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

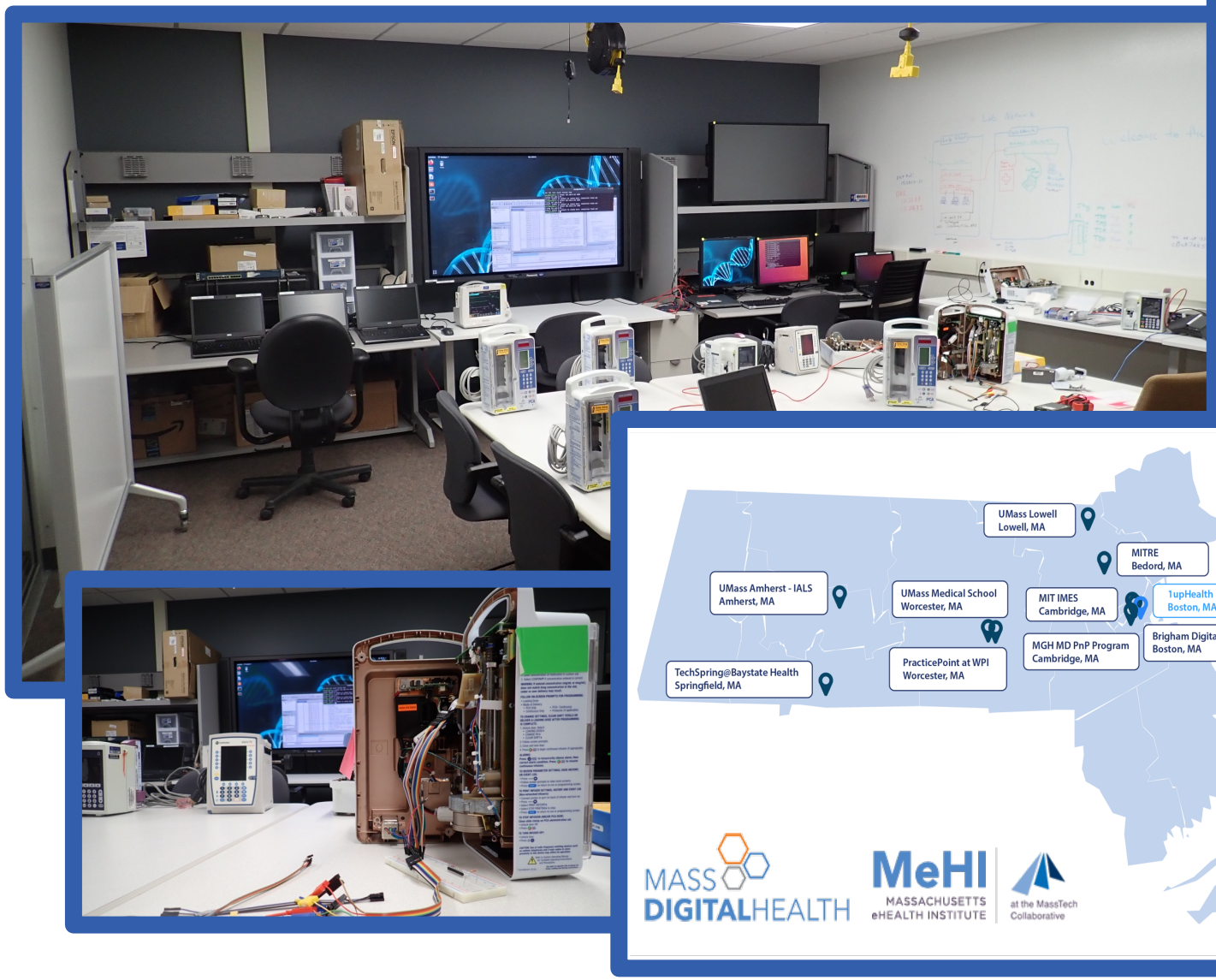
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

