MassCyberCenter
at the MassTech Collaborative

CYBERSECURITY: STAYING AHEAD OF THREATS LEVERAGING PEOPLE, PROCESS AND TECHNOLOGY

ILLUSTRATED WITH A CASE STUDY

Presentation to the New England Intergovernmental Audit Forum (NEIAF)

Erich Schumann, Founding Partner and CEO of Global Atlantic Partners LLC
Meg Speranza, Resiliency Program Manager, MassCyberCenter

21 September 2023

Agenda

- Introduction to the MassCyberCenter
- Cybersecurity Threats
- What is Cybersecurity?
- The Minimum Baseline of Cybersecurity
- Resources to help with cybersecurity

MASSACHUSETTS TECHNOLOGY COLLABORATIVE

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	MASSACHUSETTS CENTER for ADVANCED MANUFACTURING	MBI MASSACHUSETTS BROADBAND INSTITUTE	MeHI MASSACHUSETTS eHEALTH INSTITUTE	MassCyberCenter
Mission:	**Mission**:	**Mission:**	**Mission:**	**Mission:**
Innovation Economy	*Advanced Manufacturing*	*Broadband*	*Digital Health and Caregiving*	*Cybersecurity*

Mission and Strategy Pillars

MassCyberCenter **enhances 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 Sectors)

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

Communication, Collaboration, and Outreach

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

Cybersecurity Threats

- 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

MassCyberCenter
at the MassTech Collaborative

Cybersecurity Threats to local government

What makes local governments and schools 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 and schools are public-facing, providing a potent outlet and often resulting in a variety of disruptive, public consequences

Cybersecurity Threats
When Criminals gain access to networks – What could happen?

Access could allow theft of:

- Usernames/Passwords
- Banking Information
- Personal/Sensitive Information
- Business Practices
- Victim of future exploitation and attacks

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

MassCyberCenter
at the MassTech Collaborative

Cybersecurity Threats
Recent Attacks in the News

City Hit With Cyberattack, Some Data Released to Dark Web

– *NBC News, May 15, 2023*

Impact of cyberattack extends to Springfield, Mass. casino

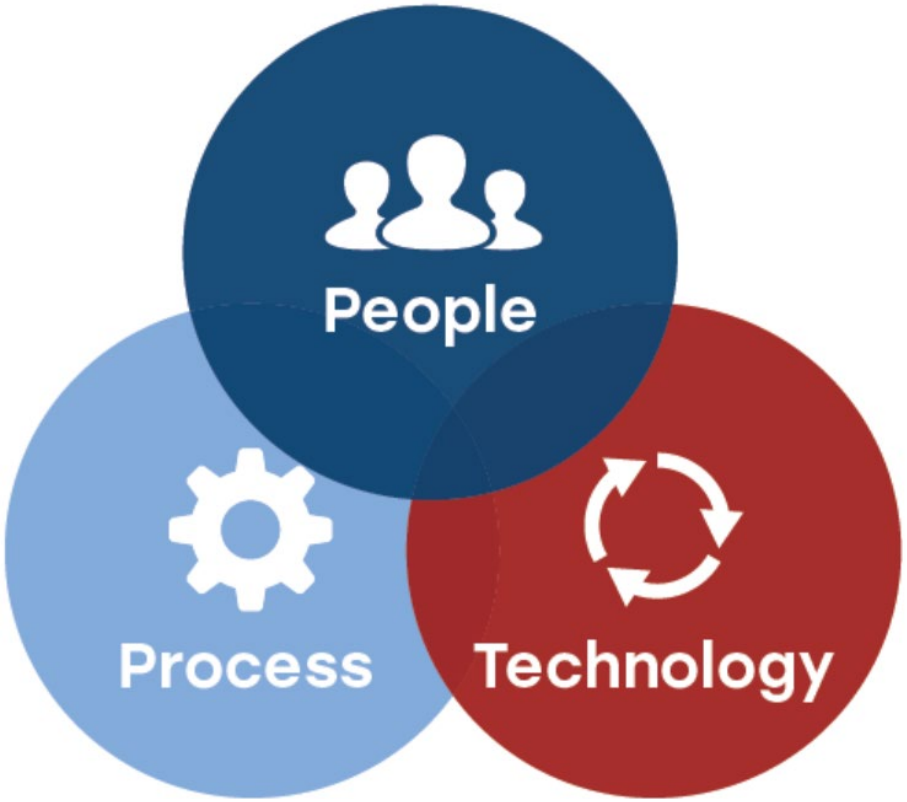
– *ABC News, Boston, September 16, 2023*

