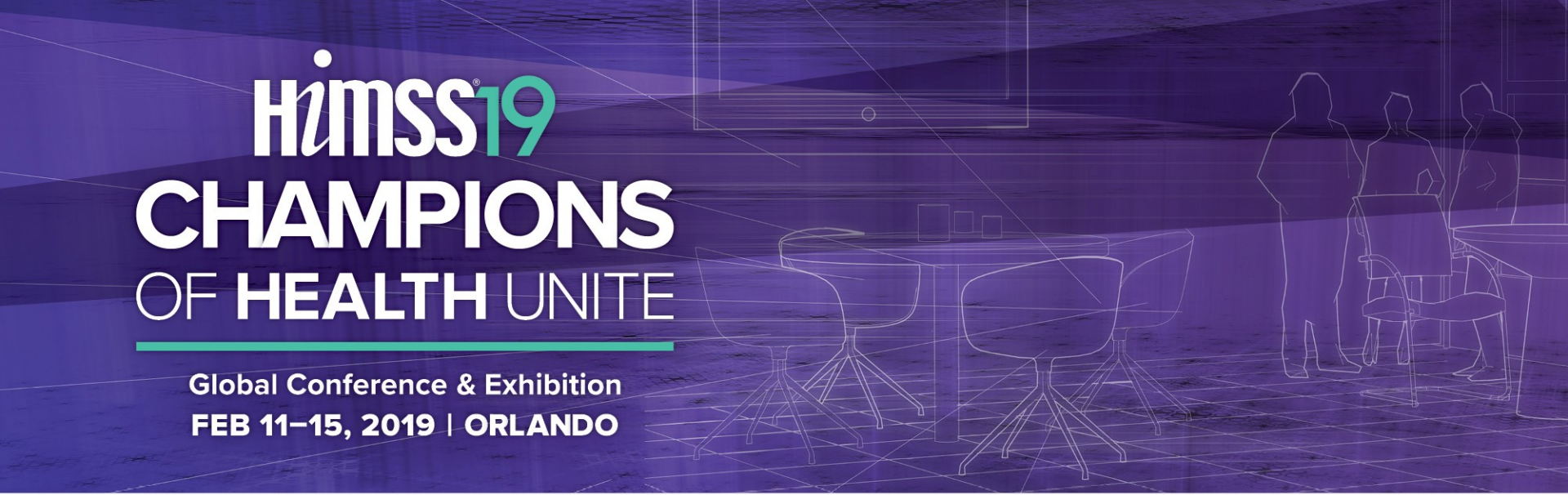


Medical Device Cybersecurity Incident Preparedness/Response

U.S. FOOD & DRUG ADMINISTRATION

Session 257, February 14, 2019

MITRE

Suzanne Schwartz, M.D., MBA, Associate Director for Science & Strategic Partnerships, Food and Drug Administration (FDA)

Margie Zuk, Senior Principal Cybersecurity Engineer, The MITRE Corporation

Conflict of Interest

Suzanne Schwartz, M.D., MBA

Margie Zuk, M.S.

Has no real or apparent conflicts of interest to report.