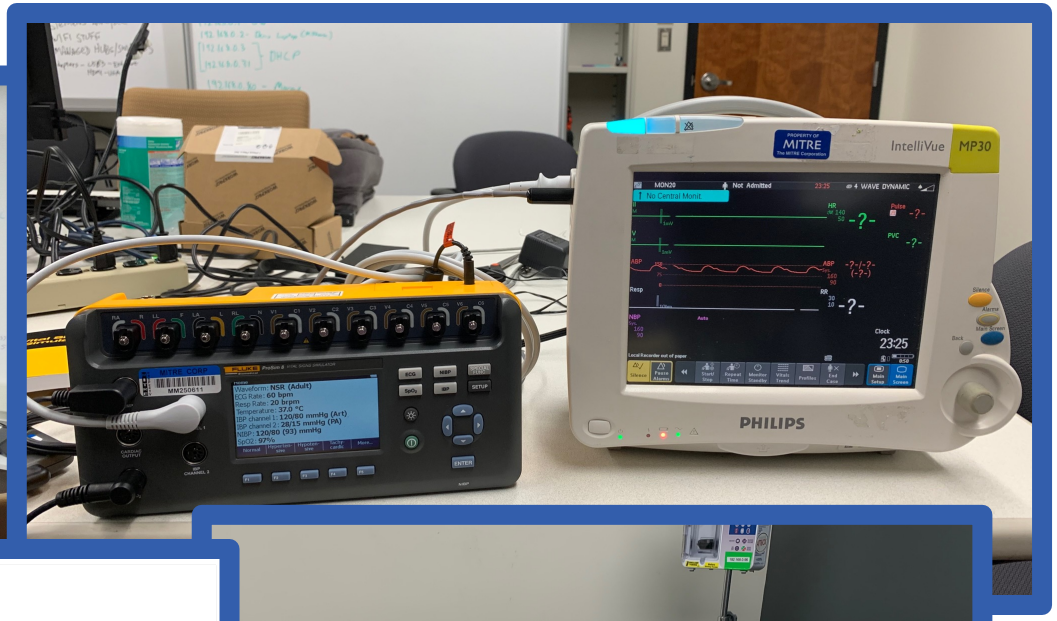
Penny Chase
MITRE

Matt Weir, PhD
MITRE

MITRE HealthCARE Lab

Health Cybersecurity and Resiliency Experimentation





Managing All-Hazards Risks in the HPH Sector

Identify Risks

- Identify and prepare for a range of potential threats and hazards.

Reduce Vulnerabilities

- Reduce the vulnerabilities of identified critical assets, systems, and networks, including those associated with critical internal and out-of-sector dependencies and interdependencies.

Mitigate Impacts

- Mitigate the potential impacts to critical infrastructure and enable the timely restoration of functionality when events and incidents do occur.

Enhance Resilience

- Adapt to changing conditions to withstand and rapidly from disruption due to emergencies, irrespective of the cause of the disruption (manmade or natural).

Source: Healthcare and Public Health Sector-Specific Plan (May 2016)

MITRE

Healthcare Cyber Attacks are Increasingly Common

Search US edition

The Guardian

News website of the year

Ransomware attack disrupts Irish health services

IT systems shut down and some medical appointments cancelled after attempt to access data

Compliancy Group

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

HEALTH IT SECURITY

xtelligent HEALTHCARE MEDIA

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

SC MEDIA

TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION

Scripps Health cyberattack, EHR downtime caused $112.7M in lost revenue, recovery

Jessica Davis August 12, 2021

Healthcare IT News

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.

JAMA Network Open

Original Investigation | Emergency Medicine

Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US

Christian Dameff, MD, MS; Jeffrey Tully, MD; Theodore C. Chan, MD; Edward M. Castillo, PhD, MPH; Stefan Savage, PhD; Patricia Maysent, MHA, MBA; Thomas M. Hemmen, MD, PhD; Brian J. Clay, MD; Christopher A. Longhurst, MD, MS

Abstract

IMPORTANCE Cyberattacks on health care delivery organizations are increasing in frequency and sophistication. Ransomware infections have been associated with significant operational disruption, but data describing regional associations of these cyberattacks with neighboring hospitals have not been previously reported, to our knowledge.

OBJECTIVE To examine an institution's emergency department (ED) patient volume and stroke care metrics during a month-long ransomware attack on a geographically proximal but separate health care delivery organization.

DESIGN, SETTING, AND PARTICIPANTS This before and after cohort study compares adult and pediatric patient volume and stroke care metrics of 2 US urban academic EDs in the 4 weeks prior to the ransomware attack on May 1, 2021 (April 3-30, 2021), as well as during the attack and recovery (May 1-28, 2021) and 4 weeks after the attack and recovery (May 29 to June 25, 2021). The 2 EDs had a combined mean annual census of more than 70 000 care encounters and 11% of San Diego County's total acute inpatient discharges. The health care delivery organization targeted by the ransomware constitutes approximately 25% of the regional inpatient discharges.