Schools Reopened Thursday After Ransomware Attack

– *Local Newspaper, January 31, 2023*

What is Cybersecurity

- Leadership Talent/employment
- Training/education
- Citizens



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

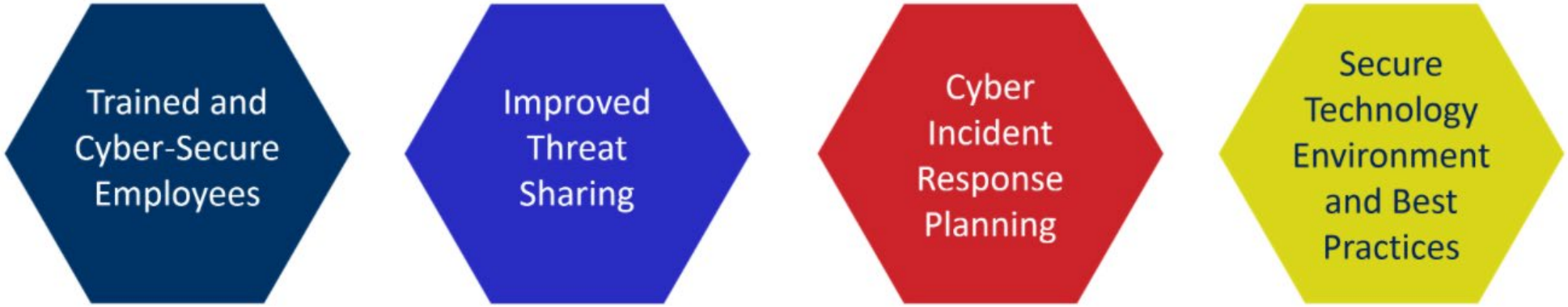
- Sensors
- Decision aids
- Defense tools

MassCyberCenter
at the MassTech Collaborative

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:



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

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

Commonwealth Cybersecurity Resources
A Cross-Agency Collaboration

EOTSS

Office of Municipal and School Technology (OMST)
Municipal Cybersecurity Awareness Grant Program
Cyber Health Checks

EOPSS

Office of Grants & Research (OGR)
Homeland Security Grant Program (HSGP)
State and Local Cybersecurity Grant Program (SLCGP)

MassCyberCenter
at the MassTech Collaborative

MassCyberCenter
Minimum Baseline of Cybersecurity
Cyber Incident Response Planning Materials

COMMONWEALTH FUSION CENTER
CFC

Massachusetts State Police – Commonwealth Fusion Center
Massachusetts Cybersecurity Program (MCP)

Community Compact Cabinet

Community Compact Program
Best Practices Program
IT Grant Program

OSD
OPERATIONAL SERVICES DIVISION

Operational Services Division (OSD)
ITS78: Statewide Contract for Cybersecurity and Incident Response Services

MassCyberCenter Team!




Visit our website to connect with us and learn more:

MassCyberCenter.org

MassCyberCenter
at the MassTech Collaborative

Thank you!

MassCyberCenter
at the MassTech Collaborative

ADDENDUM SLIDES

Helpful Massachusetts Websites and Links

- **MassCyberCenter.org**
- **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

- **Center for Internet Security and the Multi State Information Sharing and Analysis Center (MS-ISAC)**
  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 guidance for State, Local, Tribal, and Territorial Governments: https://www.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** that you can subscribe to for up-to-date information on threats, hoaxes: https://www.us-cert.gov/ncas/tips
- **Federal Bureau of Investigation (FBI)**
  - **Internet Crime Complaint Center:** https://www.ic3.gov/
  - **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.