Health Care Provider Call
February 2024

Critical Infrastructure Cybersecurity Toolkit – A Tool for Securing the Healthcare Environment

Meg Speranza
Resiliency Program Manager
Speranza@MassTech.org

MassCyberCenter
at MassTech

Cyber Incidents and Healthcare
What makes healthcare organizations attractive targets?

The American Hospital Association Reports that healthcare organizations are particularly vulnerable and targeted by cyberattacks because they possess so much information of high monetary and intelligence value to cyber thieves and nation-state actors.

Targeted data includes:

- Patients' protected health information (PHI)
- Financial information like credit card and bank account numbers
- Personally Identifying information (PII) such as Social Security numbers, and intellectual property related to medical research and innovation

Stolen health records may sell up to 10 times or more than stolen credit card numbers on the dark web.

Source: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety#:~:text=Health%20care%20organizations%20are%20particularly,thieves%20and%20nation%2Dstate%20actors.

Cyber Incident Response Planning
Who and What are the Threats?

Threat Actors

- Insider Threat
- Cybercriminals
- Nation-State
- Advanced Persistent Threat (APT) Groups
- Hacktivists
- Terrorists

Threats

- Unintended disclosures by employees
- Hacking/Malware/Ransomware
- Insider Wrong-Doing
- Zero Day Vulnerabilities
- Physical Loss
- Portable Device/ Removable Media
- Technology Intrusions
- Phishing/Spear-Phishing Schemes
- Man-in-the-Middle Attacks
- Wire Transfer Fraud
- Skimming Incidents
- Vendors/Subcontractors – Poor Security
- Protocols/Standards

MassCyberCenter
at MassTech

Cyber Incident Response Planning
Healthcare Attacks in the News

Major Massachusetts health insurer hit by ransomware attack, member data may be compromised

– *Associated Press, May 26, 2023*

Massachusetts Hospital Victimized by Hack Leaves Thousands of Patients' Info Exposed

– *Newsweek, October 28, 2021*

Massachusetts health officials warn of data breach involving more than 134K people

State health officials say 'worldwide data security incident' linked to MOVEit

– *FOXBusiness, August 16, 2023*

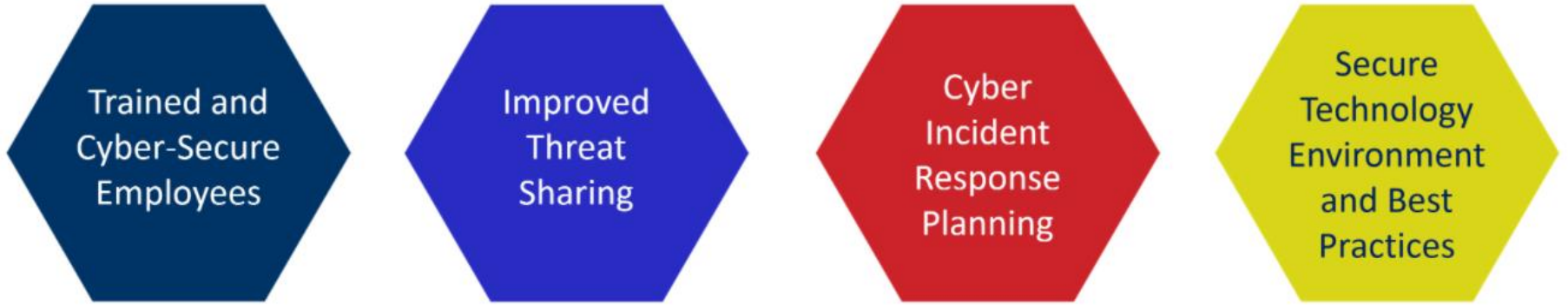
Shields Health Care Group data breach affects 2 million patients

– *Bleeping Computer, June 7, 2022*

Cyber Incident Response Planning
Minimum Baseline of Cybersecurity

A framework for helping Massachusetts organizations improve their cybersecurity posture and protect their networks and data from cyberattacks using people, process, and technology.

There are 4 goals:



Each goal contains links to Commonwealth and federal cybersecurity Resources.
For more information go to MassCyberCenter.org.

MassCyberCenter at MassTech

Secure Technology Environment and Best Practices

Critical Infrastructure (CI) Cybersecurity Toolkit – A Tool for Securing the Healthcare Environment

Operational Technology and Industrial Control Systems

MassCyberCenter at MassTech

Purpose of the CI Toolkit

Secure Technology Environment and Best Practices

- **Operational Technology (OT) and Industrial Control Systems (ICS)** "combine hardware and software to control and automate physical processes in industries. These systems are responsible for critical infrastructure, including power grids, water treatment plants, transportation systems and healthcare facilities."*

- ICS/OT systems have **unique characteristics** that differentiate them from traditional IT systems, making it challenging to implement security
  - High availability and reliability
  - Operation in harsh environments

- The **CI Toolkit** was designed to provide OT/ICS asset owners and operators with a roadmap for improving their OT/ICS cybersecurity posture and a list of resources that are available at no cost.

Definition Source: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/introduction-to-ics-ot-systems-and-their-role-in-critical-infrastructure

Recommendations from the CI Toolkit

1. Identify one role/position/title responsible for cybersecurity within your ICS/OT environment. Whoever fills this role/position/title is then in charge of all ICS/OT cybersecurity activities.
2. Conduct a Self-Assessment.
3. Use a cybersecurity framework to guide your OT Cybersecurity.
4. Create an OT/ICS Cyber Incident Response Plan.
5. Train personnel in your organization and exercise regularly.

For more information on the **CI Toolkit** and links to resources, go to:
https://masscybercenter.org/cyber-resilient-massachusetts/critical-infrastructure-toolkit

MassCyberCenter
at MassTech

Healthcare and Public Health Sector

Secure Technology Environment and Best Practices

- **About the Sector:**
  - The Healthcare and Public Health (HPH) Sector provides goods and services integral to maintaining local, national, and global health security. By its nature, it is highly dependent on other CI sectors for continuity of operations and service delivery, including Communications, Emergency Services, Energy, Food & Agriculture, IT, Transportation, and Water/Wastewater.
- **There are 6 Private Subsectors**
  - Direct Patient Care
  - Health Information Technology
  - Health Plans and Payers
  - Mass Fatality Management Services
  - Medical Materials
  - Laboratories, Blood, and Pharmaceuticals
- **There are 2 Government Subsectors**
  - Public Health
  - Federal Response and Program Offices

Voluntary collaboration is key to HPH Sector infrastructure security and resiliency,

Source: The **Cybersecurity & Infrastructure Security Agency (CISA):** - https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector

MassCyberCenter at MassTech

HPH Sector-Specific Plan

Secure Technology Environment and Best Practices

- The Government Coordinating Council and the Sector Coordinating Council represent the key organizing elements of the HPH Sector Partnership and have a number of joint working groups for collaboration and information sharing, including one focused on Cybersecurity.

- This Plan represents a collaborative effort among the private sector, SLTT governments, and federal departments and agencies to achieve the overarching goal of reducing critical infrastructure risk.

- The purpose of the Plan is to guide and integrate the Sector's efforts to secure and strengthen the resilience of HPH critical infrastructure across its physical, cyber, and human elements.

To download the **HPH Sector-Specific Plan**, go to https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

MassCyberCenter at MassTech

Key Takeaways of the HPH Sector-Specific Plan

Secure Technology Environment and Best Practices

Use collaborative risk management and public-private sector partnerships to protect the HPH Sector by:

- Assessing and managing **risk** across physical, cyber, and human elements, and
- Understanding the **cross-sector dependencies** for continuity of operations and service delivery
  - Leverage relationships and resources to assess and analyze threats & vulnerabilities
  - Enhance the resilience of the HPH Sector by translating risk analysis into actionable recommendations
  - Find ways to enhance information sharing
  - Create new ways to engage and do outreach to valued and new partners
  - Engage in response and recovery after cybersecurity incidents, and exercise response actions

To download the **HPH Sector-Specific Plan**, go to https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

MassCyberCenter at MassTech

More Cybersecurity Resources/Links for Healthcare

- **U.S. Department of Health and Human Services**

  HEALTHCARE SECTOR CYBERSECURITY

  https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

  Introduction to the Strategy of the U.S. Department of Health and Human Services

- **Health Industry Cybersecurity Practices**

  Managing Threats and Protecting Patients

  HICP-Main-508.pdf (hhs.gov)

  This guide shows how investing and implementing properly in cybersecurity protects patients and organizations from the damaging effects of cyberattacks

- **Healthcare Sector Coordinating Council**

  Cybersecurity Practices for Small Healthcare Organizations

  https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol1-508.pdf

  Recommendations on health care cybersecurity practices for small health care organizations

- **American Medical Association**

  Physician Cybersecurity

  https://www.ama-assn.org/practice-management/sustainability/physician-cybersecurity

  Resources and tips for physicians and health care staff for protecting patient health records and other data from cyberattacks

- **Massachusetts Digital Health**

  Cybersecurity Toolkit for Digital Health

  https://massdigitalhealth.org/resources/cybersecurity-toolkit-digital-health

  An educational resource for digital health companies at all stages of growth on both the fundamentals and best practices for cybersecurity and privacy protection

Questions

For more information on the Minimum Baseline of Cybersecurity and the Critical Infrastructure Toolkit, go to

MassCyberCenter.org

MassCyberCenter
at MassTech