MassCyberCenter
at the MassTech Collaborative

Strengthening Your Municipal Cybersecurity Program and Incident Response Planning

MMA Annual Meeting
January 20, 2023

Agenda

- Introductions
- Status of Municipal Cybersecurity in Massachusetts (MIT)
- Cybersecurity Incident Response – An Insurance Perspective (Mullen Coughlin)
- Commonwealth Resources
- Developing a Cyber Incident Response Plan
- Reporting to Law Enforcement (MA State Police | Commonwealth Fusion Center)
- Tabletop Exercise
- Incident Response Plan Checklist
- Cybersecurity Considerations for Leaders

Municipalities are attractive targets

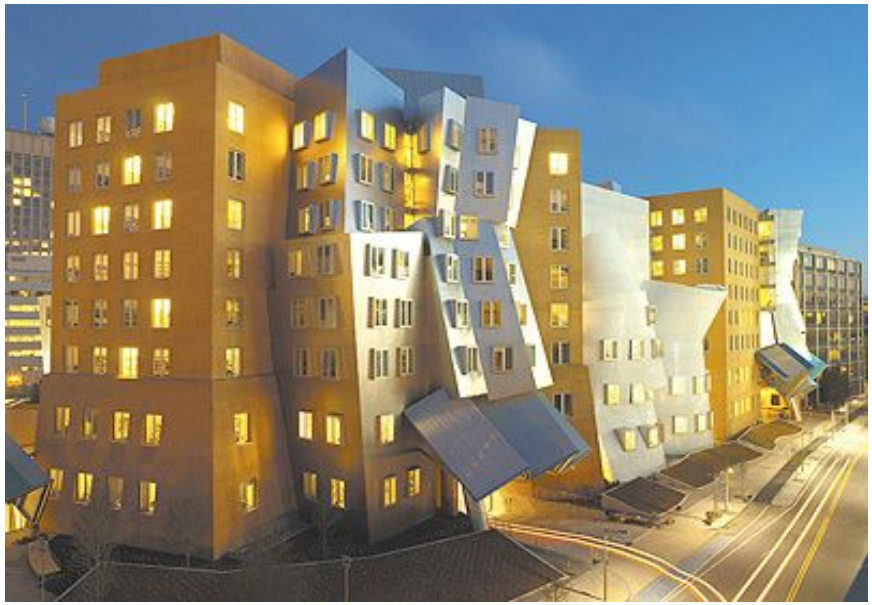
What makes local governments attractive targets for cyber attacks?

- They house private data
- Security often isn't a top (or well-funded) priority
- Attacks have been successful
- Attacks against local governments are public-facing, providing a potent outlet and often resulting in a variety of disruptive, public consequences

Cyber Threats to Municipalities

- Unintended disclosures by employees
- Hacking/Malware/Ransomware
- Insider Wrong-Doing
- Zero Day Vulnerabilities
- Physical Loss
- Portable Device/ Removable Media
- Technology Intrusions
- Phishing/Spear-Phishing Schemes
- Man-in-the-Middle Attacks
- Wire Transfer Fraud
- Skimming Incidents
- Vendors/Subcontractors – Poor Security
- Protocols/Standards

MassCyberCenter
at the MassTech Collaborative



Status of Municipal Cybersecurity in Massachusetts

MIIA Secure Cyber Survey

Spring 2022 Results

Taylor Reynolds
treyn@mit.edu
Jan 20, 2023

Internet Policy Research Initiative

Background

- **84** participating municipalities
- Secure self survey of defense maturity and losses
  - 22 controls in 10 categories
  - Controls from White House Exec Order and Memo
- Status as of June 2022

SCRAM
Secure Cyber Risk Aggregation and Measurement

Bank of America: No budget constraint for cyber

Bank of America Corp. CEO Brian Moynihan said [...] it was the first time in 20 years of corporate budgeting he had overseen a business unit [cybersecurity] with no budget. Moynihan said the only place in the company that didn't have a budget constraint was cybersecurity.

