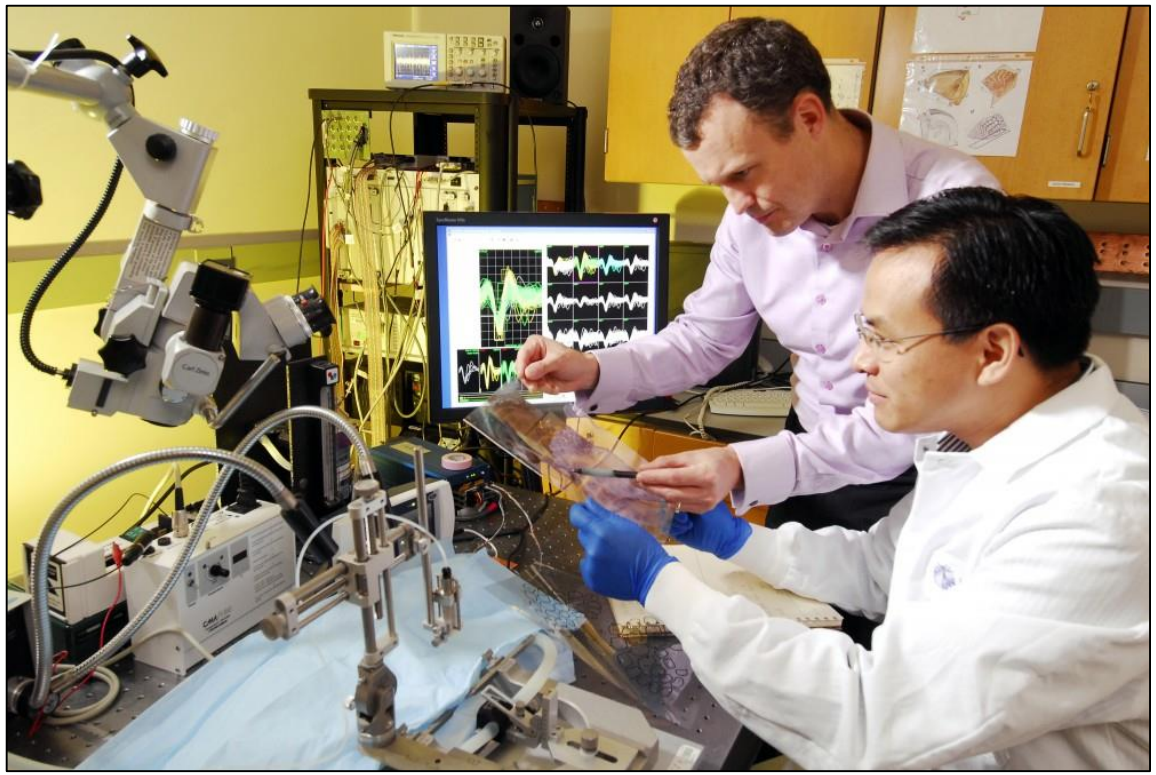
- **Bottom line up front**
- **Challenge**
- **The project**
  - Approach
  - Status

Bottom Line Up Front

MITRE

Bottom Line Up Front

MITRE is developing a Medical Device Cybersecurity training model for VA* to help raise the cybersecurity competency of Healthcare Technology Management (HTM) professionals who manage and maintain networked medical devices

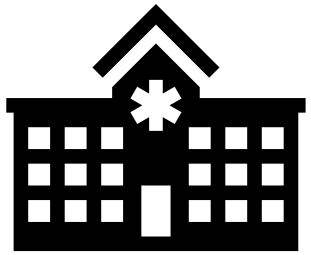


Source: http://www.industrytap.com/biomedical-engineering-revolutionizing-medicine-creating-opportunity/37543

*for VA but applicable to others in the government/healthcare community

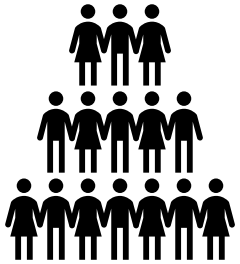
Bottom Line Up Front: U.S. Veterans Administration (VA)

- **The largest integrated health care system in the United States**
- **Current snapshot:**



1,255

Health Care Facilities

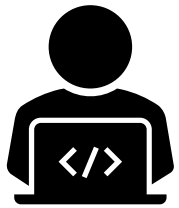


9+

Million Veterans Enrolled

55,000

Networked medical devices* (*as of 2017*)



