Healthcare Provider Cybersecurity Call:
- Overview of the Regional Preparedness and Response Playbook
- Focus on mitigating attacks and enhancing resilience

Penny Chase & Matt Weir

12 June 2024
MITRE HealthCARE Lab
Health Cybersecurity and Resiliency Experimentation
## Managing All-Hazards Risks in the HPH Sector

<table>
<thead>
<tr>
<th>Identify Risks</th>
<th>Identify and prepare for a range of potential threats and hazards.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce Vulnerabilities</td>
<td>Reduce the vulnerabilities of identified critical assets, systems, and networks, including those associated with critical internal and out-of-sector dependencies and interdependencies.</td>
</tr>
<tr>
<td>Mitigate Impacts</td>
<td>Mitigate the potential impacts to critical infrastructure and enable the timely restoration of functionality when events and incidents do occur.</td>
</tr>
<tr>
<td>Enhance Resilience</td>
<td>Adapt to changing conditions to withstand and rapidly from disruption due to emergencies, irrespective of the cause of the disruption (manmade or natural).</td>
</tr>
</tbody>
</table>

Source: Healthcare and Public Health Sector-Specific Plan (May 2016)
Healthcare Cyber Attacks are Increasingly Common

Ransomware attack disrupts Irish health services

Healthcare Vendor Ransomware Attack Stalls Cancer Treatments, 170 Health Systems Hit

UVM Health Brings EHR Back Online, One Month After Ransomware Attack

Healthcare hackers demanded an average ransom of $4.6M last year, says BakerHostetler

The report found that healthcare was one of the industries most affected by tracked ransomware incidents in 2020, second only to education.
Putting Numbers Into Perspective

6146 hospitals in the United States

141 hospitals impacted by ransomware in 2023*

That's over 2% of hospitals in the US

Cyber Attacks Compared To Other Disasters

**Differences**
- Cyber attacks tend to take longer to fully recover from
- Attackers can subvert backup and recovery processes
- Cyber attacks against other orgs can impact you
- A tornado isn’t going to sell patient data on the dark web

**Similarities**
- Preparedness requires close coordination between IT, Operations, and Emergency Preparedness teams.
- Regional relationships are important to be able to respond and continue to provide care
- Developing plans and practicing your response can help your facility to weather the storm
Regional Preparedness and Response Playbook

- After the WannaCry attack in 2017, FDA asked MITRE to develop the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook
- FDA asked MITRE to revise the playbook to better address the evolution of ransomware attacks, emerging medical device technologies (e.g., cloud), and cybersecurity initiatives across the health sector

- Published November 2022
  
Playbook Overview

- Based on NIST’s Computer Incident Response Handling Guide (NIST SP 800-61r2)
- Integrates cyber response with Health Incident Command Structure
- Emphasizes importance of regional relationships for response
- Provides suggestions for developing and conducting cyber exercises
- Includes list of resources for more detailed information and information on how to reach out to government resources (including state, HHS, DHS, and FBI)
- Developed Quick Start Companion Guide to orient new playbook users and help all users quickly identify the key parts of the playbook to turn to during a cyber incident
Example - Healthcare Incident Command System

- Entity Commanders
  - Incident Commander
    - Deputy IC
  - Communications Working Group
    - Community Health/Equity
    - Public Information Officer
    - Legal Advisor
    - Nursing Advisor
    - People Advisor
    - Chief Medical Officer

- Operations Section Chief
  - Deputy Hospital
  - Deputy Ambulatory
  - Deputy General

- Planning Section Chief
  - Deputy

- Logistics Section Chief
  - Deputy

- Finance Section Chief
  - Deputy

- Emergency Medicine
- Acute Care Hospitals
- Specialty Hospitals
- Post-Acute/Home Services
- Lab/Pathology
- Behavioral Health

- Research
- Education
- Policy

- Quality and Safety
- Gov. Affairs
- Compliance
- Credentialing
- Recovery

- HR/Workforce Support
- Labor Pool
- Reporting Analytics
- Documentation

- Digital/IS/Telecom
- Supply Chain
- Biomedical
- Security
- Facilities/Real Estate
- Pharmacy

© 2024 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 24-1708.
Preparing Regional Responses

Cybersecurity incidents are a regional risk

Recovering from them requires a regional response
# Quick Start Guide

## MEDICAL DEVICE CYBERSECURITY REGIONAL INCIDENT PREPAREDNESS AND RESPONSE PLAYBOOK QUICK START COMPANION GUIDE

### Regional Medical Device Cyber Incident Preparedness and Response (Section 5)

#### Regional Preparedness (Section 5.1)

Develop mutual aid agreements with regional partners for medical device cybersecurity, or supplements as part of broader incident response mutual aid agreements—to include loaner devices, diverting patients to a facility with operational devices, and incident response assistance.


Establish and exchange point of contact (POC) names and contact information with regional partners, to include public key infrastructures (PKIs) for more sensitive communications, as applicable.


Ensure that all key HDO medical device cybersecurity personnel have access to alerts disseminated via the regional health emergency response communication system, such as the state Health Alert Network (HAN).


