MassCyberCenter
at the MassTech Collaborative

Cyber Incident Response Planning

Cyber
Incident
Response
Planning

2022

Stephanie Helm
Director, MassCyberCenter
MassTech Collaborative

MassCyberCenter.org

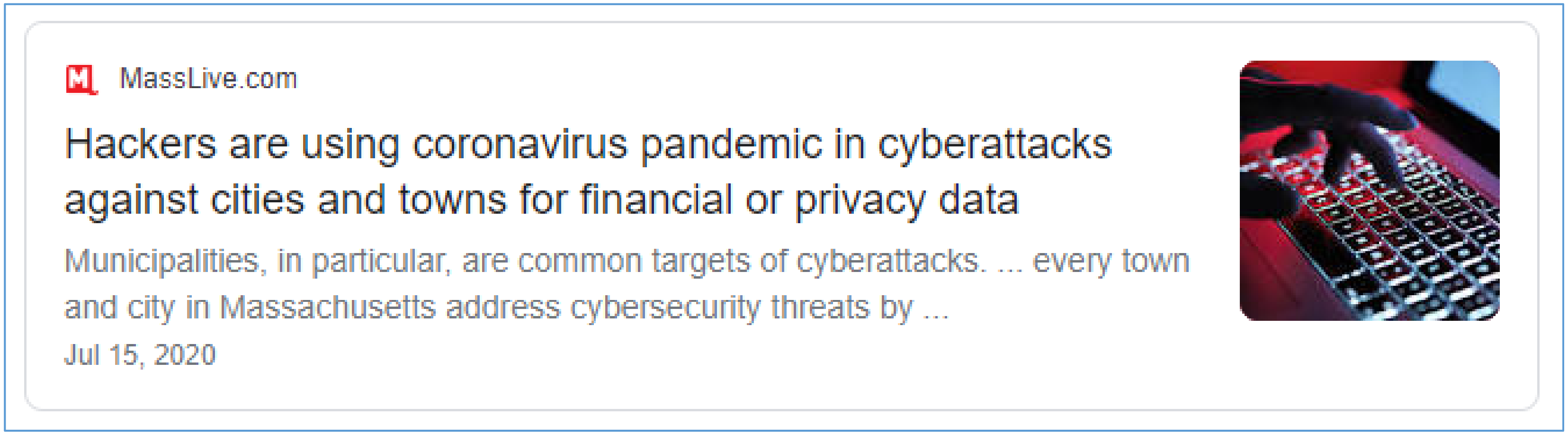
Agenda

- Introductions
- Cyber Threats
- What is cybersecurity?
- MassCyberCenter / Commonwealth Resources
- Developing a Cyber Incident Response Plan
- National Institute of Standards & Technology (NIST) Phases for Responding to a Cybersecurity Incident
    - Preparation, Detection & Analysis, Containment, Eradication & Discovery, Post-Incident Activity
- Incident Response Plan Checklist
- Maintenance & Going Forward
- Cybersecurity Considerations for Leaders

Cyber Threats to Municipalities

- 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

Recent Attacks in the News

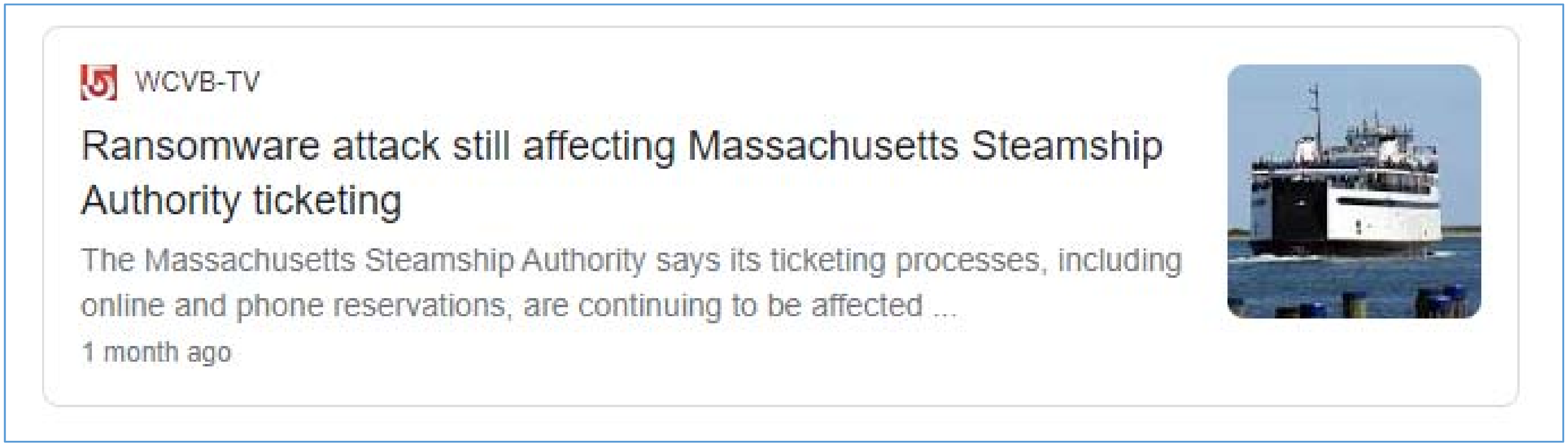


MassLive.com

Hackers are using coronavirus pandemic in cyberattacks against cities and towns for financial or privacy data

Municipalities, in particular, are common targets of cyberattacks. ... every town and city in Massachusetts address cybersecurity threats by ...

Jul 15, 2020



WCVB-TV

Ransomware attack still affecting Massachusetts Steamship Authority ticketing

The Massachusetts Steamship Authority says its ticketing processes, including online and phone reservations, are continuing to be affected ...

