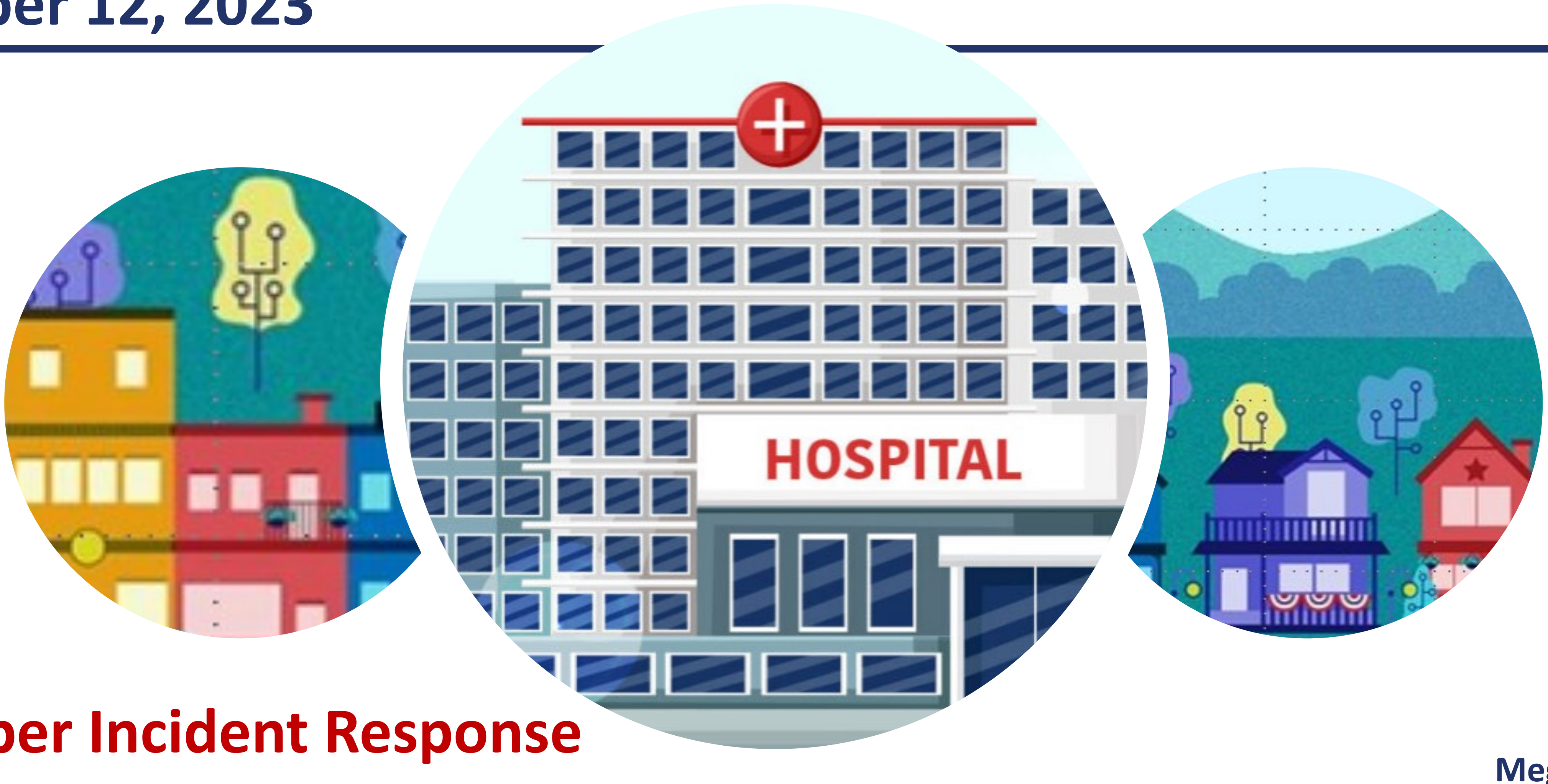
Health Care Provider Call

October 12, 2023



Cyber Incident Response Planning for Healthcare – What is it, and Why is it important?