Key Points

Question What are the associated regional health care disruptions in hospitals adjacent to health care systems under ransomware cyberattack?

Findings This cohort study of 2 academic urban emergency departments (EDs) adjacent to a health care delivery organization under a month-long ransomware attack evaluated 19 857 ED visits at the unaffected ED: 6114 in the preattack phase, 7039 in the attack and recovery phase, and 6704 in the postattack phase. During the attack and postattack phases, significant increases in patient

MITRE

Putting Numbers Into Perspective

6146 hospitals in the United States

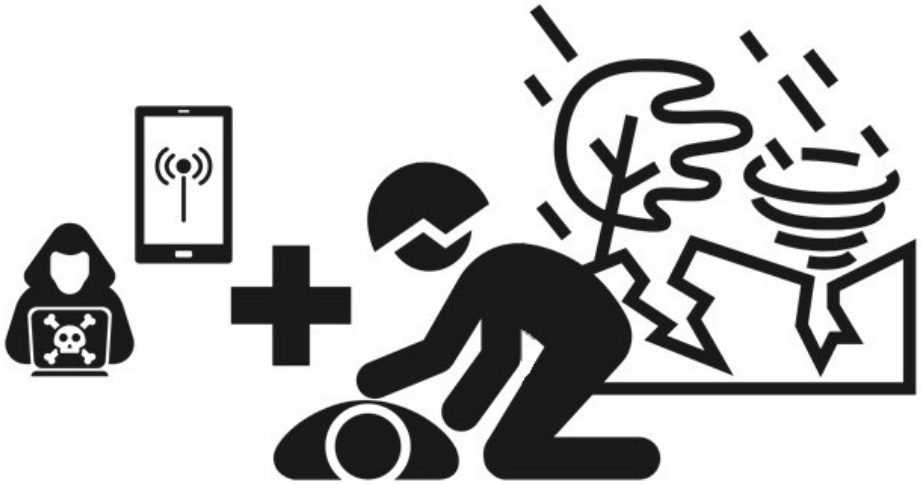
141 hospitals impacted by ransomware in 2023*

That’s over 2% of hospitals in the US

*Source: https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/

MITRE

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

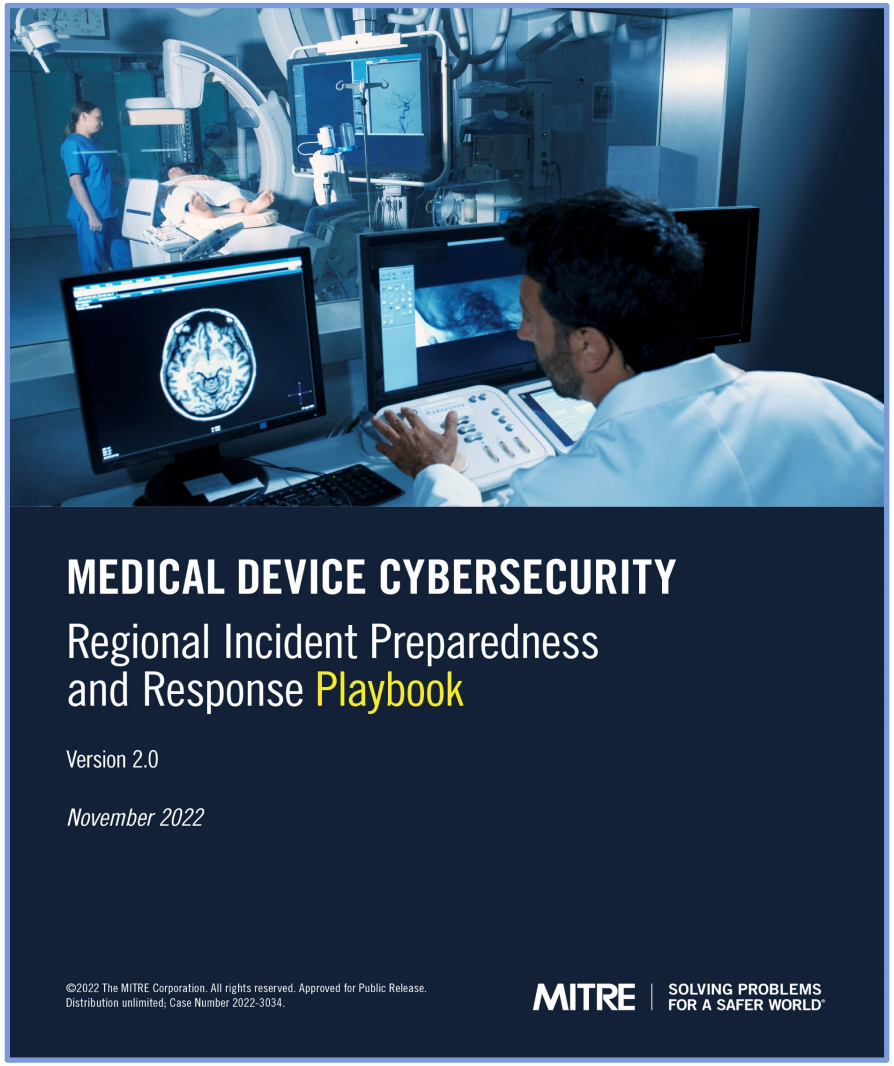
- Preparedness requires close coordination between IT, Operations, and Emergency Preparedness teams.
- Regional relationships are important to be able to respond and continue to provide care
- Developing plans and practicing your response can help your facility to weather the storm

