MassCyberCenter
at MassTech

Cybersecurity Webinar For MMA Members

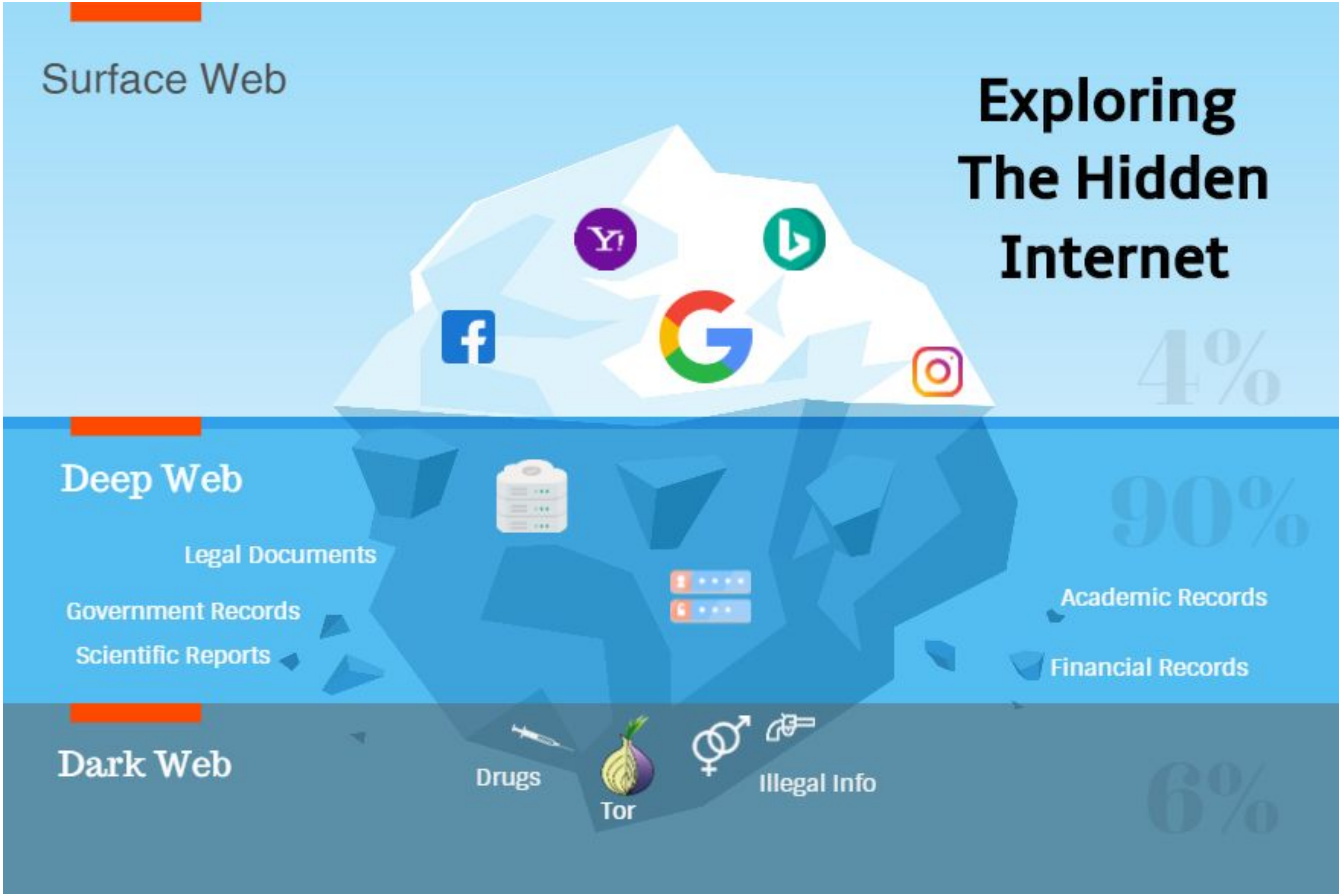
April 2020

Agenda

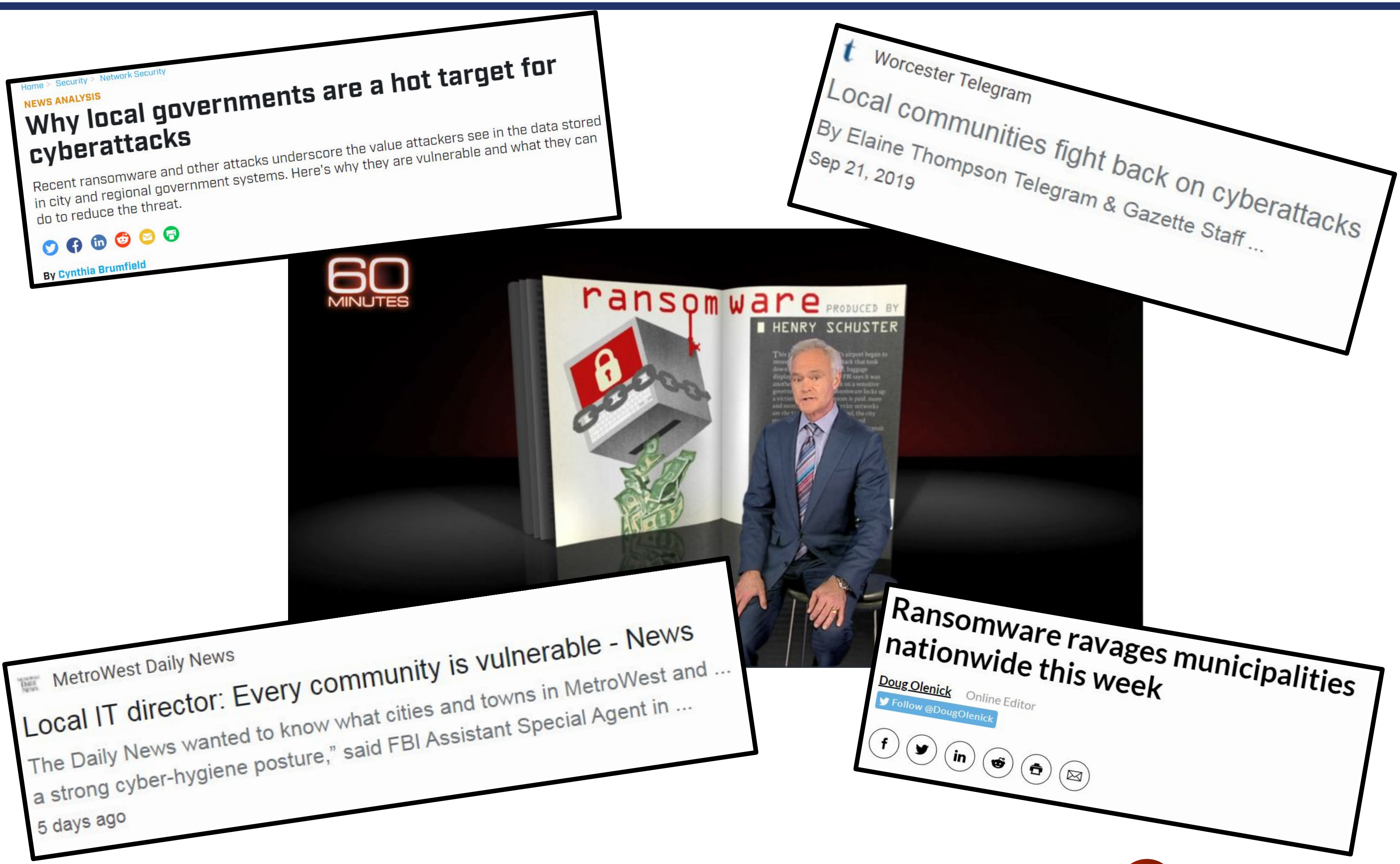
- Cybersecurity: What is it and Why is it Important?
- MassCyberCenter
- Municipalities and Cybersecurity Initiatives
- Building Cybersecurity Resiliency in your Municipality

Cybersecurity: What is it and Why is it important?