1 month ago

Updates on Cybersecurity News, including ransomware, malware, vulnerabilities and more:
mass.gov/resource/cybersecurity-awareness-bulletins

MassCyberCenter
at the MassTech Collaborative

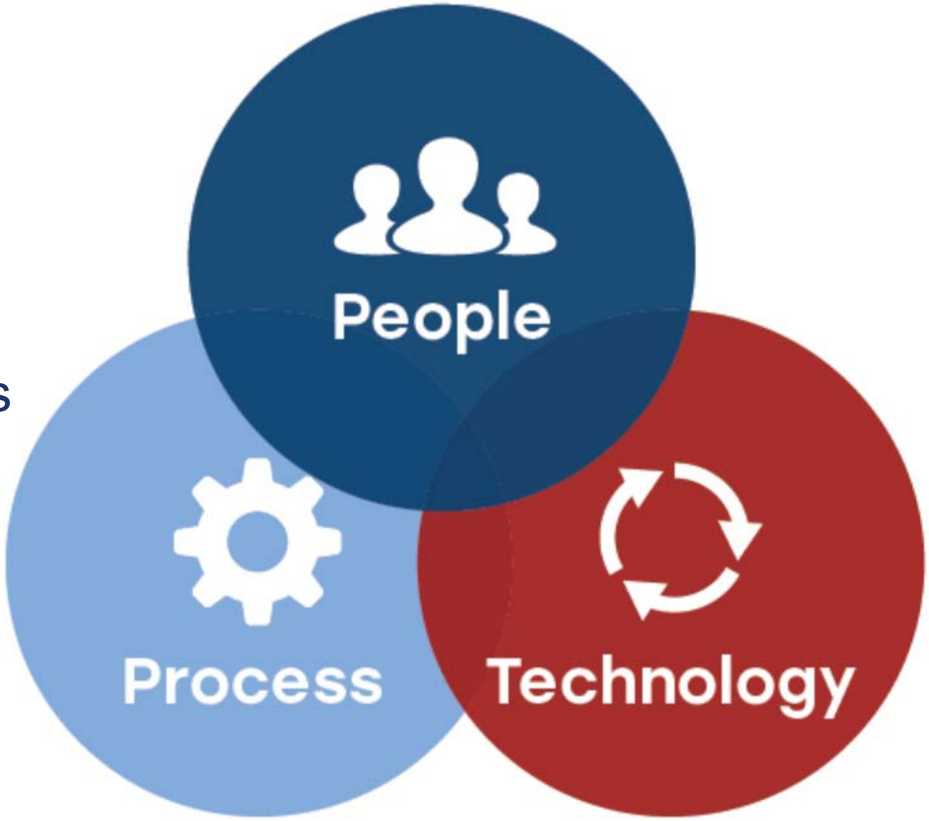
Municipalities are attractive targets

What makes local governments attractive targets for cyber attacks?

- They house private data
- Security often isn't a top (or well-funded) priority
- Attacks have been successful
- Attacks against local governments are public-facing, providing a potent outlet and often resulting in a variety of disruptive, public consequences

What is cybersecurity?

- Leadership Talent/employment
- Training/education
- Citizens



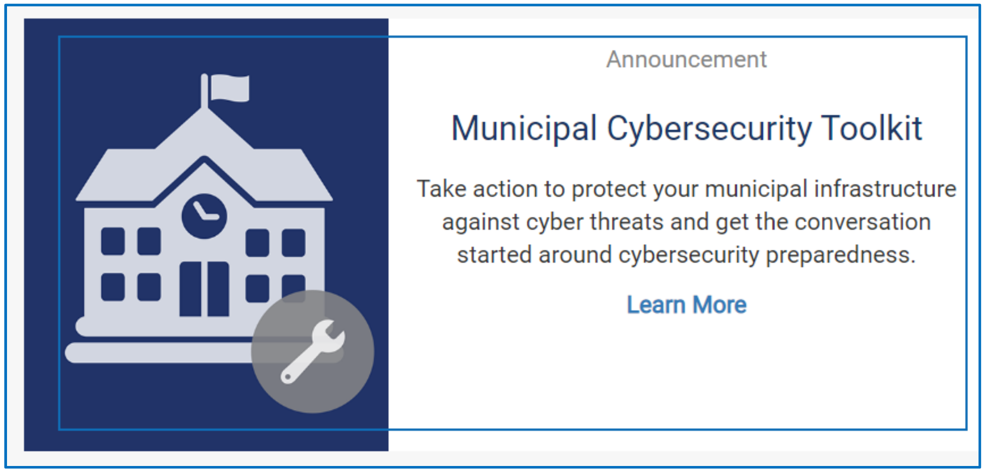
- Cyber standards and procedures
- Incident response plans/ recovery
- Engagement

- Sensors
- Decision aids
- Defense tools

Cybersecurity Considerations for Leaders

- **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

Cybersecurity Toolkit for Municipalities

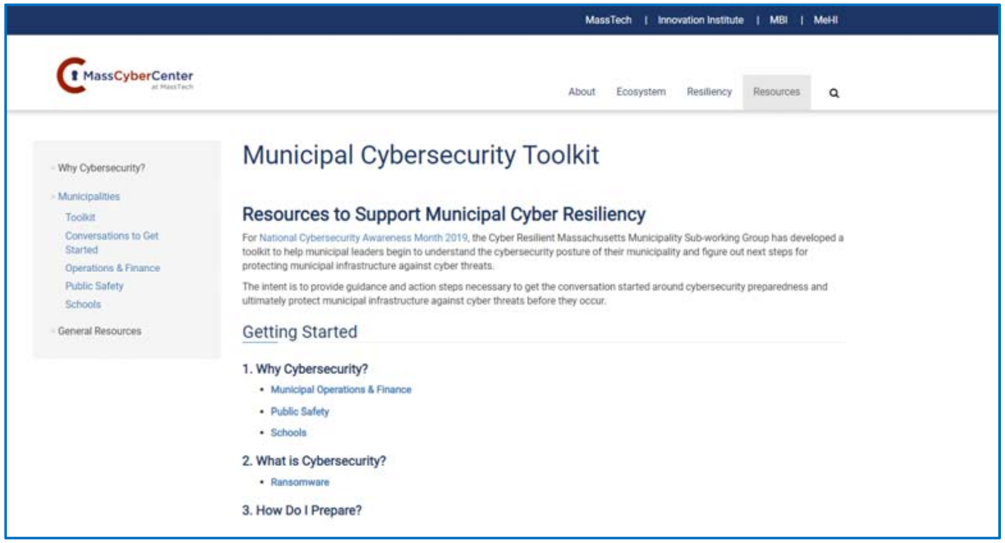


Announcement

Municipal Cybersecurity Toolkit

Take action to protect your municipal infrastructure against cyber threats and get the conversation started around cybersecurity preparedness.

Learn More



MassTech | Innovation Institute | MBI | MeHI

MassCyberCenter at MassTech

About Ecosystem Resiliency Resources

- Why Cybersecurity?
- Municipalities
  - Toolkit
  - Conversations to Get Started
  - Operations & Finance
  - Public Safety
  - Schools
- General Resources

Municipal Cybersecurity Toolkit

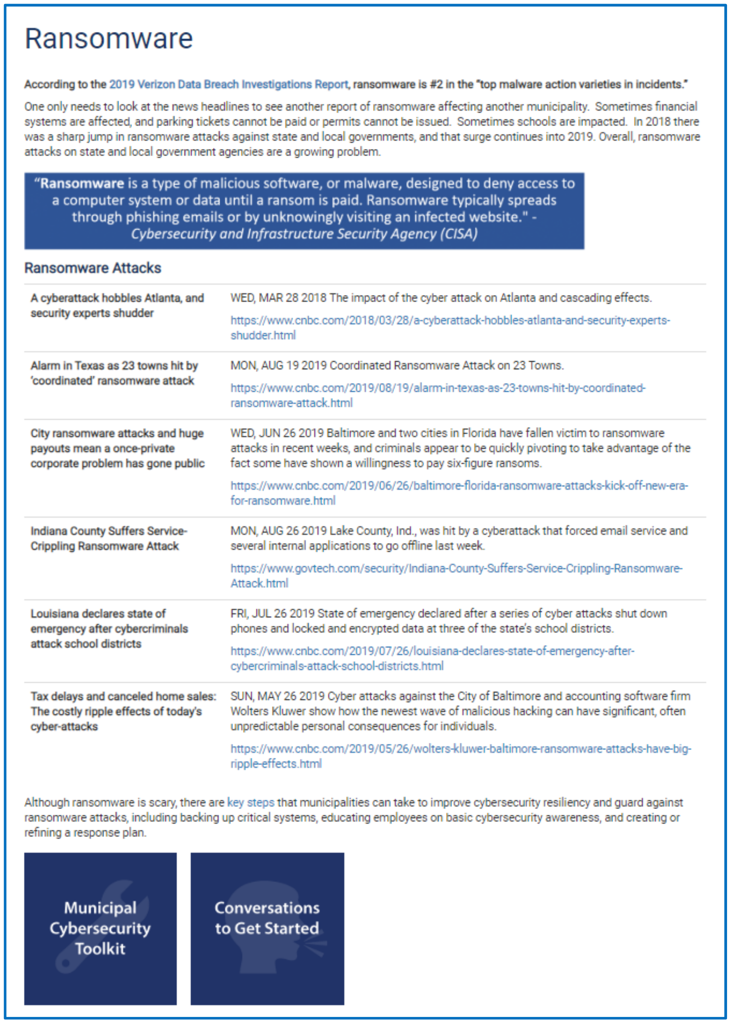
Resources to Support Municipal Cyber Resiliency

For National Cybersecurity Awareness Month 2019, the Cyber Resilient Massachusetts Municipality Sub-working Group has developed a toolkit to help municipal leaders begin to understand the cybersecurity posture of their municipality and figure out next steps for protecting municipal infrastructure against cyber threats.

The intent is to provide guidance and action steps necessary to get the conversation started around cybersecurity preparedness and ultimately protect municipal infrastructure against cyber threats before they occur.

Getting Started

1. Why Cybersecurity?
   - Municipal Operations & Finance
   - Public Safety
   - Schools
2. What is Cybersecurity?
   - Ransomware
3. How Do I Prepare?



Ransomware

According to the 2019 Verizon Data Breach Investigations Report, ransomware is #2 in the "top malware action varieties in incidents."

One only needs to look at the news headlines to see another report of ransomware affecting another municipality. Sometimes financial systems are affected, and parking tickets cannot be paid or permits cannot be issued. Sometimes schools are impacted. In 2018 there was a sharp jump in ransomware attacks against state and local governments, and that surge continues into 2019. Overall, ransomware attacks on state and local government agencies are a growing problem.

> "**Ransomware** is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website." - *Cybersecurity and Infrastructure Security Agency (CISA)*

Ransomware Attacks

A cyberattack hobbles Atlanta, and security experts shudder	WED, MAR 28 2018 The impact of the cyber attack on Atlanta and cascading effects. https://www.cnbc.com/2018/03/28/a-cyberattack-hobbles-atlanta-and-security-experts-shudder.html
Alarm in Texas as 23 towns hit by 'coordinated' ransomware attack	MON, AUG 19 2019 Coordinated Ransomware Attack on 23 Towns. https://www.cnbc.com/2019/08/19/alarm-in-texas-as-23-towns-hit-by-coordinated-ransomware-attack.html
City ransomware attacks and huge payouts mean a once-private corporate problem has gone public	WED, JUN 26 2019 Baltimore and two cities in Florida have fallen victim to ransomware attacks in recent weeks, and criminals appear to be quickly pivoting to take advantage of the fact some have shown a willingness to pay six-figure ransoms. https://www.cnbc.com/2019/06/26/baltimore-florida-ransomware-attacks-kick-off-new-era-for-ransomware.html
Indiana County Suffers Service-Crippling Ransomware Attack	MON, AUG 26 2019 Lake County, Ind., was hit by a cyberattack that forced email service and several internal applications to go offline last week. https://www.govtech.com/security/Indiana-County-Suffers-Service-Crippling-Ransomware-Attack.html
Louisiana declares state of emergency after cybercriminals attack school districts	FRI, JUL 26 2019 State of emergency declared after a series of cyber attacks shut down phones and locked and encrypted data at three of the state's school districts. https://www.cnbc.com/2019/07/26/louisiana-declares-state-of-emergency-after-cybercriminals-attack-school-districts.html
Tax delays and canceled home sales: The costly ripple effects of today's cyber-attacks	SUN, MAY 26 2019 Cyber attacks against the City of Baltimore and accounting software firm Wolters Kluwer show how the newest wave of malicious hacking can have significant, often unpredictable personal consequences for individuals. https://www.cnbc.com/2019/05/26/wolters-kluwer-baltimore-ransomware-attacks-have-big-ripple-effects.html

Although ransomware is scary, there are key steps that municipalities can take to improve cybersecurity resiliency and guard against ransomware attacks, including backing up critical systems, educating employees on basic cybersecurity awareness, and creating or refining a response plan.

Municipal Cybersecurity Toolkit

Conversations to Get Started

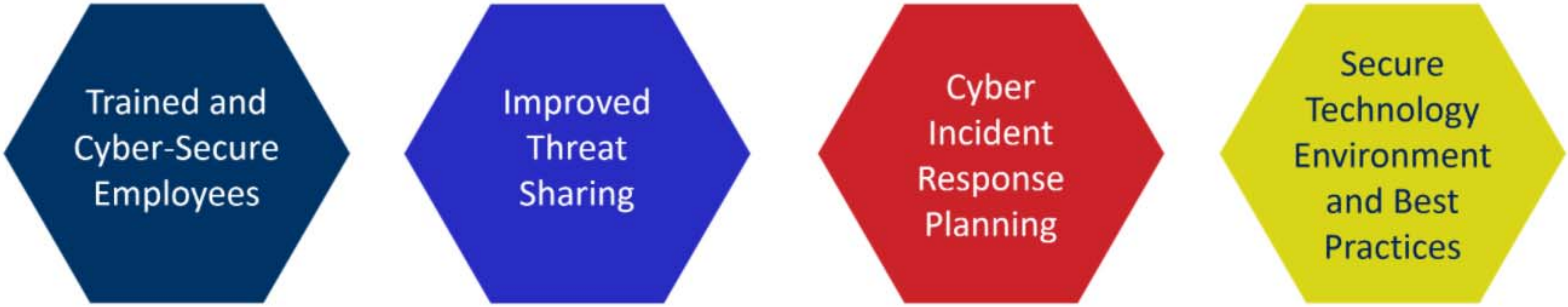
For more information, go to MassCyberCenter.org

MassCyberCenter at the MassTech Collaborative

Minimum Baseline of Cybersecurity for Municipalities

A framework for helping Massachusetts municipalities improve their cybersecurity posture and protect their municipality 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

Commonwealth Resources for Municipalities

MassCyberCenter

Municipal Cybersecurity Toolkit

Provides tools and educates municipalities statewide on best cybersecurity practices and threats.

masscybercenter.org/municipalities

Executive Office of Public Safety & Security (EOPSS)
Office of Grants & Research (OGR)

Homeland Security Grant Program

Advocates and helps with preparedness and planning for the event of a national, state, or local emergency.

mass.gov/orgs/office-of-grants-and-research

Operational Services Division (OSD)

ITS78: Statewide Contract for Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services

Offers a range of tools for municipal organizations to protect their IT infrastructure and data, including baseline assessments, remediation strategies and implementations, and cyberattack recovery solutions.

https://www.mass.gov/doc/its78/download

Link to OSD ITS78 Kickoff Event Video: ***ITS78 Kickoff (click here)***

Community Compact Cabinet

Community Compact Program

Champions municipal interests across all executive secretariats and agencies, and develops, in consultation with cities and towns, mutual standards and best practices for both the state and municipalities.

https://www.mass.gov/orgs/community-compact-cabinet

Executive Office of Technology Service and Security (EOTSS) &
Office of Municipal and School Technology (OMST)

Municipal Cybersecurity Awareness Grant Program

Provides cybersecurity end-user training, evaluation, and threat simulation to municipal governments and school districts with the goal of improving the overall cybersecurity posture.

mass.gov/how-to/apply-for-the-cybersecurity-awareness-program

Cyber Health Checks

Offers opportunities for local government to access basic cybersecurity services at no cost.

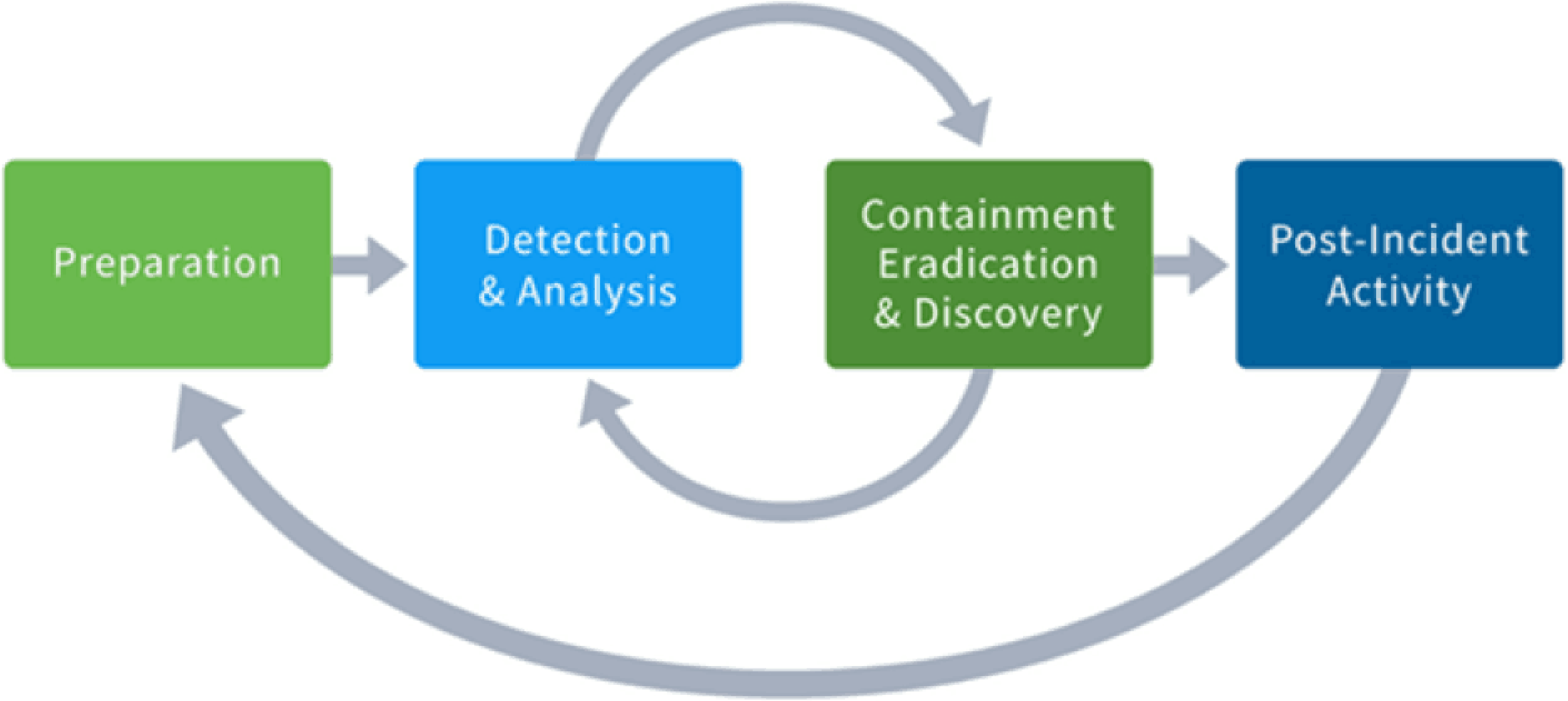
https://massgov.formstack.com/forms/cyber_security_it_health_check

Cyber Incident Response Plan:

What is it and why do we need one?

NIST Phases of Cybersecurity Incident Response

National Institute of Standards and Technology or NIST recommends four phases for responding to a cybersecurity incident



Preparation:
Developing the Incident Response Plan (“the Plan”)

- 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.

Preparation:
Who needs to be part of the Planning Team?

- **Determine who are the stakeholders:**
  - Organizational leadership
  - IT & Information Security leadership
  - Legal counsel
  - Audit
  - Finance
  - Human Resources
  - Communications
- **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

Preparation:
What Goals need to be part of the Plan

- Establish the **Incident Response Team** (the “Team”)
- Establish **definitions** – security incident, data breach
- **Assess** the incident and threat level
- **Define** the actions to be taken when an incident occurs
- **Respond** to the incident
- **Restore** - present an orderly course of action for restoring functionality
- **Document** – collect and document the incident
- **Communicate** – specify how information should be communicated, who should communicate and how
- **Mitigate** – implement processes to mitigate the effects of the incident

Preparation:
Value of 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
  - Visibility with your employees – walk the cybersecurity walk

Preparation:
Create Incident Response Team

Objectives:

- Conduct investigation into incident
- Coordinate response to incident
- Establish communication protocols
- 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 notice requirements – to any affected individuals

Preparation:
Roles of the Response Team

Incident Response Coordinator or Chief Privacy Officer

- Determines the nature and scope of the incident
- Contacts members of the Incident Response Team
- Determines which Incident Response Team members play an active role in the investigation
- Escalates to executive leadership as appropriate
- Monitors progress of the investigation
- Aids in evidence gathering, chain of custody, and preservation as appropriate
- Prepares a written summary of the incident and the corrective action taken

Preparation:
Roles of the Response Team (cont.)

Technology Coordinator or Chief Security Officer

- Determines the system(s) affected by the incident
- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
- Runs tracing tools, port monitors, and event loggers
- Contacts external Internet service provider for assistance in handling the incident if necessary
- Updates all service packs and patches on mission-critical computers as necessary
- Creates backups and that backups are in place for all critical systems
- Examines system logs of critical systems for unusual activity
- Monitors business applications and services for signs of attack
- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Coordinates with outside IT vendors/forensic analysts
- Provides recommendations for mitigation or other tools

Preparation:
Roles of the Response Team (cont.)

Communications Coordinator

- May assist with contacting appropriate affected individuals to notify them of the incident(s)
- May assist with contacting local, state, federal or other governmental entities if incident is criminal in nature
- Spearheads communication with media, as necessary
- Collates all related documentation and data of final assessment of incident for preservation purposes
- Coordinates internal and external communications and crisis management

Preparation:
Roles of the Response Team (cont.)

Internal Audit Coordinator

- Reviews systems for compliance with information security policies and controls
- Performs appropriate audit tests to keep systems current with service packs and patches
- Reports any system control gaps to management for corrective action

Preparation:
Roles of the Response Team (cont.)

Legal Counsel/Outside Legal Counsel

- Serves as Coach for Security Incident
- Coordinates legal analysis of data breach notification of individuals and/or regulatory authorities
- Assists with coordination with cyberliability insurance company
- Coordinates three-way agreement with forensic (and other) vendor(s) and municipality – protects attorney/client privilege
- Point person for government investigations and other government or regulatory communication
- Coordinates any litigation

Preparation:
Roles of the Response Team (cont.)

Human Resources

- Oversees employee discipline, as necessary
- Assists with communication and employee relations in the event of an incident that affects employee data

Preparation:
Roles of the Response Team (cont.)

Other possible team members

- Finance
- First Responders
- Operations Officer – Business Continuity

Preparation:
Building the Plan

- **Compile the following information NOW:**
  - Obtain and select insurance approved vendors, as appropriate, and maintain updated contact information for:
    - Forensic vendors
    - Credit monitoring/call center/identity theft mitigation services vendors
    - Outside legal counsel
    - Cyber insurance broker and insurance company contact information to report a breach/security incident
    - Law enforcement officials, including state and federal officials
    - Applicable regulatory body - such as the Office of the Attorney General
    - Information sharing entities

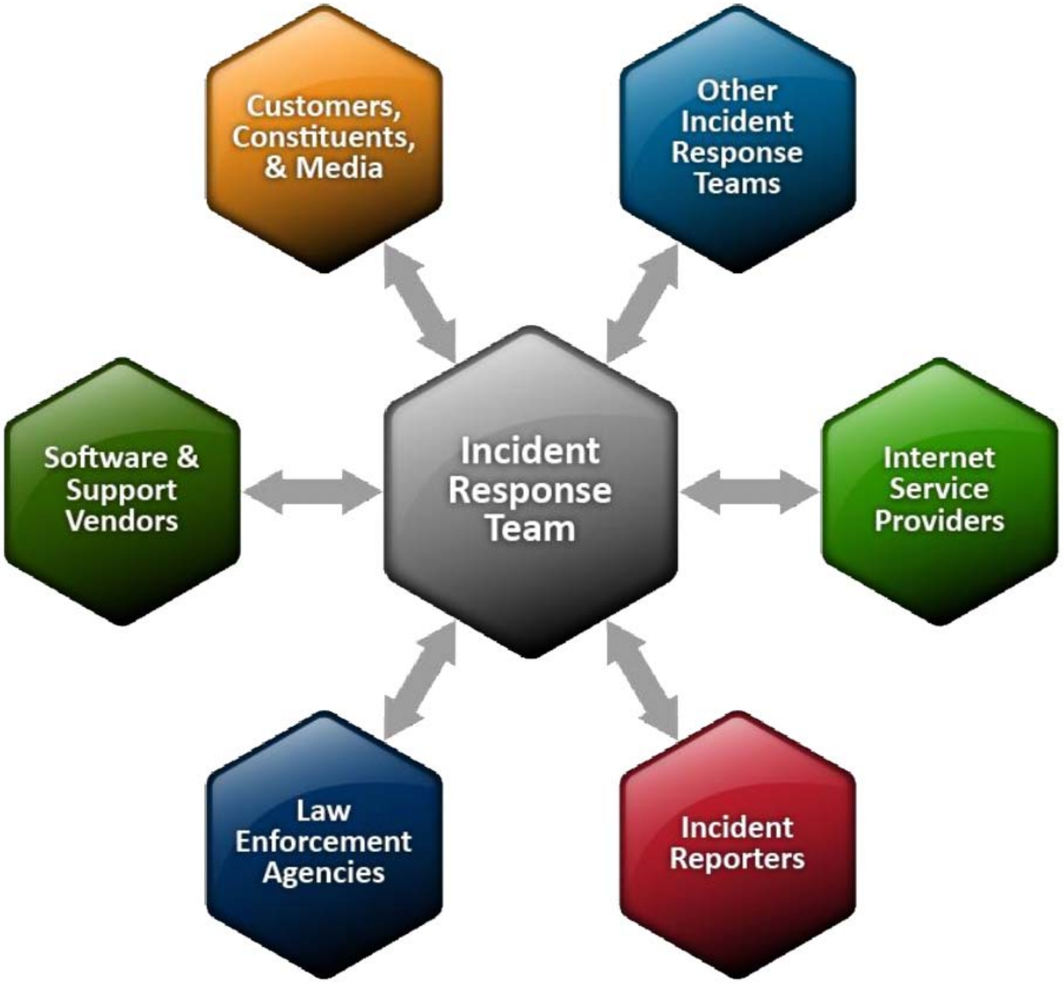
Preparation:
Building the Plan – Ransomware issues

- **Be prepared to address these questions during a ransomware incident:**
  - What is happening technically and what systems are impacted? How long will the systems be down?
  - What revenue streams or business operations are impacted due to the technical attack? Characterize the impact
  - Has any data been exposed or stolen? What type?
  - What legal requirements or regulatory requirements are in play due to the impact of business operations or loss of data?
  - What does our insurance policy cover? (payment of ransom? use of pre-approved vendor for incident response? Negotiator?)
  - Is it legal to pay the ransom? Does your oversight organization have a ransomware policy?

Preparation:
Manage Communications

NIST Model

Build a communications plan in advance


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

Detection & Analysis:
Plan Execution

- Review information received from the individual(s) reporting the security incident
- Activate Response Plan and notify Response Team members
- Work with other departments and information technology staff, as appropriate, to determine the risk of continuing operations
  - e.g. deciding whether to shut down system, disconnect from network, continue operation, etc.;
  - however, any decision to delay the containment should be discussed with legal counsel based on the liability
- Coordinate with incident response services of a third-party security firm and outside legal counsel as appropriate
- Implement processes to prevent alteration to the system(s) until a backup has been completed
- Implement processes to change passwords or other security safeguards on any compromised systems
- Maintain detailed documentation on all actions taken

Detection & Analysis:
Checklist

- ❑ Incident handling and investigation
  - ❑ Low risk level vs. high risk level incident
- ❑ Coordination of engaging legal counsel and other third parties to establish protections of documents and communication
- ❑ Notification to insurance broker, as applicable
- ❑ Coordination of responses to incidents
- ❑ Communication with employees & affected individuals
- ❑ Determination, with legal counsel, if there is a reportable data breach

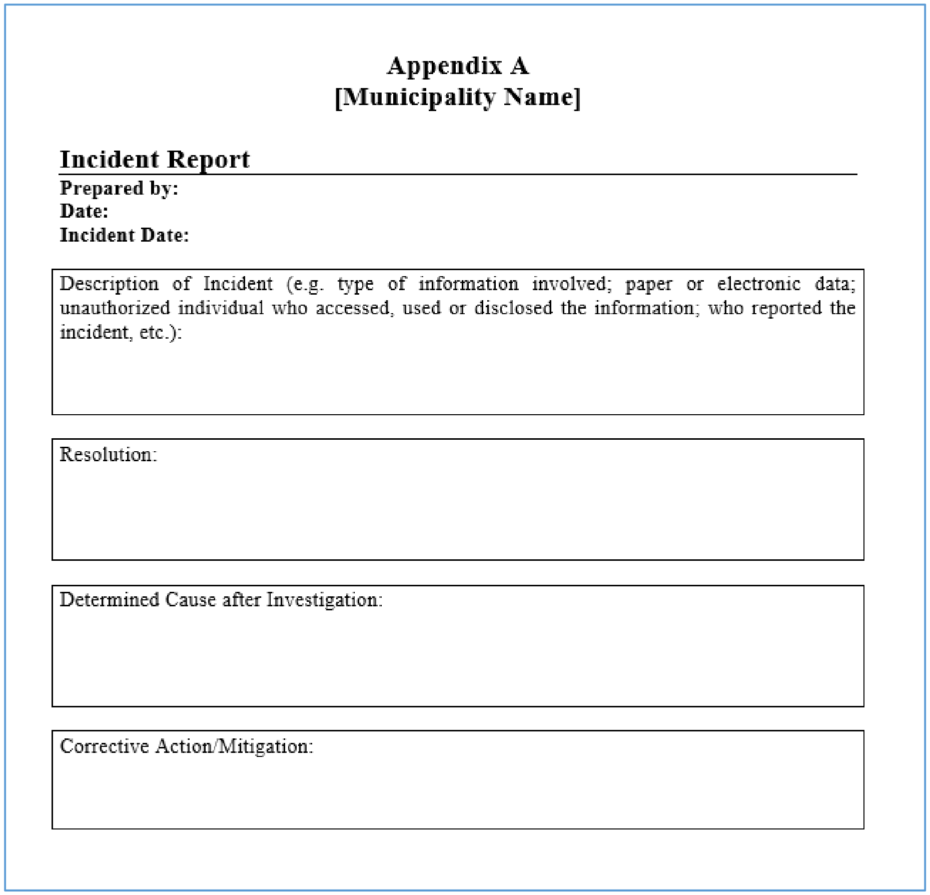
Detection & Analysis:
Checklist (cont.)

- ❑ If it is determined there is a reportable data breach:
  - ❑ Determine notification requirements to regulatory authorities, as applicable
  - ❑ Notification to law enforcement, as applicable
  - ❑ Determine notification requirements to affected individuals, as applicable

A "Data Breach," as defined by the Massachusetts Data Breach Notification Law, is the "unauthorized acquisition or use of sensitive personal information that creates a substantial risk of identity theft or fraud."

- ❑ If it is ransomware, gather information on slide 25 and analyze responses. Will paying the ransom really save you money/time/business continuity/reputation? Document gain/loss of paying the ransom. Seldom does payment equate to trouble-free restoral of systems.

Detection & Analysis: Checklist (cont.)



Appendix A
[Municipality Name]

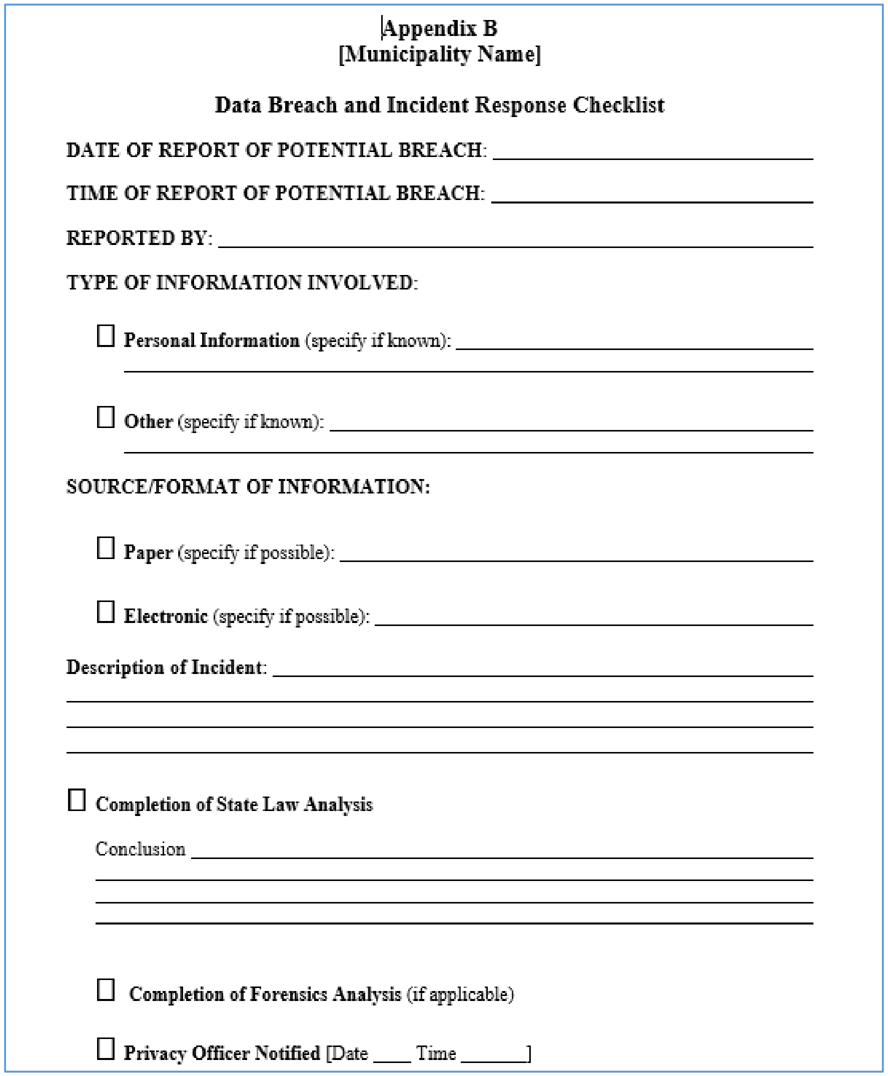
Incident Report
Prepared by:
Date:
Incident Date:

Description of Incident (e.g. type of information involved; paper or electronic data; unauthorized individual who accessed, used or disclosed the information; who reported the incident, etc.):

Resolution:

Determined Cause after Investigation:

Corrective Action/Mitigation:



Appendix B
[Municipality Name]

Data Breach and Incident Response Checklist

DATE OF REPORT OF POTENTIAL BREACH: ______________________

TIME OF REPORT OF POTENTIAL BREACH: ______________________

REPORTED BY: ______________________

TYPE OF INFORMATION INVOLVED:

□ **Personal Information** (specify if known): ______________________

□ **Other** (specify if known): ______________________

SOURCE/FORMAT OF INFORMATION:

□ **Paper** (specify if possible): ______________________

□ **Electronic** (specify if possible): ______________________

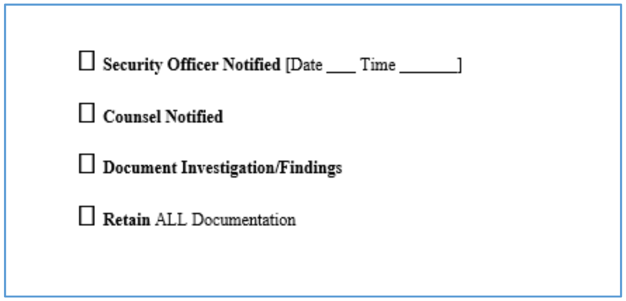
Description of Incident: ______________________

□ **Completion of State Law Analysis**

Conclusion ______________________

□ **Completion of Forensics Analysis** (if applicable)

□ **Privacy Officer Notified** [Date ____ Time _______]



□ **Security Officer Notified** [Date ___ Time _______]

□ **Counsel Notified**

□ **Document Investigation/Findings**

□ **Retain** ALL Documentation

Containment, Eradication & Discovery:
Checklist

- ❑ Implement processes to prevent alteration to the system(s) until a backup has been completed
- ❑ Implement processes to perform a full backup of the system(s) to forensically sterilize media (i.e. disk imaging) and store the backup in a secure area as an important part of the chain of custody (as applicable)
- ❑ Work with other departments and information technology staff, as appropriate, to determine the risk of continuing operations

  (e.g. deciding whether to shut down system, disconnect from network, continue operation, etc.)

NOTE THAT any decision to delay the containment should be discussed with legal counsel based on the risk and liability

Containment, Eradication & Discovery: Checklist (cont.)

- ❑ Implement processes to change passwords or other security safeguards on any compromised system
- ❑ Assign a team member to create and maintain documentation on all actions taken

Post-Incident Activity:
Checklist

❑ Responsibilities of the Response Team – Post Incident:

- Consider engaging the Planning Team as part of the post-incident activities
- Assess damage and cost; assess the damage and estimate both the damage cost and the cost of the containment efforts
- Review response and update policies, procedures, plans and guidelines; plan and take preventative steps so the intrusion will not recur
- Consider whether a procedure or policy was not followed which may have led to the intrusion
- Determine whether additional user education is warranted

Post-Incident Activity:
Checklist (cont.)

❑ Responsibilities of the Team – Post Incident:

- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Were the incident response procedures followed appropriately? How can they be improved?
- Are all systems patched, systems locked down, passwords changed, anti-virus updated, and appropriate procedures, guidelines and policies in place, etc.?
- Have changes been made to prevent a new and similar incident?
- Should any security measures be updated?
- What lessons have been learned from this experience?

Best Practices

- ❑ 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

MassCyberCenter at the MassTech Collaborative

Employee Training

Minimum Baseline of Cybersecurity Goal 1

Trained and Cyber-secure Employees

Benefits:

- Reduce the risk of cybersecurity incidents by improving the training and awareness of system users.

How to Achieve:

- Implement annual individual employee cybersecurity awareness training.
- Make it easy to do the training.
- Put incentives in place to get it done.

Go to MassCyberCenter.org
For guidance and a list of resources
to get started…

Cybersecurity Tabletop Exercises

An Important Part of Goal 3

Cyber Incident Response Planning

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!

Thank you!

For more information on Cyber Incident Response Planning and resources, go to

MassCyberCenter.org

Back Up Slides
and Additional Resources

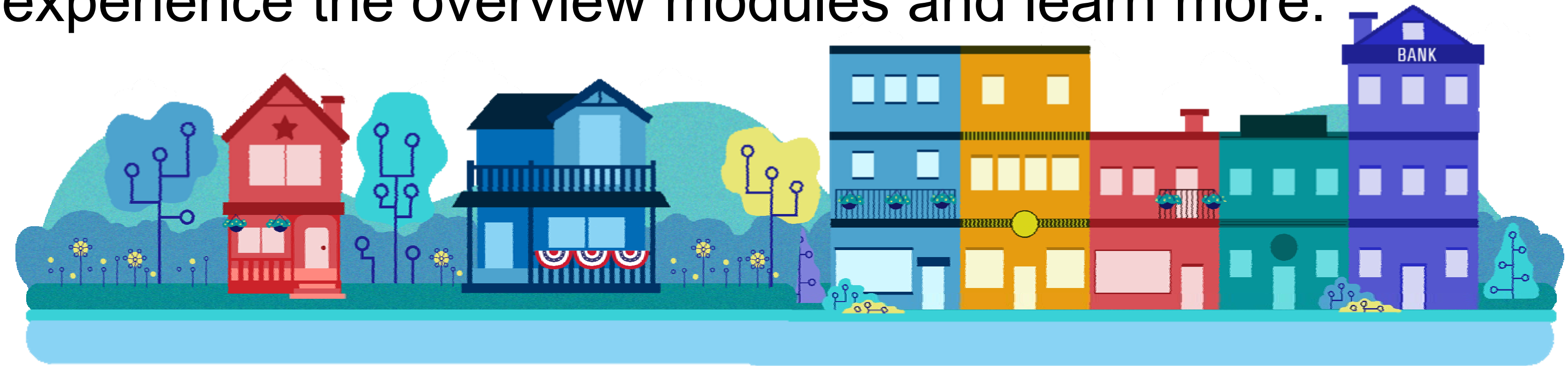
MassCyberCenter
at the MassTech Collaborative

Minimum Baseline Overview Modules

A fun way to introduce the framework and goals.

Using a notional cyberattack occurring in the fictional town of Massboro as an example to explain the Minimum Baseline of Cybersecurity, the first module introduces the Minimum Baseline, and the other four modules explain each of the four goals.

Go to MassCyberCenter.org and look under Resiliency to experience the overview modules and learn more.



MassCyberCenter at the MassTech Collaborative

Helpful Massachusetts Websites and Links

- **Mass.gov | Cybersecurity and Enterprise Risk Management Program**
  https://www.mass.gov/orgs/cybersecurity-and-enterprise-risk-management
  Program that focuses on protecting citizen data, ensuring the availability of the Commonwealth's networks and systems, and maintaining the continuity of government operations and services.
- **Mass.gov | Report a cybersecurity incident**
  - Report to your local police department and request they notify the Commonwealth Fusion Center
  - Other resources for reporting incidents:
    https://www.mass.gov/info-details/report-a-cybersecurity-incident

Helpful Federal Websites and Links

- **Multi State Information Sharing and Analysis Center (MS-ISAC) and the Center for Internet Security**
  Alerts and Advisories sent from MS-ISAC on a regular basis about threats that may impact state, local, tribal, and territorial government, plus valuable tools, resources, and services. Membership is free for municipalities: https://www.cisecurity.org/ms-isac/
- **Cybersecurity & Infrastructure Security Agency (CISA)**
  - Resources and guildance for State, Local, Tribal, and Territorial Governments: CISA.gov
  - **CISA's Cyber Essentials**—a guide for leaders of small businesses and small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices: https://www.cisa.gov/cyber-essentials
  - **CISA STOP Ransomware:** https://www.cisa.gov/stopransomware
  - **CISA CYBERSECURITY AWARENESS PROGRAM** is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online: https://www.cisa.gov/cisa-cybersecurity-awareness-program
- **US-CERT Alerts** up-to-date information on threats, hoaxes, and safety that you can subscribe to: https://www.us-cert.gov/ncas/tips
- **Federal Bureau of Investigation (FBI)**
  - **FBI Incident Response Policy:** https://www.fbi.gov/file-repository/incident-response-policy.pdf/view
  - **FBI Fact Sheet** – When to report cyber incidents to the federal government, what and how to report, and types of federal incident response: https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view

Additional Resources for Cybersecurity –
Frameworks, Best Practices, Training

- **National Institute of Standards and Technology (NIST)**
  https://www.nist.gov/
  In particular, the **Computer Security Resource Center (CSRC)** (http://csrc.nist.gov) holds a collection of papers that describe security best practices, called NIST Special Publications. They also create security assessment tools.
- **Cybrary**
  https://cybrary.it/
  Cybrary is possibly one of the best IT Security education sites on the internet. It contains full-length college course videos for everything from basic networking up to and including training for certifications, explanations of secure coding, penetration testing and everything else security related.

Additional Resources for Cybersecurity – Blogs & Podcasts

- **Krebs on Security**
  https://krebsonsecurity.com/about/
  Brian Krebs, author of Spam Nation is also one of the better-known security bloggers in the world, having written over a thousand articles on security.
- **Security Nation Podcast**
  https://www.rapid7.com/blog/series/security-nation/security-nation-season-5/
  Security Nation is a podcast dedicated to celebrating the champions in the cybersecurity community who are advancing security in their own ways.
- **Security Now! Podcast**
  https://www.grc.com/securitynow.htm
  A weekly security-focused podcast that covers all topics from law, current events, to conference reviews and explanations of specific exploits as they are discovered in the world.
- **Robinson + Cole Blog - Data Privacy Security Insider**
  www.dataprivacyandsecurityinsider.com
  Weekly posts on cybersecurity and risk management