MITRE

Regional Preparedness and Response Playbook

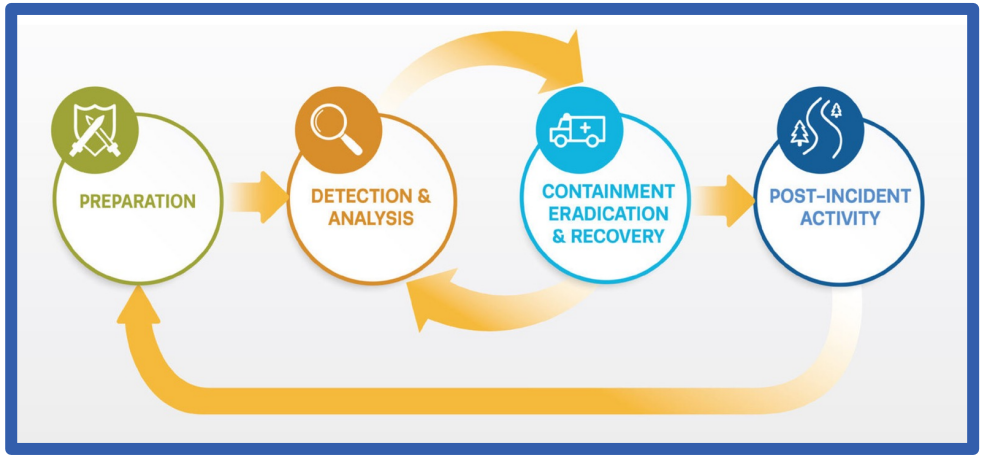
- After the WannaCry attack in 2017, FDA asked MITRE to develop the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook
- FDA asked MITRE to revise the playbook to better address the evolution of ransomware attacks, emerging medical device technologies (e.g., cloud), and cybersecurity initiatives across the health sector
- **Published November 2022**

