MassCyberCenter
at the MassTech Collaborative

MMA
Massachusetts Municipal Association

Massachusetts Cybersecurity Update

MMA Annual Meeting
January 19, 2024

Agenda

- Introductions and program updates
- Panel: Status of Municipal Cybersecurity Programs in Massachusetts
- Questions and Answers

John Petrozzelli
Director
MassCyberCenter

MassCyberCenter Overview

The MassCyberCenter convenes the Massachusetts cybersecurity ecosystem to improve cybersecurity resiliency, workforce development, and public awareness within the Commonwealth by developing cutting edge programs, organizing engaging events, and leading collaborative working groups

Cybersecurity Ecosystem Development

- Cybersecurity Training and Education Working Group
- Jobs Board
- Cybersecurity Mentorship Program
- Cybersecurity SOC/Range

Resiliency for the Commonwealth
(Public and Private Sector)

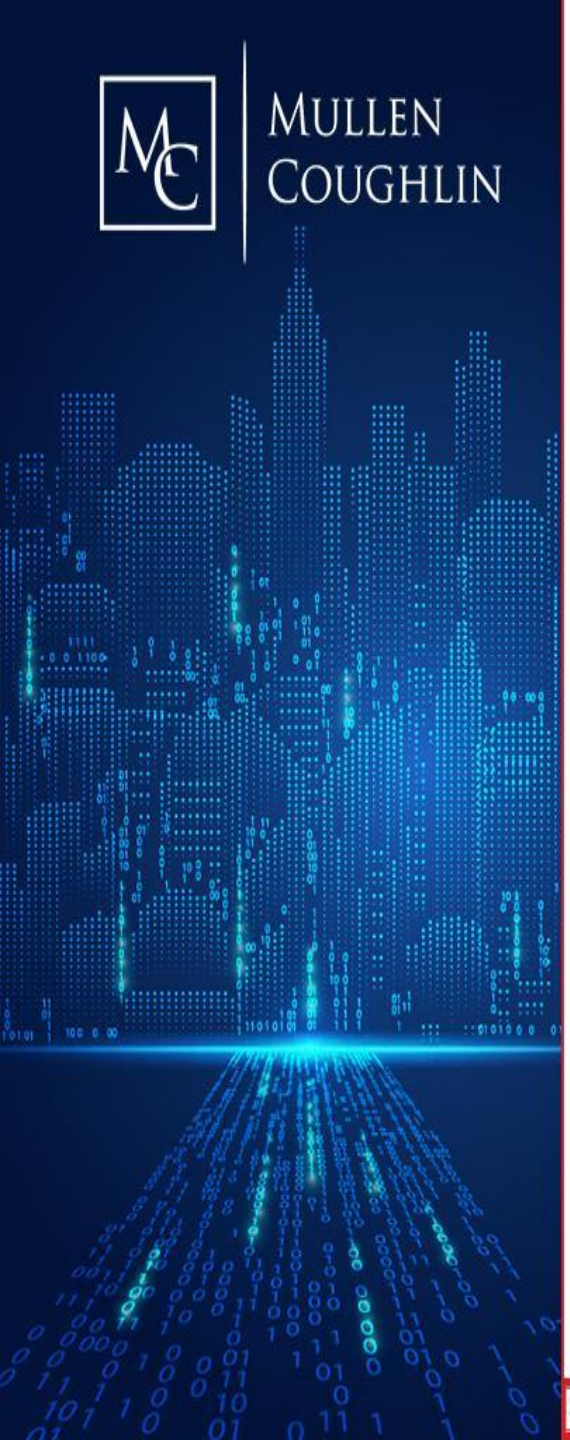
- Cyber Resilient Massachusetts Working Group
- Tabletop exercises
- Cyber Incident Response Plan Workshops
- Resources for Municipalities

