Navigating Cyber Threats: Empowering Municipal Executives

MMA Connect 351

Today's Agenda

Navigating Cyber Threats

John Petrozzelli, Director
MassCyberCenter
Petrozzelli@MassTech.org

MIIA Risk Overview

Joe Callahan
Cabot Risk Management
joe.callahan@cabotrisk.com

Cyber Incident Response through MIIA

Gregory Bautista, Partner
Mullen Coughlin
gbautista@mullen.law

EOTSS Office of Municipal & School Technology

Susan Noyes, Director
susan.noyes@mass.gov

Massachusetts Cybersecurity Program (MCP)

Detective Lieutenant Brian Gavioli
Commonwealth Fusion Center
brian.gavioli@mass.gov

MassCyberCenter
at the MassTech Collaborative

Navigating Cyber Threats

• Three Threat Vectors

- **Social Engineering, Insider Threats, & Identity Attacks**: Cyber criminals use email and other methods of social interaction to manipulate users, get passwords, and gain access to networks and applications in order to steal data, financial information, and more. Cybersecurity awareness and technical "defense-in-depth" measures provide added layers of protection.
- **System Intrusions**: Attackers gain unauthorized access to a network, server, or computer.
- **Web Application Attacks:** Unauthorized intruders gain access to networks, servers, or computers through internet-facing software that has not been updated, virtual private networks with vulnerabilities, or software with vulnerabilities exploited by hackers before the vender becomes aware of them (Zero-Day).

• Protecting the Castle

Why does it Matter ?

- 68 percent of breaches contain a human element
- System intrusions account for 35-50 percent of data breaches
- Volt Typhoon, Flax Typhoon, Silk Typhoon – China Threat
- Ukraine War – Russia's response to perceived NATO actions

Source: 2024 Verizon DBIR

Verizon DBIR – Public Administration

Frequency	Threat Actors	Top Patterns	Ransomware	Third Party Risks
• 12, 217 incidents 1085 breaches	• Internal 59% • External 41%	• System Intrusion and Social Engineering	• 32% of breaches	• 15% of breaches through third parties

Misdelivery accounted for approx. 40% of incidents

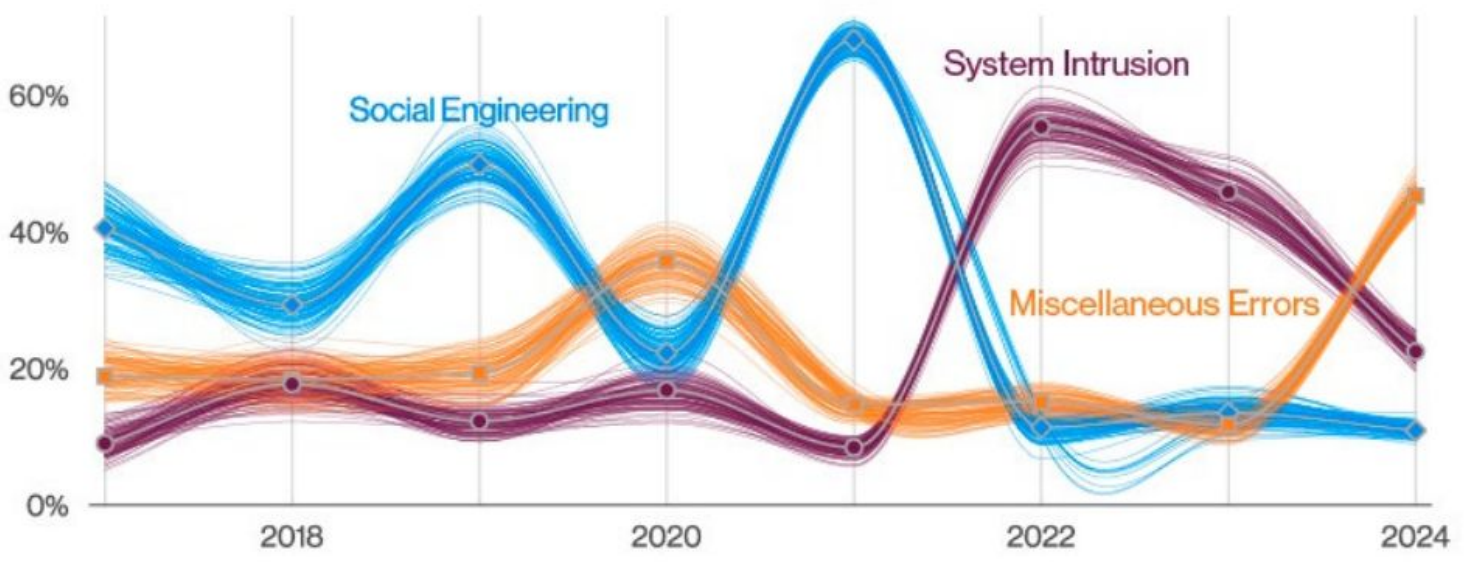


Figure 70. Top patterns over time in Public Administration industry breaches

MassCyberCenter
at the MassTech Collaborative

Global Statistics - Incident Type

2021

Incident Type	Count
Ransomware	1,153 (29%)
Business Email Compromise (BEC) – Total	1,059 (27%)
BEC – Other	698
BEC – Wire Fraud	361
Vendor 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%)
Vendor 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%)
Vendor Breach	749 (19%)
Other	403 (10%)
Network Intrusion	323 (8%)
Inadvertent Disclosure	218 (6%)
Total	**3,920 (100%)**

2024

Incident Type	Count
Business Email Compromise (BEC) – Total	1,601 (38%)
BEC – Other	1,224
BEC – Wire Fraud	377
Ransomware	1,011 (24%)
Vendor Breach	747 (18%)
Other	346 (8%)
Network Intrusion	322 (7%)
Inadvertent Disclosure	228 (5%)
Total	**4,255 (100%)**

Global Statistics - Industry Sector

2021

Industry Sector	Count
Professional Services	1,024 (26%)
Manufacturing and Distribution	704 (18%)
Healthcare and Life Sciences	520 (13%)
Financial Services	461 (12%)
Technology	372 (9%)
Education	215 (5%)
Non-Profit	205 (5%)
Government	200 (5%)
Hospitality and Entertainment	152 (4%)
Retail/e-Commerce	73 (2%)
Energy	37 (1%)
Other	7 (<1%)
Total	**3,970 (100%)**

2022

Industry Sector	Count
Professional Services	773 (26%)
Manufacturing and Distribution	448 (15%)
Healthcare and Life Sciences	376 (13%)
Financial Services	350 (12%)
Technology	333 (11%)
Non-Profit	157 (5%)
Education	142 (5%)
Hospitality and Entertainment	139 (5%)
Government	122 (4%)
Retail/e-Commerce	84 (3%)
Energy	34 (1%)
Other	1 (<1%)
Total	**2,959 (100%)**

2023

Industry Sector	Count
Professional Services	928 (24%)
Financial Services	588 (15%)
Healthcare and Life Sciences	572 (15%)
Manufacturing and Distribution	538 (14%)
Technology	372 (9%)
Education	245 (6%)
Non-Profit	208 (5%)
Hospitality and Entertainment	169 (4%)
Government	138 (4%)
Retail/e-Commerce	130 (3%)
Energy	32 (1%)
Other	0 (0%)
Total	**3,920 (100%)**

2024

Industry Sector	Count
Professional Services	1,241 (29%)
Healthcare and Life Sciences	656 (15%)
Manufacturing and Distribution	563 (13%)
Financial Services	488 (11%)
Technology	342 (8%)
Education	241 (6%)
Non-Profit	212 (5%)
Hospitality and Entertainment	194 (5%)
Government	155 (4%)
Retail/e-Commerce	112 (3%)
Energy	51 (1%)
Other	0 (0%)
Total	**4,255 (100%)**

Global Statistics - Ransomware Incidents

2021	
Number of RW Incidents	1,153 (29%)
Number of RW Incidents Paid	314 (27%)
Average Ransom Demand	$2,126,671
Average Ransom Payment	$500,951
Median Ransom Payment	$216,093
Ransom Payment Reason	Delete Only – 44 (14%) Key and Delete – 150 (48%) Key Only – 120 (38%)

2022	
Number of RW Incidents	732 (25%)
Number of RW Incidents Paid	97 (13%)
Average Ransom Demand	$2,272,682
Average Ransom Payment	$400,791
Median Ransom Payment	$150,000
Ransom Payment Reason	Delete Only – 21 (22%) Key and Delete – 39 (40%) Key Only – 37 (38%)

2023	
Number of RW Incidents	884 (23%)
Number of RW Incidents Paid	138 (16%)
Average Ransom Demand	$2,243,227
Average Ransom Payment	$937,751
Median Ransom Payment	$200,000
Ransom Payment Reason	Delete Only – 42 (30%) Key and Delete – 56 (41%) Key Only – 40 (29%)

2024	
Number of RW Incidents	1,011 (24%)
Number of RW Incidents Paid	133 (13%)
Average Ransom Demand	$1,890,232
Average Ransom Payment	$519,395
Median Ransom Payment	$265,065
Ransom Payment Reason	Delete Only – 53 (40%) Key and Delete – 49 (37%) Key Only – 31 (23%)

Business Email Compromise Incidents

2021	
Number of BEC Incidents	1,059 (27%)
Number of BEC-WF Incidents	361 (34%)
Average Amount Fraudulently Wired	$343,303
Median Amount Fraudulently Wired	$131,440

2022	
Number of BEC Incidents	1,077 (36%)
Number of BEC-WF Incidents	344 (32%)
Average Amount Fraudulently Wired	$376,234
Median Amount Fraudulently Wired	$145,000

2023	
Number of BEC Incidents	1,343 (34%)
Number of BEC-WF Incidents	347 (26%)
Average Amount Fraudulently Wired	$824,704
Median Amount Fraudulently Wired	$148,867

2024	
Number of BEC Incidents	1,601 (38%)
Number of BEC-WF Incidents	377 (24%)
Average Amount Fraudulently Wired	$442,961
Median Amount Fraudulently Wired	$154,622

Cyber Crimes By Incident Type - Government Sector

2021

Incident Type	Count
Vendor Breach	60 (30%)
Ransomware	49 (24%)
Business Email Compromise (BEC) – Total	39 (20%)
BEC – Other	33
BEC – Wire Fraud	6
Network Intrusion	21 (10%)
Inadvertent Disclosure	20 (10%)
Other	11 (6%)
Total	**200 (100%)**

2022

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%)
Vendor 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
Vendor Breach	29 (21%)
Ransomware	25 (18%)
Network Intrusion	15 (11%)
Inadvertent Disclosure	13 (10%)
Other	10 (7%)
Total	**138 (100%)**

2024

Incident Type	Count
Business Email Compromise (BEC) – Total	47 (31%)
BEC – Other	40
BEC – Wire Fraud	7
Ransomware	42 (27%)
Vendor Breach	31 (20%)
Inadvertent Disclosure	15 (10%)
Network Intrusion	10 (6%)
Other	10 (6%)
Total	**155 (100%)**

Ransomware-Specific - Government Sector

2021	
Number of RW Incidents	49 (24%)
Number of RW Incidents Paid	9 (18%)
Average Ransom Demand	$1,892,082
Average Ransom Payment	$252,044
Median Ransom Payment	$125,000
Ransom Payment Reason	Delete Only – 2 (23%) Key and Delete – 3 (33%) Key Only – 4 (44%)

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

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

2024	
Number of RW Incidents	42 (27%)
Number of RW Incidents Paid	1 (3%)
Average Ransom Demand	$2,747,443
Average Ransom Payment	$750,000
Median Ransom Payment	$750,000
Ransom Payment Reason	Delete Only – 0 (0%) Key and Delete – 1 (100%) Key Only – 0 (0%)

Business Email Compromise-Specific

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

2024	
Number of BEC Incidents	47 (31%)
Number of BEC-WF Incidents	7 (15%)
Average Amount Fraudulently Wired	$128,726
Median Amount Fraudulently Wired	$78,891

Number of Lit./Reg. Inv. Matters - Government Sector

2021 – Lit./Reg. Inv. Matters

	Jan.	Feb.	Mar.	Apr.	May	June	July	Aug.	Sep.	Oct.	Nov.	Dec.	Total
Number of Incidents	4	14	7	2	4	10	2	5	6	4	5	1	64
	Q1			Q2			Q3			Q4			
	25			16			13			10			