  https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response

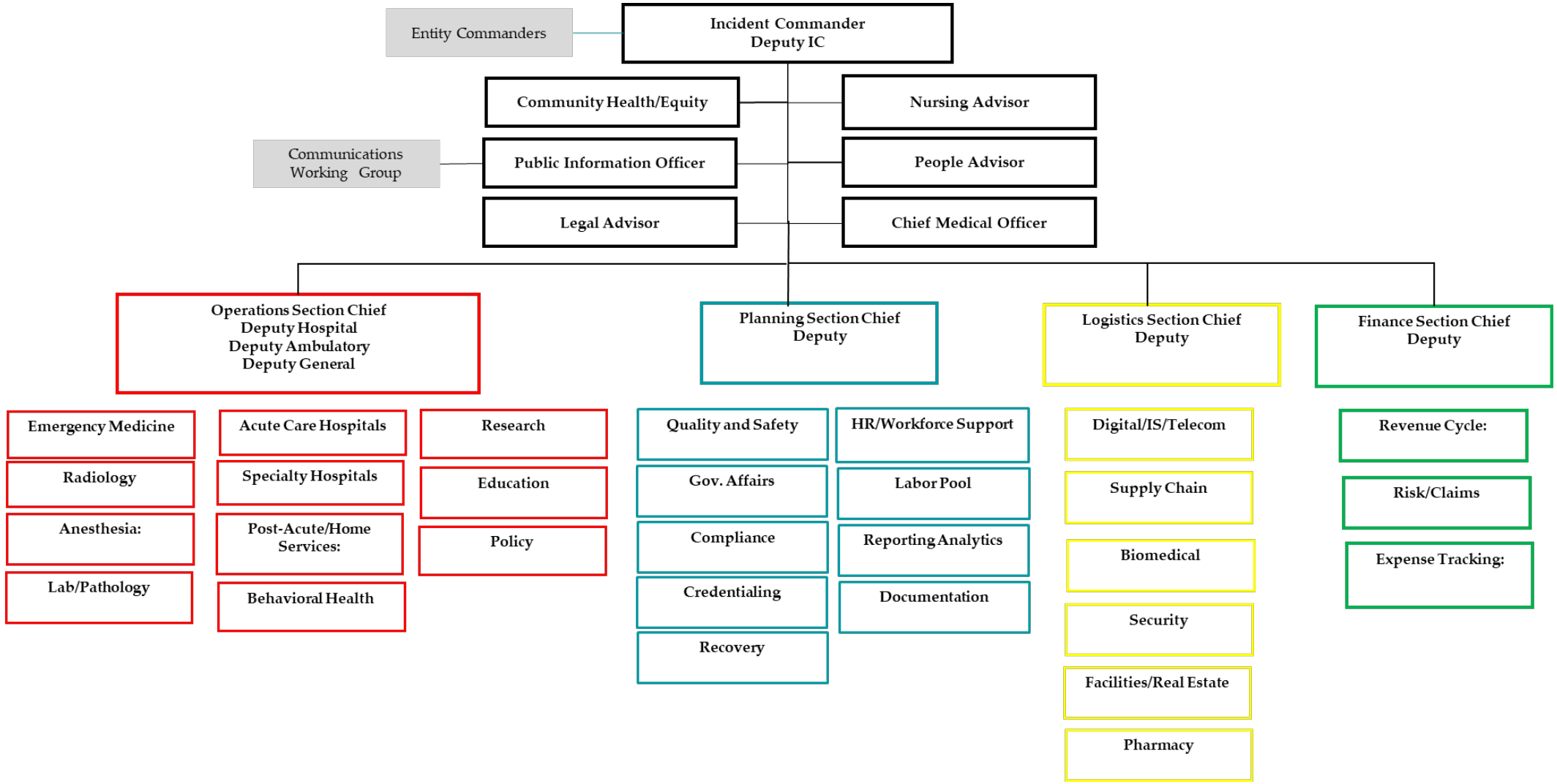


Playbook Overview

- 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

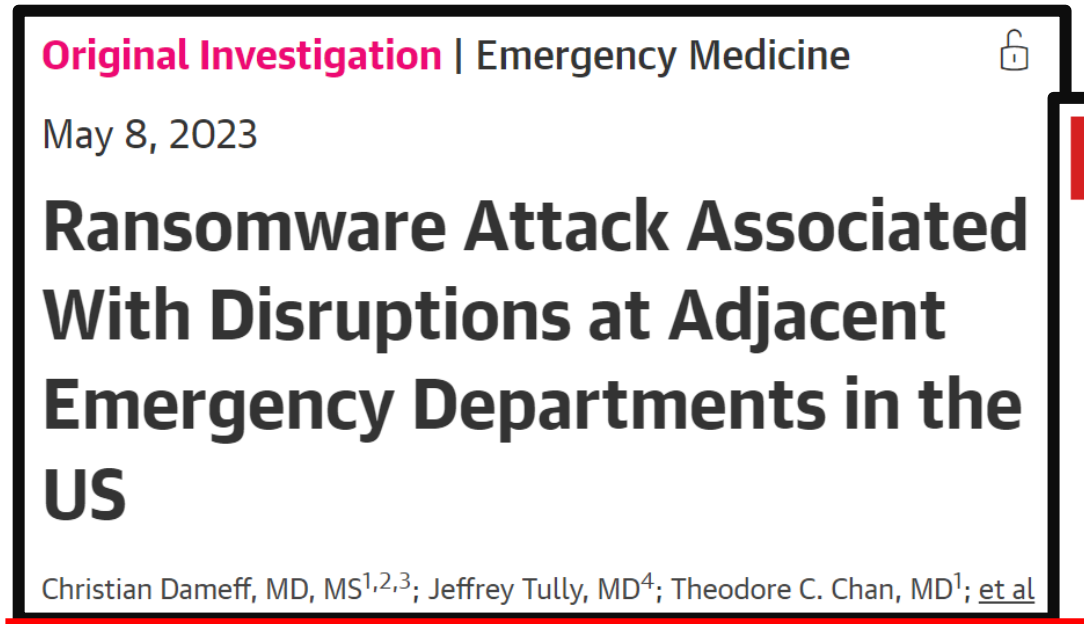


Example - Healthcare Incident Command System



Preparing Regional Responses

Cybersecurity incidents are a regional risk



Original Investigation | Emergency Medicine

May 8, 2023

Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US

Christian Dameff, MD, MS[1,2,3]; Jeffrey Tully, MD[4]; Theodore C. Chan, MD[1]; et al

npr

NATIONAL SECURITY

Cyberattacks on hospitals 'should be considered a regional disaster,' researchers find

JUNE 25, 2023 · 5:00 AM ET

Jenna McLaughlin

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.

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Establish and Operationalize a Health Care Coalition – Page 10, Develop a Health Care Coalition Response Plan – Page 27)

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf (Coordination with External Partners – Page 19)

https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf (National Incident Management System Guideline for Mutual Aid)

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.

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Develop a Health Care Coalition Preparedness Plan – Page 17)

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).

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Utilize Information Sharing Procedures and Platforms– Page 28)

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

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Plan and Conduct Coordinated Exercises with Health Care Coalition Members and Other Response Organizations – Page 20)