Layers of the Web



Threats



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

Worcester Telegram

Local communities fight back on cyberattacks

By Elaine Thompson Telegram & Gazette Staff ...

Sep 21, 2019

MetroWest Daily News

Local IT director: Every community is vulnerable - News

The Daily News wanted to know what cities and towns in MetroWest and ... a strong cyber-hygiene posture," said FBI Assistant Special Agent in ...

5 days ago

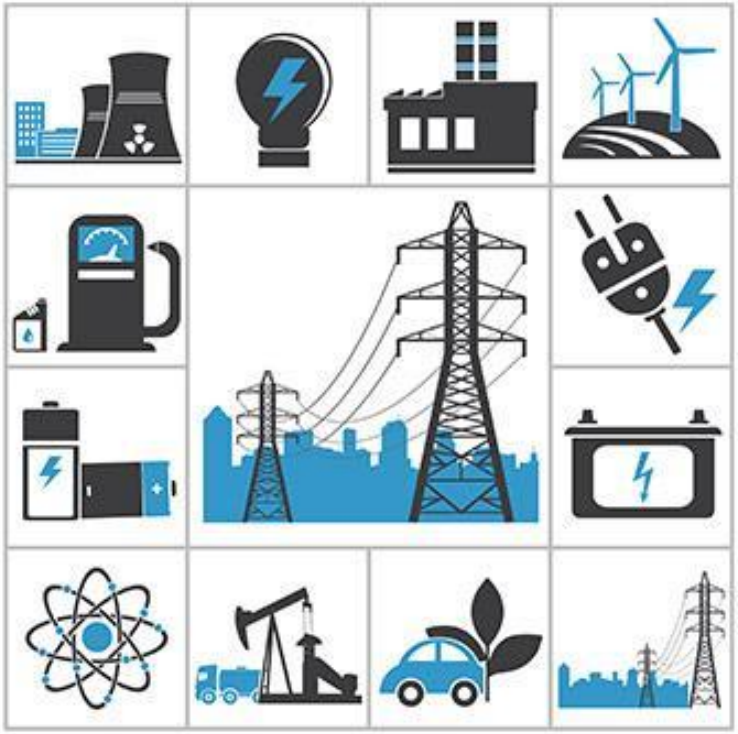
Ransomware ravages municipalities nationwide this week

Doug Olenick Online Editor

Follow @DougOlenick

Threat Targets: Information and Safety

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



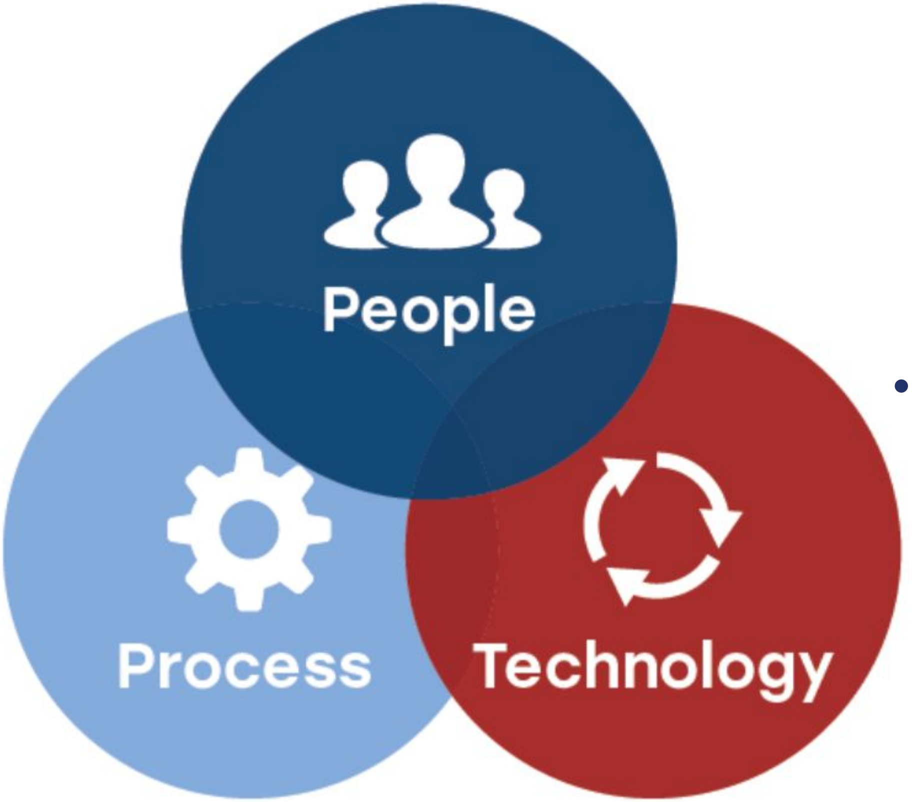
National Institute of Standards and Technology