1,300+

Healthcare Technology Management (HTM) Professionals Employed

Sources: National Center for Veterans Analysis and Statistics, www.va.gov/vetdata; *Strengthening medical device cybersecurity across the healthcare ecosystem* report, https://connect.ul.com/rs/365-LEA-623/images/LHS-UL-VA-Research-Report-StrengtheningMedicalDeviceCybersecurityAcrosstheHealthcareEcosystem.pdf; *American College of Clinical Engineering (ACCE) News,* Volume 29 Issue 3: May—June 2019

*55,000 networked medical devices within VA medical centers and clinics; there are an additional 55K++ networked, implantable or wearable medical devices on or in VA patients

MITRE

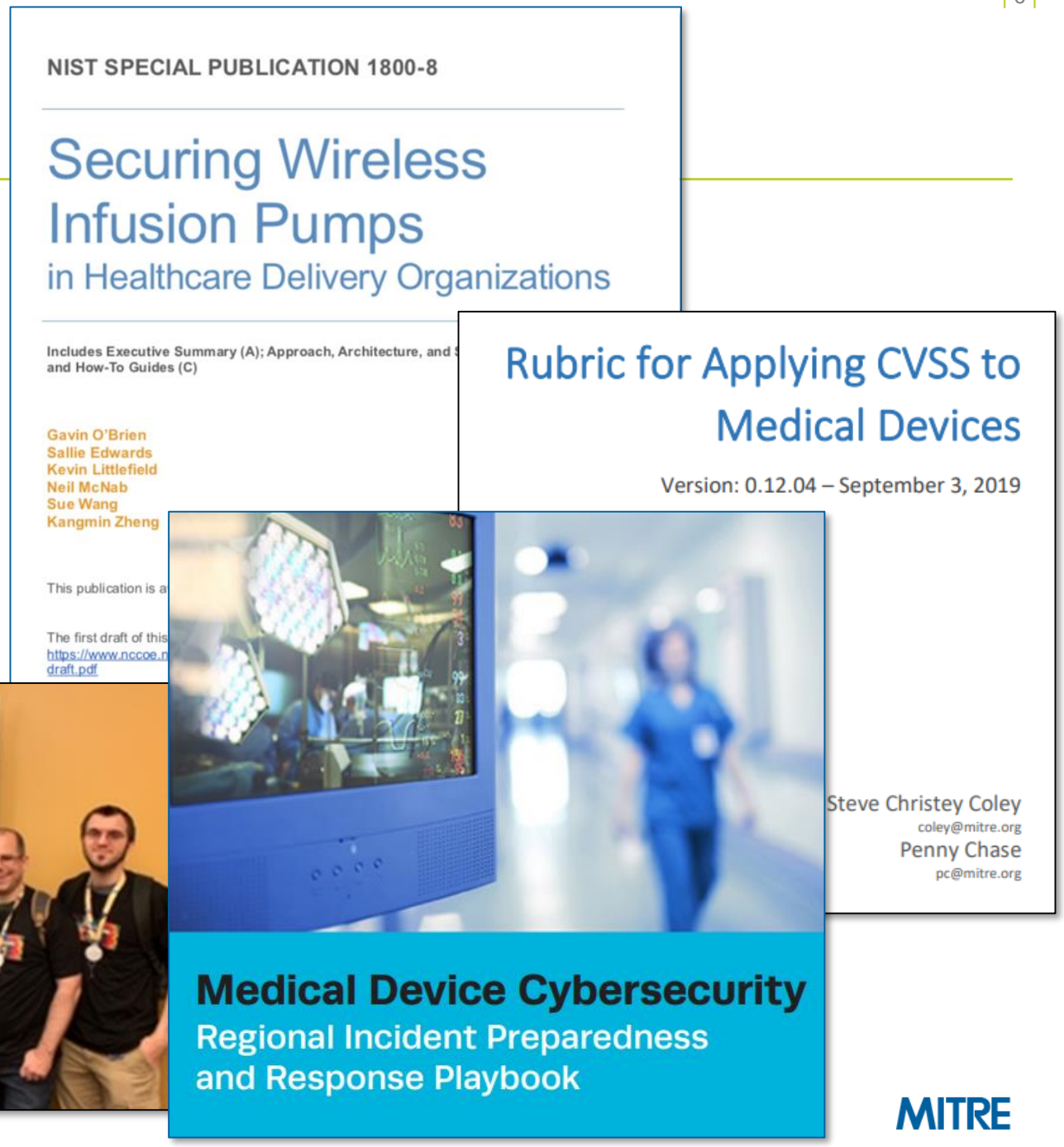
Bottom Line Up Front: The MITRE Corporation

