Healthcare Cybersecurity Preparedness & Response

Margie Zuk and Penny Chase

March 7, 2018

HIMSS Federal Health IT Solutions Pavilion

MITRE

Bottom Line Up Front

- **Recent events, such as the WannaCry attack, have demonstrated that medical device cybersecurity preparedness and response activities are critical for healthcare delivery organizations (HDOs)**
- **FDA is actively helping HDOs evolve their medical device cybersecurity preparedness and response activities**
- **In particular, FDA and MITRE are developing a regional medical device cybersecurity preparedness and response playbook, and we're seeking your input on it**

Medical Devices in the Clinical Environment

- **The health care and public health (HPH) critical infrastructure sector represents a significantly large attack surface for national security today**
- **Connected medical devices, like all other computer systems, incorporate software that are vulnerable to threats**
- **We are aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations**
- **When medical device vulnerabilities are not addressed and remediated, they can serve as access points for entry into hospital/health care facility networks**

FDA's Goals for Medical Device Cybersecurity

- **Meet FDA's Center for Devices and Radiological Health's (CDRH) mission:** ***safe and effective devices***
- **Goals**:
  - Raise cybersecurity awareness
  - Promote safety and security by design through establishing clear regulatory expectations
  - Promote coordinated vulnerability disclosure & proactive vulnerability management
  - Minimize reactive approaches
  - Foster *"whole of community"* approach

FDA and CAMH*

- **MITRE helping to advance the FDA medical device cybersecurity vision**
  - Medical device cybersecurity stakeholder engagement study and gap analysis
  - Tailoring the Common Vulnerability Scoring System for healthcare
  - Participating in medical device vulnerability and threat information sharing activities
  - Evolve processes for preparedness and response related to medical device cybersecurity events at the Federal and regional levels

* The MITRE Corporation operates the Centers for Medicare & Medicaid Services (CMS) Alliance to Modernize Healthcare (CAMH), a federally funded research and development center (FFRDC) dedicated to strengthening the nation's health care system. MITRE operates CAMH in partnership with CMS and the Department of Health and Human Services.

WannaCry Attack

- **Starting on May 12, 2017, the WannaCry ransomware affected millions of unpatched Windows machines in over 150 countries**
- **Impact on the healthcare sector**
  - UK National Health Services hard hit (34% of trusts affected)
    - Thousands of appointments and operations canceled
    - Patients diverted
  - Medical devices were also affected

US Federal Response to WannaCry Attack

- **On May 12, HHS Secretary activated the Secretary's Operation Center (SOC)**
  - HHS activated its Emergency Management Group to support internal response and private sector
  - Began coordinating the U.S. investigation into incident with respect to the HPH Sector
- **Assistant Secretary for Preparedness and Response (ASPR)/Critical Infrastructure Protection (CIP) coordinated the response**
  - Held daily sector-wide call
  - Held daily calls with key trade association partners
  - Coordinated messaging across sector
  - Coordinated with DHS, FBI, and CIP partners

FDA Identified a Need to Improve 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 FDA and regional medical device preparedness and response playbooks

MITRE

Regional Healthcare Delivery Organization Medical Device Cybersecurity Workshop – December 2017

- **MITRE and the Partners/MGH Medical Device Plug and Play (MD PnP) Lab organized a workshop to**
  - Share lessons learned from managing medical devices during the WannaCry attack
  - Identify opportunities to better prepare health systems for future cyber attacks
  - Identify opportunities to improve regional and national sharing
  - Compile key meeting takeaways to inform FDA
- **Brought together information security staff, information technology staff, biomedical engineers, and clinicians from Boston-area hospitals**
- **Observations**
  - Manufacturers' responses varied in terms of amount/quality of information and patching/mitigation timelines
  - Used various sources of information – social media and personal network, ICS-CERT, HHS calls, NH-ISAC

Key Take-aways from Workshop

- **HDOs need actionable information (not just "good cyber hygiene"): Is there a vulnerability? What is it? Can we fix it and how? Timeline? Cost?**
- **Managing medical device inventories and patching requires coordination and strategy**
- **Incident response planning**
  - Needs to include cybersecurity
  - Should take into account the types of devices impacted and the effect on device operation
  - Conduct regular reviews of plans and exercise/train
- **Saw value of cybersecurity sandbox**
  - Could be a "Go To" site for regional HDOs and manufacturers to come together an test, evaluate, and communicate

Medical Device Cybersecurity Sandbox Goals

- **The ability to test and validate vulnerabilities, mitigation strategies, and cyber resilient, clinical configurations that enable continued clinical operation in the face of cyber-physical hazards, in support of local, regional, and national preparedness goals.**
- **A realistic, biomedical environment that supports both preparedness exercises and live cyber-physical incident response activities, with the capability to test solutions in real time.**
- **The identification and sharing of medical device vulnerabilities, vetted mitigation strategies, and cyber resilient configurations, in direct support of the FDA's postmarket guidance policy calling for greater transparency and adoption of coordinated vulnerability disclosures.**

Collaboration Between Partners Healthcare/MGH MD PnP Lab, MITRE, and FDA

- **Cybersecurity Sandbox Approach**
  - Develop overarching test strategy
  - Select devices
    - Develop test plans
    - Execute test plans
    - Report results
- **Leverage MD PnP Lab Capabilities**
  - Advanced re-configurable networking infrastructure and tools to support research in
    - Interoperability
    - Cybersecurity
    - Biomedical Engineering/Computer Science/Cyber Physical Systems/Medical IoT
    - Clinical workflow simulation
  - Diverse medical technology
    - Patient monitors, infusion pumps, ventilators, IoT devices, etc.
    - Patient simulators - Electronic, mechanical, and software

MITRE

Develop Repeatable and Scalable Medical Device Cybersecurity Response Processes for Regions and FDA

- Increased cyber mutual aid across hospitals
- Enhanced and expanded collaboration across stakeholders in the medical device ecosystem
- Clarification of lines of communication and concept of operations (CONOPs) across hospitals, medical device manufacturers, state and local government and federal government
- A regional preparedness and response model for medical device cyber resiliency that can be implemented in regions across the nation
- Increased awareness and capability for FDA HQ and field staff to respond to medical device cybersecurity public health concerns

Playbooks for Responding to Significant Cybersecurity Events

- **Develop FDA and regional medical device cybersecurity playbooks focused on medical device cybersecurity preparedness and response activities that may result from large-scale threats or vulnerabilities that may have multi-patient patient safety impacts**
  - Regional playbook will draw upon regional cyber preparedness exercises, cybersecurity clinical simulations, and stakeholder feedback
  - FDA playbook will draw upon previous vulnerability disclosure table top exercises, the regional exercises, lessons learned from WannaCry, and FDA's pre- and post-market medical device cybersecurity guidance cybersecurity public health response

Regional Playbook

- **Purpose – serve as a model for regional readiness and response activities to ensure that HDOs can address emerging cybersecurity threats**
- **Audience – HDO staff responsible for preparedness and response activities for medical device cybersecurity**
- **Leverages**
  - NIST's Computer Security Incident Handling Guide (NIST SP 800-61 rev 2)
  - CMS Core Elements of Emergency Preparedness
- **Preparation**
  - Establish team that includes IT, information security, privacy, clinical, compliance, legal, public affairs, facilities management, business continuity/disaster response
  - Identify external stakeholders including device manufacturers, SW vendors, customers, law enforcement, Internet Service Providers, Information Sharing and Analysis Organizations
  - Develop plan
  - Exercises and training – tabletops, emergency preparedness exercises, clinical simulations, cyber ranges

Regional Playbook (Continued)

- **Detection**
  - Identified by HDO during procurement or operations
  - External communication from device manufacturers, peers, National Health Information Sharing and Analysis Center (NH-ISAC), Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) advisory, FDA safety notice, InfraGard (FBI)
- **Classify and Handle Incident**
  - Type
  - Severity – Impact? How widespread? Zero day?
  - Impact to operations and level of effort for resolution
- **Communications Strategy**
  - Internal – e.g., the IR team, impacted staff, C-Suite
  - External – e.g., device manufacturer, partners, customers, compliance and regulatory, law enforcement, public affairs messaging

Questions for Discussion

- What information are you looking for in a medical device cybersecurity playbook to help evolve your preparedness and response activities?
- What are your pain points during a cybersecurity event?
- What are your information sources during a cyber incident?
- Are you able to obtain all the information you need to help resolve a cyber incident? If not, what's missing?
- Whom do you work with internally (e.g., IT, biomedical engineering,) and externally (e.g., state department of health, public safety office, healthcare coalitions, manufacturers)?

Follow up

To download a copy of this presentation, visit:

https://health.mitre.org/himss18

Protecting Data
& Devices

Follow us on social media: @MITREhealth

MITRE