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. Community Emergency F

…(Continues)…

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.

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Establish and Operationalize a Health Care Coalition – Page 10, Develop a Health Care Coalition Response Plan – Page 27)

https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf (Coordination with External Partners – Page 19)

https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf (National Incident Management System Guideline for Mutual Aid)

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.

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Develop a Health Care Coalition Preparedness Plan – Page 17)

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).

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Utilize Information Sharing Procedures and Platforms– Page 28)

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

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf (Plan and Conduct Coordinated Exercises with Health Care Coalition Members and Other Response Organizations – Page 20)

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. Community Emergency F

…(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

-------FOR EXERCISE USE ONLY--------
- This is for a Cybersecurity Exercise -
-------FOR EXERCISE USE ONLY--------

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.

Lessons Learned From Exercises (1 of 2)

Cyber exercises are emergency preparedness exercises!!!

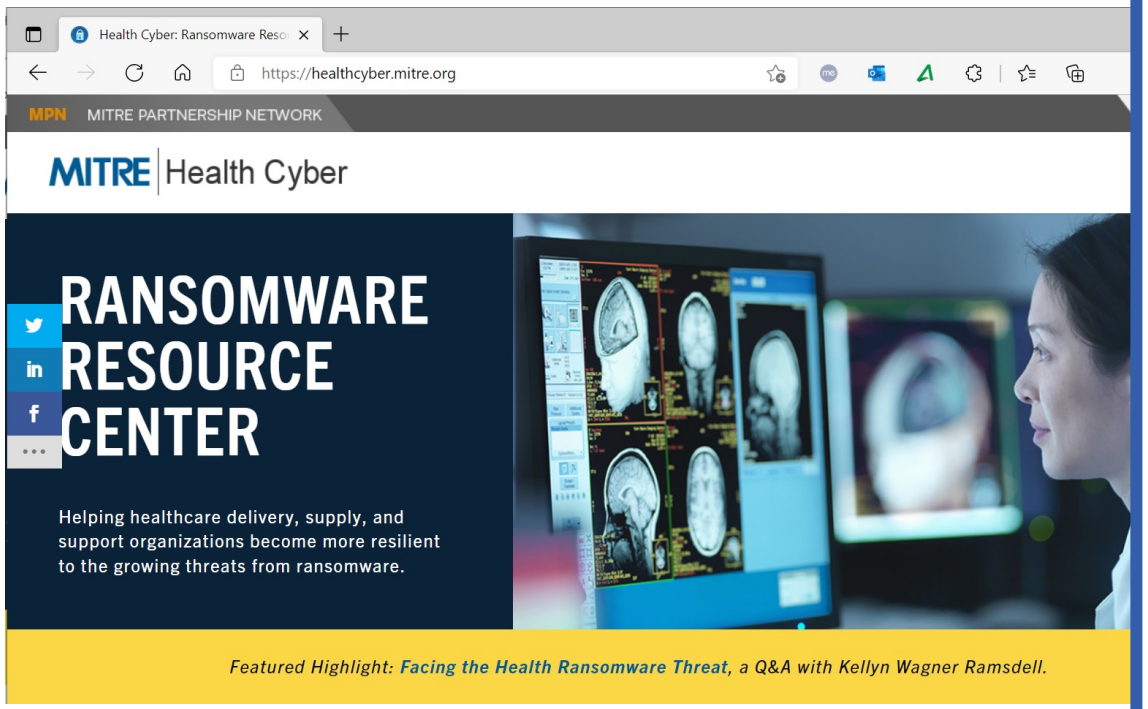
Clinical and Emergency Management experts are required

