Municipal Cybersecurity: Safeguarding Communities Online

CONNECT 351

An interactive Tabletop Exercise Card Game

Led by the **MassCyberCenter**

January 24, 2026

MassCyberCenter
at the MassTech Collaborative

Your Guides on this Adventure

John Petrozzelli
Director
MassCyberCenter
Petrozzelli@MassTech.org

Gregory Bautista
Partner
Mullen Coughlin LLC
gbautista@mullen.law

David Dowd
President
Cabot Risk Strategies
ddowd@mma.org

Susan Noyes
Director
EOTSS Office of Municipal and School Technology
Susan.Noyes@mass.gov

MassCyberCenter

Municipal Cybersecurity: Safeguarding Communities Online

Presented to the **Massachusetts Municipal Association** by:

Gregory Bautista, *Partner* – Mullen Coughlin LLC

January 24, 2026

Incident Response Statistics

2022-2025

Incident Type

Incident Type	2022	2023	2024	2025	Total
Business Email Compromise (BEC)	1,075 (36%)	1,343 (34%)	1,601 (38%)	1,666 (39%)	**5,685 (37%)**
BEC – Other	731	996	1,224	1,266	4,217
BEC – Wire Fraud	344	347	377	400	1,468
Ransomware	735 (25%)	883 (23%)	1,011 (24%)	1,134 (26%)	**3,763 (24%)**
Vendor Breach	315 (11%)	749 (19%)	747 (18%)	592 (14%)	**2,403 (16%)**
Network Intrusion	382 (13%)	323 (8%)	322 (7%)	343 (8%)	**1,370 (9%)**
Other	245 (8%)	403 (10%)	346 (8%)	368 (9%)	**1,362 (9%)**
Inadvertent Disclosure	207 (7%)	218 (6%)	228 (5%)	188 (4%)	**841 (5%)**
Total	***2,959 (100%)***	***3,919 (100%)***	***4,255 (100%)***	***4,291 (100%)***	***15,424 (100%)***

RW & BEC Incidents

RW Incidents	2022	2023	2024	2025	Total
Number of RW Incidents	735 (25%)	883 (23%)	1,011 (24%)	1,134 (26%)	**3,763 (24%)**
Number of RW Incidents Paid	114 (16%)	156 (18%)	161 (16%)	132 (12%)	**563 (15%)**
Average Ransom Demand	$2,241,753	$2,180,723	$1,755,468	$2,887,234	**$2,259,948**
Average Ransom Payment	$438,901	$818,177	$452,530	$1,631,153	**$862,453**
Median Ransom Payment	$208, 774	$192,278	$220,000	$150,000	**$184,555**
Ransom Payment Reason	Delete Only – 26 (23%) Key & Delete – 48 (42%) Key Only – 40 (35%)	Delete Only – 50 (32%) Key & Delete – 66 (42%) Key Only – 40 (26%)	Delete Only – 66 (41%) Key & Delete – 61 (38%) Key Only – 34 (21%)	Delete Only – 47 (36%) Key & Delete – 35 (26%) Key Only – 50 (38%)	**Delete Only – 189 (34%)** **Key & Delete – 210 (37%)** **Key Only – 164 (29%)**

BEC Incidents	2022	2023	2024	2025	Total
Number of BEC / BEC – WF Incidents	1,075 (36%)	1,343 (34%)	1,601 (38%)	1,666 (39%)	**5,685 (37%)**
Number of BEC – WF Incidents	344 (32%)	347 (26%)	377 (24%)	400 (24%)	**1,468 (26%)**
Average Amount Fraudulently Wired	$374,434	$824,704	$442,961	$796,942	**$556,052**
Median Amount Fraudulently Wired	$144,000	$148,867	$154,622	$114,000	**$147,606**

Incident Type: Government

Incident Type	2022	2023	2024	2025	Total
Business Email Compromise (BEC)	32 (36%)	46 (33%)	47 (31%)	52 (37%)	**177 (32%)**
BEC – Other	25	38	40	42	**145**
BEC – Wire Fraud	7	8	7	10	**32**
Ransomware	34 (28%)	25 (18%)	42 (27%)	36 (26%)	**137 (25%)**
Vendor Breach	15 (12%)	29 (21%)	31 (20%)	23 (17%)	**98 (17%)**
Inadvertent Disclosure	18 (15%)	13 (10%)	15 (10%)	10 (7%)	**56 (10%)**
Network Intrusion	16 (13%)	15 (11%)	10 (6%)	7 (5%)	**48 (9%)**
Other	7 (6%)	10 (7%)	10 (6%)	11 (8%)	**38 (7%)**
Total	***122 (100%)***	***138 (100%)***	***155 (100%)***	***139 (100%)***	***554 (100%)***