Communication, Collaboration, and Outreach

- Massachusetts Cybersecurity Month (October)
- Citizen awareness
- Ecosystem promotion
- Talent recruitment
- National cyber events

Gregory Bautista
Partner

MULLEN COUGHLIN



MULLEN COUGHLIN

MMA Annual Meeting

Cybersecurity Legal Trends and Incident Response Statistics

1.19.2024

Mullen Coughlin Practices and Services

Advisory Compliance

- Incident Response Plan (IRP) Development
- Cyber Incident Response Tabletop Exercises
- Data Privacy Compliance Program Development
- HIPAA Compliance
- Artificial Intelligence (AI)
- Vendor Contract Review/Negotiation and Development of Vendor Management Program
- Data Transfer and Processing Agreement Development
- Security and Risk Assessments
- Data and Network Infrastructure Mapping
- Employee, Executive, and Board Data Privacy and Information Security Training
- Website Marketing Information, Privacy Policy and Terms-of-Use Development
- Document Retention/Destruction, Business Continuity and Data Recovery Plan Development
- M&A Due Diligence

Incident Response (Breach Coach)

- Detection of Incident and Mobilization of Incident Response Team
- Identification and Containment of Incident
- Forensic Collection and Analysis
- External Stakeholder Engagement
- Data Mining
- Legal Analysis/Notification and Disclosure
- Data Restoration, Ransomware Negotiation and Payment
- Post-Investigation Provisions

Regulatory Investigation

- Federal Bureau of Investigation (FBI)
- U.S. Department of Defense (DoD) and the DoD Cyber Crime Center (DC3)
- U.S. Department of Education
- U.S. Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR)
- U.S. Department of Homeland Security (DHS)
- U.S. Department of Justice (DOJ)
- U.S. Department of the Treasury and the Office of the Comptroller of the Currency (OCC)
- U.S. Federal Trade Commission (FTC)
- U.S. Federal Deposit Insurance Corporation (FDIC)
- U.S. Secret Service (USSS)

Privacy Litigation

- Single-plaintiff, class action and business-to-business disputes related to:
  - data privacy and security incidents
  - misuse of website tracking technologies
  - wiretapping
  - wire transfer fraud
  - technology-related errors and omissions
  - violations of U.S. state data privacy laws

New/Amended State Laws

Cybersecurity

- California (1/1/23)
- Iowa (7/1/23)
- Oklahoma (11/1/23)

Data Breach

- Connecticut (7/1/23)
- Nevada (Lenders) (3/31/24)
- Texas (7/1/23)
- Utah (5/3/23)

Data Broker

- Oregon (1/1/24)
- Texas (7/1/24)

Health Law

- California (Mental Health) (1/1/23)
- Nevada (3/31/24)
- New York (Healthcare Geofence Prohibition) (7/2/23)
- Washington (6/30/24)

Insurance Data Security Law

- Illinois (1/1/24)
- Pennsylvania (12/11/23)

Genetic Law

- Montana (10/1/23)
- Tennessee (7/1/23)
- Texas (9/1/23)
- Virginia (7/1/23)

Social Media/Children Law

- Arkansas (9/1/23)
- California (1/1/24)
- Connecticut (7/1/23)
- Louisiana (7/1/24)
- Ohio (1/15/24)
- Utah (5/3/23)

Student Law

- Arkansas (6/1/24)
- California (1/1/23)
- Florida (7/1/23)
- Utah (7/1/23)

Trends and Predictions: Threat Landscape

- Attack vectors
  - MFA bypass/fatigue
  - Sophisticated phishing/vishing
    - SIM swapping
  - Zero-Day/Firewall vulnerabilities
  - SaaS technology providers
  - Remote Desktop Protocol (RDP)
  - VPN credential stealers/brute force
- Threat groups
  - New/emerging groups
  - Splinter groups/RaaS

Incident Response

2020-2023

Incident Type

2020

Incident Type	Count
Ransomware	1,006 (29%)
Business Email Compromise (BEC) – Total	794 (23%)
BEC – Other	607
BEC – Wire Fraud	187
Third-Party Breach	583 (17%)
Network Intrusion	450 (13%)
Other	381 (11%)
Inadvertent Disclosure	214 (7%)
Total	**3,428 (100%)**

2021

Incident Type	Count
Ransomware	1,153 (29%)
Business Email Compromise (BEC) – Total	1,059 (27%)
BEC – Other	698
BEC – Wire Fraud	361
Third-Party Breach	623 (16%)
Network Intrusion	559 (14%)
Other	367 (9%)
Inadvertent Disclosure	209 (5%)
Total	**3,970 (100%)**

2022

Incident Type	Count
Business Email Compromise (BEC) – Total	1,077 (36%)
BEC – Other	733
BEC – Wire Fraud	344
Ransomware	732 (25%)
Network Intrusion	382 (13%)
Third-Party Breach	316 (11%)
Other	245 (8%)
Inadvertent Disclosure	207 (7%)
Total	**2,959 (100%)**

2023

Incident Type	Count
Business Email Compromise (BEC) – Total	1,343 (34%)
BEC – Other	996
BEC – Wire Fraud	347
Ransomware	884 (23%)
Third-Party Breach	749 (19%)
Other	403 (10%)
Network Intrusion	323 (8%)
Inadvertent Disclosure	218 (6%)
Total	**3,920 (100%)**

Government

Incident Type

2020

Incident Type	Count
Ransomware	72 (40%)
Inadvertent Disclosure	26 (14%)
Network Intrusion	25 (14%)
Business Email Compromise (BEC) – Total	24 (13%)
BEC – Other	21
BEC – Wire Fraud	3
Third-Party Breach	19 (10%)
Other	16 (9%)
Total	**182 (100%)**

2021

Incident Type	Count
Third-Party Breach	60 (30%)
Ransomware	49 (25%)
Business Email Compromise (BEC) – Total	39 (20%)
BEC – Other	33
BEC – Wire Fraud	6
Network Intrusion	21 (10%)
Inadvertent Disclosure	20 (10%)
Other	11 (5%)
Total	**200 (100%)**

202

Incident Type	Count
Ransomware	34 (28%)
Business Email Compromise (BEC) – Total	32 (26%)
BEC – Other	25
BEC – Wire Fraud	7
Inadvertent Disclosure	18 (15%)
Network Intrusion	16 (13%)
Third-Party Breach	15 (12%)
Other	7 (6%)
Total	**122 (100%)**

2023

Incident Type	Count
Business Email Compromise (BEC) – Total	46 (33%)
BEC – Other	38
BEC – Wire Fraud	8
Third-Party Breach	29 (21%)
Ransomware	25 (18%)
Network Intrusion	15 (11%)
Inadvertent Disclosure	13 (10%)
Other	10 (7%)
Total	**138 (100%)**

Ransomware-Specific

2020	
Number of RW Incidents	72 (40%)
Number of RW Incidents Paid	13 (18%)
Ransom Payment Reason	Delete Only – 0 (0%) Key and Delete – 2 (15%) Key Only – 11 (85%)
Average Ransom Demand	$524,478
Average Ransom Payment	$245,216
Median Ransom Payment	$140,000

2021	
Number of RW Incidents	49 (25%)
Number of RW Incidents Paid	9 (18%)
Ransom Payment Reason	Delete Only – 2 (23%) Key and Delete – 3 (33%) Key Only – 4 (44%)
Average Ransom Demand	$1,892,082
Average Ransom Payment	$252,044
Median Ransom Payment	$125,000

2022	
Number of RW Incidents	34 (28%)
Number of RW Incidents Paid	4 (12%)
Ransom Payment Reason	Delete Only – 1 (25%) Key and Delete – 2 (50%) Key Only – 1 (25%)
Average Ransom Demand	$894,444
Average Ransom Payment	$165,000
Median Ransom Payment	$80,000

2023	
Number of RW Incidents	25 (18%)
Number of RW Incidents Paid	0 (0%)
Ransom Payment Reason	Delete Only – N/A Key and Delete – N/A Key Only – N/A
Average Ransom Demand	$1,110,000
Average Ransom Payment	N/A
Median Ransom Payment	N/A

Business Email Compromise-Specific

2020	
Number of BEC Incidents	24 (13%)
Number of BEC-WF Incidents	3 (13%)
Average Amount Fraudulently Wired	$474,647
Median Amount Fraudulently Wired	$182,500

2021	
Number of BEC Incidents	39 (20%)
Number of BEC-WF Incidents	6 (15%)
Average Amount Fraudulently Wired	$94,000
Median Amount Fraudulently Wired	$94,000

2022	
Number of BEC Incidents	32 (26%)
Number of BEC-WF Incidents	7 (22%)
Average Amount Fraudulently Wired	$251,867
Median Amount Fraudulently Wired	$196,822

2023	
Number of BEC Incidents	46 (33%)
Number of BEC-WF Incidents	8 (17%)
Average Amount Fraudulently Wired	$198,825
Median Amount Fraudulently Wired	$148,926

Taylor Reynolds
Technology Policy Director
MIT's Computer Science and Artificial Intelligence Laboratory

Brian Gavioli
Detective Lieutenant | Unit Commander, Criminal Information Section
Commonwealth Fusion Center | Division of Homeland Security and Preparedness | Massachusetts State Police

Massachusetts cybersecurity program overview

The Massachusetts Cybersecurity Program (MCP) was established in 2016 in response to the growing concerns and threats to cybersecurity in the Commonwealth. The MCP is a program within the Commonwealth Fusion Center focused on cybersecurity threat reporting, training, education, and awareness. The MCP, through the Commonwealth Fusion Center, aims to be an integral point of contact in the Commonwealth in regard to cyber incidents. The MCP works closely with local, state, federal, and private sector agencies to establish effective communication and relationships.

- Information Sharing
  - MCP Distro List – Bulletins
- Training & Awareness
- Threat Briefings
  - MA Cyber Joint Monthly Threat Briefing Call
  - CRMWG
  - MeHI
- Reporting
- Coordination with Federal, State, Local partners
  - BRIC
  - FBI
  - DHS CISA, DHS I&A, MS-ISAC
  - USSS
  - MA-CIRT
  - EOTSS SOC
- Vulnerability & Threat Intelligence Project (VTIP)
  - Passive attack surface monitoring
  - Stolen/Leaked credentials, typosquatting

Reporting to law enforcement – what to expect?

We will:

✓ Work discretely and confidentially with your organization's Incident Response Team, Legal Department, and/or a third-party incident response firm to identify and collect potential evidence.

✓ Work with federal and local law enforcement partners and prosecutors to coordinate the investigation to identify, locate, apprehend, and ultimately prosecute the threat actor(s).

✓ Facilitate communications with other organizations that could help mitigate the incident.

✓ Compare Indicators of Compromise and Tactics, Techniques, and Procedures in your incident with other similar incidents.

✓ Remain in contact with your organization throughout the investigation.

✓ Work with you to determine if you are amenable to pertinent threat intelligence being shared in a non-attributable manner to protect others who may be affected by the same type of attack.

We will NOT:

- Contact the media or issue public statements.
- Notify regulatory agencies about a potential data breach.
- Perform services an incident response firm would provide such as the removal of malware or mitigation of the infection from your systems or network(s).
- Provide complete mitigation and remediation support.

IBM COST OF A Data breach report 2023

Key takeaways:

- USD $ 470,000 Additional cost experienced by organizations that didn't involve law enforcement in a ransomware attack . This year's research shows that excluding law enforcement from ransomware incidents led to higher costs. While 63% of respondents said they involved law enforcement, the 37% that didn't also paid 9.6% more and experienced a 33-day longer breach lifecycle.
- Nearly 25% attacks involved ransomware
  - Ransomware costs increased significantly avg $5.13M
  - 37% ransomware victims opted not to involve LE (avg cost $5.11M)
    - **Avg cost with LE involved $4.64M (-9.6%/$470K savings)**
    - Time to ID and contain with LE involvement
      - 11.4% or **33 days shorter (273 vs 306 days)**
      - Mean time to contain ransomware breach 63 days vs 80 days without

Colby Cousens

Co-founder, North Shore IT Collaborative

North Shore IT Collaborative

Our mission is to secure our systems, improve services, and control costs through collaboration.

Website security	B 644	0	3	13	3
Email security	C 534	0	1	0	1
Network security	A 908	1	1	4	1
Phishing & malware	A 950	0	0	0	0
Brand & reputation risk	A 950	0	0	0	0

Free external scan and security report card

Email securityreportcard@danversma.gov

Pete Sherlock

President/CEO

cybertrust Massachusetts

A non-profit corporation committed to strengthening cyber capabilities statewide as a trusted partner to government, industry and higher education.

Our Mission

Grow the Cyber Workforce
Increase the pipeline of skilled, experienced, and diverse cyber candidates.

Create Opportunities
Statewide, access to advanced cyber programs linked to cyber employers.

Strengthen Security
Affordable cyber services for local governments, non-profits and small businesses.

Our Initiatives

Cyber Range Facilities

Business/Higher Ed Collaboration

Security Operations Centers

- Hybrid professional/student workforce
- Industry-leading technology and service partners
- Campus-based local facilities
- Directly available to municipalities statewide

NEW for municipalities in 2024:

- Assessment and Advisory services
- Managed Endpoint Detection and Response service

Susan Noyes
Director, Office of Municipal and School Technology
Executive Office of Technology Services and Security

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

Cybersecurity/IT Health Checks

Partnered with ITS78 Vendors through an RFQ Vetting Process

- **Category #1 - Policies & Procedures (9 unique services)**
- **Category #2 - Cyber Security (22 distinctive services**
- **Category #3 - Other (12 special services)**

OMST will be announcing an enhanced Cybersecurity Health Check Program in coming weeks with more Vendors and Services Available

For Information and Application:
https://www.mass.gov/info-details/cybersecurity-health-check-program

Municipal Cybersecurity Awareness Grant Program (MCAGP)

Cyber Criminals never give up.

Many Massachusetts Towns, Schools, and Police Departments Have Already Been Victims of Cyber Attacks

- Springfield Public Schools (October 2020) - ransomware
- Nantucket (January 2023) - ransomware
- Swansea Public Schools (January 2023) - ransomware
- Chicopee (November 2019) - ransomware
- Lowell (April 2023)
- Bedford Police Department
- Douglas Police Department
- Brockton Police Department (July 2
- Lawrence (April 2021) – ransomwar
- Winthrop and Winthrop Public Sch

- Charlton (September 2019)– network attacked, main servers, emails frozen
- Leominster School District (April 2018) – ransomware
- Lynn (May 2019) – Online Parking Ticket Payment System – ransomware
- New Bedford (July 2019) - $5.3 million requested – ransomware
- Grafton Public Schools (November 2020) - DDoS attack
- Sandwich Public Schools (October 2020) – DDoS attack
- Tewksbury (March 2022) – BEC scam, $102,000 lost
- Quincy (Feb 2022) – BEC scam, $3.5 million of pension fund wired to wrong account

Just one click…

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

- 2023 Verizon Data Breach Investigation Report

(16,312 incidents examined, of which 5,199 were confirmed data breaches; Northern America 9.036 incidents of which 1,924 confirmed data disclosure)

The most successful techniques to breach a system do not depend on sophisticated malware but on how they manipulate human emotions.