2022 – Lit./Reg. Inv. Matters

	Jan.	Feb.	Mar.	Apr.	May	June	July	Aug.	Sep.	Oct.	Nov.	Dec.	Total
Number of Incidents	4	5	9	15	17	25	10	18	47	6	8	7	171
	Q1			Q2			Q3			Q4			
	18			57			75			21			

2023 – Lit./Reg. Inv. Matters

	Jan.	Feb.	Mar.	Apr.	May	June	July	Aug.	Sep.	Oct.	Nov.	Dec.	Total
Number of Incidents	6	12	5	8	22	24	35	28	39	34	18	39	270
	Q1			Q2			Q3			Q4			
	23			54			102			91			

2024 – Lit./Reg. Inv. Matters

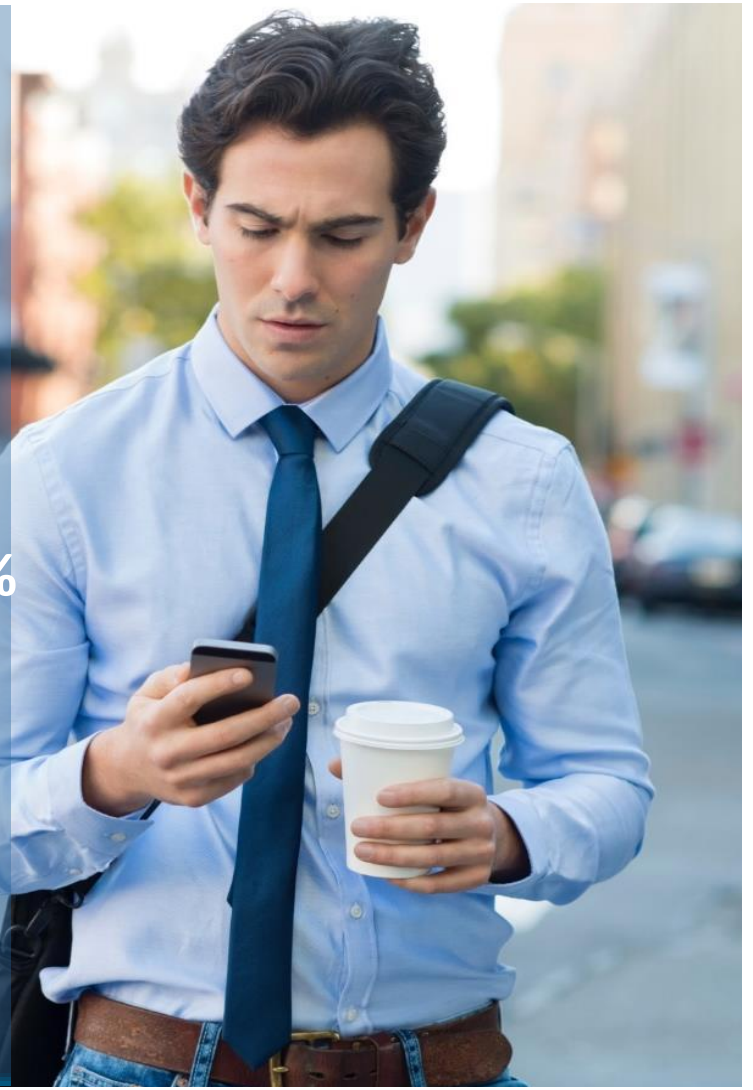
	Jan.	Feb.	Mar.	Apr.	May	June	July	Aug.	Sep.	Oct.	Nov.	Dec.	Total
Number of Incidents	69	52	38	28	40	40	22	37	40	30	47	59	502
	Q1			Q2			Q3			Q4			
	159			108			99			136			

MIIA Cyber Risk

DO YOU KNOW WHERE YOUR DATA HAS BEEN TODAY?

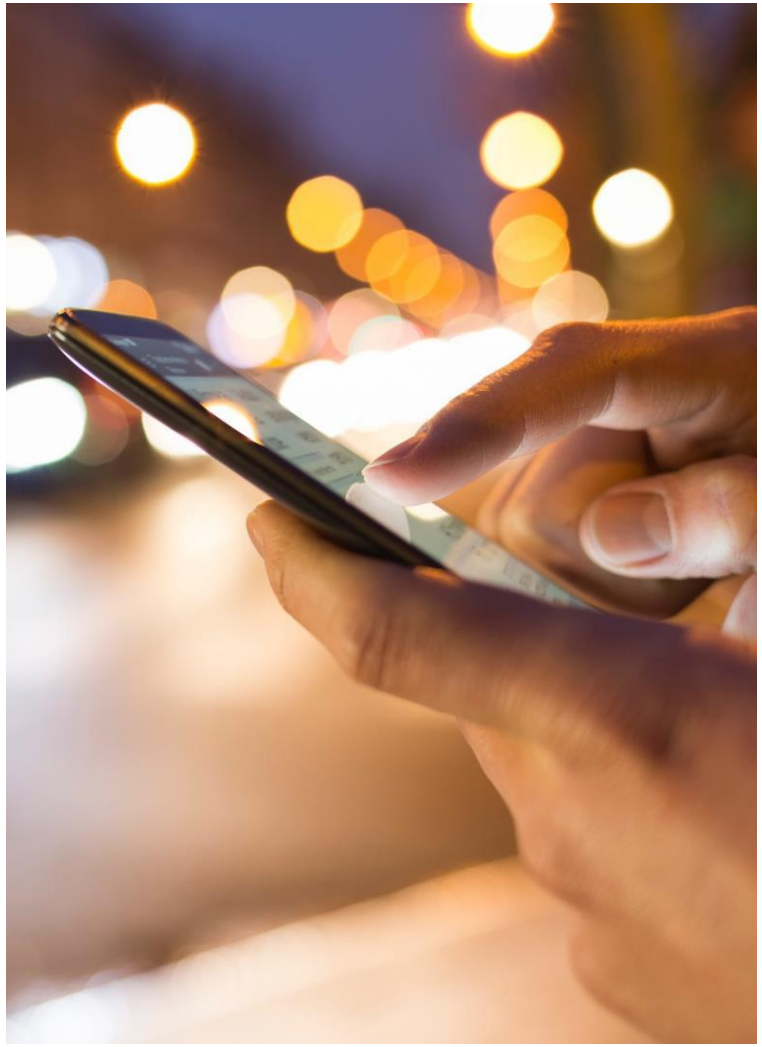
Causes of Data Breaches

Hacking (includes skimming/phishing /malware/ransomware)	59.5%
Employee Negligence	10.4%
Accidental Exposure	6.4%
3rd Party Theft	7.5%
Insider Theft	5.3%
Physical Theft	4.5%



MIIA Nonprofit Locally based Member driven
Serving Massachusetts communities since 1982

MIIA Cyber Risk



TYPES OF BREACHES:

- Employees & Social Media
- Employee carelessness/negligence
- Ransomware (i.e. CryptoLocker, etc.)
- Rogue employees
- Phishing Schemes
- Lost/stolen devices

Part I: Social Engineering and Identity Attacks

Social Engineering and Identity Attacks

A type of attack that uses human interaction to trick people into sharing sensitive information.

- Leading cause of these types of incidents is Phishing and Pretexting via email, accounting for 73% of breaches.
- Technical “defense-in-depth” measures provide added layers of protection.
- Social Engineering attacks are easier with public-facing organizations.

Source: 2024 Verizon DBIR

Relevant ATT&CK techniques

Compromise Accounts: T1586
- Email Accounts: T1586.002

Establish Accounts: T1585
- Email Accounts: T1585.002

External Remote Services: T1133

Internal Spearphishing: T1534

Phishing: T1566
- Spearphishing Attachment: T1566.001
- Spearphishing Link: T1566.002
- Spearphishing via Service: T1566.003

Phishing for Information: T1598
- Spearphishing Service: T1598.001

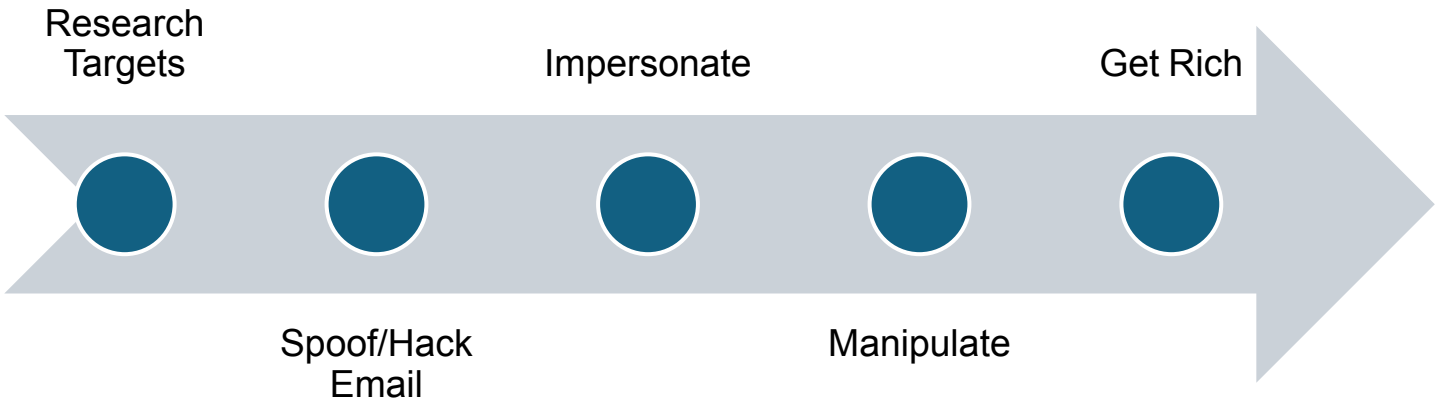
Use Alternate Authentication Material: T1550
- Application Access Token: T1550.001

Valid Accounts: T1078
- Domain Accounts: T1078.002

What is Business Email Compromise (BEC)?

*Using **social engineering**, attackers gain access to email systems to trick targets into:*

- *transferring funds,*
- *disclosing sensitive information, or*
- *executing unauthorized actions.*



General BEC Framework

Part II: System Intrusions

System Intrusions

Attackers gain unauthorized access to a network, server, or computer.

Relevant ATT&CK techniques

Exploit vuln (VERIS)

- Exploit Public-Facing Application: T1190
- Exploitation for Credential Access: T1212
- Exploitation for Defense Evasion: T1211
- Exploitation for Privilege Escalation: T1068
- Exploitation of Remote Services: T1210
- External Remote Services: T1133
- Vulnerability Scanning: T1595.002

Use of stolen creds (VERIS)

- Compromise Accounts: T1586
  - Social Media Accounts: T1586.001
  - Email Accounts: T1586.002
- External Remote Services: T1133
- Remote Services: T1021
  - Remote Desktop Protocol: T1021.001
- Use Alternate Authentication Material: T1550
  - Web Session Cookie: T1550.004
- Valid Accounts: T1078
  - Default Accounts: T1078.001
  - Domain Accounts: T1078.002
  - Local Accounts: T1078.003
  - Cloud Accounts: T1078.004