https://www.nist.gov/news-events/news/2015/12/nist-seeks-comments-cybersecurity-framework-use-potential-updates-and

MassCyberCenter
at MassTech

What is Cybersecurity?

- Leadership Talent/employment
- Training/education
- Citizens



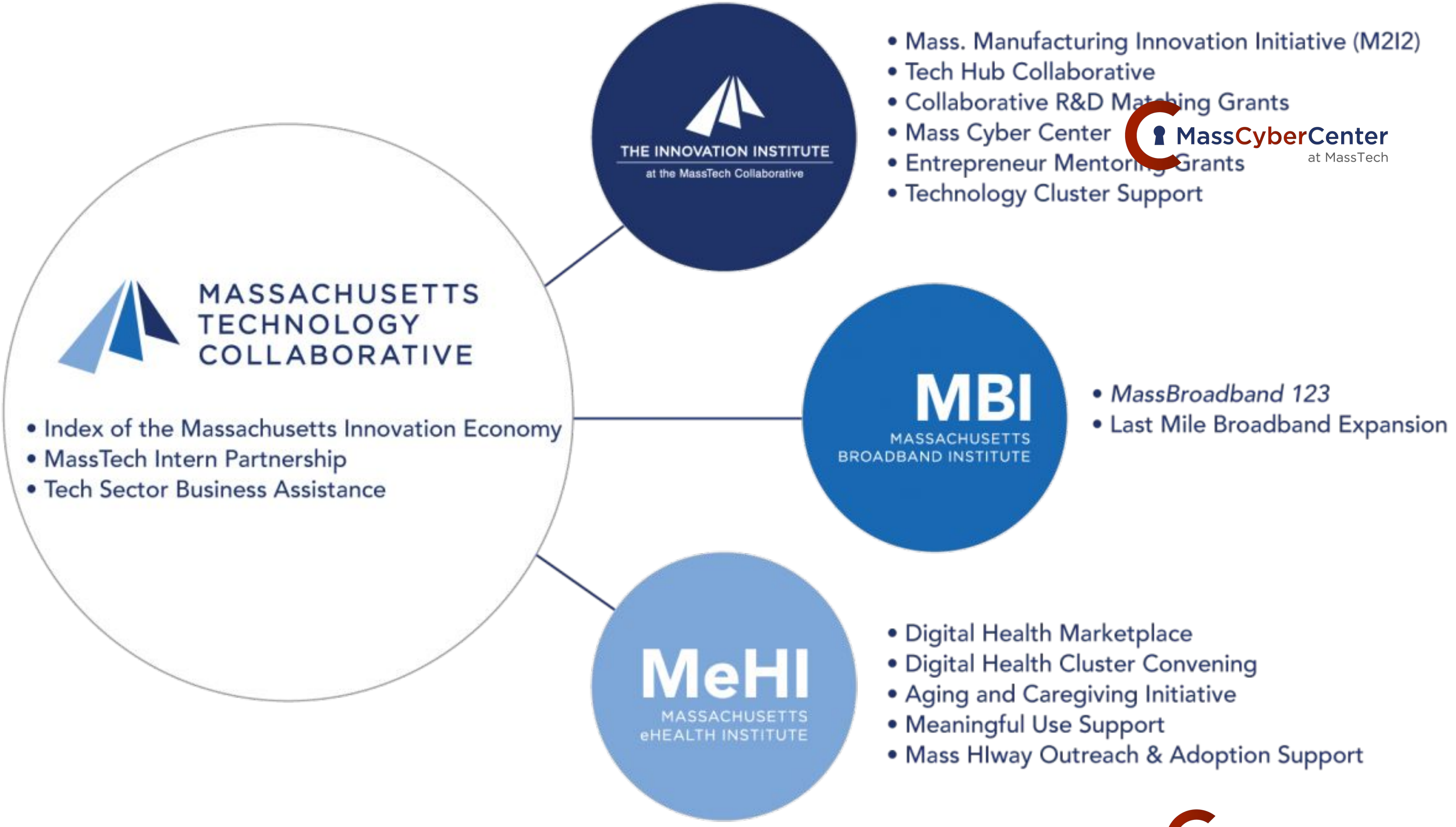
- Cyber standards and procedures
- Incident response plans/ recovery
- Engagement