Attackers are leveraging natural curiosity, impulsiveness, ambition and empathy.

EOTSS Office of Municipal and School Technology (OMST) procures licenses and manages the Municipal Cybersecurity Awareness Grant Program (MCAGP) – **making the program FREE to participating organizations.**

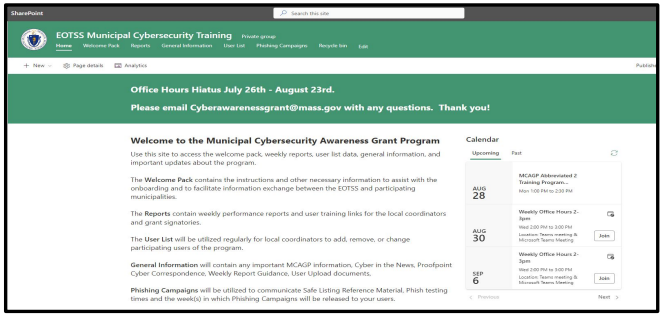
OMST is migrating to the KnowBe4 Cybersecurity Vendor Training Platform for the MCAGP and it will include:

- Assessments
- Online modules
- Phishing campaigns
- Additional resources (posters, newsletters, webinars, etc.)
- Local Coordinator access to the training platform
- PDPs for those in Education (in alignment with the DESE PD requirements)
- Participants will have access to a Home Course that they may share with their Friends and Family

Municipal Cybersecurity Awareness Grant Program (MCAGP)

2024 Learning Paths include:

Traditional **Advanced** **Comprehensive** **Education**



SharePoint and Newsletters are used as Communication Vehicles:

- Quick summaries of current and upcoming training
- Tips to achieve high engagement
- Answers to frequently asked questions
- Special Events

Overcoming Challenges

‘Municipal departments don’t have time!’

Less than 5 minutes a day will lead to completion of all assignments

‘I know this already!’

Experts recommend continuous training to ensure cybersecurity remains top of mind. Annual training is not enough.

Teachers’ unions are pushing back.

Get creative…

- Wellesley - offers PD credit for the yearlong training
- Oxford - offers a 'free pass' from staff meeting if they complete the current assignment
- Walpole, Mansfield – sets aside specific time during PD days for teachers to complete the training

New this year!
As a state agency, we are able to provide PDPs for this Cybersecurity program in alignment with the DESE PD requirements.
More details to come!

Additional Programs and Offerings

Community Compact Cabinet

This funding is available through the Division of Local Services and communities must apply to be considered. If you received a grant in the prior FY, you are not qualified and will not appear in the list of communities.

IT Best Practices – Opens in August and remains open until all funds are expended.
IT Grant Program – Open in September and is typically open for 30 days.
Efficiency & Regionalization – Opens in January and is open for approximately one month.

Municipal Fiber Grant *– Opens in March and application must be submitted by the April deadline**.**
**On January 9th, the Governor's Office, announced the IT Bond Bill or the "Future Technology Act" – the Municipal Fiber Grant will be moved to this in FY25, more to come on this.*

State and Local Cybersecurity Grant Program (SLCGP)

This funding will be available through the Office of Grants and Research. The projects that have been approved are dot gov domain (.gov), multi-factor authentication (MFA), and cybersecurity training. More details will be forthcoming.

Massachusetts Municipal Cybersecurity Roadmap

Developed as a guideline to help you identify your organization's level of maturity and map them to the four minimum baseline of cybersecurity goals. The result is a single resource that will assist you with navigating to the information, tools, and resources needed to improve and strengthen your cybersecurity posture.

Coming in 2024

- Municipal CISO Council
- County Networking Groups
- Collaborative Environment for Municipal Technology Professionals

Panel Q & A

MassCyberCenter.org

Questions?

MassCyberCenter.org

Thank you!

MassCyberCenter.org