2021: BoA spent more than $1 billion on cyber defense

https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#77f9c4be264c
https://www.cnbc.com/2021/06/14/bank-of-america-spends-over-1-billion-per-year-on-cybersecurity.html

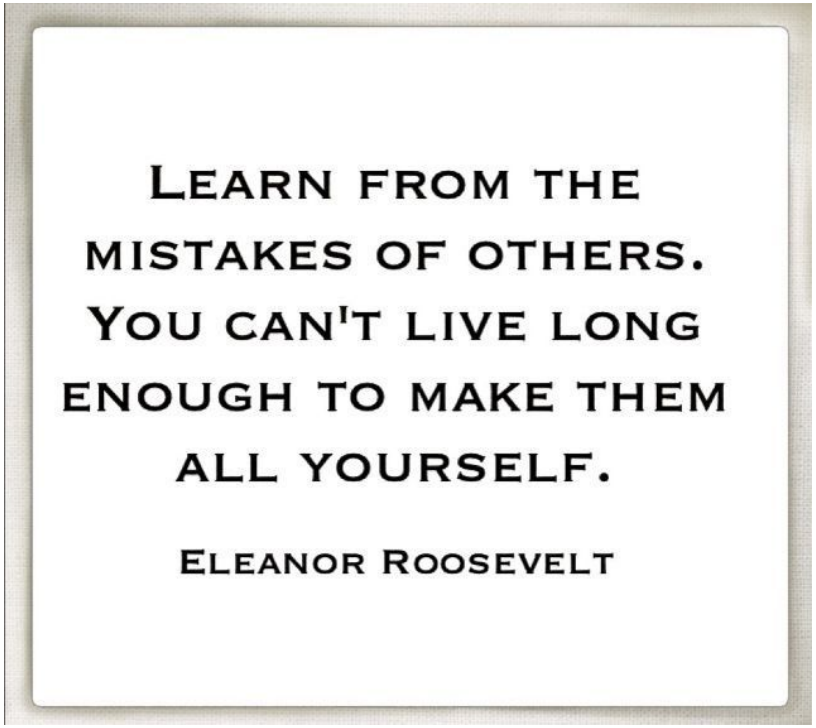
SCRAM
Secure Cyber Risk Aggregation and Measurement

Why firms hesitate to share data

- Risk of regulatory scrutiny or fines
- Reputational harm
- Legal liability
- Gives their competitors an advantage

SCRAM
Secure Cyber Risk Aggregation and Measurement

Result: Attacks happen, but we don’t learn much

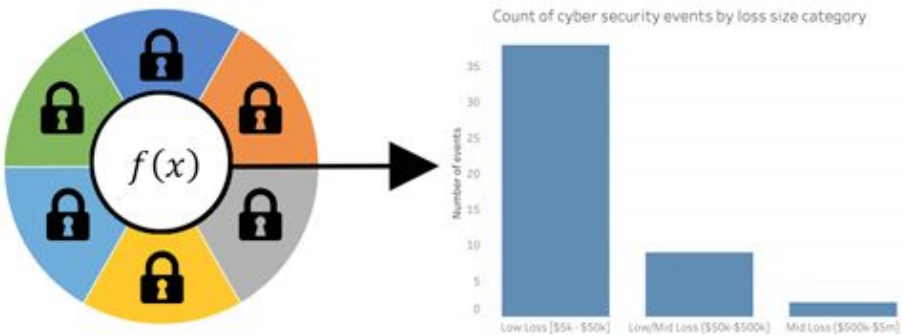


SCRAM
Secure Cyber Risk Aggregation and Measurement

Our solution: SCRAM

Using our new cryptographic platform (multi-party computation), firms can securely and privately contribute sensitive data for calculating aggregate frequency and loss data without disclosure to anyone - including MIT!