- **Not-for-profit, trusted third party, working in the public interest**
- **Cybersecurity expertise**
- **Since 2014, has been partnering with the U.S. Food & Drug Administration (FDA) and others to improve medical device cybersecurity**

CVE®

mCODE™

ATT&CK™



MITRE

Challenge

Historical Workforce Development: Different Trajectories

Medical Devices

- **Managed by HTM professionals**
  - Biomedical engineering degree, and/or
  - Biomedical equipment technician
- **Unique hardware and function**
- **Different technologies & subspecialties**
  - Sterilization
  - Medical air
  - Imaging

- **Clinical expertise**
- **Patient safety focus**
- **Different vocabulary**
- **Organizationally within clinical organization**

IT Systems and Networks

- **Managed by IT, system, software, hardware, and network specialists**
  - Computer science, computer engineering, information systems degree, and/or
  - Systems administration
- **More commoditized hardware and software**
  - Servers
  - Operating systems
  - Laptops
  - Applications
  - EHR

- **Availability and confidentiality focus**
  - HIPAA
- **Organizationally under CIO**

https://www.securityinformed.com/insights/adapting-servers-ip-video-surveillance-systems-co-10265-ga-sb.1547618266.html

Medical Device Risks

- **Medical devices are increasingly networked**
- **Incidents with medical devices can impact patient safety**
- **Medical devices can serve as an access point to sensitive healthcare data**

The Challenge

- **Expand the scope of training for HTM professionals to include cybersecurity—tailored to medical device uses—that is designed to meet the specific needs and organization of the VA, *such as those noted in the VA HTM job description excerpts below***
  - HTMs know number/location of medical devices; understand criticality, lifecycle, and supportability issues
  - Limited applied cybersecurity competency
  - Geographically-dispersed workforce

"[illegible] guidance in [illegible] medical [illegible] ACL development."

Some Examples of Cybersecurity Risks to Networked Medical Devices[1]

Risk Description	C	A	I	PS
Failure to provide timely security software updates and patches to medical devices and networks and address related vulnerabilities in older medical devices (legacy devices)	X	X	X	X
Malware which alters data on a diagnostic device			X	X
Device reprogramming which alters device function (by unauthorized users, malware, etc.)	X	X	X	X
Denial of service attacks which make a device unavailable		X		X
Exfiltration of patient data or PHI from the network	X			

C: Confidentiality, A: Availability, I: Integrity, PS: Patient Safety

[1] *Adapted from "Health Care Industry Cybersecurity Task Force Report," June 2017*

Challenges to Securing Medical Devices

- **Medical device inventories are often incomplete**
- **Vulnerability scanning may adversely impact medical device operation**
- **Legacy devices and platforms inhibit patching of devices**
- **Medical device cybersecurity responsibilities shared among**
  - IT staff
  - Healthcare technology management (HTM) staff
  - Device manufacturers
  - Clinicians

The Project

The Approach

Bridging the Gap Between Knowledge and Competency

Training Needs Analysis

Learning Objectives

Instructional Design Methods

Learning Assessment and Evaluation

Project Status

- **Training Needs Analysis**
  - Multiple interviews
    - VA/VHA staff
    - Other government (e.g., Food and Drug Administration (FDA), Defense Health Agency (DHA), and the NIST National Cybersecurity Center of Excellence
    - Medical device manufacturers
    - Private hospitals/HDOs
    - Academia, trade associations, non-profits
  - Extensive literature survey
    - 90+ articles, books, course curricula, etc.
  - Training platform reviews
    - VA, Department of Defense, Department of Homeland Security, Coursera, SANS, MITRE Institute, university-sponsored, Biohacking Village, OpenICE, etc.

