

Building a Culture of Cybersecurity: Minimum Baseline of Cybersecurity for Municipalities

Monday, February 14, 2022
Massachusetts Municipal Association
Workshop

Workshop Panelists

- **Sam Curry**, Chief Security Officer, *Cybereason*; President, *Cybereason Government Inc.*; and Visiting Fellow at the *National Security Institute*
- **Lt. Brian Gavioli**, *Massachusetts State Police*, *Commonwealth Fusion Center*
- **Susan Noyes**, Information Technology Manager, *Executive Office of Technology Services and Security*, *Office of Municipal and School Technology*
- **Meg Speranza**, Resiliency Program Manager, *MassCyberCenter*
- **Stephanie Helm (Moderator)**, Director, *MassCyberCenter*

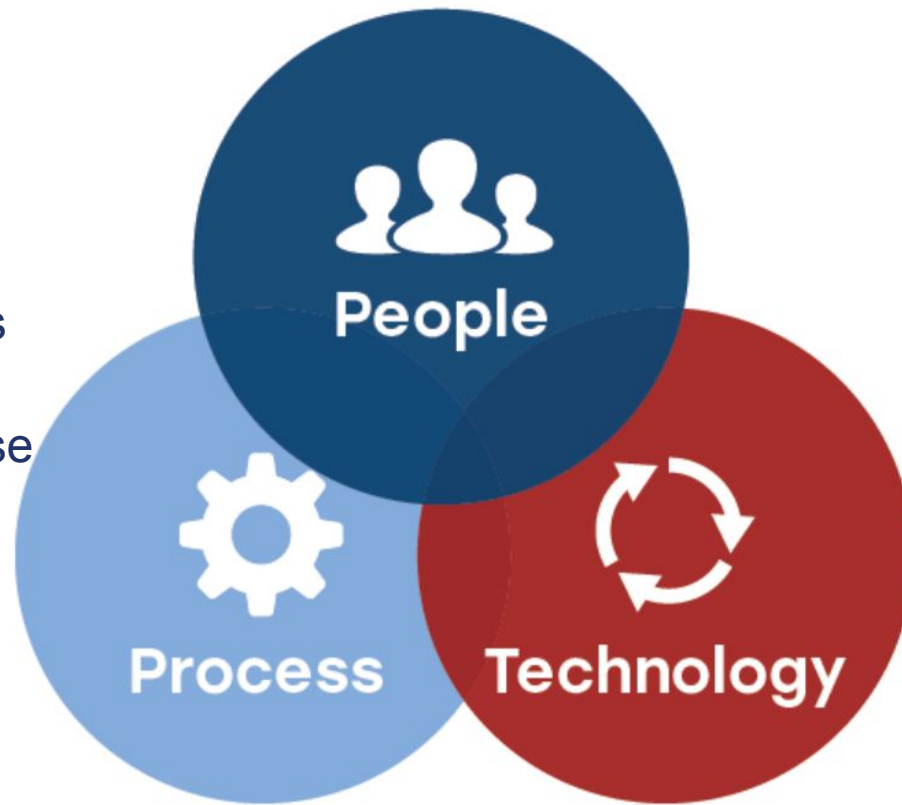
Municipal Cybersecurity Threats

*What are they, and
how are they changing?*

What is Cybersecurity?

- Leadership Talent/employment
 - Training/education
 - Citizens

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



- Sensors
- Decision aids
- Defense tools

Minimum Baseline of Cybersecurity for Municipalities

The Minimum Baseline of Cybersecurity for Municipalities is 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:

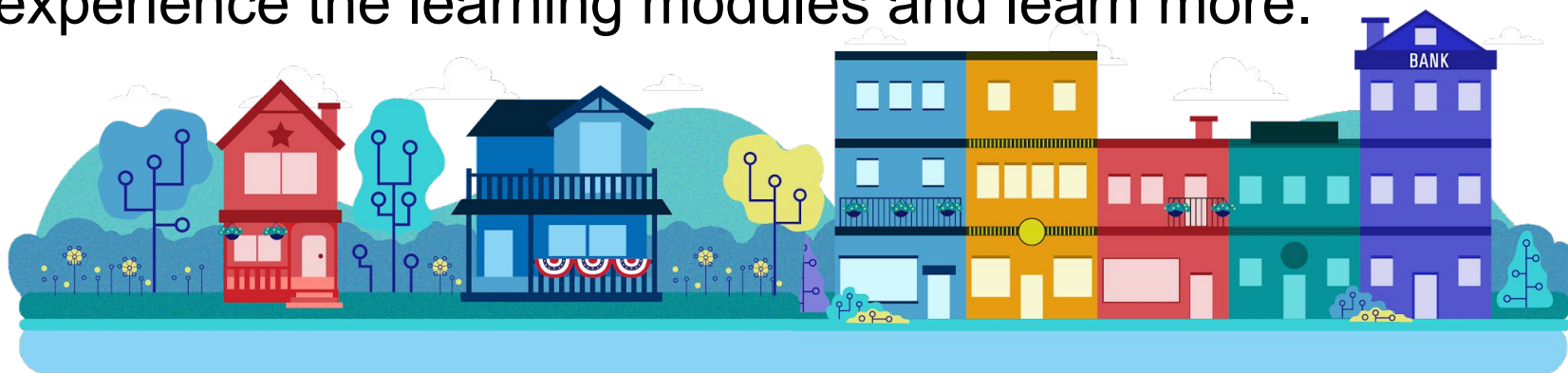


Minimum Baseline Learning Modules

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 learning modules and learn more.



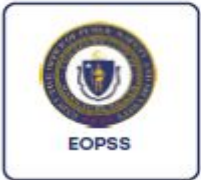
Commonwealth Resources for Municipalities



MassCyberCenter

Municipal Cybersecurity

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

Homeland Security Grant Program

Advocates and helps with preparedness and planning for the event of a national, state, or local emergency. mass.gov/service-details/homeland-security-grants



Operational Services Division (OSD)

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

Provides a list of approved vendors that offer 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.

mass.gov/doc/its78/download



Community Compact Cabinet

Community Compact Program

Champions municipal interests across all executive secretariats and agencies, and to develop, in consultation with cities and towns, mutual standards and best practices for both the state and municipalities. mass.gov/best-practices-program



Executive Office of Technology Services and Security (EOTSS)

Municipal Cybersecurity Awareness Grant Program

Offers 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

Office of Municipal and School Technology

IT & Cybersecurity Health Check Programs

Provides opportunities for local government to access basic cybersecurity services at no cost. mass.gov/orgs/office-of-municipal-and-school-technology

SAVE-THE-DATE



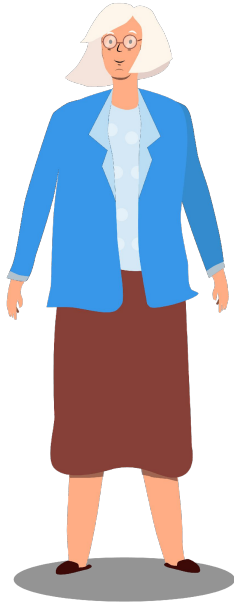
Massachusetts Municipal
Cybersecurity Summit
6 October 2022

What topics would you like to see covered?

Please put ideas in the *Q&A Chat feature* or email
MassCyberCenter@MassTech.org

We hope to see you there!

Election Security for Municipalities



Your best resource for local election security is your **City or Town Clerk**

Your Clerk has information and access to resources from the *Secretary of the Commonwealth's Office*, including Election Security Analysts and training



Challenges to Building a Culture of Cybersecurity in your Municipality

What challenges do you face?

(Enter your challenge or question into the Q&A Chat feature)

ADDITIONAL INFORMATION

Security and Public Records Requests – MassCyberCenter and MMA/MIIA

Collaboration on memorandum about the Massachusetts Public Records Law (M.G.L. c. 66) to provide municipalities with guidelines for handling public records requests about information technology and internal computer systems.

- **Concern that such records requests may facilitate unauthorized access to systems and data for malicious purposes.**
- **Records custodians may invoke exemptions in M.G.L. c. 4, § 7(26):**
 - ***Exemption (n)*** states that certain types of records shall not be considered “public records” if, in the reasonable judgment of the record custodian, they are likely to jeopardize public safety or cyber security.
 - ***Exemption (a)*** if the requested records may disclose records that are “specifically or by necessary implication exempted from disclosure by statute” (like health information).



Municipalities should consult with their city solicitor or town counsel regarding Massachusetts law and direct inquiries regarding the Public Records Law to the Division of Public Records at (617) 727-2832 or pre@sec.state.ma.us.