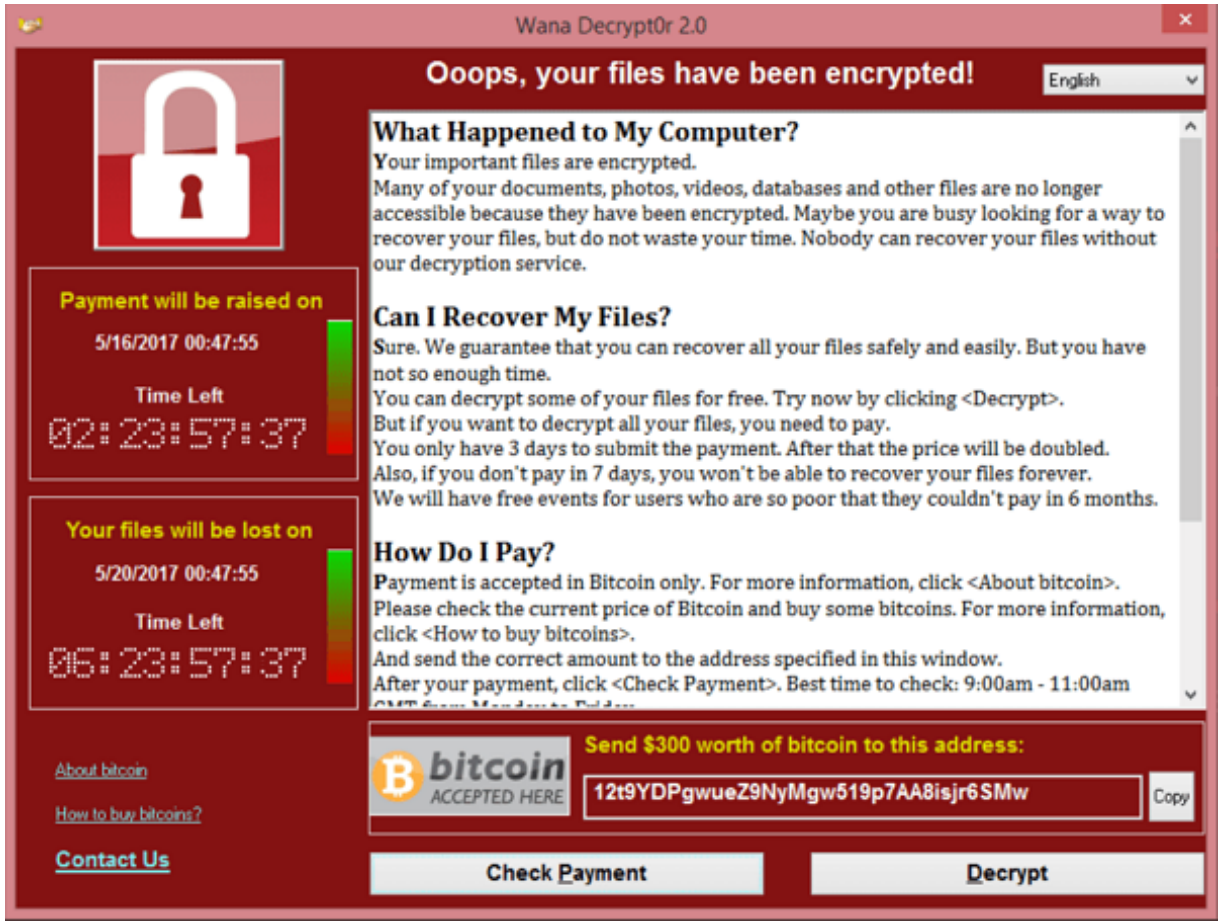
Agenda

- Medical Device Cybersecurity Incident Response Challenges
- FDA Initiatives
  - Medical Device Safety Action Plan
  - Premarket Guidance
  - Medical Device Cybersecurity Sandbox
  - Regional Response Playbook
- Future Directions

Learning Objectives

- Describe some of the challenges a Health Delivery Organization (HDO) may face in responding to a cybersecurity incident potentially affecting one or more of its medical devices
- Identify regional entities an HDO may collaborate with in preparing for and responding to a medical device cybersecurity incident
- Discuss some of the ways that HDOs and device manufacturers can improve medical device cybersecurity incident preparedness and response

Challenges



Challenges: Evolving Our Thinking

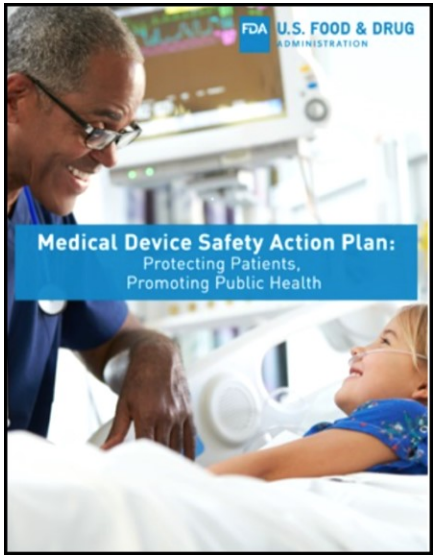
- **Coordinated** vs. **non-coordinated** disclosure of device vulnerabilities
  - Ability to get to ground truth as fast as possible so that mitigations can be proactively communicated and executed in a timely manner
    - JnJ Animas Insulin Pump
  - Non-coordinated disclosure results in delayed assessments, communications, and mitigations
    - St Jude/Abbott pacemakers and ICDs

Challenges: Evolving Our Thinking (Continued)

- Impact on HPH critical infrastructure and potential disruption of clinical care
  - Patching OS is not routine with safety-critical systems
    - WannaCry Global Cyber Attack (May 2017)
    - Petya/notPetya (July 2017)
  - Delays in diagnosis/treatment intervention can result in patient harm too
- Potential for remote, multi-patient (i.e., scaled) attack of highest concern for harm

Medical Device Safety Action Plan: Advancing Medical Device Cybersecurity

- Update 2014 premarket guidance
- Consider seeking additional premarket and postmarket authorities to:
  - Require firms to build capabilities to **update & patch device security into a product's design** and to include appropriate data supporting this capability in premarket submissions to FDA for review
  - Require firms to develop a "**Software Bill of Materials" (SBOM)** and to share with customers
  - Require that firms adopt policies and procedures for **coordinated disclosure of vulnerabilities** as they are identified