Competency Gaps Identified (partial list)*

- **Infrastructure Design:** Basic and advanced networking; configuration management
- **Threat Analysis:** Knowledge of threats and skill in identifying them
- **Vulnerabilities Assessment:** Ability to conduct vulnerability scans and recognize vulnerabilities in security systems
- **Data Privacy and Protection:** Knowledge of, and ability to apply, PHI data security standards
- **Risk Management:** HTMs as FISMA system owners and security controls assessors; RMF knowledge; system provisioning/procurement
- **Incident Management:** VA-specific incident response procedures

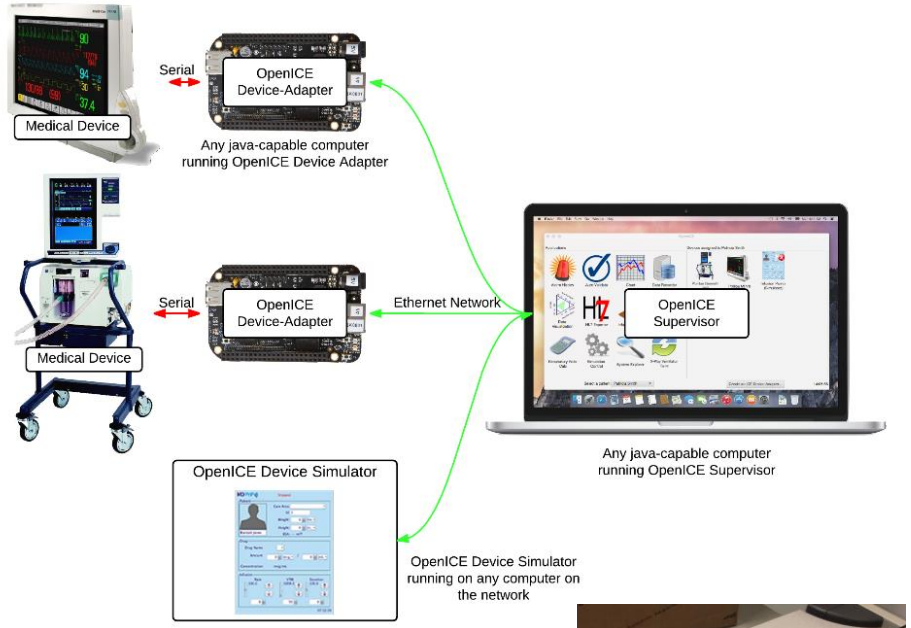
** A partial list from preliminary findings aligned to NICE competencies*

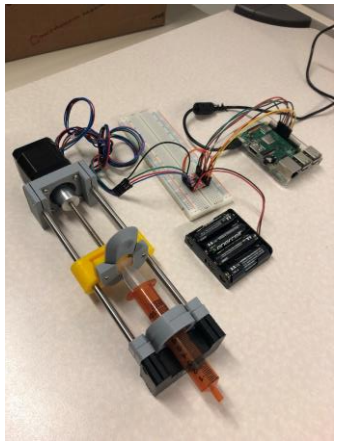
Training Needs Analysis

- **Shorter, continuous trainings**
  - Reinforce cybersecurity behavior/culture among HTMs
  - Build skills, not just awareness/compliance and information dissemination
- **Training for large, geographically dispersed workforce**
- **Desire for medical device cybersecurity certification for HTMs**
- **Build cybersecurity into Biomedical Engineering curriculum**
- **Hands-on, experiential learning is key**

Experiential Learning Approach

- **Hands-on skills training**
- **Remote access to real medical devices**
- **Remote access to virtual devices**
- **Cloud-based training**
  - Prototype on MITRE cloud
  - Evolve to VA Cloud
- **Facility Kits**
  - Prepare kits that VA admins can install at VA Medical Center (VAMCs)
- **Device Learning Kits**
  - Low-cost open source medical devices bundled with lab exercises





MITRE

Looking Ahead

- **Finalize training design document**
- **Provide recommendations and roadmap for VA HTM cybersecurity training model**
- **Parallel efforts to support training model**
  - **Continue collaboration with** U.S. Food and Drug Administration (FDA) and Defense Health Agency (DHA) and **broader health/cyber community**
  - Continue medical device cybersecurity hands-on testing, collaboration, and demonstration, within MITRE and with external partners

MITRE

MITRE is a not-for-profit organization whose sole focus is to operate federally funded research and development centers, or FFRDCs. Independent and objective, we take on some of our nation's—and the world's—most critical challenges and provide innovative, practical solutions.

Learn and share more about MITRE, FFRDCs, and our unique value at www.mitre.org

Julie Connolly, jconnoll@mitre.org

Eileen Division, edivision@mitre.org