- Sensors
- Decision aids
- Defense tools

Massachusetts Cybersecurity Center

MassCyberCenter

Massachusetts Technology Collaborative



MASSACHUSETTS TECHNOLOGY COLLABORATIVE

- Index of the Massachusetts Innovation Economy
- MassTech Intern Partnership
- Tech Sector Business Assistance

THE INNOVATION INSTITUTE at the MassTech Collaborative

- Mass. Manufacturing Innovation Initiative (M2I2)
- Tech Hub Collaborative
- Collaborative R&D Matching Grants
- Mass Cyber Center
- Entrepreneur Mentoring Grants
- Technology Cluster Support

MassCyberCenter at MassTech

MBI MASSACHUSETTS BROADBAND INSTITUTE

- *MassBroadband 123*
- Last Mile Broadband Expansion

MeHI MASSACHUSETTS eHEALTH INSTITUTE

- Digital Health Marketplace
- Digital Health Cluster Convening
- Aging and Caregiving Initiative
- Meaningful Use Support
- Mass HIway Outreach & Adoption Support

Mission and Strategy Pillars

MassCyberCenter will **enhance conditions for economic growth** through **outreach to the cybersecurity ecosystem** of Massachusetts while **fostering cybersecurity resiliency** within the Commonwealth.

Cybersecurity Ecosystem Development

- Vendors
- Tech Companies
- R&D
- Key Sectors
- Non-Profits
- Customers
- Talent

Resiliency for the Commonwealth (Public and Private Sector)

- State agencies
- Federal partners
- Municipalities
- Critical infrastructure owners
- Citizens

Communication, Collaboration, and Outreach

- Citizen awareness
- Ecosystem promotion
- Talent recruitment
- Academia
- Research
- Innovators

Cyber Resilient Massachusetts Working Group

Mission

Bring together public and private sector leaders to identify ways the Commonwealth's innovative technology ecosystem can help Massachusetts municipalities and critical institutions protect sensitive data, increase cybersecurity awareness, and respond to emerging threats.