Lessons Learned From Exercises (2 of 2)

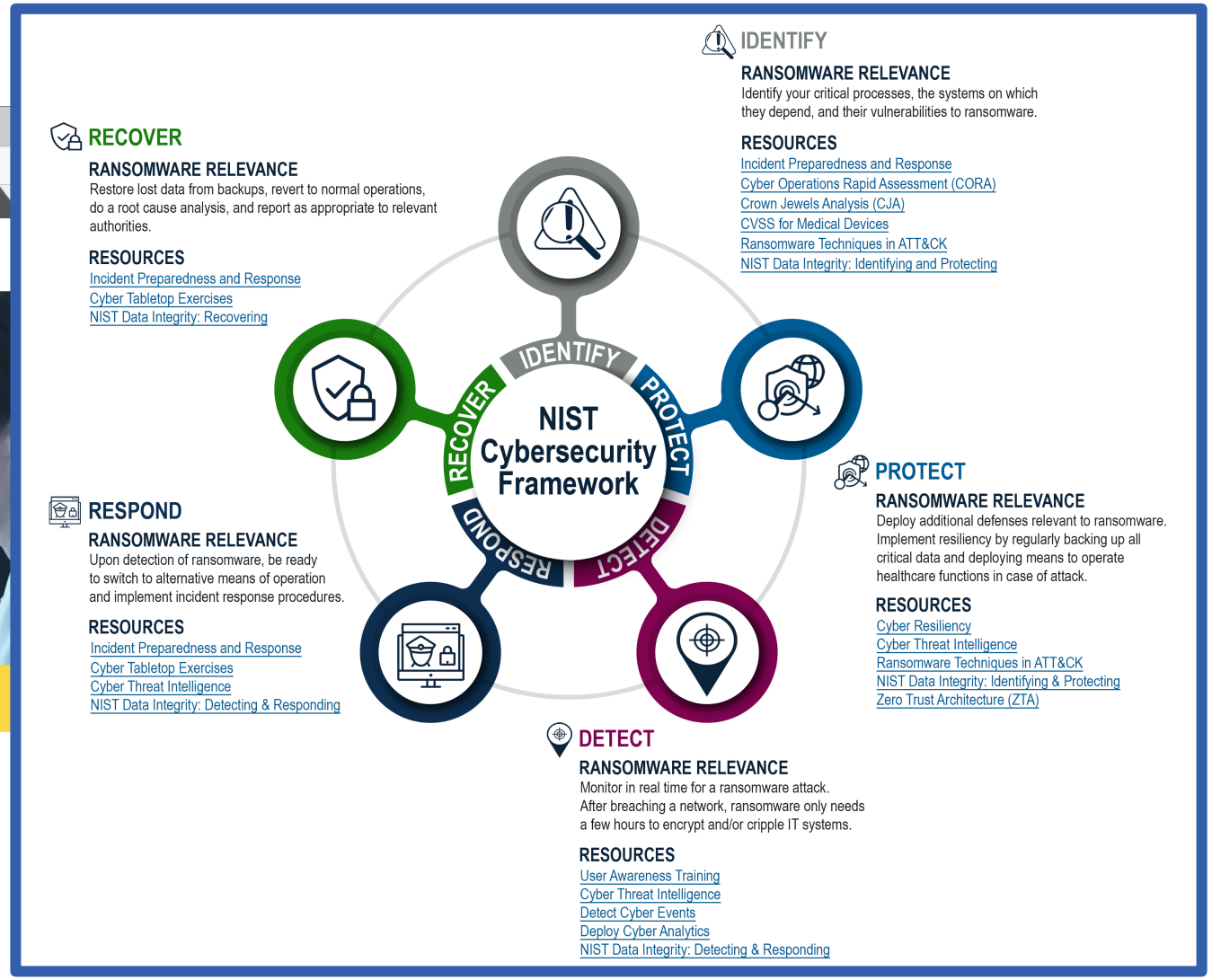
- **Understanding impacts of response actions is hard**
  - What happens when you lose internet connectivity?
- **Response coordination is hard**
- **Exercises can help develop as sense of understanding about how different teams can partner together**
- **It's important to have a response plan before 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