Execution: TA0002

Persistence: TA0003

Privilege Escalation: TA0004

Defense Evasion: TA0005

Credential Access TA0006

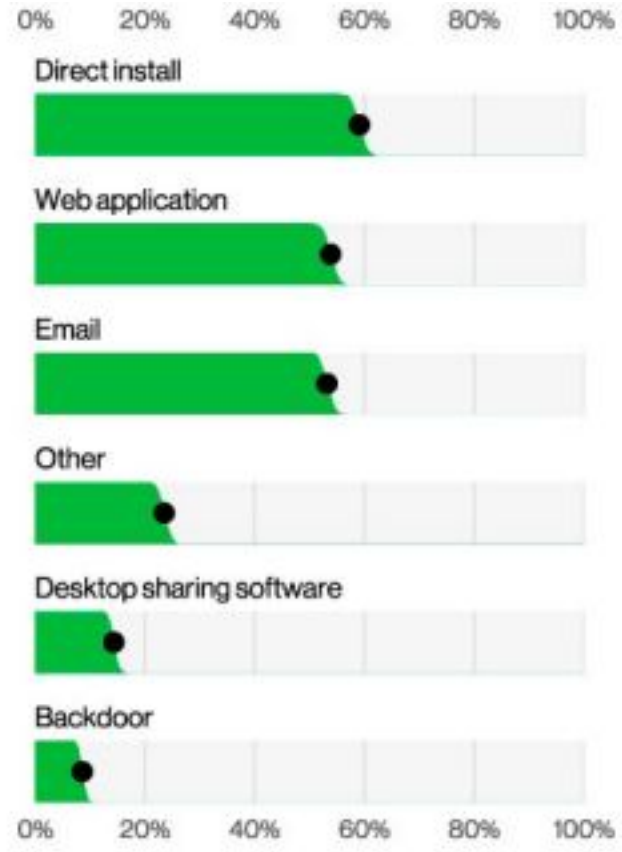
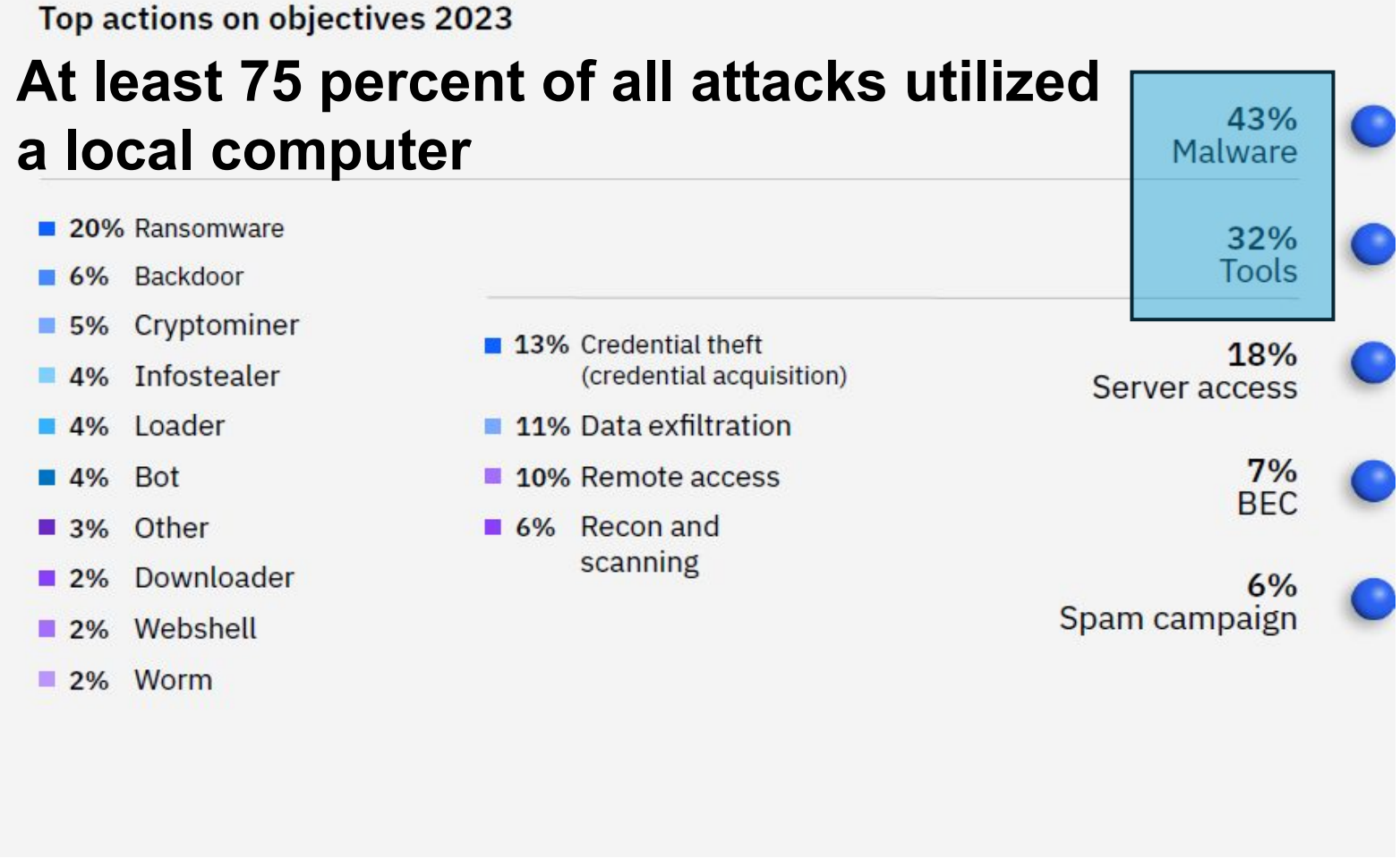


Figure 29. Top Action vectors in System Intrusion incidents (n=1,789)

System Intrusions: IBM Threat Report

- **Endpoint detection and response is critical to identifying and stopping these attacks.** EDR can also detect 'living off the land' usage by threat actors. EDR can also identify software reaching out to remote command and control sites.
- MITRE has a free tool that evaluates EDR/MDR: https://mitre-engenuity.org/cybersecurity/attack-evaluations/



Source: IBM X-Force Threat Intelligence Index 2024

System Intrusions:

CISA Risk and Vulnerability Assessment Report

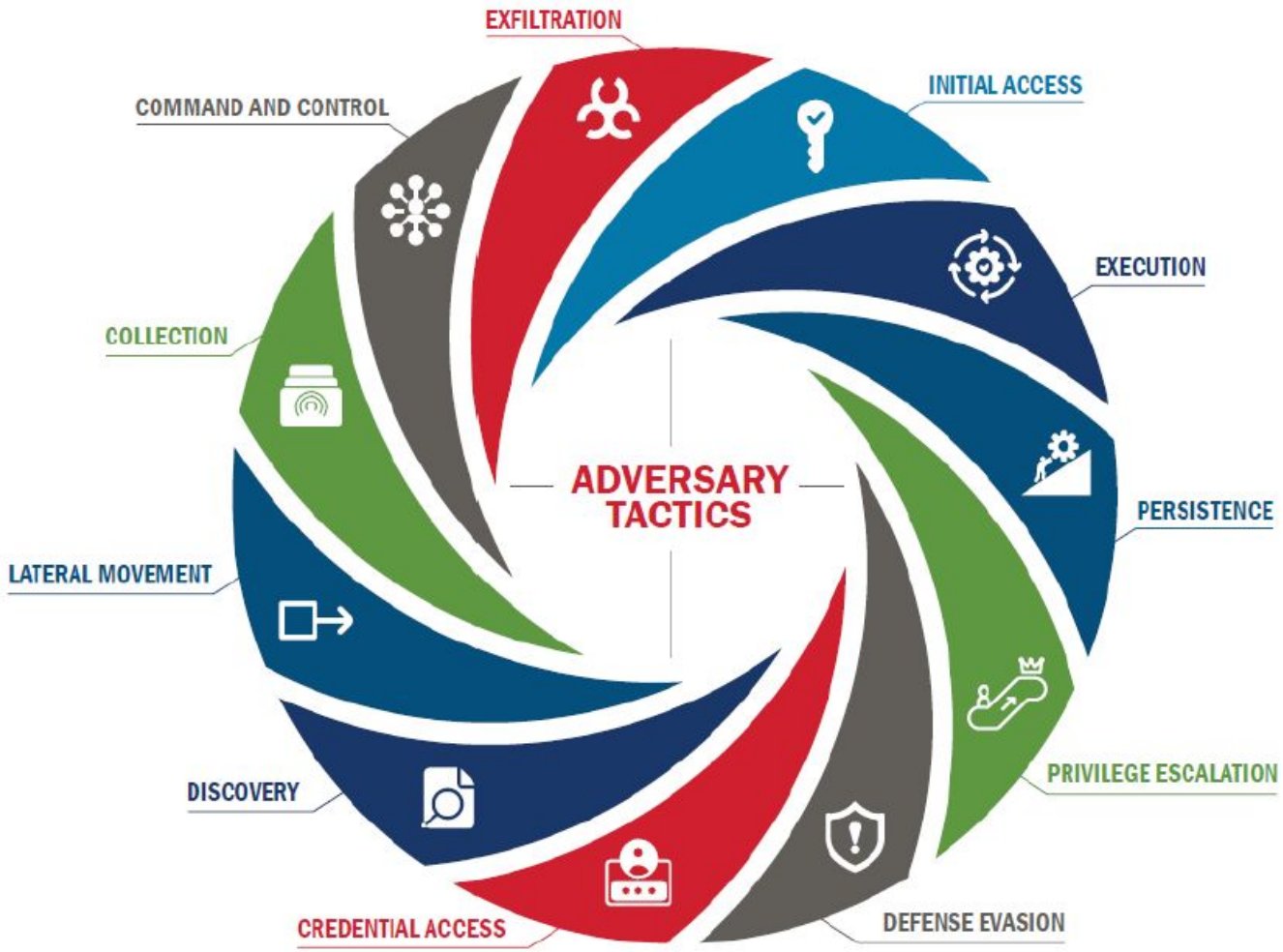


Figure 1: Adversary Tactics

- 143 RVAs, multiple critical infrastructure sectors.
- Mapped 11 of the 14 MITRE ATT&CK framework tactics.
- Initial Access Successes:
  - Used valid accounts: 41%
  - Spearphishing: 29%.

MassCyberCenter
at the MassTech Collaborative

System Intrusions: Credential Theft

IBM X-Force Report 2024

266%

Upsurge in use of infostealers
X-Force has observed threat groups who have previously specialized in ransomware showing increasing interest in infostealers. And a number of prominent new infostealers recently debuted and demonstrated increased activity in 2023, such as Rhadamanthys, LummaC2 and StrelaStealer.

*An infostealer is a type of malware, surreptitiously installed on a computer, that targets its victim by stealing sensitive information that can include passwords, login credentials, and other personal data. After collecting such data, the stealer sends it to the threat actor's command and control (C2) system.

30%

Share of security misconfigurations among web application vulnerabilities identified
X-Force penetration testing engagements revealed that the most observed web application risk across client environments globally was security misconfigurations. Of these misconfigurations, the top offenses included allowing concurrent user sessions in the application, which could weaken multifactor authentication (MFA) through session hijacking.

32%

Percentage of incidents that involved malicious use of legitimate tools
Nearly one-third of incidents that X-Force responded to were cases where legitimate tools were used for malicious purposes, such as credential theft, reconnaissance, remote access or data exfiltration.

50%

Market share threshold likely to trigger attacks against AI platforms
X-Force analysis indicates that the establishment of AI market dominance will signal AI attack surface maturity. This analysis suggests that once a single AI technology approaches 50% market share, or when the market consolidates to three or less technologies, the cybercriminal ecosystem will be incentivized to invest in developing tools and attack paths targeting AI technologies.

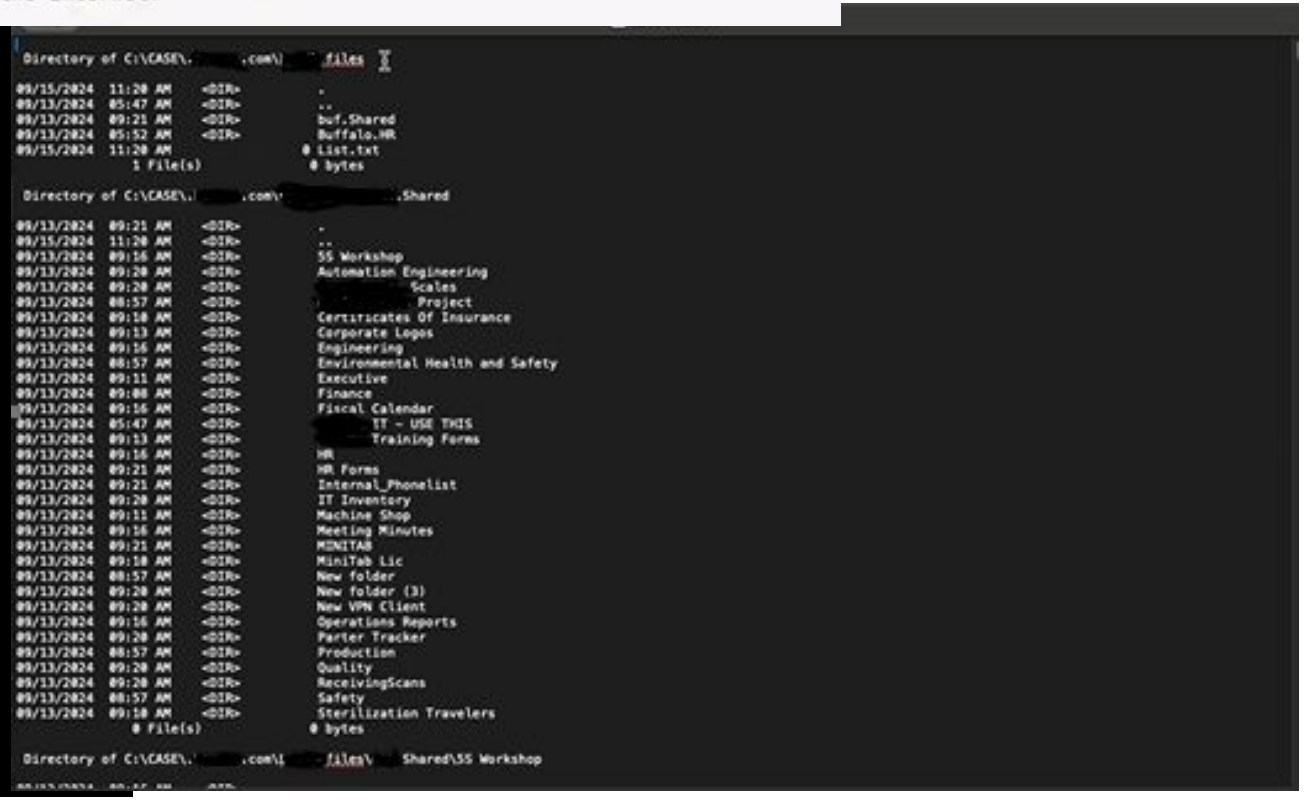
Source: IBM X-Force Threat Intelligence Index 2024

RANSOMWARE DOUBLE (OR TRIPLE) EXTORTION

0 0
o

You're probably very curious about the letter you're reading right now, and you're wondering what's going on with your systems?
Be informed, there was a Ghost in your network! But don't get Spooked, ghost is friendly and we can help you handle with it.
There are two serious issues should be discussed in Chat:
1. Whole your network with all servers and hosts can be restored easily with our special Decryption Key, we will provide you the proofs of properly working decryption tool.

2. Our little spectrum analysis shows that your network is highly vulnerable, also the data on your file-servers was stored insecurely. So, the ghost has taken your data as evidence, and if you're not going to cooperate and make a deal, then all your confidential files will be published on the internet.



To Pay or Not to Pay, that is the question.

- Is this legal? What steps do I have to take?
- Are there funds available to pay the demand?
- What is the approval process/how long does it take?
- What happens if the attacker doesn’t provide the decryption key?
- What happens if data is leaked?
- At what point are we calling the authorities?

Lessons Learned from Municipal Cyber Attacks

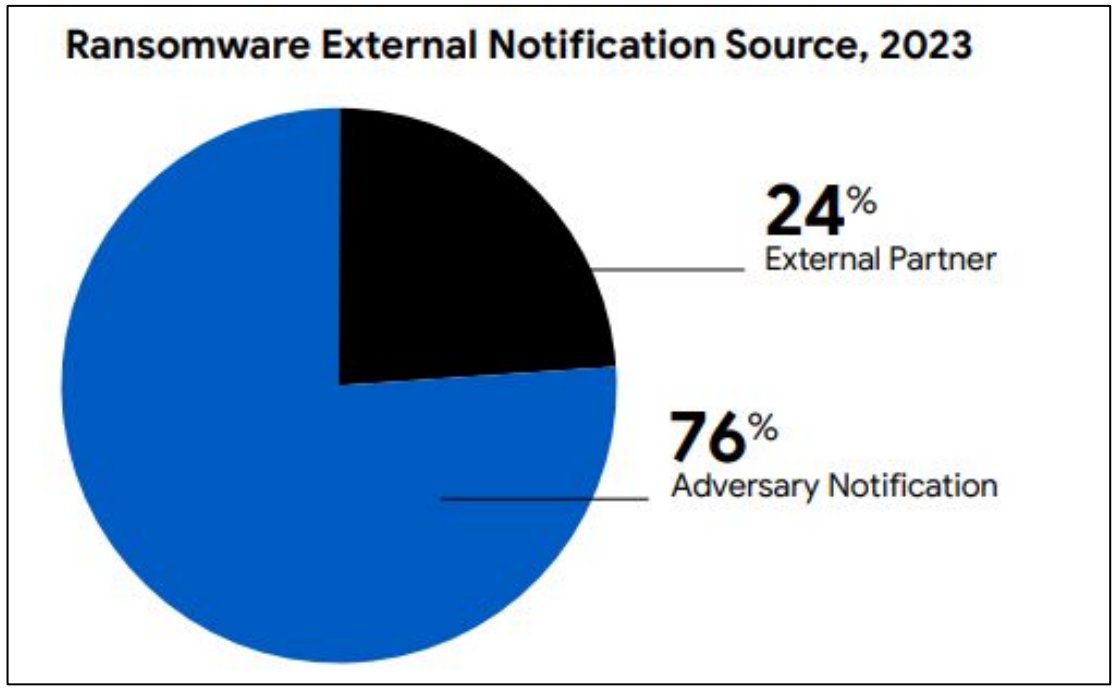
- Identify 1 or 2 leaders to guide the town's response.
- Are there approvals/limitations on third party contracts?
- Engage with insurance resources early in the response.
- Are there public meetings?
- Prepare for the media.
- Segment municipal resources networks data and/or systems to limit scope of impact.
- Can you pay a ransom? Impact of fund transfer fraud?

Mandiant Threat Report

Internal vs. External Detection Trends

Outliers

- Of internally discovered intrusions, 85% did not involve ransomware.
- For ransomware-related intrusions, **70% of organizations were externally notified**, in most cases, via a ransom demand from the attacker.



Source: Mandiant 2024 Threat Report

MassCyberCenter
at the MassTech Collaborative

Part III: Basic Web Application Vulnerabilities

Basic Web Application Vulnerabilities

Internet facing software that has not been updated, virtual private networks with vulnerabilities, or software with vulnerabilities exploited by hackers before the vender becomes aware of them (Zero-Day)

Relevant ATT&CK techniques

Brute Force: T1110
- Credential Stuffing: T1110.004
- Password Cracking: T1110.002
- Password Guessing: T1110.001
- Password Spraying: T1110.003

Compromise Accounts: T1586
- Email Accounts: T1586.002

Exploit Public-Facing Application: T1190

External Remote Services: T1133

Valid Accounts: T1078
- Default Accounts: T1078.001
- Domain Accounts: T1078.002

Use Alternate Authentication Material: T1550
- Application Access Token: T1550.001

Active Scanning: T1595
- Vulnerability Scanning: T1595.002

Basic Web Application Vulnerabilities

Resources

- **Cyber Resilient Massachusetts Grant Program** provides up to $25,000 to fix these vulnerabilities.
- **Mass State Police Cybersecurity Program** can assist in identifying these vulnerabilities.
- **CISA Cyber Hygiene (CYHY)** and **Web Application Scanning (WAS)** can assist in identifying these. CYHY and WAS were part of the mandated tools to use for SLCGP applicants.
- Some **Endpoint Detection and Response tools** can identify software and hardware needing updates.

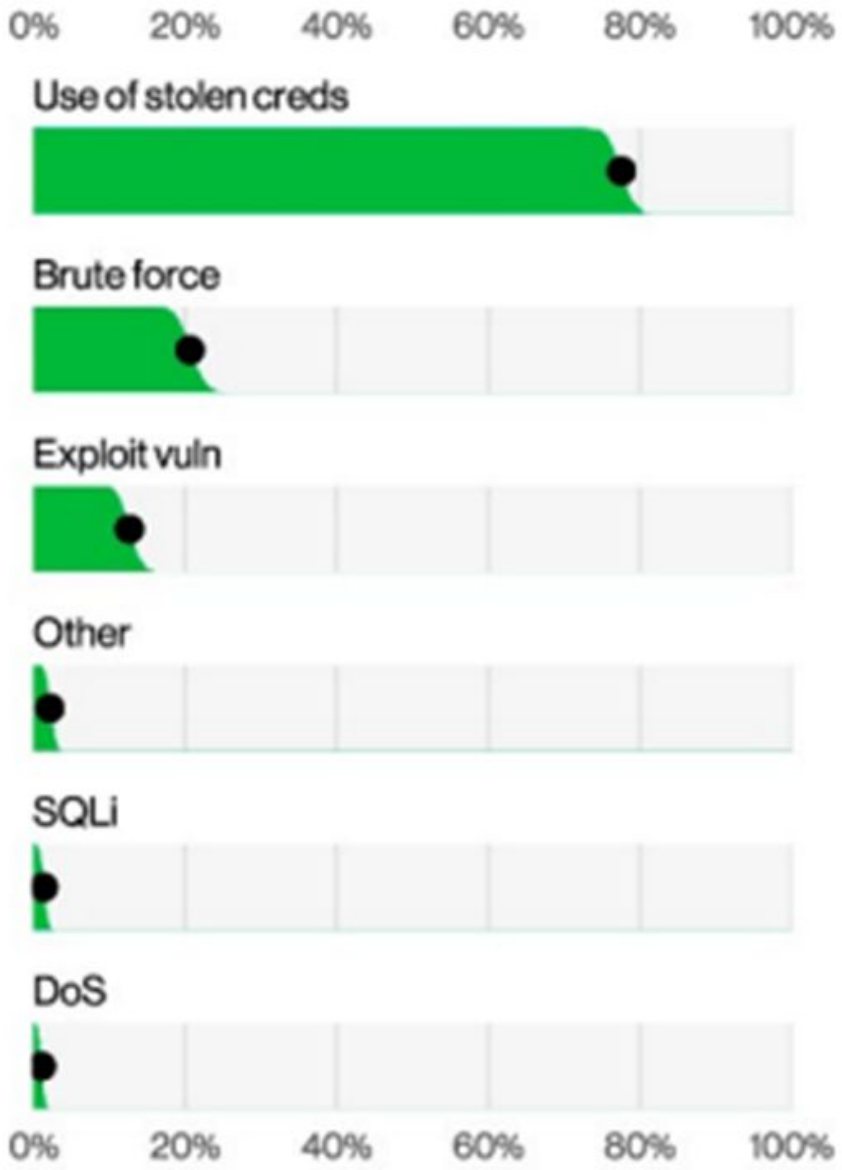
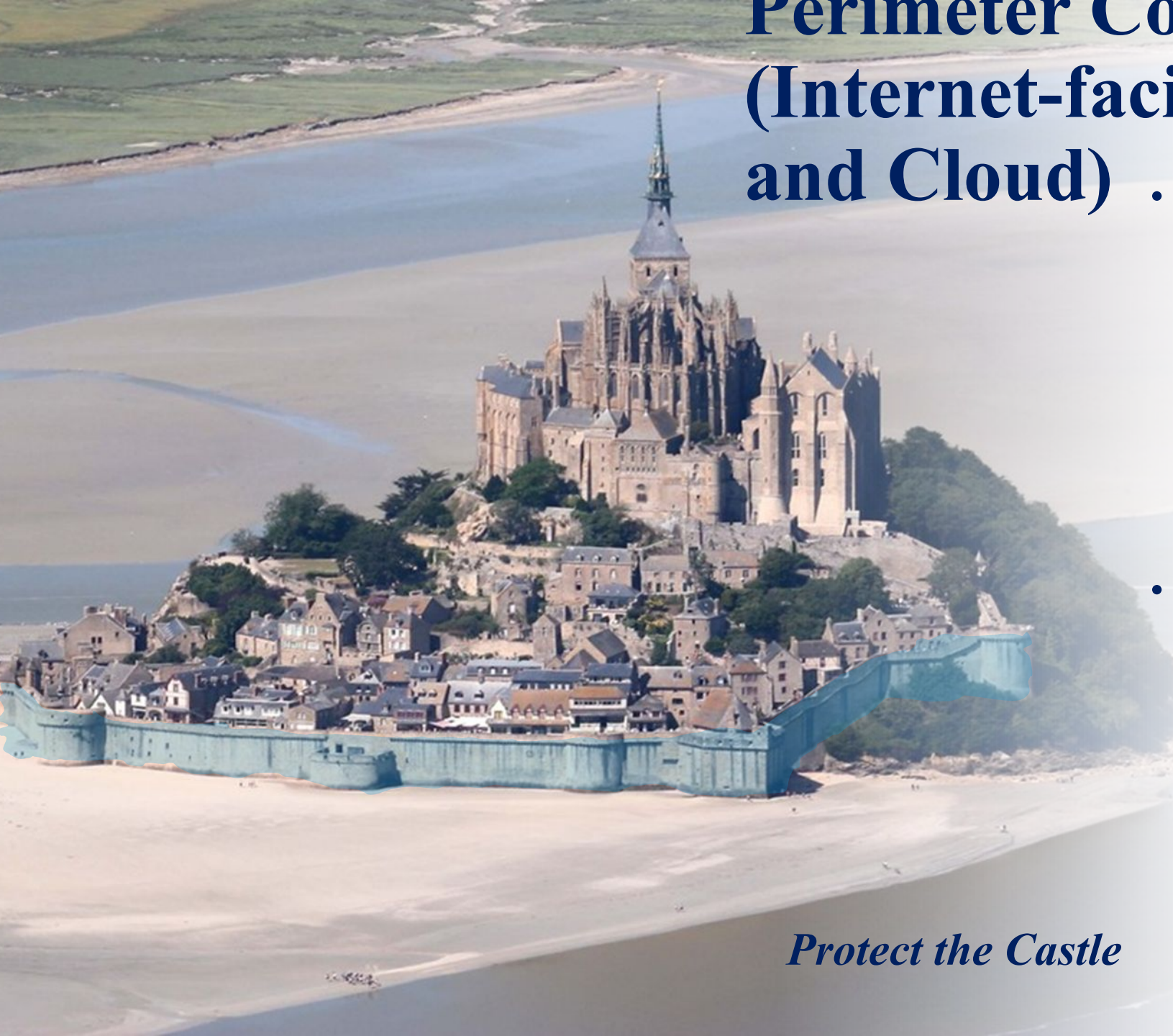


Figure 41. Top Hacking actions in Basic Web Application Attacks breaches (n=713)

MassCyberCenter
at the MassTech Collaborative

Protect the Castle – Defense in Depth



Perimeter Coverage (Internet-facing Infrastructure and Cloud)

- Security tools that can defend the perimeter
  - Firewall
  - Email Security
  - Secure Access Service Edge
  - Zero Trust
  - Breach Detection
  - Security Information Event Management
- Free State and Federal Resources
  - CISA Cyber Hygiene (CyHy)
    - Web Application Scanning (WAS)
    - CISA Remote Penetration Testing
  - EOTSS Cybersecurity Health Check
  - Municipal Local Cybersecurity Grant Program – SLCGP (MFA funding and Awareness Training)
  - Community Compact Cabinet Grants
  - Cyber Resilient Mass Grant Program
  - EOTSS Cyber Awareness Training Grant

Protect the Castle

Inside the Town Gates – Inner Perimeter (Network)

- Free State and Federal Resources
  - MassCyberCenter Minimum Baseline of IT
  - CISA Critical Infrastructure Toolkit for Education/Government
  - Community Compact
  - State and Local Cybersecurity Grant Program (Incident Response Training and TTX)
  - MassCyberCenter Cyber Resilient Grant Program
- Security Tools
  - Demilitarized Zone
  - Network Detection and Response (CyberTrust SOC Services))
  - Subnets

MassCyberCenter
at the MassTech Collaborative

Within the Town
(Devices in the Network and Working from Home)

- Security Tools
  - Guards – Endpoint Detection and Response (EDR) or 24/7 Managed Detection and Response (MDR)
  - Investigators – SIEM Agents, Threat Hunting
  - Spies – Insider Threat Monitoring
  - Informants – Auditing software, Sensors
  - Citizens – Awareness Training and Incident Response Plan Training
- Free State and Federal Resources
  - MassCyberCenter Minimum Baseline of IT
  - CISA Critical Infrastructure Toolkit for Government
  - EOTSS Cyber Awareness Training grant
  - Community Compact
  - MassCyberCenter Cyber Resilient Grant Program
  - Endpoint Managed Detection and Response
    - CyberTrust SOC (SentinelOne 24/7)
    - MS-ISAC SOC (Crowdstrike)
  - CISA Logging Made Easy

Guarding the Keep ('Crown Jewels', Servers, Data, etc.)

- Zero Trust Tools (e.g. Windows Applocker)
- Free State and Federal Resources
  - MassCyberCenter Minimum Baseline of IT
  - CISA Critical Infrastructure Toolkit
  - EOTSS Cyber Awareness Training grant
  - Community Compact
  - Endpoint Managed Detection and Response
    - CyberTrust SOC (SentinelOne 24/7)
    - MS-ISAC SOC (Crowdstrike)
  - MassCyberCenter Cyber Resilient Grant Program

MIIA Cyber Risk Overview

December 2024

MIIA
Nonprofit
Locally based
Member driven
Serving Massachusetts communities since 1982

MIIA Cyber Risk

COVERAGE FORM A-J

MIIA Cyber Risk

Cyber Highlights – 3 Coverage Parts

✔ **Liability**

- Care + Custody of Data
- Regulatory Compliance
- Monitoring of Credit

✔ **Property**

- Destruction of Data

✔ **Time Element**

- Loss of Revenue and Extra Expense to
- Rebuild and Restore Data

MIIA Cyber Risk
Coverage Descriptions

COVERAGE A: Multimedia Liability

- Coverage for third party claims alleging liability resulting from the dissemination of online or offline media material, including claims alleging copyright/trademark infringement, libel/slander, plagiarism, or personal injury.

COVERAGE B: Security & Privacy Liability

- Coverage for claims alleging liability resulting from a security breach or privacy breach, including claims alleging failure to safeguard personal information.

COVERAGE C: Privacy Regulatory Defense & Penalties

- Coverage for regulatory fines and penalties and regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, or local governmental agencies.

COVERAGE D: PCI DSS Liability

- Coverage for assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.

MIIA Cyber Risk

Coverage Descriptions

COVERAGE E: Breach Event Costs

- Coverage for mitigation costs and expenses incurred because of a privacy breach, security breach or adverse media report, including legal expenses, public relations expenses, IT forensic expenses, and costs to provide credit monitoring and identity theft assistance to affected individuals.

COVERAGE F: BrandGuard®

- Coverage for loss of net profit incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach.

COVERAGE G: Network Asset Protection

- Coverage for reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased or corrupted due to (1) accidental damage or destruction of electronic media or computer hardware, (2) administrative or operational mistakes in the handling of electronic data, or (3) computer crime/attacks including malicious code and denial of service attacks. Coverage also extends to business income loss and interruption expenses incurred because of a total or partial interruption of an insured computer system directly caused by any of the above events.

MIIA Cyber Risk

Coverage Descriptions

COVERAGE H: Cyber Extortion

- Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.

COVERAGE I: Cyber Crime

- Coverage for loss of money or securities incurred due to financial fraud, including wire transfer fraud; charges incurred for unauthorized calls resulting from fraudulent use of an Insured's telephone system; expenses incurred to notify customers of phishing schemes that impersonate the Insured or the Insured's brands, products or services, and the costs of reimbursing customers for loss they sustain as a result of such phishing schemes.

COVERAGE J: Dependent System Failure

- Coverage for a business' loss of income and interruption expenses incurred as a result of a third-party service provider's system going down.

MIIA Cyber Risk

Cyber Response Resources

Tokio Marine HCC's team of incident response experts are leaders in their field and are here to help you with notification and credit monitoring services, assistance in data recovery, and much more. From the moment a claim is reported, service providers are engaged to support and quickly resolve any issues that may arise.

Breach Counsel

- *Develops response plan in the case of a cybersecurity breach that will minimize both potential reputational damage and monetary vulnerability.*
- *Execute an investigation, produce notifications for clients, manage the investigation, and more.*

Forensic Firms

Forensic investigation to evaluate the source of the breach and secure your information

Notification & Credit Monitoring

To keep your information protected, each of our top-of-the-line specially selected group of vendors offer unparalleled credit monitoring and notification services.

MIIA Cyber Claim Reporting

ALL Incident and Claim Reporting

MIIA Claims Contact:

David Dowd

Jillian McMartin

Phone: 800-526-6442

Email: MIIAclaims@MMA.org

Fax: 781-376-9907

Details:

1) Authorized Contact Name
2) Any documents to support incident or claim
3) Brief description of event

Important: All incidents and claims need to be reported immediately (Within 24 hours) to MIIA.

Executive Office of Technical Services and Security (EOTSS)

Office of Municipal & School Technology (OMST)

https://www.mass.gov/orgs/office-of-municipal-and-school-technology

January 24, 2025

Office of Municipal & School Technology (OMST

Susan Noyes – Director
Barnstable, Dukes, Essex, Nantucket Counties
email: susan.noyes@mass.gov, phone: (617) 626-4403

- **Suzanne Zarges – MCAGP Program Coordinator, Worcester County**
  email: cyberawarenessgrant@mass.gov

- **Ralph DeLeo - Bristol & Plymouth Counties, Regional Planning Commissions**
  email: ralph.deleo@mass.gov

- **Stephanie Brown – Middlesex, Norfolk, Suffolk Counties**
  email: stephanie.brown5@mass.gov

- **Ken Wedge - Berkshire, Franklin, Hampshire, and Hampden Counties**
  email: kenneth.wedge@mass.gov

- **Hannah Peterson, Municipal & School IT Analyst, Muni-IT-Dir SharePoint, Communication**
  email: hannah.peterson@mass.gov

Office of Municipal & School Technology (OMST)

We serve local government agencies across the Commonwealth by:

- Providing information about technology grants available to local government.
- Creating opportunities for regional in-person and virtual collaboration.
- Guide communities on technology initiatives.
- Promoting state resources that can improve local government operations.

State, Local, and Partner Programs

- Municipal Cybersecurity Awareness Grant Program (MCAGP)
- Cybersecurity Health Check Program
- Community Compact Cabinet Grant Program (CCC)
- Professional Licensing API
- State and Local Cybersecurity Grant Program (MLCGP)
- Mass Cyber Resilient Grant Program

Municipal Cybersecurity Awareness Grant Program (MCAGP) FREE

Training is most effective when taken over the course of time, not all in one sitting.

Learning Paths

- **Traditional:** This training path is intended for users who have completed a foundational level of training already. It includes short modules meant to serve as a refresher of known information. (approximately 1 hour total)

- **Advanced:** This training path is intended for a subset of users that have a solid foundation of cybersecurity awareness training. Users in this path are able to test out of modules. (less than 1 hours total if all tests passed on initial attempt)

- **Comprehensive:** This training path offers longer, more in-depth modules intended for newer employees or those who may require additional training to gain a foundational understanding of cybersecurity awareness. (approximately 4 hours total)

- **Education:** This training path was designed with the public school sector in mind. This path includes a modules of varying length and format, along with assessments, for a total of 10 hours. Users will earn **10 Professional Development Points (PDPs)** upon completion.

Note – Schools may enroll users in either the Education path or the Traditional/Advanced/Comprehensive path

MCAGP KnowBe4 Provides…

Individual Console

- Upload and maintain your users
- Full Access to content, tools, user management and reports
- Real time access to user progress

Content

- Hundreds of Training Modules, Micro Modules and Video Modules
- Posters, Newsletters and Security Documents
- Scam of the Week and Security Tips and Hints
- Games, Badges and Leaderboards

Resources

- KnowBe4 Support
- KnowBe4 Knowledge Base
- KnowBe4 Community

MCAGP OMST Staff Provides

Pre-Designed Training Campaigns

- Diamond Level Subscription
- Customizable notifications
- Ability to set your own due dates

Monthly Phishing Campaigns

- Multiple templates randomly delivered to your users over the course of a day
- Phish Prone Percentage available for Learner Dashboards
- Ability to create smartgroups to track repeat clickers

Support

- Cyberawarenessgrant@mass.gov
- 1:1 Guidance
- MCAGP Share Point Site
- MCAGP Bi-Weekly Newsletter

Cybersecurity Health Check Program - FREE

Problem

- Organizations seeking guidance on vulnerabilities and exposures and/or network structure
- Struggle to identify where to start, what to do first and how to best utilize limited funds with competing priorities

Timeline

- 4-6 weeks to completion

Goal

- Identify gaps and areas of weakness
- Increase cybersecurity and strength of IT network
- Align needs with funding opportunities

Deliverable

- Written report, final meeting & recommendations/remediation actions

OMST Building Connections & Driving Engager

- Municipal IT SharePoint – secure information sharing site and collaboration opportunities across City/Town/School IT Depts
- IT Accessibility resources and information https://www.mass.gov/it-accessibility
- Coordinate & participate in Local and Regional IT /Tech Director Meetings
- Conduct Tabletop (TTX) Exercises within a city/town/school or more broadly
- Assist with identifying resources, grants, and programs to address specific needs
- Provide Guidance with Cyber Incident Response Planning (CIRP)

Massachusetts Cybersecurity Program Overview

MCP
Massachusetts
Cybersecurity Program

COMMONWEALTH FUSION CENTER

MCP HISTORY

- Established in 2016 to address increasing cyber threats to Critical Infrastructure
- Information Sharing, Awareness Bulletins, Trainings, Pass-through Alerts, Threat Briefings
- MCP distro
- Partnerships

Commonwealth Fusion Center
Massachusetts

(U) Massachusetts State Police, Commonwealth Fusion Center
Malicious USB Attacks
4 March 2022

(U) Overview

(U) The FBI released an alert that cybercriminals are mailing malicious USB flash drives[1] through the US Postal Service. FIN7, a cybercrime threat group, has been conducting USB attacks by mailing USBs laced with malware to US organizations in US defense, transportation, and private sector entities. FIN7 has used two different schemes to trick victims into plugging in the malicious USBs. One scheme contains a package that appears to come from the US Department of Health and Human Services that reportedly contains information on current pandemic guidelines. The second lure comes as an Amazon gift box which contains a thank you letter, USB, and counterfeit gift card. According to the FBI, both packages contain USBs that when connected to a computer will send preconfigured commands that download malicious software, creating direct back door access for cybercriminals to deploy ransomware.

(U) Cybercriminals have also been known to plant malicious USBs in public areas hoping that unsuspecting victims will pick them up. "Lost and Found" USB attacks rely on victim's curiosity to see who the owner of the USB is or what type of files it contains. Cybercriminals may entice victims by labeling the USB as "finances, bonuses, payroll" or any title that may bait victims into plugging it into their computer.

(U) Never plug an unknown USB into your personal or work computer!

(U) Response Considerations

(U) Report incidents to your police department of jurisdiction.
(U) To report a suspected Internet-facilitated crime to the Federal Bureau of Investigation, follow the link to the Internet Crime Complaint Center (IC3):

- Internet Crime Complaint Center - WWW.IC3.GOV

(U) Outlook

(U) The Massachusetts State Police, CFC is providing this information for situational awareness purposes only. Please report any suspicious activity to your police department of jurisdiction.

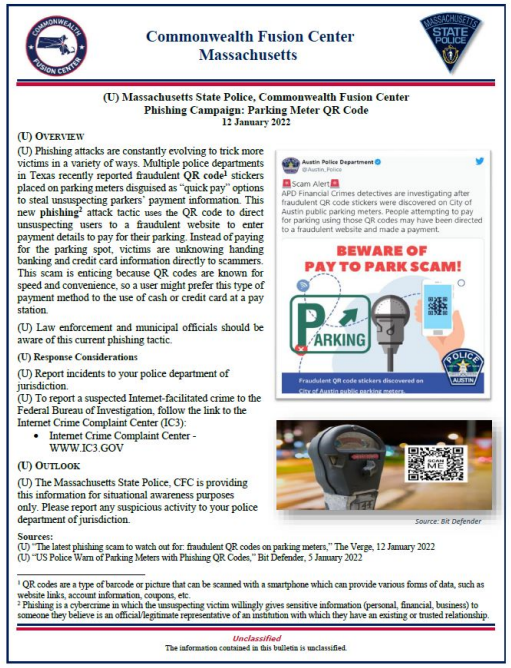
Sources:

(U) "FBI Warns FIN7 Campaign Delivers Ransomware via BadUSB," Dark Reading, 10 January 2022
(U) "FBI: Hackers use BadUSB to target defense firms with ransomware," Sleeping Computer, 7 January 2022
(U) "FIN7 Targets US Enterprises Via BadUSB," Bank Info Security, 11 January 2022
(U) "FBI warns cybercriminals have tried to hack US firms by mailing malicious USB drives," CNN, 7 January 2022

[1] USB Flash Drive – A removable data storage device that can plug into a computer's USB port.

Unclassified
The information contained in this bulletin is unclassified.

Types of MCP Bulletins Created



Commonwealth Fusion Center
Massachusetts

(U) Massachusetts State Police, Commonwealth Fusion Center
Phishing Campaign: Parking Meter QR Code
12 January 2022

(U) Overview

(U) Phishing attacks are constantly evolving to trick more victims in a variety of ways. Multiple police departments in Texas recently reported fraudulent QR code[1] stickers placed on parking meters disguised as "quick pay" options to steal unsuspecting parkers' payment information. This new phishing[2] attack tactic uses the QR code to direct unsuspecting users to a fraudulent website to enter payment details to pay for their parking. Instead of paying for the parking spot, victims are unknowing handing banking and credit card information directly to scammers. This scam is enticing because QR codes are known for speed and convenience, so a user might prefer this type of payment method to the use of cash or credit card at a pay station.

(U) Law enforcement and municipal officials should be aware of this current phishing tactic.

(U) Response Considerations

(U) Report incidents to your police department of jurisdiction.
(U) To report a suspected Internet-facilitated crime to the Federal Bureau of Investigation, follow the link to the Internet Crime Complaint Center (IC3):

- Internet Crime Complaint Center - WWW.IC3.GOV

(U) Outlook

(U) The Massachusetts State Police, CFC is providing this information for situational awareness purposes only. Please report any suspicious activity to your police department of jurisdiction.

Source: Bit Defender

Sources:
(U) "The latest phishing scam to watch out for: fraudulent QR codes on parking meters," The Verge, 12 January 2022
(U) "US Police Warn of Parking Meters with Phishing QR Codes," Bit Defender, 5 January 2022

[1] QR codes are a type of barcode or picture that can be scanned with a smartphone which can provide various forms of data, such as website links, account information, coupons, etc.
[2] Phishing is a cybercrime in which the unsuspecting victim willingly gives sensitive information (personal, financial, business) to someone they believe is an official/legitimate representative of an institution with which they have an existing or trusted relationship.

Unclassified
The information contained in this bulletin is unclassified.

Commonwealth Fusion Center
Massachusetts

(U) Massachusetts State Police, Commonwealth Fusion Center
Malicious USB Attacks
4 March 2022

(U) Overview

(U) The FBI released an alert that cybercriminals are mailing malicious USB flash drives[1] through the US Postal Service. FIN7, a cybercrime threat group, has been conducting USB attacks by mailing USBs laced with malware to US organizations in US defense, transportation, and private sector entities. FIN7 has used two different schemes to trick victims into plugging in the malicious USBs. One scheme contains a package that appears to come from the US Department of Health and Human Services that reportedly contains information on current pandemic guidelines. The second lure comes as an Amazon gift box which contains a thank you letter, USB, and counterfeit gift card. According to the FBI, both packages contain USBs that when connected to a computer will send preconfigured commands that download malicious software, creating direct back door access for cybercriminals to deploy ransomware.

Source: Bank Info Security

(U) Cybercriminals have also been known to plant malicious USBs in public areas hoping that unsuspecting victims will pick them up. "Lost and Found" USB attacks rely on victim's curiosity to see who the owner of the USB is or what type of files it contains. Cybercriminals may entice victims by labeling the USB as "finances, bonuses, payroll" or any title that may bait victims into plugging it into their computer.

Source: PC Mag

(U) Never plug an unknown USB into your personal or work computer!

(U) Response Considerations

(U) Report incidents to your police department of jurisdiction.
(U) To report a suspected Internet-facilitated crime to the Federal Bureau of Investigation, follow the link to the Internet Crime Complaint Center (IC3):

- Internet Crime Complaint Center - WWW.IC3.GOV

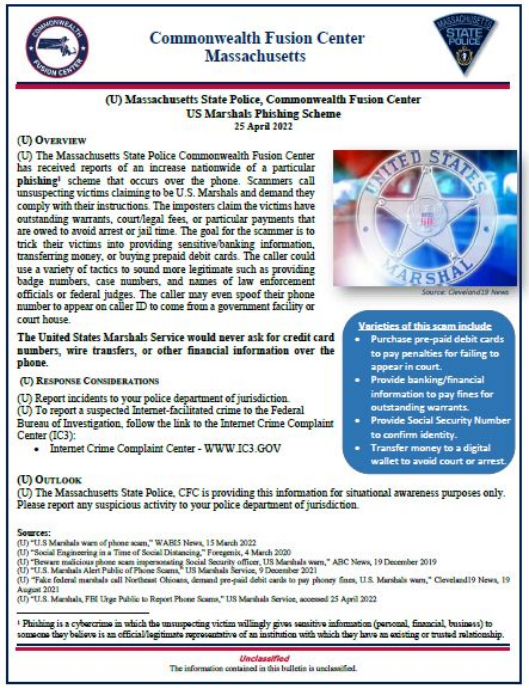
(U) Outlook

(U) The Massachusetts State Police, CFC is providing this information for situational awareness purposes only. Please report any suspicious activity to your police department of jurisdiction.

Sources:
(U) "FBI Warns FIN7 Campaign Delivers Ransomware via BadUSB," Dark Reading, 10 January 2022
(U) "FBI: Hackers use BadUSB to target defense firms with ransomware," Blooping Computer, 7 January 2022
(U) "FIN7 Targets US Enterprises Via BadUSB," Bank Info Security, 11 January 2022
(U) "FBI warns cybercriminals have tried to hack US firms by mailing malicious USB drives," CNN, 7 January 2022

[1] USB Flash Drive – A removable data storage device that can plug into a computer's USB port.

Unclassified
The information contained in this bulletin is unclassified.



Commonwealth Fusion Center
Massachusetts

(U) Massachusetts State Police, Commonwealth Fusion Center
US Marshals Phishing Scheme
25 April 2022

(U) Overview

(U) The Massachusetts State Police Commonwealth Fusion Center has received reports of an increase nationwide of a particular phishing[1] scheme that occurs over the phone. Scammers call unsuspecting victims claiming to be U.S. Marshals and demand they comply with their instructions. The imposters claim the victims have outstanding warrants, court/legal fees, or particular payments that are owed to avoid arrest or jail time. The goal for the scammer is to trick their victims into providing sensitive/banking information, transferring money, or buying prepaid debit cards. The caller could use a variety of tactics to sound more legitimate such as providing badge numbers, case numbers, and names of law enforcement officials or federal judges. The caller may even spoof their phone number to appear on caller ID to come from a government facility or court house.

Source: Cleveland19 News

The United States Marshals Service would never ask for credit card numbers, wire transfers, or other financial information over the phone.

Varieties of this scam include:

- Purchase pre-paid debit cards to pay penalties for failing to appear in court.
- Provide banking/financial information to pay fines for outstanding warrants.
- Provide Social Security Number to confirm identity.
- Transfer money to a digital wallet to avoid court or arrest.