- **Improve cybersecurity resiliency in the Commonwealth through planning**
- **Collaboration through outreach and education**
- **Sub-Working Groups**
  - Massachusetts Cyber Incident Response Framework
  - Tabletop Exercises
  - **Municipal Cybersecurity**
  - Critical Infrastructure

CRMWG Membership - Commonwealth

Secretary of the Commonwealth

Executive Offices

- Administration and Finance
    - Operational Services Division
- Education
- Health and Human Services
- Housing and Economic Development
    - Division of Banks
- Public Safety and Security
    - Massachusetts Army and Air National Guard
    - Massachusetts Emergency Management Agency
    - State Police, Commonwealth Fusion Center
    - Metro Boston Homeland Security Region
    - Western Region Homeland Security Advisory Council
- Technology Services and Security

State Auditor's Office

Authorities

- Massachusetts Bay Transportation Authority
- Massachusetts Convention Center Authority

CRMWG Membership - Other

Associations

- Advanced Cyber Security Center
- Community Action Pioneer Valley
- Massachusetts Health and Hospital Association
- Mass Municipal Association
- Northeast Public Power Association

Federal Government

- Department of Homeland Security
- Federal Bureau of Investigations
- Federal Emergency Management Agency
- Transportation Security Administration
- United States Secret Service
- U.S. Coast Guard

Municipalities

- City of Boston
- Town of Lexington
- Town of Princeton
- Town of Somerset
- City of Worcester

Municipalities and Cybersecurity Initiatives

What is the Municipality Cybersecurity Posture?

Massachusetts Municipal Association (MMA) Survey

- Eight question survey sent from MMA to Chief Municipal Officers in all 351 municipalities
- Results gathered between Thursday, October 17, and Friday, November 4
- 76 responses received

Overall Responses

- Only 10% (8) reported having an incident response plan; 79% do not have a plan; and the rest “Don’t Know”
- 93% backup critical business systems; 66% backup systems DAILY
- 84% use Cloud Hosting Services for one or more of the following: website hosting, communications, email, financial systems, payment services, permit services, and backups
- 20% have “0” on their IT team; 54% have 1 or 2 people on their IT Team; 13% have 3-5 on their IT Team; 13% have more than 5 on their IT Team
- Half reported having cybersecurity as a specific aspect of the IT job
- Half reported using a third-party vendor to manage their IT environments
  - 46% use vendors for all aspects of IT; 20% use vendors only to implement infrastructure and programs, but then let their IT personnel take over
- One third reported receiving some form of information security training
- One third reported that all municipal buildings are on the same network; the rest reported various configurations, including using VLANs to separate networks and multiple physical networks

Cybersecurity Toolkit for Municipalities

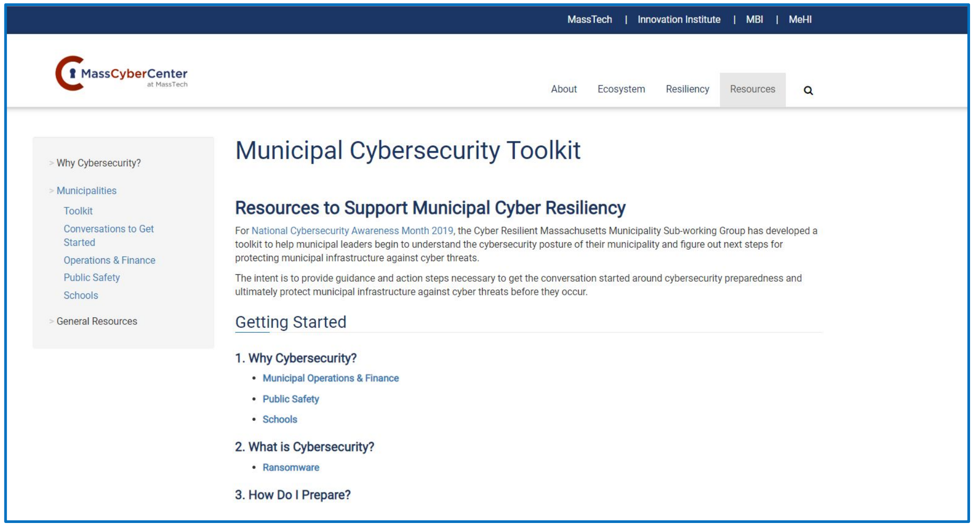
https://masscybercenter.org/municipal-toolkit