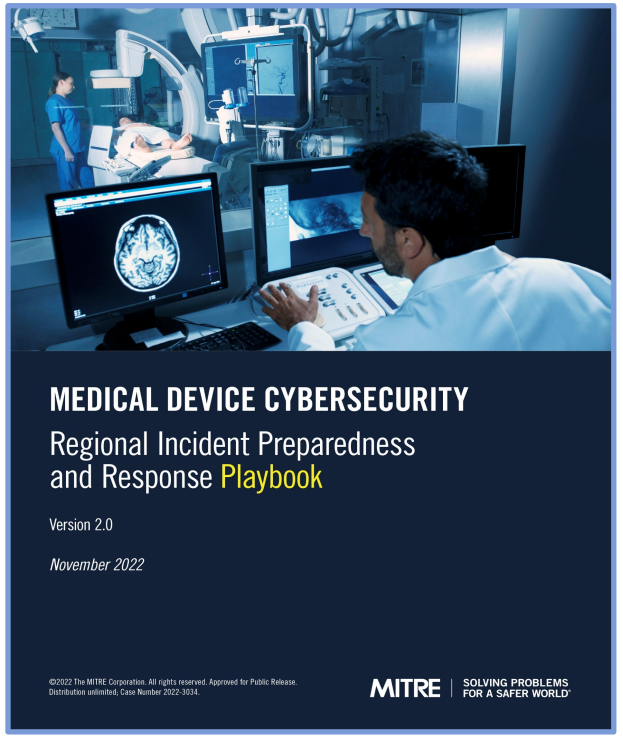
linkedin.com/in/pennychase/

Matt Weir

cweir@mitre.org

linkedin.com/in/matt-weir-54a2192

Download the playbook:



https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

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 (aami.org): https://array.aami.org/doi/10.2345/0899-8205-52.2.103
  - MITRE products sponsored by FDA
    - Playbook for Threat Modeling Medical Devices | MITRE: https://www.mitre.org/news-insights/publication/playbook-threat-modeling-medical-devices
    - Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook | MITRE: https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response
    - 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: 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
- **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/
      - Health Industry Cybersecurity Artificial Intelligence Machine Learning: https://healthsectorcouncil.org/wp-content/uploads/2023/02/Health-Industry-Cybersecurity-Artificial-Intelligence-Machine-Learning_1.pdfx

Healthcare Cybersecurity Resources (5/5)

- **Sector Activities**
  - Health Sector Coordinating Council (HSCC) Cybersecurity Working Group
    - Publications – some selected ones:
      - Incident Response and Business Continuity - Response Plan (HIC-CHIRP): https://healthsectorcouncil.org/wp-content/uploads/2023/07/HIC-CHIRP-FINAL_1.pdf
      - Incident Response and Business Continuity - Incident Checklist (OCCI): https://healthsectorcouncil.org/wp-content/uploads/2022/05/Operational-Continuity-Cyber-Incident-OCCI.pdf
      - Health Industry Cybersecurity Managing Legacy Technology Security (HIC-MaLTS): https://healthsectorcouncil.org/wp-content/uploads/2023/03/Health-Industry-Cybersecurity-Managing-Legacy-Technology-Security-HIC-MaLTS.pdf
      - Model Contract-Language for Medtech Cybersecurity (MC2): https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/