Conduct joint exercises with regional partners and participate in collaborative clinical simulations.


Identify a primary and backup regional incident command/coordination center for use during incidents (e.g., state CCIC, state Emergency Response command center).

- [https://emsa.ca.gov](https://emsa.ca.gov)

... (Continues) ...
Establish and exchange point of contact (POC) names and contact information with regional partners, to include public key infrastructures (PKIs) for more sensitive communications, as applicable.
Running Cyber Table-Top Exercises (TTxs)

From: HackU<exercise_redacted>@protonmail.com
Sent: Friday, November 5, 202
To: <exercise_redacted>
Subject: RE: Our ownership of all your systems

It’s good to communicate directly. We want to resolve this for everyone involved as quickly as possible. Upon payment we will help you get your systems operational as quickly as possible. We will also remove ourselves from your network. If you don’t pay us though, we can’t be held responsible if other things break. The longer you wait, the higher chance things go wrong. Maybe it requires more work on our end? If so, the price we’re charging you go up. Don’t try to mess with us. Just pay us and we can put this all behind us.

Remember, 1 million dollars in BTC to the wallet:

1CvBMSEYst<exercise_redacted>

If you have any problems buying bitcoin let us know. We offer top tier service and support. It’s in everyone’s best interest that we get paid! If you have any questions, please reach out to us. We hope to resolve this quickly for everyone involved. Once we have our money, we can get your systems back up and delete all these files.

--------FOR EXERCISE USE ONLY--------
- This is for a Cybersecurity Exercise   -
--------FOR EXERCISE USE ONLY--------
Cyber exercises are emergency preparedness exercises!!!

Clinical and Emergency Management experts are required
Lessons Learned From Exercises (2 of 2)

- Understanding impacts of response actions is hard
  - What happens when you lose internet connectivity?
- Response coordination is hard
- Exercises can help develop a sense of understanding about how different teams can partner together
- It’s important to have a response plan before an event occurs, and update it based on the exercise findings
What resources are currently available?
Ransomware Resource Center

https://healthcyber.mitre.org
Questions?

Penny Chase
pc@mitre.org
linkedin.com/in/pennychase/

Matt Weir
cweir@mitre.org
linkedin.com/in/matt-weir-54a2192

Download the playbook:
Resources
Healthcare Cybersecurity Resources (1/5)

- **FDA**
  - [Cybersecurity | FDA](https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity)
  - MITRE/FDA article - [The Evolving State of Medical Device Cybersecurity | Biomedical Instrumentation & Technology](https://array.aami.org/doi/10.2345/0899-8205-52.2.103)
  - MITRE products sponsored by FDA
    - [Rubric for Applying CVSS to Medical Devices | MITRE](https://www.mitre.org/news-insights/publication/rubric-applying-cvss-medical-devices)
Healthcare Cybersecurity Resources (2/5)

- **HHS**
  - [HPH Cybersecurity Gateway](https://hhs.gov): HPH Cybersecurity Gateway (hhs.gov)
  - [ASPR TRACIE Cybersecurity](https://asprtracie.hhs.gov/cybersecurity)
  - [HHS 405(d) - Health Care Industry Practices (HICP) and Hospital Resiliency Landscape Analysis](https://405d.hhs.gov/information)
  - [Health Sector Cybersecurity Coordination Center (HC3)](https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html)

- **DHS Cybersecurity & Infrastructure Security Agency (CISA)**
  - [Healthcare and Public Health Sector: Strengthen your Defenses and Mature your Cybersecurity Efforts | CISA](https://www.cisa.gov/

- **NIST National Cybersecurity Center of Excellence (NCCoE)**
  - [Healthcare Projects](https://www.nccoe.nist.gov/healthcare)
Healthcare Cybersecurity Resources (3/5)

- **Sector Activities**
  - Cybersecurity Information Sharing Act (CISA) of 2015 Health Care Industry Cybersecurity Task Force:
    https://www.phe.gov/Preparedness/planning/CyberTF/Pages/default.aspx
  - Health Sector Coordinating Council (HSCC) Cybersecurity Working Group
    - **Home Page**: https://healthsectorcouncil.org/
    - **2024 Task Groups**: https://healthsectorcouncil.org/task-groups/
Healthcare Cybersecurity Resources (4/5)

- **Sector Activities**
  - Health Sector Coordinating Council (HSCC) Cybersecurity Working Group
    - Publications – some selected ones:
      - [Cybersecurity for the Clinician Video Series](https://healthsectorcouncil.org/cyberclinicianvideos/)
      - [HPH Cybersecurity Framework Implementation Guide](https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx)
      - [Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)](https://healthsectorcouncil.org/info-sharing-guide/)
Healthcare Cybersecurity Resources (5/5)

- **Sector Activities**
  - Health Sector Coordinating Council (HSCC) Cybersecurity Working Group
    - **Publications** – some selected ones:
      - **Health Industry Cybersecurity Managing Legacy Technology Security (HIC-MaLTS):**
      - **Model Contract-Language for Medtech Cybersecurity (MC2):** https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/