RW & BEC Incidents: Government

RW Incidents	2022	2023	2024	2025	Total
Number of RW Incidents	34 (28%)	25 (18%)	42 (27%)	36 (26%)	**137 (25%)**
Number of RW Incidents Paid	5 (15%)	0 (%)	1 (2%)	4 (11%)	**10 (7%)**
Average Ransom Demand	$894,444	$907,500	$2,914,667	$689,545	**$1,378,697**
Average Ransom Payment	$377,500	N/A	$750,000	$60,700	**$278,089**
Median Ransom Payment	$300,000	N/A	$750,000	$70,000	**$100,000**
Ransom Payment Reason	Delete Only – 1 (20%) Key & Delete – 3 (60%) Key Only – 1 (20%)	N/A	Key & Delete – 1 (100%)	Delete Only – 2 (50%) Key & Delete – 1 (25%) Key Only – 1 (25%)	**Delete Only – 3 (30%)** **Key & Delete – 5 (50%)** **Key Only – 2 (20%)**

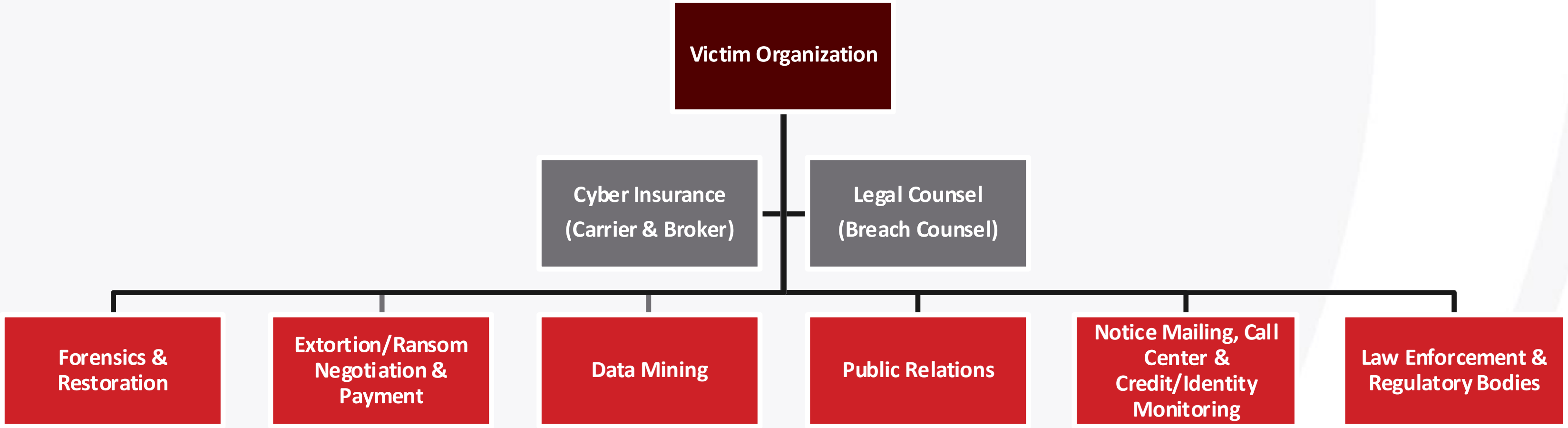
BEC Incidents	2022	2023	2024	2025	Total
Number of BEC / BEC – WF Incidents	32 (36%)	46 (33%)	47 (31%)	52 (37%)	**177 (32%)**
Number of BEC – WF Incidents	7 (22%)	8 (17%)	7 (15%)	10 (19%)	**32 (18%)**
Average Amount Fraudulently Wired	$251,867	$198,825	$128,726	$490,691	**$278,592**
Median Amount Fraudulently Wired	$196,822	$148,926	$78,891	$369,840	**$147,572**

Who Are The Players?

Internal Stakeholders

- Information Technology
- Town Counsel
- Risk Manager
- Human Resources
- Communications
- Municipal Leadership

External Stakeholders



Victim Organization

Cyber Insurance (Carrier & Broker)

Legal Counsel (Breach Counsel)

Forensics & Restoration

Extortion/Ransom Negotiation & Payment

Data Mining

Public Relations

Notice Mailing, Call Center & Credit/Identity Monitoring

Law Enforcement & Regulatory Bodies

Contact

Gregory Bautista, *Partner*
Mullen Coughlin LLC
☎ (267) 930-1509
✉ gbautista@mullen.law

If you suspect your organization is currently experiencing a data privacy and security incident, contact the 24/7/365 Mullen Coughlin U.S. Incident Response Hotline at (844) 885-1574 or via email at breachhotline@mullen.law.

CITY OF LOWELL

Video

April 2023 Cyber Incident

Produced by EOTSS/OMST

Executive Office of Technology Services and Security (TSS)

Our mission is to provide technology leadership across the Commonwealth to enhance the quality of public service and foster positive community outcomes

CyberSecureDeck: *Defend the Network* Card Game

Purpose & Objectives

The **purpose** of this interactive session is to provide participants with a better understanding of what happens during a cybersecurity incident and to emphasize the importance of collaboration across the organization—including leadership and all departments—during an incident.

The **objective** of this session is to provide an opportunity to:

- *Collaborate and practice* cyber incident response actions within a safe, no-fault environment
- *Assess* what information and resources are needed to respond to and recover from an incident
- *Identify* opportunities to improve cyber incident response plans

*This card game was developed by the **Cyber Resilient Massachusetts Working Group.** To download a copy of the game, go to **MassCyberCenter**.org.*

MassCyberCenter

CyberSecureDeck: *Defend the Network* Card Game

Components of Today's Game

Facilitators

The Facilitator guides players through the game. They do not "play" the game or represent a Role or have a purpose within the Organization.

Roles – The 8 Roles make up the Organization

Leader * Human Resources (HR) * Finance * Communications/Media * Operations * Information Technology (IT) * Legal/Risk/Compliance * Security/Law Enforcement

Scenarios & Injects

The Facilitator has chosen one Scenario that has 12 Injects.

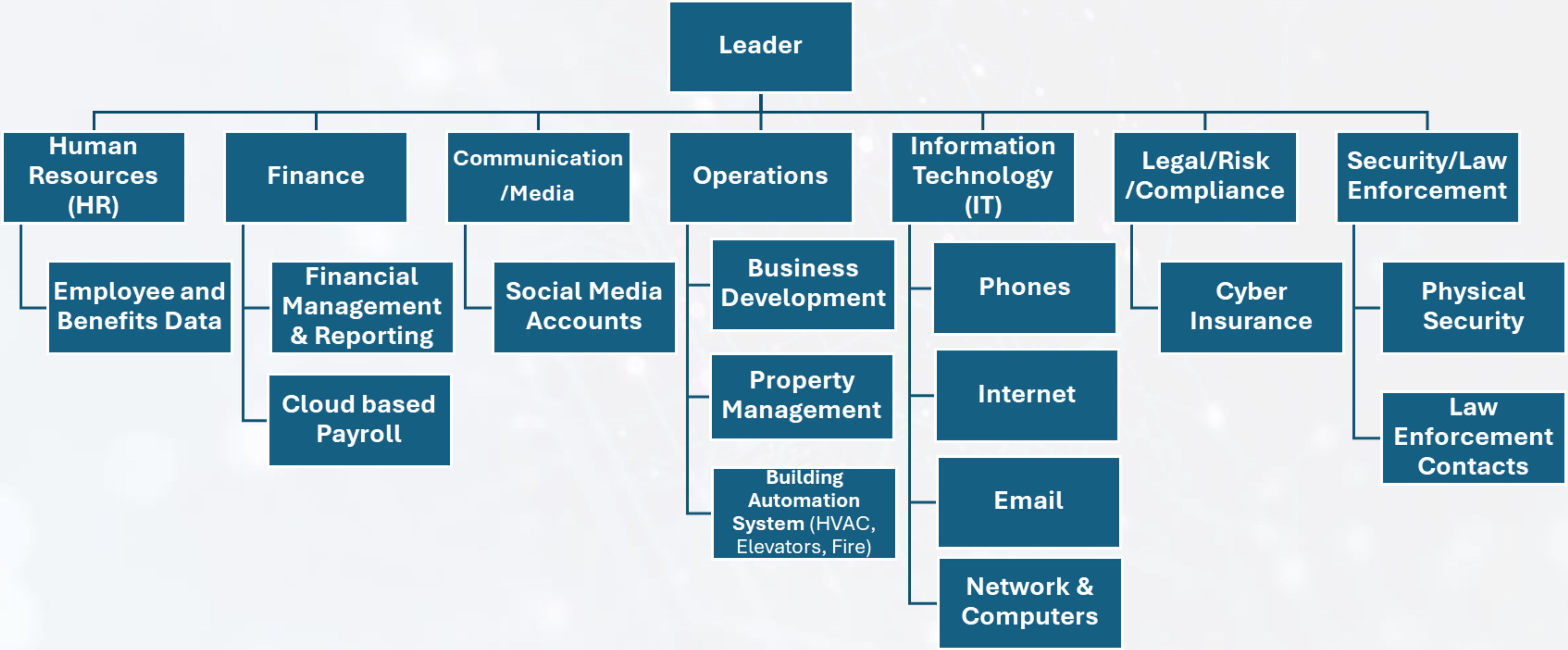
CyberSecureDeck: *Defend the Network* Card Game
Components of Today's Game (continued)

Organization

- The Organization is based in Massachusetts and represents a business, corporation, non-profit, school, public agency, or local government.
- The Organization provides services to citizens/customers/students and is made up of the 8 roles.
- The Organization may collect and/or hold citizen/customer/student data, and that data will include employee data and may include citizen/customer/student Personally Identifiable Information (PII) and Personal Health Information (PHI) as well as financial information.
- Citizens/customers/students rely on the Organization.

CyberSecureDeck: *Defend the Network* Card Game

Components of Today's Game (continued)



- Leader
  - Human Resources (HR)
    - Employee and Benefits Data
  - Finance
    - Financial Management & Reporting
    - Cloud based Payroll
  - Communication /Media
    - Social Media Accounts
  - Operations
    - Business Development
    - Property Management
    - Building Automation System (HVAC, Elevators, Fire)
  - Information Technology (IT)
    - Phones
    - Internet
    - Email
    - Network & Computers
  - Legal/Risk /Compliance
    - Cyber Insurance
  - Security/Law Enforcement
    - Physical Security
    - Law Enforcement Contacts

CyberSecureDeck: *Defend the Network* Card Game

Getting Started

Each Group

- 8 Role Cards
- Directions: ROLES Card
- GAME PURPOSE, OBJECTIVE and COMPONENTS Sheet (including Organization Chart)

Choose a Role Card

Choose a Role from the Role cards—if there are less than 8 players in a group, please take a second Role to fill all the Roles. *Every Role should be filled.*

Review your Role and other materials

Scenario and Injects

The Scenario has been chosen and will be revealed during the Hot Wash after the game.

Each inject card should be picked up from the deck one-by-one (in order) and handed to the player with the corresponding Role indicated on the inject card. That player should read the card and then all players should consider “What would you do with this information?” as part of the discussion.

When a player in a Role receives an Inject card, they may choose to share the information with other Roles or the Organization (all 8 Roles*) in-whole* or *in-part* or *not at all*.

Tabletop Exercises in Your Pocket

MassCyberCenter

Scenario: PHISHING
Inject 1 and 2

ROLE: ***OPERATIONS***

DETAIL:

- Shortly after 9 a.m. employees begin reporting that the phone system is offline.
- Employees from several different Organization locations are calling Operations to say that the HVAC is not working in their location.
- Operations is unable to log into the Building Automation System portal to check temperatures and adjust settings.

What do you do with this information?

Scenario: PHISHING
Inject 3

ROLE: ***INFORMATION TECHNOLOGY***

DETAIL:

- The IT team discovers a recent email containing a suspicious URL that was clicked on by an Organization employee.
- This caused several small binary files to be downloaded onto the employee's computer.
- These files created an encrypted connection from the computer to a remote system.
- That connection remained active until the computer was quarantined and removed from the network.
- The file signature of a file found on the computer matches a newly-reported keylogger and ransomware variant.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Email Security (2.M)

Scenario: PHISHING
Inject 4

ROLE: ***LEADER***

DETAIL:

- The Leader receives a call on their cellphone from a local news reporter asking for a comment on a just-published cybersecurity blog that mentions a *Ransomware-for-Hire* request targeting the Organization.

What do you do with this information?

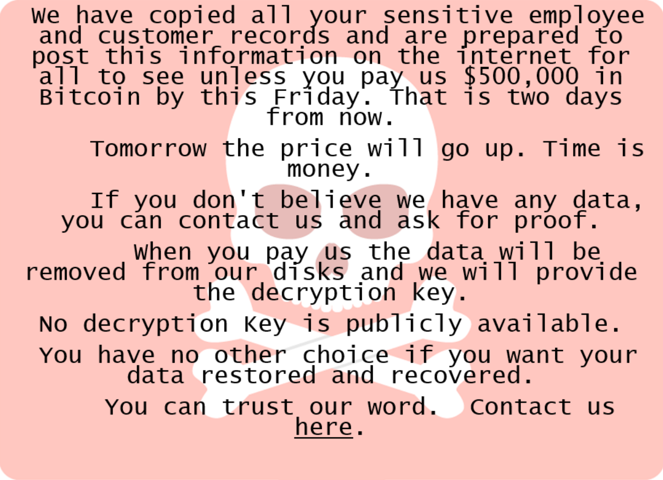
CISA Cybersecurity Performance Goal:
Secure Sensitive Data (2.L)

Scenario: PHISHING
Inject 5

ROLE: ***FINANCE***

DETAIL:

- 15 minutes after the Finance team logged into their computers this morning, the computers stopped responding. Shortly thereafter, the computers all displayed this message:



We have copied all your sensitive employee and customer records and are prepared to post this information on the internet for all to see unless you pay us $500,000 in Bitcoin by this Friday. That is two days from now.

Tomorrow the price will go up. Time is money.

If you don't believe we have any data, you can contact us and ask for proof.

When you pay us the data will be removed from our disks and we will provide the decryption key.

No decryption Key is publicly available.

You have no other choice if you want your data restored and recovered.

You can trust our word. Contact us here.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Hardware and Software Approval Process (2.Q)

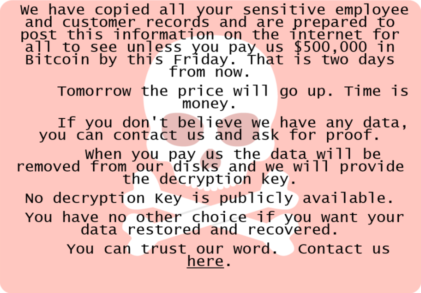
MassCyberCenter.org

Scenario: PHISHING
Inject 6 and 7

ROLE: ***INFORMATION TECHNOLOGY***

DETAIL:

- The VOIP (voice over internet protocol) server is displaying a Ransomware notice on its login screen similar to the one observed in Finance.
- The local on-site backup server is displaying a Ransomware notice on its login screen similar to the one observed in Finance.
- The local on-site backup server is displaying a Ransomware notice on its login screen similar to the one observed in Finance



We have copied all your sensitive employee and customer records and are prepared to post this information on the internet for all to see unless you pay us $500,000 in Bitcoin by this Friday. That is two days from now.

Tomorrow the price will go up. Time is money.

If you don't believe we have any data, you can contact us and ask for proof.

When you pay us the data will be removed from our disks and we will provide the decryption key.

No decryption Key is publicly available.

You have no other choice if you want your data restored and recovered.

You can trust our word. Contact us here.

What do you do with this information?

Scenario: PHISHING
Inject 8

ROLE: ***HUMAN RESOURCES***

DETAIL:

- The HR Director just received an email from a strange email address that claims to be from the Ransomware attacker.

> We have copied all your sensitive employee and customer records and are prepared to post this information on the internet for all to see unless you pay us $500,000 in Bitcoin by this Friday. That is two days from now.
>
> Tomorrow the price will go up. Time is money.
>
> If you don’t believe we have any data you can contact us and ask for proof.
>
> When you pay us the data will be removed from our disks and we provide decryption key
>
> Contact us here.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Reporting (4.A)

Scenario: PHISHING
Inject 9

ROLE: ***INFORMATION TECHNOLOGY***

DETAIL:

- The Managed Services Provider (MSP) supporting your team called and said that it will take about 10 - 14 days to restore all systems from existing backups.
- Upon request, the MSP told you the estimated cost for the MSP to surge overtime to restore all backups within 5 days is $250,000.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Planning and Preparedness (5.A)

Scenario: PHISHING
Inject 10

ROLE: ***COMMUNICATIONS***

DETAIL:

- Multiple customers are posting on social media that they received an email from hackers stating that their data has been stolen due to the Organization's lax security practices and that they should sue the Organization.
- In an escalated demand, the attackers had said that they would consider not making the customer data public if the customer pays $5 million in Bitcoin.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Reporting (4.A)

Scenario: PHISHING
Inject 11

ROLE: ***SECURITY/LAW ENFORCEMENT***

DETAIL:

- You receive a call from a Law Enforcement partner
  1. Asking if you need help, and
  2. Providing a friendly reminder about State Data Breach Notification Laws

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Reporting (4.A)

Scenario: PHISHING

Inject 12

ROLE: ***INFORMATION TECHNOLOGY***

DETAIL:

- The Incident Responder's forensic review revealed the following information:
  - Finance received an email, purportedly from a trusted vendor, asking for a review of an invoice. An employee clicked on the link, causing a malicious file to be downloaded to the Organization's network.
  - The file remained undetected and was used by hackers to conduct reconnaissance and password stealing for several days before the hackers became operational.
  - Hackers used administrative privileges to execute their attack and gain access to the building automation system, phone system, and multiple computers on the network.

What do you do with this information?

Scenario: PHISHING
Inject 13

ROLE: ***LEADER***

DETAIL:

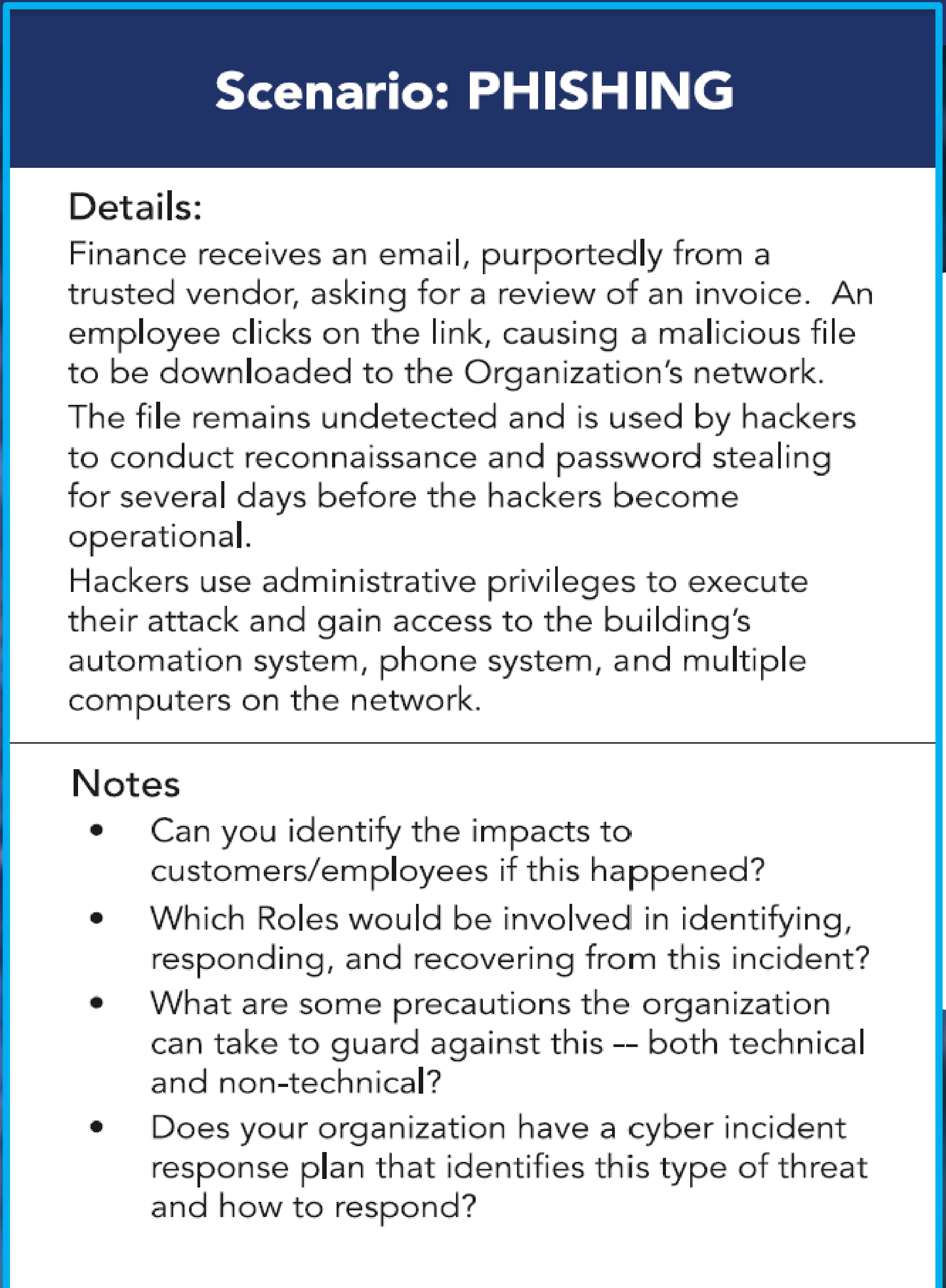
- The Leader asks the team to convene for a meeting to discuss several items:
  - What is the business impact of this cybersecurity incident?
  - What are the best options? Backups? Pay ransom?
  - Who do we notify? When?
  - What are the projections for service disruptions?

What do you do with this information?

CISA Cybersecurity Performance Goal:
Incident Planning and Preparedness (5.A)

Tabletop Exercises in Your Pocket

Scenario Reveal



Scenario: PHISHING

Details:

Finance receives an email, purportedly from a trusted vendor, asking for a review of an invoice. An employee clicks on the link, causing a malicious file to be downloaded to the Organization's network.

The file remains undetected and is used by hackers to conduct reconnaissance and password stealing for several days before the hackers become operational.

Hackers use administrative privileges to execute their attack and gain access to the building's automation system, phone system, and multiple computers on the network.

Notes

- Can you identify the impacts to customers/employees if this happened?
- Which Roles would be involved in identifying, responding, and recovering from this incident?
- What are some precautions the organization can take to guard against this -- both technical and non-technical?
- Does your organization have a cyber incident response plan that identifies this type of threat and how to respond?

Tabletop Exercises in Your Pocket
Hotwash

Game Discussion

- What is happening within the Organization during the Game?
- What steps is each Role taking to respond to events?
- How should all this information come together?
- What communications are important during an event like this?
- Who should communications be prioritized with (internally/externally)?
- Do you consider activating a Cyber Incident Response Plan (CIRP)? When and Why?
- How did the game go? What would you do differently?

MassCyberCenter

OMST
OFFICE OF MUNICIPAL & SCHOOL TECHNOLOGY

Massachusetts Municipal Association (MMA)

Connect351 - January 24, 2026

Susan Noyes

Director, Office of Municipal and School Technology

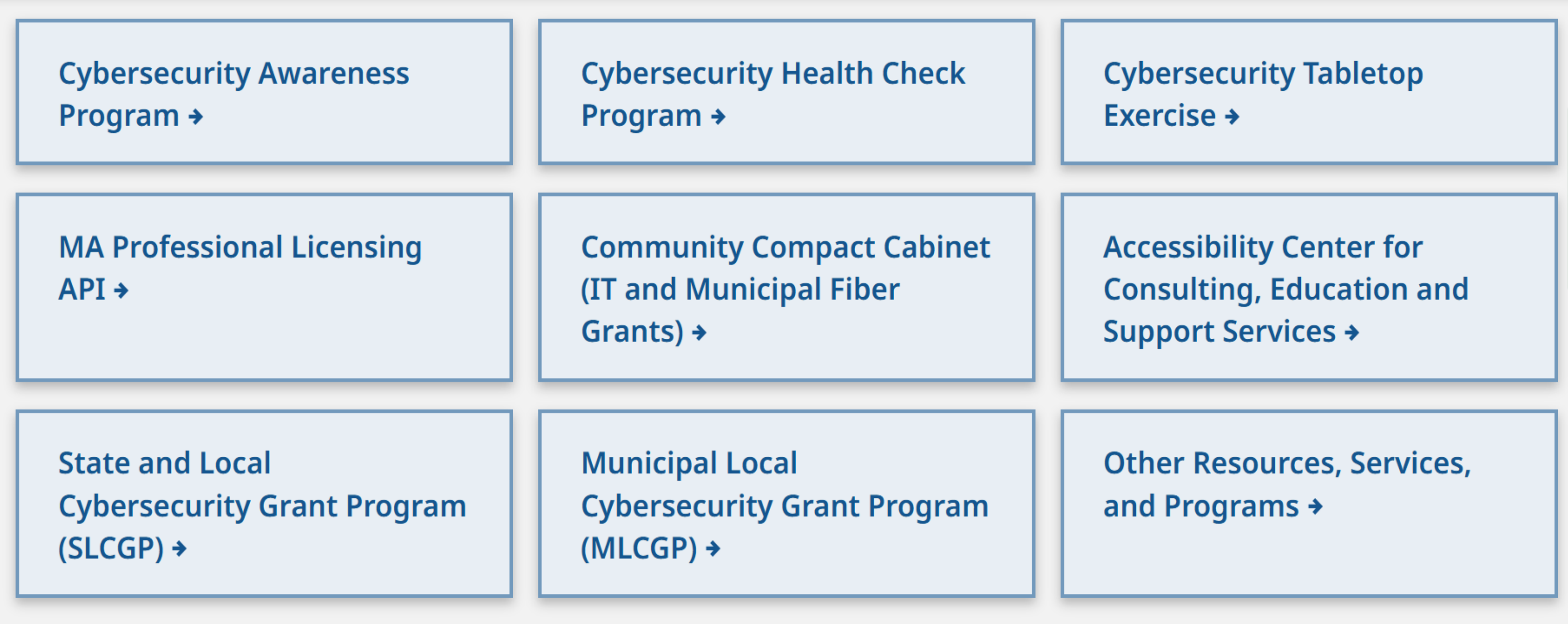
susan.noyes@mass.gov

Executive Office of Technology Services and Security (TSS)

Our mission is to provide technology leadership across the Commonwealth to enhance the quality of public service and foster positive community outcomes

OMST
OFFICE OF MUNICIPAL
& SCHOOL TECHNOLOGY

OMST strives to promote a connected Commonwealth of innovative and resilient local government agencies, empowered by the strategic use of technology through collaboration, guidance, and access to state and partner resources.



Cybersecurity Awareness Program →

Cybersecurity Health Check Program →

Cybersecurity Tabletop Exercise →

MA Professional Licensing API →

Community Compact Cabinet (IT and Municipal Fiber Grants) →

Accessibility Center for Consulting, Education and Support Services →

State and Local Cybersecurity Grant Program (SLCGP) →

Municipal Local Cybersecurity Grant Program (MLCGP) →

Other Resources, Services, and Programs →

Executive Office of Technology Services and Security (TSS)

Our mission is to provide technology leadership across the Commonwealth to enhance the quality of public service and foster positive community outcomes

OMST
OFFICE OF MUNICIPAL
& SCHOOL TECHNOLOGY

Cybersecurity Awareness Program – FREE and in it's seventh year

Cybersecurity awareness training will help ensure your employees know the latest techniques cyber criminals are using, how to identify phishing emails, and their role in keeping your organization safe from cyber attacks. We received over 300 applications to reserve over 100,000 licenses for 2026. Wait list requests should be emailed to OMST-cyber-training@mass.gov

Cybersecurity Health Check Program - FREE

Our **FREE** Cybersecurity Health Check service assesses how your organization is aligned to mitigate risk and identify security deficiencies by identifying technology gaps, best practices, and recommend key areas of improvement that will better protect the organization and their data from cyber threats. They assist with:

- Prioritization of identified cybersecurity gaps & building out a cybersecurity roadmap
- Recommend best practices
- Identify improvements in your IT environment
- Provide additional context related to budgetary requests

Municipal CISO Council Please email omst@mass.gov with topic & speaker suggestions

Cyber351 EOTSS/OMST hosted regionally focused Cybersecurity Event

Cybersecurity Tabletop Exercises (TTXs)

Apply for a free cybersecurity tabletop exercise (TTX) for your organization, facilitated by the Office of Municipal and School Technology (OMST).

OMST Collaborative Knowledge Base SharePoint Site

Access by invitation for municipal and school leaders responsible for IT. Myriad of information on Cybersecurity, Best Practices, Trends and OMST hosted Webinars. (previously named Muni-IT-Dir) AI Governance & Compliance Policy Templates and Webinar can be accessed here

IT Digital Accessibility

WCAG 2.1 Level A and AA is the Commonwealth's minimum technical standard for digital asset accessibility including but not limited to web and desktop applications, mobile applications, multimedia content, social media content, electronic documents and artificial intelligence integrations, as established in the *Commonwealth's* ***Enterprise Digital Accessibility Policy***. Specific to the federal rule, state organizations and larger municipalities with more than 50,000 residents have two (2) years (April 24, 2026) to comply with the federal rule. Small municipalities and government entities with a population less than 50,000 have three (3) years (April 26, 2027) to comply with the federal rule.

Community Compact Cabinet (CCC) Grant Program

IT Grant

The Community Compact IT grant program supports the implementation of projects by funding capital needs such as new (not replacement) technology infrastructure or software. Eligible costs include incidental or one-time expenses related to capital planning, design, installation, implementation, and initial training. This year, applications for Digital Accessibility will be given priority. Application opened on January 5th and closes on February 5th

Municipal Fiber Grant

The Community Compact Municipal Fiber grant program focuses on connecting municipality-owned facilities and helping communities achieve goals for protecting against cyber security exploits and increasing the ease of interacting with local government online. A cohesive municipal network also creates opportunities for economies of scale by aggregating internet bandwidth purchases and associated security infrastructure. Application opens on March 2nd and closes on April 2nd

Municipal Local Cybersecurity Grant Program

This funding was established to assist local government with improving cybersecurity by reducing susceptibility to cybersecurity threats, reducing cybersecurity vulnerabilities, and mitigating the consequences of cybersecurity attacks by enhancing specific cybersecurity capabilities. The 2024 program applications were due March 8th, Award Notifications May 2024, with a Performance Period of May 2024 - June 30, 2025.

Priority areas included:

- Development of a written cybersecurity incident response plan.
- Tabletop exercises (TTX) involving cross-functional staff members, including senior leadership of the applicant to exercise, test, and refine written cyber incident response plans.
- Cybersecurity awareness training –with a .gov domain or a network email domain owned and managed by a state unit of government are eligible to apply under this objective.
- Migration to the .gov internet domain.
- Implementation of multi-factor authentication (MFA).

FUTURE PROGRAM FUNDING TBD

OMST

OFFICE OF MUNICIPAL
& SCHOOL TECHNOLOGY

Please contact omst@mass.gov with any questions

Executive Office of Technology Services and Security (TSS)

Our mission is to provide technology leadership across the Commonwealth to enhance the quality of public service and foster positive community outcomes

Municipal Cybersecurity: Safeguarding Communities Online

Wrap Up and Thank You

For more information or to download a copy of the game, go to ***MassCyberCenter.org.***

MassCyberCenter
at the MassTech Collaborative