Announcement

Municipal Cybersecurity Toolkit

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

Learn More



Municipal Cybersecurity Toolkit

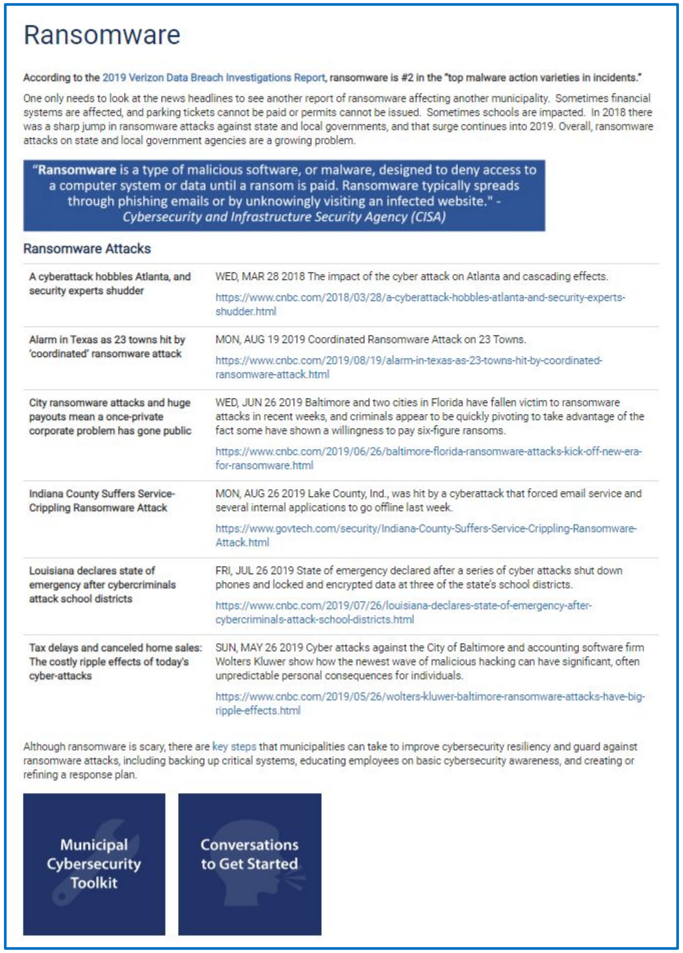
Resources to Support Municipal Cyber Resiliency

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.

Incident Response Plan Workshops

- Governor Baker announced in October 2019 $300,000 to facilitate a series of statewide workshops
- Provide municipalities with the tools to develop or review their cyber incident response plans and facilitate collaboration with neighboring communities.
- Through the planning process cities and towns will:
  - Prioritize the assets they need to protect,
  - Build a cybersecurity team,
  - Create processes to mitigate vulnerabilities, and
  - Raise awareness internally about the importance of cybersecurity.
- Strengthen regional collaboration around cybersecurity.
- RFP closed February 14, 2020.

Building Cybersecurity Resilience in Your Municipality

Cybersecurity Considerations for Leaders

- **Have a plan (PARTICIPATE IN OUR WORKSHOP!!)**
  - Address all aspects of key municipal operations
  - Prioritize key cybersecurity operations for protection and restoral
  - Include public relations, HR, risk management and legal experts in the planning process
- **Have a team and a leader**
  - 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 Programs

- **Employee Training on Cybersecurity**
  - Basic Cybersecurity Hygiene tailored to YOUR team and YOUR plan
  - Anti-phishing competitions and reminders
  - No one uses a muni system until basic training is received
- **MS-ISAC, CISA and other resources**
  - Free alerts from many agencies
  - Government discounts
- **Collaborate**
  - Invite your residents to get involved with awareness (Council on Aging or local library events)
  - Participate with regional cybersecurity working groups

Meet the MassCyberCenter Team!