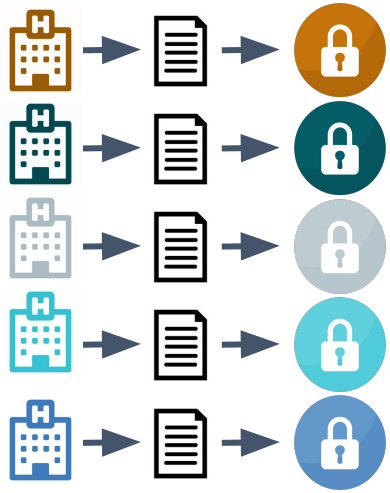
Homomorphic encryption → Elegant way of computing on encrypted data



scram.mit.edu

Step 1: Lock the data

Organizations



Step 2: Aggregate the data

Multi-party computation

Step 3: Unlock the result

Multi-party decryption

Unlock only the encrypted result

SCRAM

Secure Cyber Risk Aggregation and Measurement

SCRAM

MIT Internet Policy Research Initiative

Ready	
100	Checksum

Step 1: Population estimate

		Input number	Status
Population	0a. The population of your municipality (rough estimates okay)	12,987	OK

Step 2: Maturity levels

Category	Control	Mark with an "x"				Status
		Not Implemented	Partially Implemented	Largely Implemented	Fully Implemented	
1. MFA	1a. Deploy multi-factor authentication across the enterprise	1				OK
2. EDR	2a. Deploy an endpoint detection and response (EDR) system / host-based IPS agent	1				OK
	2b. Hunt for malicious activity		1			OK
3. Encryption	3a. Encrypt data in transit		1			OK
	3b. Encrypt data at rest			1		OK
4. Empowerment	4a. Remove barriers to sharing threat intelligence		1			OK
	4b. Receive external threat intelligence				1	OK
5. Training	5a. Evaluate employee skills		1			OK
	5b. Deliver regular training		1			OK
6. Backup	6a. Perform regular backups of systems		1			OK
	6b. Test backup data			1		OK
	6c. Protect backups		1			OK
	6d. Store backups in offline location			1		OK
7. Patch	7a. Deploy updates and patches in a timely manner		1			OK
	7b. Implement a centralized patch management system			1		OK
	7c. Apply patches using a risk-based approach	1				OK
8. Incident response	8a. Codify an incident response plan	1				OK
	8b. Test your incident response plan		1			OK
	8c. Maintain your incident response plan	1				OK
9. Check the work	9a. Establish an external penetration testing program			1		OK
	9b. Perform red team exercises			1		OK
10. Segment	10a. Adopt network segmentation to ensure isolation of critical systems in an attack				1	OK

Step 4: Identifying failures

	Mark with an "x"	Status
	Select **up to 5 controls** that failed during incidents that incurred the greatest financial losses. This includes either a control failure, or a lack of a control that could have prevented the loss.	
1a	1	OK
2a	1	OK
2b		OK
3a		OK
3b		OK
4a		OK
4b		OK
5a	1	OK
5b		OK
6a		OK
6b		OK
6c		OK
6d	1	OK
7a		OK
7b		OK
7c		OK
8a		OK
8b		OK
8c		OK
9a		OK
9b		OK
10a	1	OK

or

Note: If there were no incidents in 2019, 2020, of 2021 with losses over $1,000, then stop here. Otherwise, continue to Step 3 (below) and Step 4 (to the right)

Step 3: Incidents and losses

		Input number	Status
Incidents	11a. Number of significant incidents over three years (sum of 2019, 2020, 2021) (see note*):	4	OK
Cyber loss estimate (all incidents)	11b. Total cyber losses for all incidents combined over 3 years, US$, (sum of 2019, 2020, 2021):	$6,000	OK

Maturity scale

Not implemented	Partially implemented	Largely implemented	Fully implemented
0%	**34%**	**67%**	**100%**

SCRAM
Secure Cyber Risk Aggregation and Measurement

Summary

Defense maturity (self rated)