Medical Device Safety Action Plan (Continued)

- Request appropriations for seeding establishment of a **CyberMed Safety (Expert) Analysis Board (CYMSAB)** functioning as a public-private model, and serving the ecosystem as a neutral entity

2018 Highlights

- *Medical Device Safety Action Plan* (April 2018)
- Perspective piece in American Heart Association Journal *Circulation* (September 2018)
- FDA Commissioner's Statement (October 2018):
  - Strong commitment to efforts that bolster medical device cybersecurity
  - Regional Incident Preparedness & Response Playbook – MITRE publication (October 2018)
  - Execution of 3-way MOUs with H-ISAC for 2 newly stood up ISAOs for medical device vulnerability reporting (October 2018):
    - MedISAO
    - Sensato

2018 Highlights (Continued)

- Report on Advancing Coordinated Vulnerability Disclosure – MDIC publication (October 2018)
- Execution of Memorandum of Agreement with Department of Homeland Security (October 2018)
- New FDA Draft Premarket Cybersecurity Guidance & Announcement of FDA-convened Public Workshop, January 29-30, 2019

2018 Premarket Draft Guidance: Revision Background

- New guidance is needed as medical device cybersecurity continues to evolve
- Changes proposed to the guidance based on lessons learned from routine vulnerability management, response activities, engaging stakeholders including working with manufacturers pre- and post-market.
- Examples of recent threats:
  - Malware/ransomware attacks, e.g., WannaCry, notPetya, Meltdown and Spectre

Revision Approach

- Leveraged the 2014 premarket guidance document
  - Kept alignment with NIST 5 core functions
  - Similar structure
  - Maintained focus on documentation related to requirements of the QSR (21 CFR Part 820)
- Provided additional granularity to help manufacturers implement cybersecurity in the premarket setting
  - Expanded on maintaining properties of authenticity, availability, integrity, and confidentiality through design, risk management, and labeling
  - Labeling grounded in statutory and regulatory requirements; for example:
    - Adequate directions for use, 21 CFR 801.5
    - For prescription devices, 21 CFR 801.109(c)

What's New

- Designing trustworthy devices
- Preventing multi-patient attacks
- Tiering system – information to be provided in premarket submission is geared to level of risk:
  - Tier 1 – higher risk
  - Tier 2 – lower risk
- Cybersecurity Bill of Materials
  - Leverages purchasing controls in QSR (21 CFR 820.50)
- System level threat models

Tier Criteria

Tier 1 "Higher Risk"

A device is a Tier 1 device if the following criteria are met:

- The device is capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, or to a network, or to the Internet; AND
- A cybersecurity incident affecting the device could directly result in patient harm to multiple patients.

Examples of Tier 1 devices:

implantable cardioverter defibrillators (ICDs), pacemakers, left ventricular assist devices (LVADs), brain stimulators and neurostimulators, dialysis devices, infusion and insulin pumps; and the supporting connected systems that interact with these devices such as home monitors and those with command and control functionality such as programmers.

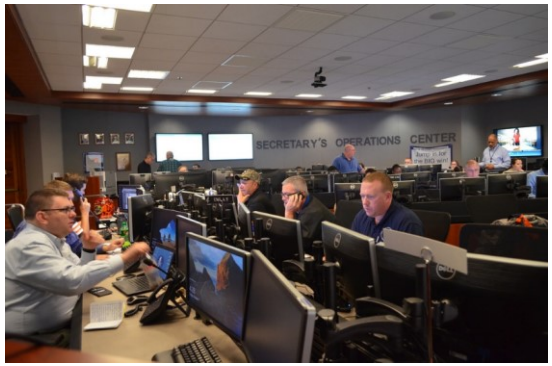
Tier Criteria (Continued)

Tier 2 “Standard Risk”

- A medical device for which the criteria for a Tier 1 device are not met.

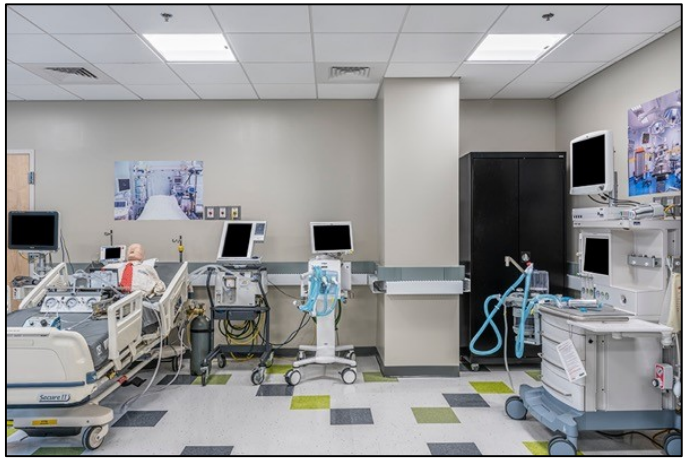
Improving Preparedness and Response for Medical Device Cybersecurity Events