Visit our website to connect with us:
https://www.masscybercenter.org

MassCyberCenter
at MassTech

Additional Information

CRMWG Sub-working Groups

Massachusetts Cyber Incident Response Framework (MCIRF) Sub-working Group – February 2019

Led by John Merto, CISO, Executive Office of Technology Services & Security

The Mission of the MCIRF Sub-working Group is to proactively create a Massachusetts Cyber Incident Response Framework that includes key stakeholders and provides a framework for a state-wide, coordinated response to a significant cyber incident.

Tabletop Exercises (TTX) Sub-working Group – March 2019

Led by COL Mark Kalin, Massachusetts Army National Guard

The Mission of the TTX Sub-working Group is to build cybersecurity resiliency for the Commonwealth through collective exercise design and execution in collaboration with public and private stakeholders.

CRMWG Sub-working Groups (continued)

Municipal Cybersecurity (Muni) Sub-working Group – March 2019

Led by the Office of Municipal & School Technology, EOTSS

The Mission of the Muni Sub-working Group is to Identify resources and provide guidance to improve the cybersecurity resiliency for 351 municipalities, and their public and private partners, across the Commonwealth of Massachusetts

Critical Infrastructure (CI) Sub-working Group – October 2019

Led by Major Scott Range, Massachusetts State Police, and Commander of the Commonwealth Fusion Center

The Mission of the CI Sub-working Group is to bring together public and private organizations to improve cybersecurity across Critical Infrastructure in the Commonwealth through collaboration and response planning. Initial focus will include four Critical Infrastructure Sectors: *Communications, Energy, Financial Services,* and *Healthcare & Public Health*

.

EOTSS Cybersecurity Training Grants

Purpose

The purpose of the Cybersecurity Awareness Grant Program is to provide cybersecurity end-user training, evaluation, and threat simulation to municipal governments and school districts with the goal of improving the overall cybersecurity posture.

- The 2019 grants, announced in October, provided cybersecurity awareness training for 94 municipalities and public school systems intended to help municipal officials better identify and mitigate the growing risk of cyber threats
- More than 42,000 employees of Massachusetts municipalities and school districts have the opportunity to receive the cybersecurity training

"These first-ever cybersecurity grant funds are a crucial tool to complement the over $9 million in funding for municipal IT infrastructure projects through the Community Compact program…"

– Lt. Gov. Karyn Polito

Community Compact Cabinet Program

Program Information

- Created in 2015, the Community Compact Cabinet 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. Offerings include:
  - Best Practices Program Grants
  - Efficiency & Regionalization (E&R) Grants
  - IT Grants
- In January 2020, the Lt. Governor announced $3 million in Community Compact Information Technology (IT) grants to help 51 municipalities strengthen their own technological infrastructure.
- Total amount of municipal IT grants awarded over the past five years is $12 million – a significant investment that is supporting over 300 municipal and school district projects designed to modernize and improve technology systems.
- MassCyberCenter continues to support collaboration across the Commonwealth to promote leveraging shared resources and expertise.

2020 Homeland Security Grant Program (HSGP)

Program Information

- Part of Department of Homeland Security (DHS) and Federal Emergency Management Agency's (FEMA's) focus to enhance and support SLTT's ability to prevent terrorism and other catastrophic events and prepare for security threats and hazards. Focus is on the 4 national priority areas:
    - Cybersecurity (including election security)
    - Soft targets/crowded places
    - Information and intelligence sharing
    - Emerging threats
- Administered through the Massachusetts Office of Public Safety and Security (EOPSS) Office of Grants and Research (OGR) and managed by the Homeland Security Planning Regions:
    - Metro Boston Homeland Security Region
    - Northeast Homeland Security Regional Advisory Council
    - Central Region Homeland Security Advisory Council
    - Southeast Region Homeland Security Advisory Council
    - Western Region Homeland Security Advisory Council
- MassCyberCenter and CRMWG working with HSRACs to create state-wide coordinated grant proposals for cyber initiatives.