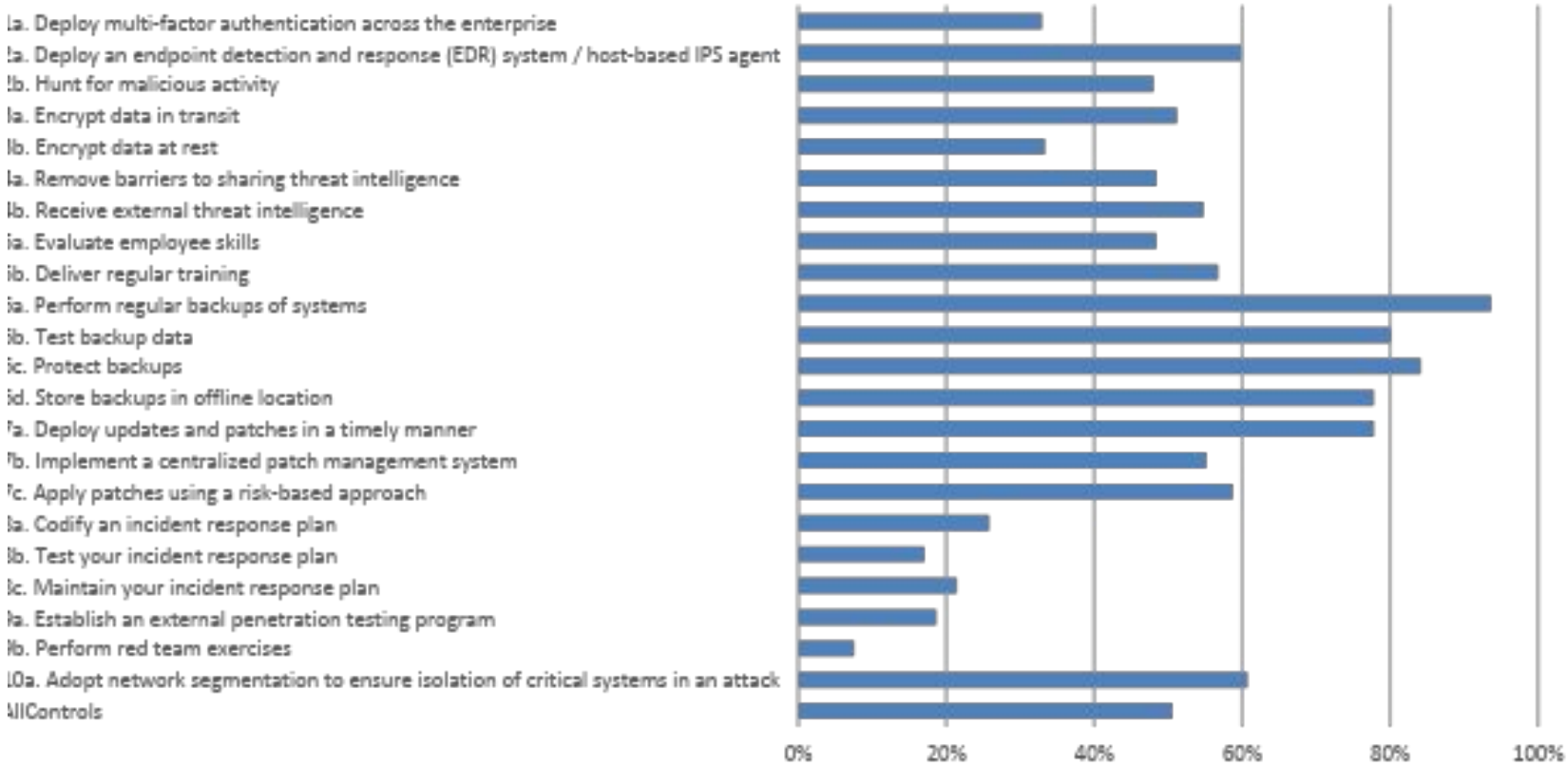
- **Overall maturity** of **51%** across all controls
- Most mature areas: **Backups** (84%), **Patching** (64%), **Segmentation** (61%)
- Least mature areas: **Check the work** (13%), **Incident response** (21%)
- Strongest control: **Perform regular backups of systems** (94%)
- Weakest control: **Red team exercises** (8%)

Losses

- **4** Incidents caused by **14** control failures
- Led to **$628,000** in total losses
- Largest losses from failures of
  - Deliver regular training: $131,000 losses from 3 attributions
  - Evaluate employee skills: $116,000 losses from 2 attributions