- Preparedness
  - Pre-position research about medical device vulnerabilities and proposed mitigations
    - ➢ Develop **medical device cybersecurity sandbox**
- Response
  - Enhance readiness and coordinated response to exploits or attacks affecting medical devices across all levels of government as well as the user community
    - ➢ Develop **regional medical device preparedness and response playbook**



Medical Device Cybersecurity Sandbox

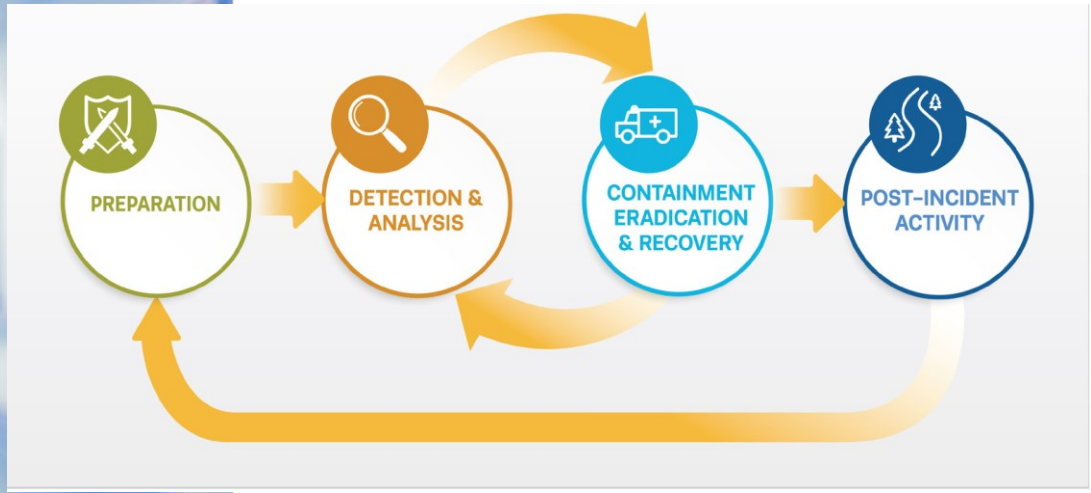
- **Collaboration between Partners Healthcare/MGH's Medical Device Plug and Plan (MD PnP) Lab, MITRE, and FDA**
  - Working with medical device manufacturers to validate the concept of a cyber sandbox using physical devices in a realistic biomedical environment
  - Developing clinical scenarios and use cases based on devices and known vulnerabilities
  - Develop and validate mitigations
  - Red teaming / penetration testing the devices



Playbook for Responding to Significant Cybersecurity Events

- *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook*
  - Published playbook based on:
    - input from HDO focus groups
    - observing cybersecurity exercises in NY and DE
    - organizing a Boston-area workshop on WannaCry experiences
  - Playbook goal: better integrate cyber, clinical and preparedness/ response activities

Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook



Draft Published October 2018:
https://www.mitre.org/securemed

Comments accepted at securemed@mitre.org

Looking Ahead 2019

- Complete CVSS clinical rubric & submit for Medical Device Development Tool (MDDT) qualification
- Further enhance public-private partnership collaborations to collectively address CISA
  - Healthcare Industry Cybersecurity Task Force
  - 405D
  - HSCC Task Group 1B *Joint Security Plan*
  - Dedicated effort on defining and operationalizing Software Bill of Materials
- CYMSAB Pilot currently under development (with MITRE support)
- Additional ISAOs in formation for device vulnerability info-sharing

Looking Ahead 2019 continued

- International Medical Device Regulators Forum (IMDRF) new medical device cybersecurity work item:
  - FDA and Health Canada co-leads
- Expand x-stakeholder participation in DefCon Biohacking Village Device Hacking Lab, with the following goals:
  - Increase medical device manufacturer (MDM) presence
  - Introduce to clinical community
  - Engage HDOs
- Leverage cross-agency / multi-stakeholder collaborative efforts:
  - NTIA (Dept of Commerce) Multi-stakeholder engagement on software component transparency includes representation on WGs from: HDOs, MDMs, device trade organizations and FDA
  - NCCoE (NIST/Dept of Commerce) working with industry to develop use cases for medical device security

Questions?

- Please complete online session evaluation

#HIMSS19

Medical device cybersecurity is a shared responsibility

Your input is important to us!

Suzanne.Schwartz@fda.hhs.gov

Or email the FDA team:
CyberMed@fda.hhs.gov

Margie Zuk, mmz@mitre.org

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm