

# **Cybersecurity for Local Government:**

## **Minimum Baseline of Cybersecurity for Municipalities**

**Stephanie Helm**

**Director, MassCyberCenter**

Thursday 31 March 31 2022

New England States Government Finance Officers Association Workshop



MASSACHUSETTS  
TECHNOLOGY  
COLLABORATIVE

**OUR MISSION:**

We strengthen the competitiveness of the tech and innovation economy by driving strategic investments, partnerships, and insights that harness the talent of Massachusetts.



THE INNOVATION INSTITUTE

**Mission:**

*Innovation  
Economy*



MASSACHUSETTS CENTER for  
ADVANCED MANUFACTURING

**Mission:**

*Advanced  
Manufacturing*



MASSACHUSETTS  
BROADBAND INSTITUTE

**Mission:**

*Broadband*



MASSACHUSETTS  
eHEALTH INSTITUTE

**Mission:**

*Digital Health  
and Caregiving*



MassCyberCenter

**Mission:**

*Cybersecurity*

---

# Municipal Cybersecurity Threats

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

# Threats

Security Boulevard

**U.S. Healthcare Data Breach Cost \$4 Billion in 2019. 2020 Won't Be Any Better**  
Ransomware will continue to be a plague on healthcare: While ransomware attackers will target any business they believe that they can infect ...

Worcester Telegram

**Local communities fight back on cyberattacks**  
Local communities fight back on cyberattacks ... the police department in this northwestern Worcester County town of about 12,000 is still not ...  
Sep 21, 2019

60 MINUTES

TechRepublic

**FBI, Secret Service investigating cyberattack on Florida water treatment plant**  
Federal law enforcement is now looking into a cyberattack at a water treatment plant in Oldsmar, FL where someone was able to remotely ...  
4 weeks ago



ransomware PRODUCED BY HENRY SCHUSTER



**Ransomware ravages municipalities nationwide this week**  
Doug Olenick Online Editor  
Follow @DougOlenick



Home > Security > Network Security

NEWS ANALYSIS

**Why local governments are a hot target for cyberattacks**

Recent ransomware and other attacks underscore the value attackers see in the data stored in city and regional government systems. Here's why they are vulnerable and what they can do to reduce the threat.



By Cynthia Brumfield

BetaBoston

**Hacking attacks plague Massachusetts schools**  
Hacking attacks plague Massachusetts schools ... disrupted in multiple districts, forcing schools to pay thousands of dollars in cyber-protection.  
4 weeks ago



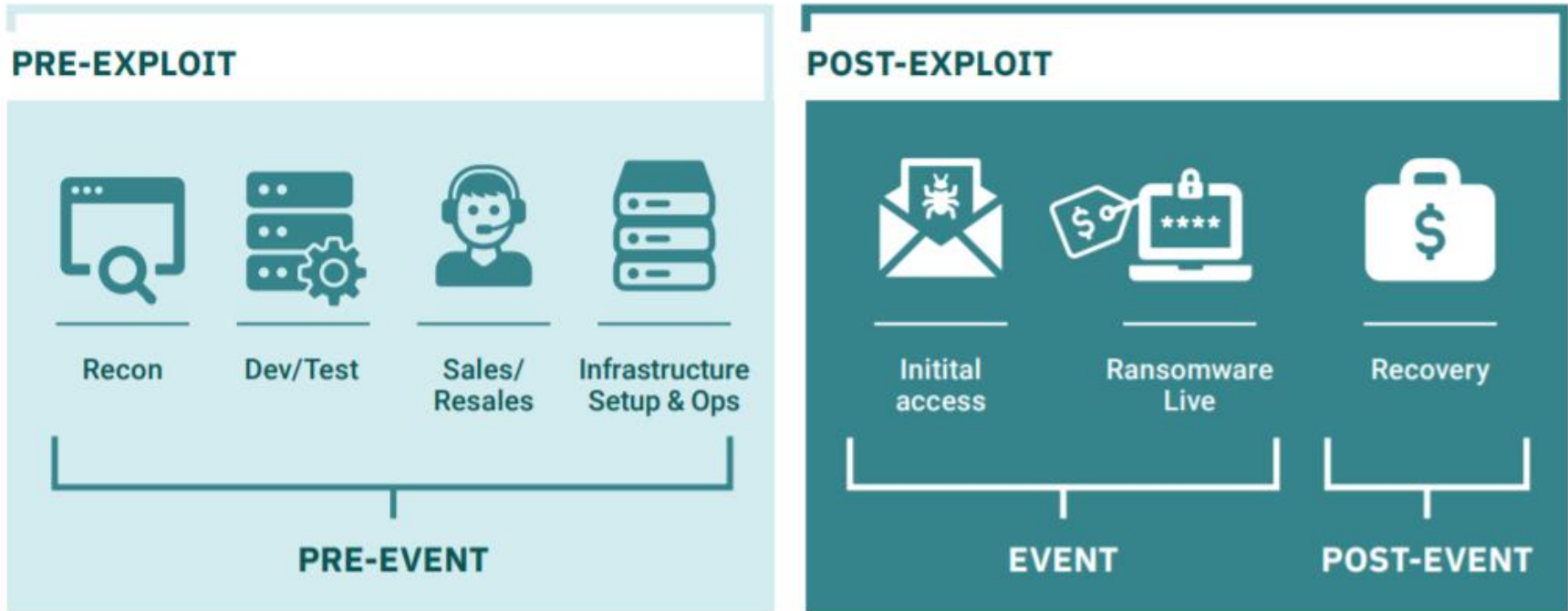
**Cyberattack hits Augusta municipal operations; City Center closed**

Officials say a nasty, intentionally deployed virus shut down public safety computers and made the city's entire network unusable, but the phone system and public safety radio system were not affected.

BY KEITH EDWARDS KENNEBEC JOURNAL



# Ransomware Kill Chain

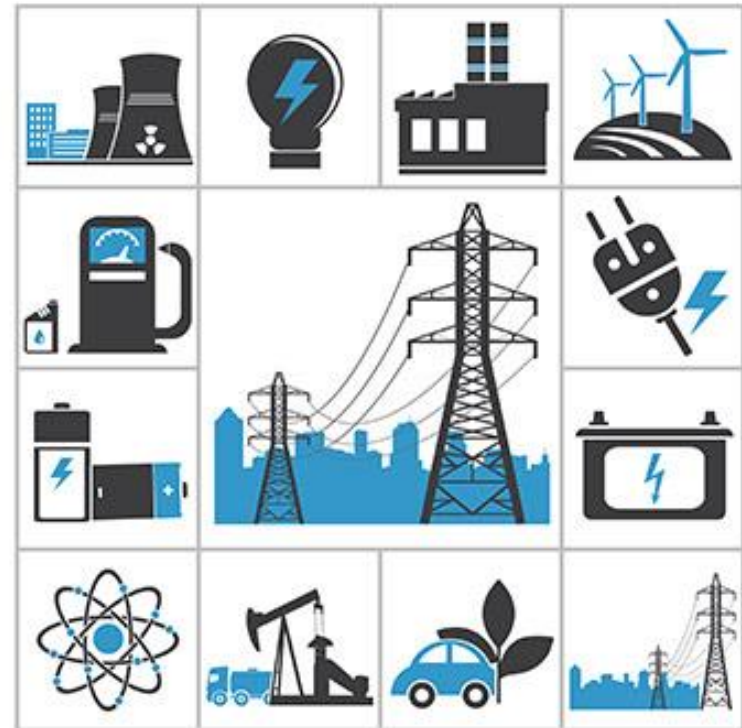


Source: World Economic Forum's Partnership against Cybercrime in collaboration with Accenture

# Threat Targets: Information and Safety



Federal Trade Commission <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security>

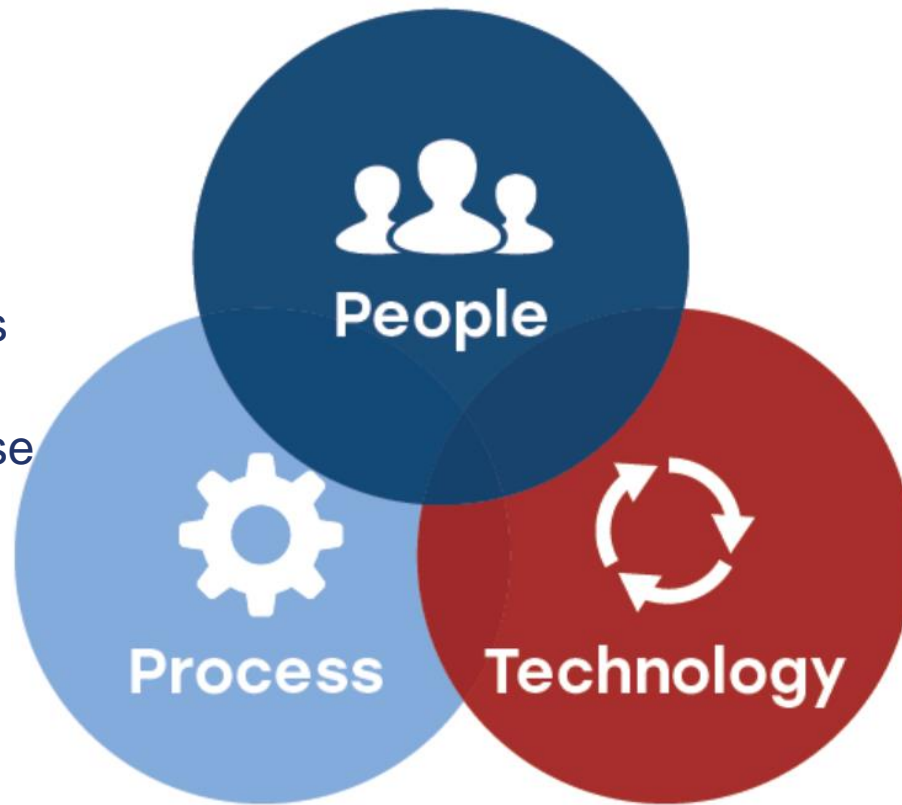


National Institute of Standards and Technology  
<https://www.nist.gov/news-events/news/2015/12/nist-seeks-comments-cybersecurity-framework-use-potential-updates-and>

# What is Cybersecurity?

- Leadership Talent/employment
  - Training/education
  - Citizens


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



- Sensors
- Decision aids
  - Defense tools

# Cybersecurity Toolkit for Municipalities

<https://masscybercenter.org/municipal-toolkit>



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 | MelH

MassCyberCenter at MassTech

About Ecosystem Resiliency 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. <a href="https://www.cnbc.com/2018/03/28/a-cyberattack-hobbles-atlanta-and-security-experts-shudder.html">https://www.cnbc.com/2018/03/28/a-cyberattack-hobbles-atlanta-and-security-experts-shudder.html</a>
Alarm in Texas as 23 towns hit by 'coordinated' ransomware attack	MON, AUG 19 2019 Coordinated Ransomware Attack on 23 Towns. <a href="https://www.cnbc.com/2019/08/19/alarm-in-texas-as-23-towns-hit-by-coordinated-ransomware-attack.html">https://www.cnbc.com/2019/08/19/alarm-in-texas-as-23-towns-hit-by-coordinated-ransomware-attack.html</a>
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. <a href="https://www.cnbc.com/2019/06/26/baltimore-florida-ransomware-attacks-kick-off-new-era-for-ransomware.html">https://www.cnbc.com/2019/06/26/baltimore-florida-ransomware-attacks-kick-off-new-era-for-ransomware.html</a>
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. <a href="https://www.govtech.com/security/Indiana-County-Suffers-Service-Crippling-Ransomware-Attack.html">https://www.govtech.com/security/Indiana-County-Suffers-Service-Crippling-Ransomware-Attack.html</a>
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. <a href="https://www.cnbc.com/2019/07/26/louisiana-declares-state-of-emergency-after-cybercriminals-attack-school-districts.html">https://www.cnbc.com/2019/07/26/louisiana-declares-state-of-emergency-after-cybercriminals-attack-school-districts.html</a>
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. <a href="https://www.cnbc.com/2019/05/26/wolters-kluwer-baltimore-ransomware-attacks-have-big-ripple-effects.html">https://www.cnbc.com/2019/05/26/wolters-kluwer-baltimore-ransomware-attacks-have-big-ripple-effects.html</a>

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.





# 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.

## Four goals:



# Minimum Baseline Learning Modules

## Introduction to the framework and goals

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

Go to [MassCyberCenter.org](https://MassCyberCenter.org) and look under Resiliency to experience the learning modules and learn more.



# 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



# Commonwealth Resources for Municipalities



## MassCyberCenter

### Municipal Cybersecurity

Provides tools and educates municipalities statewide on best cybersecurity practices and threats. [masscybercenter.org/municipalities](https://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](https://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](https://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](https://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](https://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](https://mass.gov/orgs/office-of-municipal-and-school-technology)

# SAVE-THE-DATE



Massachusetts Municipal  
**Cybersecurity Summit**  
6 October 2022

**We hope to see you there!**

*For last year's Summit, check out the recordings at  
<http://masscybercenter.org/events/massachusetts-municipal-cybersecurity-summit>*

# MassCyberCenter Team!



**Visit our website to connect with us and learn more:**

**[MassCyberCenter.org](https://www.masscybercenter.org)**

---

# ADDITIONAL INFORMATION

# 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](https://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

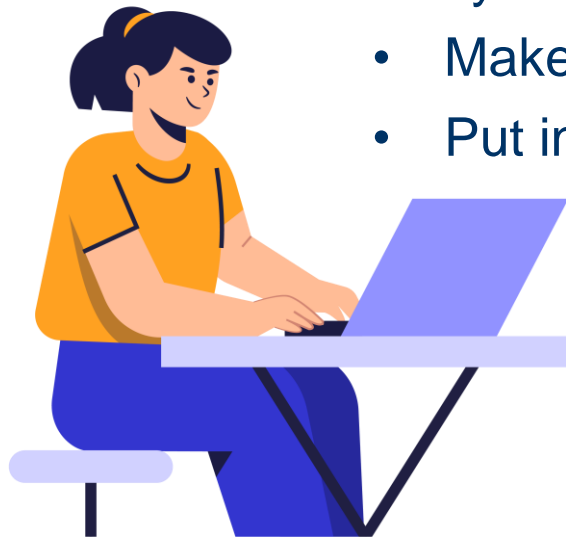
Trained and  
Cyber-secure  
Employees

### 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](https://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...**