Meg Speranza
Resiliency Program Manager
Speranza@MassTech.org

MassCyberCenter
at MassTech

Cyber Incident Response Planning

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

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

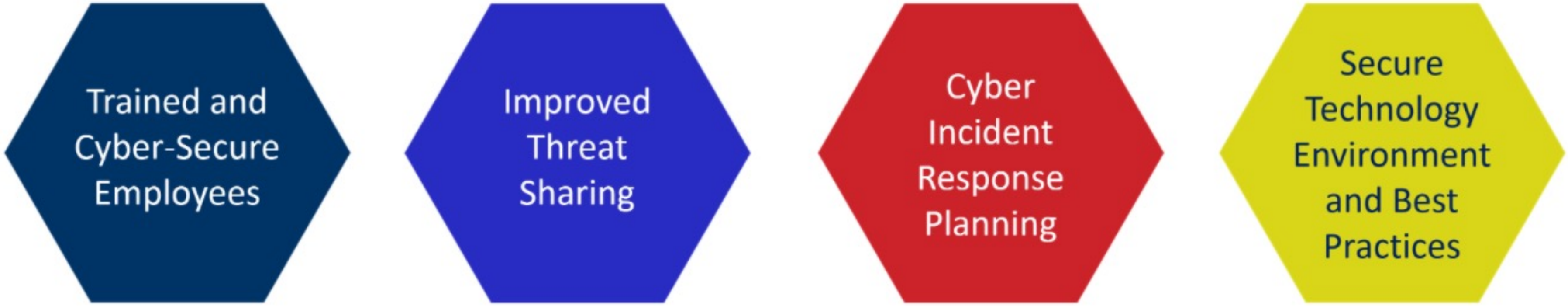
Shields Health Care Group data breach affects 2 million patients

– 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:



Trained and Cyber-Secure Employees

Improved Threat Sharing

Cyber Incident Response Planning

Secure Technology Environment and Best Practices

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

MassCyberCenter
at MassTech

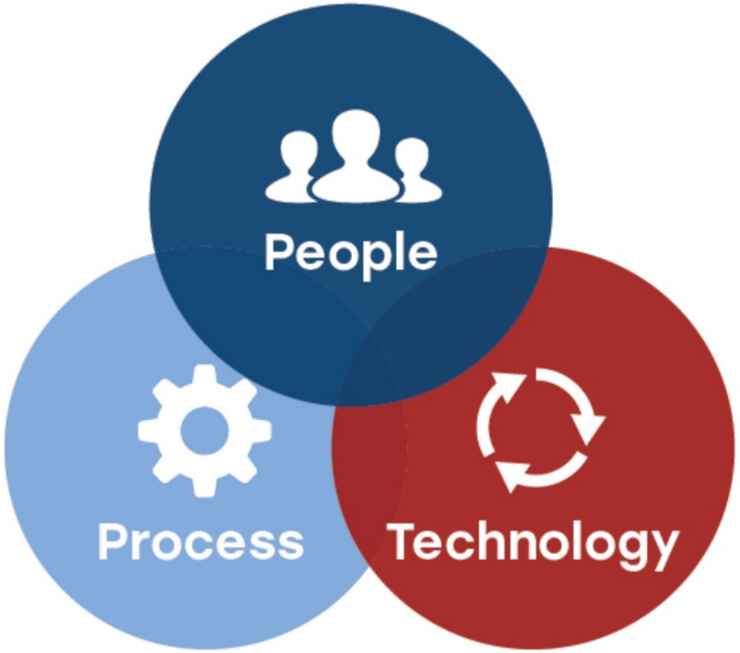
Developing a Cyber Incident Response Plan:

What is it and why do we need one?

Cyber Incident Response Planning
What is Cybersecurity?

- Leadership Talent/employment
- Training/education
- Citizens

- Cyber standards and procedures
- Incident response plans/ recovery
- Engagement



- Sensors
- Decision aids
- Defense tools

Developing a Cyber Incident Response Plan

What is a Plan and Why is it Important?

Cyber Incident Response Planning

- The **Plan** is designed to provide a well-defined, organized approach for handling any potential security breaches, or threats to a Municipality's data, systems, and infrastructure.

- The **Plan** defines what constitutes a security incident, identifies the areas of responsibility, establishes a process for documenting the incident and includes assessment procedures.

Developing a Cyber Incident Response Plan
Value of Planning & Being Prepared

Cyber Incident Response Planning

- **Create the team approach before an incident**
  - Names, contact information and responsibilities
  - Team meetings to study threats, review plans and update each other on issues
  - Understand the roles of third-party vendors before an incident
  - Establish communications pathways and trust
- **Prioritize key systems in advance**
  - "Critical" systems should be at the top of the list
  - Establish restoral priorities and authorities to modify
- **Exercise the plan to set you up for success**
  - Time for training and testing of response plan is important to promote a culture of cybersecurity preparedness

MassCyberCenter at MassTech

Does your organization have a *written* Cyber Incident Response Plan?

Developing a Cyber Incident Response Plan
What’s in a Plan – How do we get started

- What is the definition of an incident?
- If something happens, when should we contact someone?
- Who should we contact, and how do we contact them?

Detection & Analysis

Containment, Eradication & Discovery

Post-Incident Activity

Create a Planning Team to get started!

Developing a Cyber Incident Response Plan

Creating a Planning Team to *Develop the Plan*

Cyber Incident Response Planning

- **Determine who are the stakeholders:**
  - Organizational leadership
  - IT & Information Security leadership
  - Legal counsel
  - Auditor and Vendors/MSP
  - Finance
  - Human Resources
  - Communications
  - Local Police
- **Determine what decisions need to be made:**
  - When does the Response Plan get activated and who decides
  - Obtain or clarify cyber liability insurance information and requirements
  - Determine vendors needed such as forensics, outside legal counsel, mitigation and communications services
- **Determine who should be on the Cyber Incident Response Team**

Developing a Cyber Incident Response Plan

Who should be part of the Cyber Incident Response Team

Cyber Incident Response Planning

Purpose: Effectively respond to & mitigate cyber incidents

Objectives:

- Coordinate response to incident
- Establish communication protocols
- Conduct investigation into incident
- Provide notice to appropriate regulatory authorities
- Coordinate with third-party service providers
- Act as liaison to law enforcement or information sharing agencies, including state and federal
- Determine notification requirements – to any affected individuals

MassCyberCenter at MassTech

Developing a Cyber Incident Response Plan

Who should be part of the Cyber Incident Response Team

Cyber Incident Response Planning

Recommended Team Members:

- Incident Response Coordinator or Chief Privacy Officer
- Technology Coordinator or Chief Security Officer
- Legal Counsel | Outside Legal Counsel
- Communications Coordinator
- Internal Audit Coordinator
- Human Resources
- Finance
- Operations
- First Responders

Developing a Cyber Incident Response Plan

Building the Plan – Who to contact in the event of an Incident

Cyber Incident Response Planning

- **Compile and maintain updated contact information* NOW:**
  - Legal Counsel | Outside Legal Counsel
  - Law enforcement officials, including state and federal officials
  - Third-party vendors, such as MSPs, etc.
  - Forensic vendors
  - Credit monitoring/call center/identity theft mitigation services vendors
  - Cyber insurance broker and insurance company contact information to report a security incident
  - Applicable regulatory body - such as the Office of the Attorney General
  - Information sharing entities

* If you have cyber insurance, remember to select insurance-approved vendors.

Developing a Cyber Incident Response Plan

During an Incident, be prepared to answer these Questions

Cyber Incident Response Planning

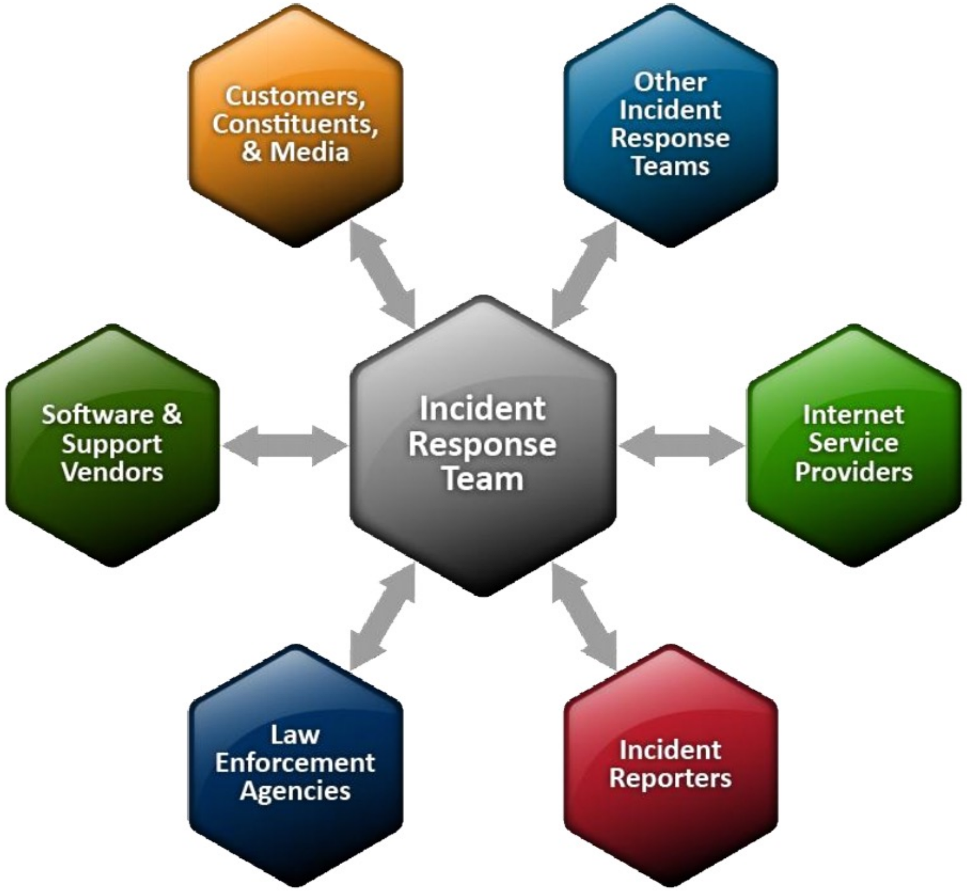
- **What is happening technically?**
  - What systems are impacted? How long will the systems be down?
- **What revenue streams or business operations are impacted due to the attack?**
  - Characterize the impact.
- **Has any data been exposed or stolen?**
  - What type of data and how many records?
- **What legal requirements or regulatory requirements are in play due to the impact of business operations or loss of data?**
- **What does the organization's insurance policy cover?**
  - Cybersecurity?
  - Payment of ransom?
  - Use of pre-approved vendor for incident response?
  - Negotiator?
  - Other operational costs for recovery?
- **Does your oversight organization have a ransomware policy?**
- **Is it legal to pay ransom?**

Developing a Cyber Incident Response Plan
Build a Communications Plan!

Create a communications plan in advance of an incident:

- Include Legal Counsel in creation and approval of a plan!
- Create communications for internal stakeholders (employees) as well as external stakeholders (citizens, students, 3rd parties, media, etc.)

Remember: An attack is an "incident" until there is theft of data—then it is a "breach". Using the word "breach" has legal consequences.


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Developing a Cyber Incident Response Plan

Cybersecurity Considerations for Leaders

Cyber Incident Response Planning

- **Have a Plan**
  - Address all aspects of key operations based on risk assessments
  - Prioritize key cybersecurity operations for protection and restoration
  - Include IT, HR, operations, admin managers, finance, risk management, and legal experts in the planning process
- **Have an Incident Response Team with strong leadership**
  - Ensure the team meets before a crisis
  - Incorporate non-IT leadership in cybersecurity discussions

- **Make it a priority**
  - Time for training, planning, and testing of cybersecurity practices
  - Resources to support good IT architecture, back up management, and employee training
  - Visibility with your employees – walk the cybersecurity walk

Developing a Cyber Incident Response Plan

Best Practices for Maintaining the Plan

- Determine who has responsibility for maintaining the Plan
- Make sure the Plan is distributed as appropriate, within the organization
- Review Plan at least annually
- Conduct regular staff, user and employee education and training in privacy and security
- Conduct tabletop exercises at least annually

Developing a Cyber Incident Response Plan

Tabletop Exercises – An important part of the Plan

A Cybersecurity tabletop exercise (TTX) is a discussion-based event, in an informal setting, to assess response plans, policies, and procedures and understand people's roles and responsibilities when a Cyber incident or crisis occurs.

TTXs can be just a 15-minute discussion at a regular meeting, focused on one aspect of your plan; or day-long, off-site events.

Make it work for your organization!

November 2022 Healthcare Tabletop Exercise

Key Takeaways

- The cause of the incident is not as relevant as operational and clinical impacts
  - Providers want to know if system is up/down; data accurate
  - Requirements for data entry, authorization, and billing do not allow for manual process in case of incident
  - What are the impacts to patient care?
    - Will appointments/procedures/surgeries need to be rescheduled?
    - Will patients need referral to external health systems? If so, those organizations not impacted by cyber event may still need to plan for inflow of patients from other systems
- Hard to understand system and process dependencies across healthcare that may be impacted by cyber incident
  - There is a need to work across the organization to understand any system integrations that may impact internal systems and the systems of affiliated and external partners

November 2022 Healthcare Tabletop Exercise

Cyber Incident Response Planning

Key Takeaways (Continued)

- How can government share information about threats so healthcare organizations can determine risks
  - DPH/Commonwealth Fusion Center/Other
  - There is consensus that healthcare orgs should notify DPH of event immediately to support communications with other healthcare entities, but that process needs to be better documented
- Communication is key
  - Informing leadership of incident is a priority and will inform communications with internal departments and external partners
  - Can use morning “huddles” to share key information with clinical and administrative staff
- Leverage existing processes and plans to include cybersecurity – ie. Make cybersecurity part of disaster recovery processes.
- Leverage cybersecurity vendor to determine which systems impacted by incident

Reporting an Incident

WHEN should an Incident be Reported?

- A cyber incident is *an event that could risk the confidentiality, integrity, or the availability of information systems*. Cyber-incidents could lead to a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Victims are encouraged to report cyber incidents that may:
  - Indicate unauthorized access to, or malicious software present on system and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, economic security, public health or safety, or any combination of those matters.
  - Result in a significant loss of data, system availability, or control of systems.
  - Impact a large number of victims.
- There are no minimum monetary loss thresholds for reporting.

Reporting an Incident

HOW should an Incident be Reported?

- Follow your existing notification process, which may include the Department of Public Health (DPH) and Law Enforcement.
- *It is important to establish a working relationship and protocols with DPH and law enforcement points of contact and incorporate them into your incident response plan well in advance of a crisis.*
- If you do not have an existing notification process that includes your local police department, you may contact the Commonwealth Fusion Center directly via telephone at **508-820-2233** (24x7x365).
- Once notified, someone from the Commonwealth Fusion Center will contact your organization’s designated point of contact.
- Report the incident to other regulatory entities and Federal Law Enforcement in accordance with your organization’s policies. Reporting a Cyber Incident to Law Enforcement **does not** fulfill regulatory data breach reporting requirements.

Questions

For more information on the Minimum Baseline of Cybersecurity and Cyber Incident Response Planning resources, go to

MassCyberCenter.org