Third-Party Risk – Review and Manage Contracts

Third-Party Risk can be defined as the potential risk that arises from an organization relying on outside parties to perform business services or activities on their behalf.



- **Review Contracts Carefully**

- When does the vendor have a requirement to communicate an incident to you?

- **SUSPECTED vs. KNOWN Malicious Activity**

- What are your contractual obligations?
- What are the vendor's contractual obligations?

- **Best Practices**

- Service Levels – Contractually defined
- Contractual Obligations – language mandating specific behavior and/or action by vendor
- Governance - Defined periodic meetings with service provider reviewing performance
- Special Termination Rights – ID in MSA or supporting SOWs

Minimum Baseline of Cybersecurity Goals

Trained and
Cyber-secure
Employees

Benefits

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

How

- Annual individual employee cybersecurity awareness training.
- Make it easy and put incentives in place to get it done.

Improved
Threat
Sharing

Benefits

- Respond faster to threats and improve regional awareness and resilience by sharing cyber threat information.

How

- Sign up for threat sharing alerts through MS-ISAC or CISA; get to know neighboring towns; join a regional IT group.

Cyber
Incident
Response
Planning

Benefits

- Strengthen defenses and minimize cyber incident impacts by creating an effective strategy for handling cyber incidents.

How

- Use tools and resources to create a cyber incident response plan to protect against and respond to cyberattacks. Go to MassCyberCenter.org for more information.

Secure
Technology
Environment
and Best
Practices

Benefits


- Reduce the threat of cybersecurity incidents and minimize incident impacts by implementing best practices to make your technology environment more secure.

How

- Some basic best practices for getting started include backing up critical data and systems, requiring strong passwords, and updating and patching systems regularly.

Minimum Baseline of Cybersecurity

Goal 1



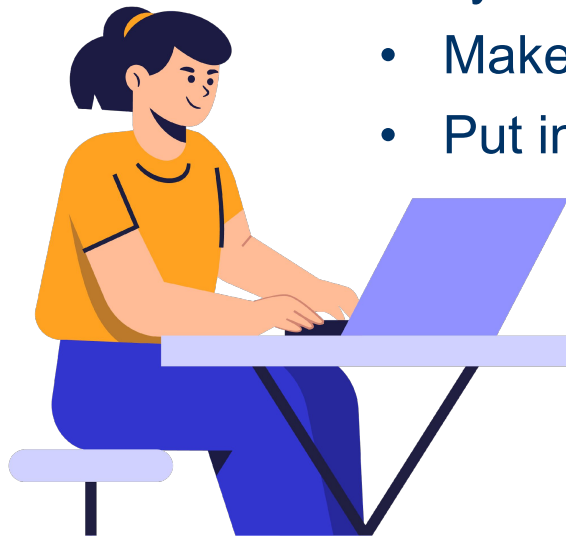
Trained and
Cyber-secure
Employees

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.



**Guidance and a list of
resources to get started...**

Minimum Baseline of Cybersecurity

Goal 2

Benefits:

- Respond faster to threats and improve regional awareness and resilience by sharing cyber threat information.



Improved
Threat
Sharing

How to Achieve:

- Sign up for threat-sharing alerts from MS-ISAC (it's FREE).
- Get to know your neighboring cities and towns.
- Join a regional IT group through the EOTSS Office of Municipal and School Technology.

Guidance and a list of resources to get started...



Minimum Baseline of Cybersecurity

Goal 3

Cyber
Incident
Response
Planning

Benefits:

- Strengthen municipal defenses and minimize cyber incident impacts by creating an effective strategy for handling cyber incidents.

How to Achieve:

- Use the tools and resources at MassCyberCenter.org to create a cyber incident response plan to protect against and respond to a cyberattack.



**Guidance and a list of
resources to get started...**

Minimum Baseline of Cybersecurity

Goal 4

Benefits:

- Reduce the threat of cybersecurity incidents and minimize incident impacts by implementing some basic best practices to make your technology environment more secure.



How to Achieve:

- There are many best practices listed in the resources. Here are a few to get started:
 - Require strong passwords
 - Backup critical data and systems
 - Update and patch systems regularly
 - Do annual vulnerability assessments



Guidance and a list of resources to get started...