(U) Response Considerations

(U) Report incidents to your police department of jurisdiction.
(U) To report a suspected Internet-facilitated crime to the Federal Bureau of Investigation, follow the link to the Internet Crime Complaint Center (IC3):

- Internet Crime Complaint Center - WWW.IC3.GOV

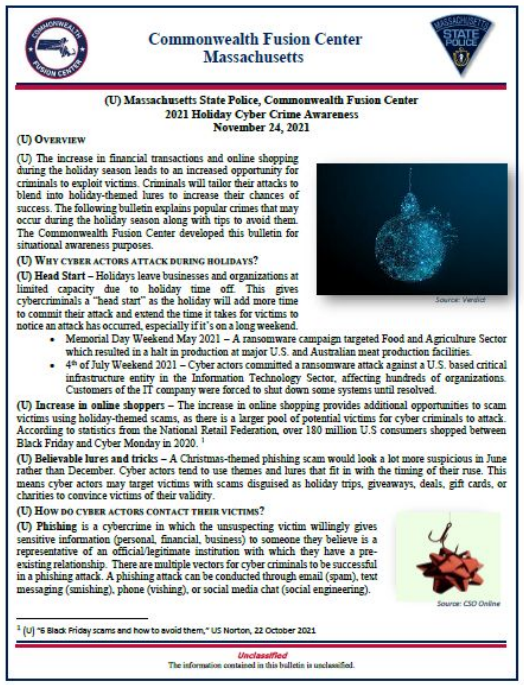
(U) Outlook

(U) The Massachusetts State Police, CFC is providing this information for situational awareness purposes only. Please report any suspicious activity to your police department of jurisdiction.

Sources:
(U) "U.S Marshals warn of phone scam," WAR5 News, 15 March 2022
(U) "Social Engineering in a Time of Social Distancing," Foregenix, 4 March 2020
(U) "Beware malicious phone scam impersonating Social Security office, US Marshals warn," ABC News, 19 December 2019
(U) "U.S. Marshals Alert Public of Phone Scams," US Marshals Service, 9 December 2021
(U) "Fake federal marshals call Northeast Ohioans, demand pre-paid debit cards to pay phoney fines, U.S. Marshals warn," Cleveland19 News, 19 August 2021
(U) "U.S. Marshals, FBI Urge Public to Report Phone Scams," US Marshals Service, accessed 25 April 2022

[1] Phishing is a cybercrime in which the unsuspecting victim willingly gives sensitive information (personal, financial, business) to someone they believe is an official/legitimate representative of an institution with which they have an existing or trusted relationship.

Unclassified
The information contained in this bulletin is unclassified.



Commonwealth Fusion Center
Massachusetts

(U) Massachusetts State Police, Commonwealth Fusion Center
2021 Holiday Cyber Crime Awareness
November 24, 2021

(U) Overview

(U) The increase in financial transactions and online shopping during the holiday season leads to an increased opportunity for criminals to exploit victims. Criminals will tailor their attacks to blend into holiday-themed lures to increase their chances of success. The following bulletin explains popular crimes that may occur during the holiday season along with tips to avoid them. The Commonwealth Fusion Center developed this bulletin for situational awareness purposes.

Source: Verdict

(U) Why cyber actors attack during holidays?

(U) Head Start – Holidays leave businesses and organizations at limited capacity due to holiday time off. This gives cybercriminals a "head start" as the holiday will add more time to commit their attack and extend the time it takes for victims to notice an attack has occurred, especially if it's on a long weekend.

- Memorial Day Weekend May 2021 – A ransomware campaign targeted Food and Agriculture Sector which resulted in a halt in production at major U.S. and Australian meat production facilities.
- 4th of July Weekend 2021 – Cyber actors committed a ransomware attack against a U.S. based critical infrastructure entity in the Information Technology Sector, affecting hundreds of organizations. Customers of the IT company were forced to shut down some systems until resolved.

(U) Increase in online shoppers – The increase in online shopping provides additional opportunities to scam victims using holiday-themed scams, as there is a larger pool of potential victims for cyber criminals to attack. According to statistics from the National Retail Federation, over 180 million U.S consumers shopped between Black Friday and Cyber Monday in 2020. [1]

(U) Believable lures and tricks – A Christmas-themed phishing scam would look a lot more suspicious in June rather than December. Cyber actors tend to use themes and lures that fit in with the timing of their ruse. This means cyber actors may target victims with scams disguised as holiday trips, giveaways, deals, gift cards, or charities to convince victims of their validity.

(U) How do cyber actors contact their victims?

(U) Phishing is a cybercrime in which the unsuspecting victim willingly gives sensitive information (personal, financial, business) to someone they believe is a representative of an official/legitimate institution with which they have a pre-existing relationship. There are multiple vectors for cyber criminals to be successful in a phishing attack. A phishing attack can be conducted through email (spam), text messaging (smishing), phone (vishing), or social media chat (social engineering).

Source: CSO Online

[1] (U) "6 Black Friday scams and how to avoid them," US Norton, 22 October 2021

Unclassified
The information contained in this bulletin is unclassified.

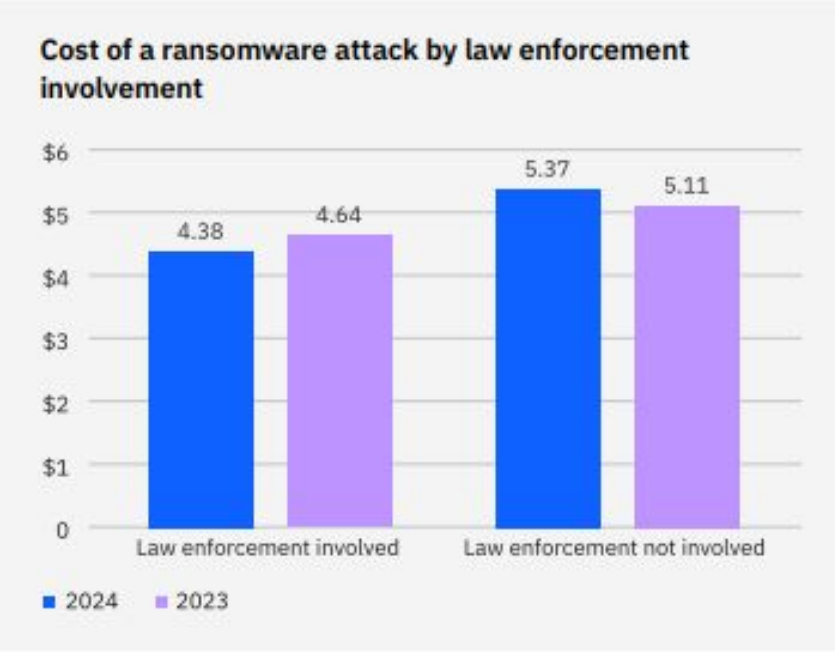
Cyber Threats and Response

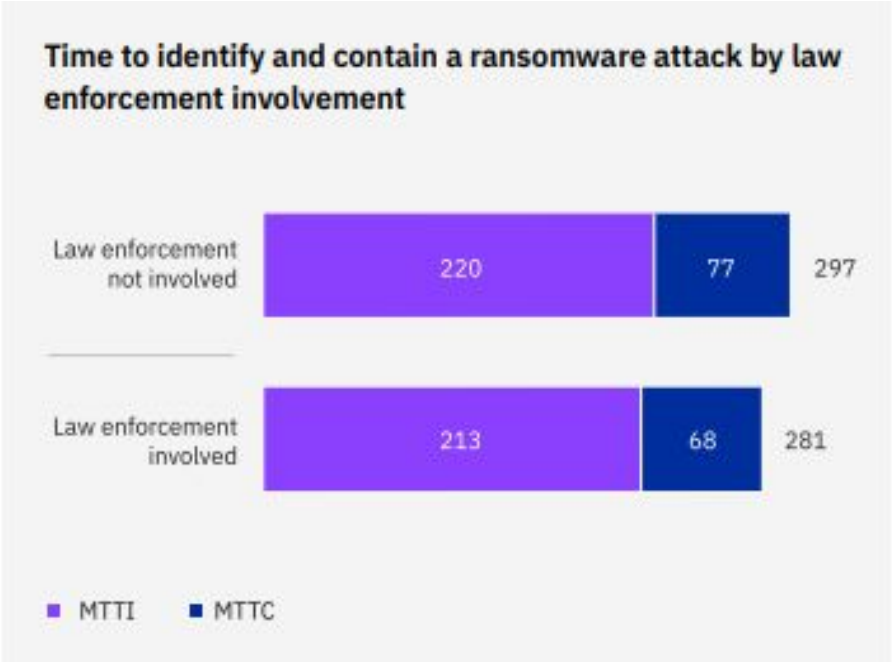
- Vulnerability & Threat Intelligence Project (VTIP)
- Passive Attack Surface Monitoring
- Vulnerabilities, exposures, stolen/leaked creds, typosquatting
  - OT/ICS/SCADA/BAC
  - Remote Access Entry Points/VPNs
    - Crown Jewels
      - Sensitive systems/data (PII, financial, etc)
      - Mission critical assets

REPORTING

- **You are our best source of Cyber Threat Intelligence!**
- Reporting entity **will not** be identified when sharing out information
  - *“a municipality in Massachusetts” , “a K-12 organization in Massachusetts”, “a public safety agency in Massachusetts”*
- **Shared information passed on to larger community for situational awareness and as actionable, timely, relevant CTI via MCP Distro**

IBM COST OF A DATA BREACH Report 2024



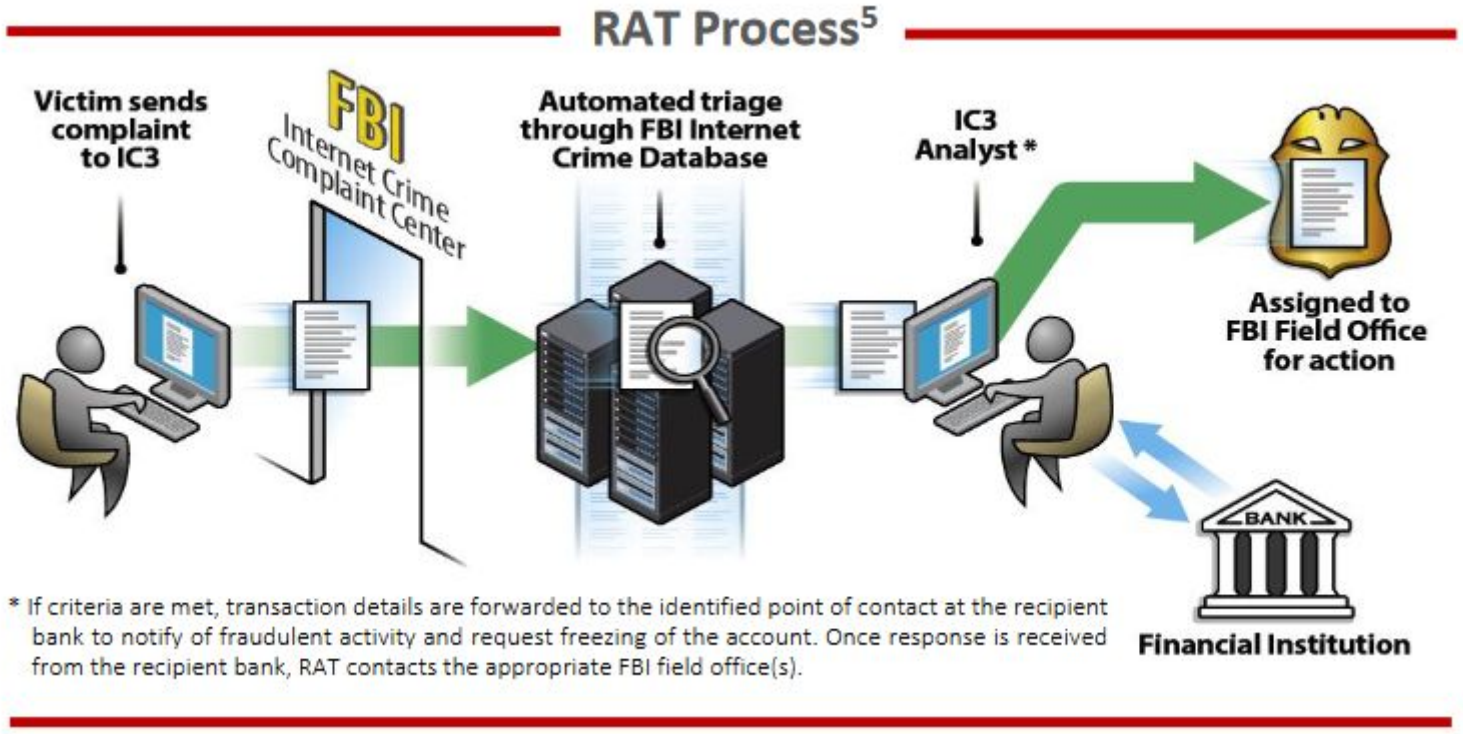


$1M USD or approximately 20%
cost savings when law enforcement is involved in ransomware attacks

Law Enforcement involvement also sped up the time it took to identify and contain a breach (9% reduction in combined Mean Time to Identify & Mean Time to Resolve)

Post BEC: Contact with Law Enforcement

FBI Recovery Asset Team can work with FINCEN to recover funding within 72 hours of loss



Verizon DBIR

- 18 Percent of incidents had nothing frozen.
- 50 percent of incidents had 79% of losses frozen.

Reporting Cyber Incidents – How?

Report to:

- Cyber Insurance
- Local Police Department
- Commonwealth Watch Center 508-820-2233
- EOTSS SOC
  - (*Strongly Encouraged* under Executive Order 602)
- FBI – www.IC3.gov
- For BEC with financial loss – file www.IC3.gov report **AND** contact your financial institution immediately
- Others according to IRP*

Communication Channels/Bands:

- Use *out-of-band* channels
- May tip off threat actor, allow them access to communications discussing response

 Enterprise Email, Teams, VOIP (O365, Google)

✓ Cellphones

✓ Non-VOIP landlines

✓ Pre-configured out-of-band accou

✓ Personal email (GMail, etc)

✓ End-to-end encrypted cha

Reporting Cyber Incidents – 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.

COMMONWEALTH FUSION CENTER

MA CIRT & Coordination with EOTSS

- EOTSS & CFC routinely share information
  - Vulnerabilities & exposures
  - Reported incidents
- MA CIRT formalized in December 2022
  - Executive Order 602
  - EOTSS, EOPSS, MANG, MEMA
  - CFC & MSP Cyber Crime Unit
    - CFC Intelligence/Information Sharing, coordination with Federal Partners & LE
    - MSP CCU Threat Response (DFIR), Criminal Investigation

Massachusetts Joint Cybersecurity Threat Briefing

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

MCP
Massachusetts Cybersecurity Program

No portion of the presentation should be video or audio recorded, copied, or photographed.

TLP GREEN

TLP GREEN

MCP

Massachusetts Cybersecurity Program

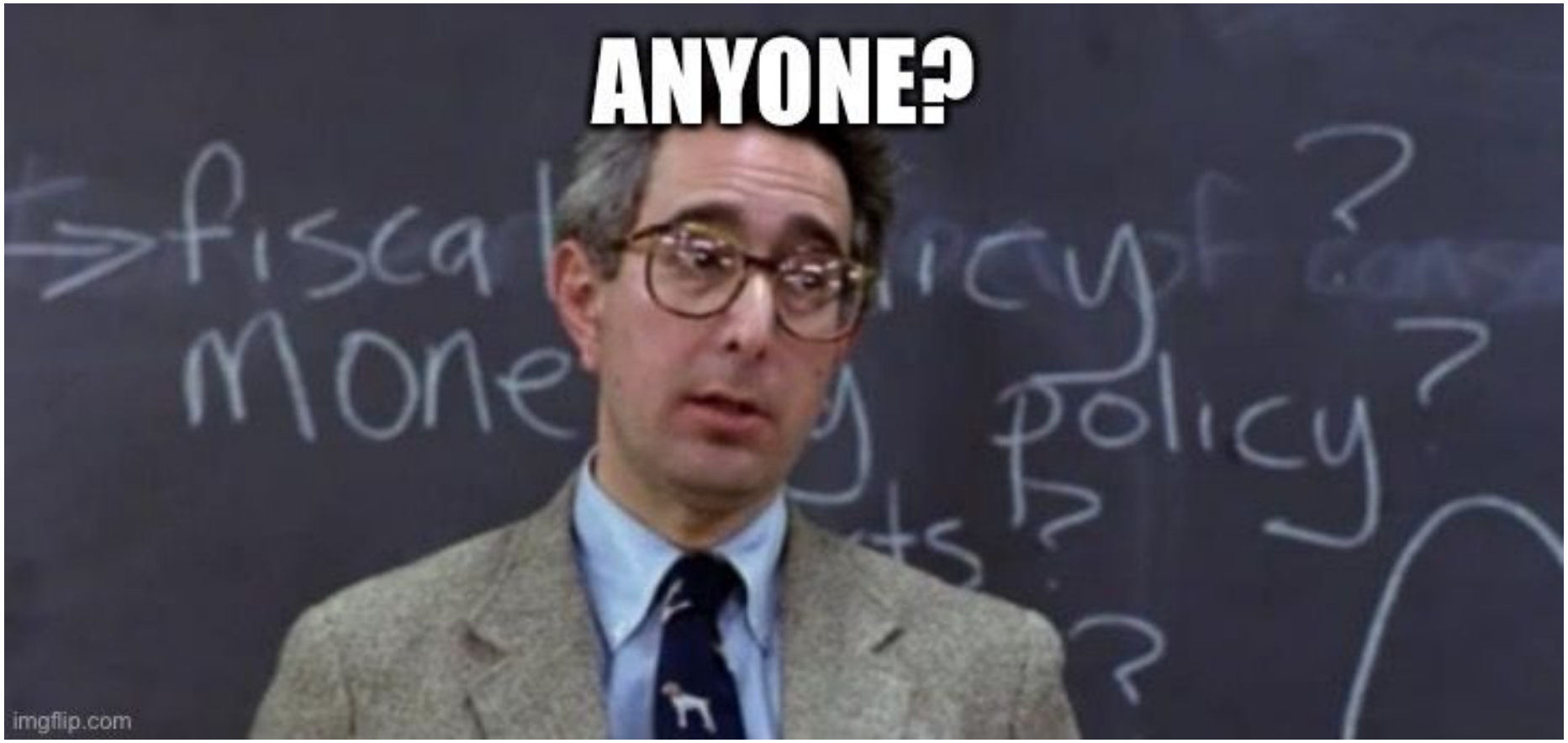
Detective Lieutenant Brian Gavioli

978-451-3557 email: brian.gavioli@mass.gov

General Inquiries: mcppol@pol.state.ma.us

Report an Incident: 508-820-2233

Wrap Up & Questions



ADDENDUM SLIDES

Presentation Resources

Speaker Information:

John Petrozzelli, Director
MassCyberCenter
Petrozzelli@MassTech.org

Joe Callahan
Cabot Risk Management
joe.callahan@cabotrisk.com

Gregory Bautista, Partner
Mullen Coughlin
gbautista@mullen.law

Susan Noyes, Director
EOTSS Office of Municipal & School Technology
susan.noyes@mass.gov
General Inquiries: OMST@mass.gov
(617) 626-4403

Detective Lieutenant Brian Gavioli
Commonwealth Fusion Center – MA Cybersecurity Program
brian.gavioli@mass.gov
(978) 451-3557
General Inquiries: mcppol@pol.state.ma.us
Report an Incident: 508-820-2233

Data Sources:

Presentation Resources

Toolkits, Programs, and Services:

Services

CISA Cyber Hygiene (CyHy)

Free cybersecurity services to help organizations reduce their exposure to threats by taking a proactive approach to monitoring and mitigating attack vectors.

- Vulnerability Scanning
- Web Application Scanning (WAS)
- CISA Remote Penetration Testing

CISA Logging Made Easy

Endpoint Managed Detection and Response (EDR/MDR)

- CyberTrust SOC (SentinelOne 24/7)
- MS-ISAC SOC (Crowdstrike)

EOTSS Cybersecurity Health Check Program

Cybersecurity Assessments to identify security gaps and an organization's ability to protect data and systems from cyber threats.

Presentation Resources

Grants

Cyber Resilient Massachusetts Grant Program

Grants to help municipalities remediate cybersecurity vulnerabilities and defend against cybersecurity threats by funding narrowly focused cybersecurity technology upgrades identified through a cybersecurity vulnerability assessment.

State and Local Cybersecurity Grant Program

Massachusetts Municipal Local Cybersecurity Grant Program

Grants to assist municipal governments in strengthening cybersecurity while reducing systemic cyber risk, especially for

- Multifactor Authentication (MFA) implementation
- Cybersecurity Awareness Training
- Cyber Incident Response Planning
- Cybersecurity Tabletop Exercises
- Migration to the .gov domain

Community Compact Cabinet Grants

Best Practices Program

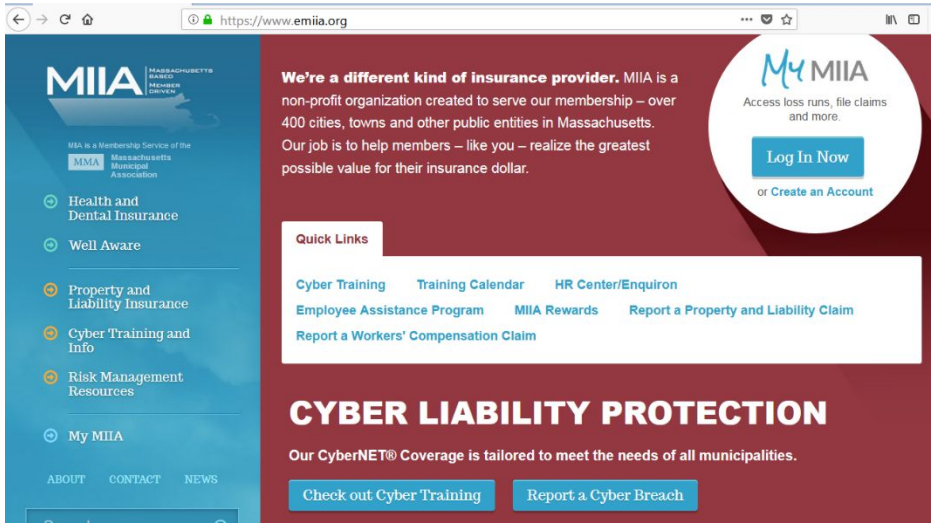
Opportunities to implement IT best practices related to planning and security.

IT Grant Program

MIIA Cyber Risk

- **Cyber Training**
  - *Courses*
  - *Guides*
  - *Webinars*
- **Sample Policies**
  - *Data Security Policies*
  - *Plans*
  - *Procedures*
- **Incident Response Plans**
- **Best Practices**

www.emiia.org



https://emiia.nascybernet.com/index.php

Mullen Coughlin

- Founded in **2016**
- **130+** attorneys across the United States and the United Kingdom
- **One firm, one focus: Cyber**
  - Advisory Compliance
    - Counseled **over 1,200** organizations between 2020 and 2023
  - Incident Response
    - Handled **over 14,000** incidents between 2020 and 2023
  - Privacy Litigation Defense
    - Defended **over 540** organization in single-plaintiff, class action and B2B privacy litigation between 2020 and 2023
  - Regulatory Investigation Defense
    - Responded to **thousands** of *informal* and *formal* investigations between 2020 and 2023

Things to Think About Before an Incident

- Incident Response Plan
- Ransomware – Recovery and Negotiations
- Data Mapping and Identification
- Communications

Things to Think About Before an Incident Takeaways

- What could sidetrack your response?
- Evaluate your recovery plan and downtime procedures
- Structured vs. Unstructured Data, Notice Timelines
- Who gets to speak? What do they say?

Contact Information

Gregory Bautista
Partner – Mullen Coughlin LLC

E: gbautista@mullen.law

24/7/365 Incident Response Hotline
844.885.1574

MULLEN.LAW | LINKEDIN
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

MassCyberCenter Team

John Petrozzelli
Director
Petrozzelli@masstech.org

Meg Speranza
Resiliency Program Manager
Speranza@masstech.org

Max Fathy
Senior Program Manager, Cybersecurity Innovation
Fathy@masstech.org

Nick Butts
Outreach Program Manager
Butts@masstech.org

Questions?

Visit our website to connect with us and learn more:

MassCyberCenter.org

MCP

Massachusetts Cybersecurity Program

Detective Lieutenant Brian Gavioli

978-451-3557 email: brian.gavioli@mass.gov

General Inquiries: mcppol@pol.state.ma.us

Report an Incident: 508-820-2233