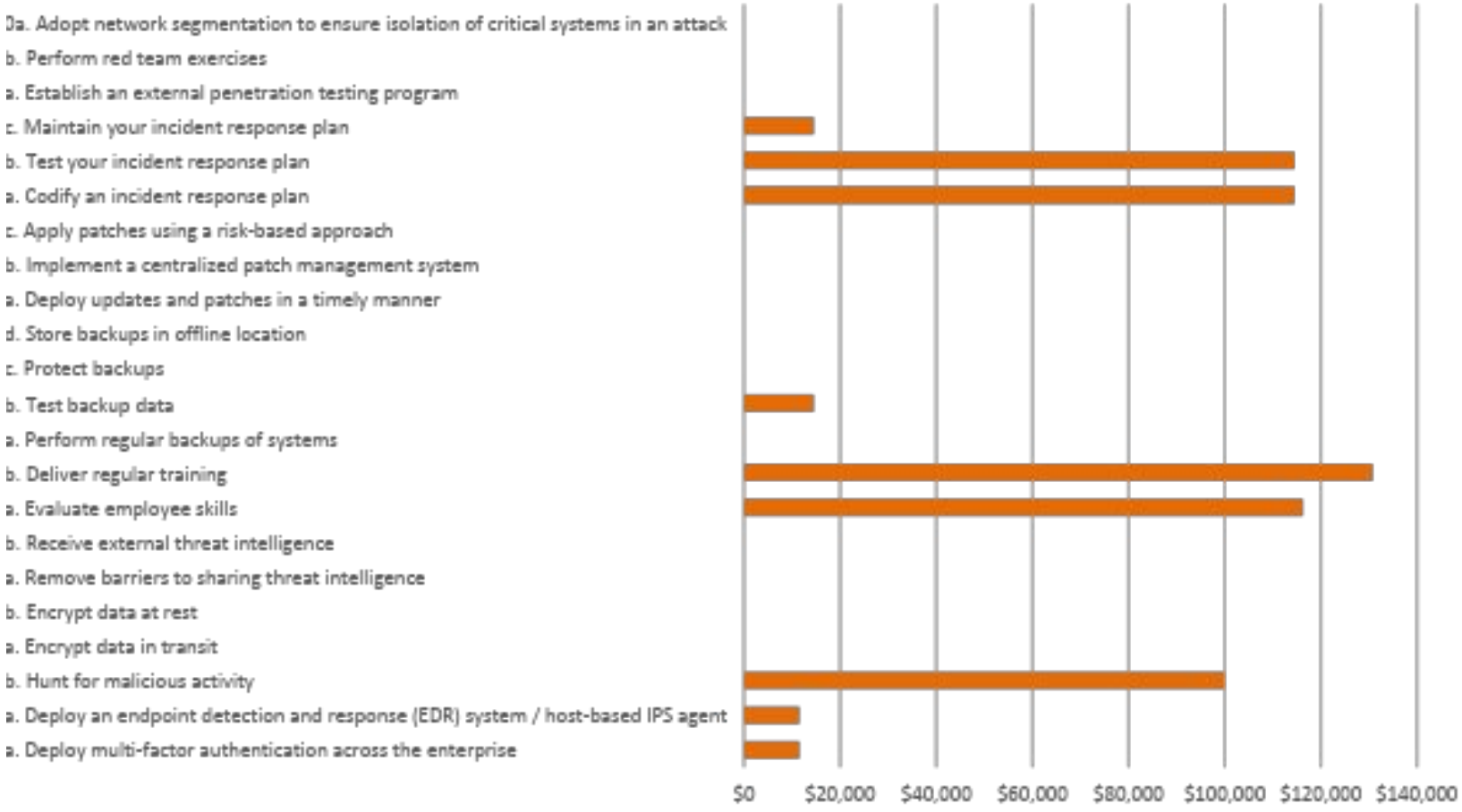
SCRAM
Secure Cyber Risk Aggregation and Measurement

Security control maturity, by control, average of municipalities



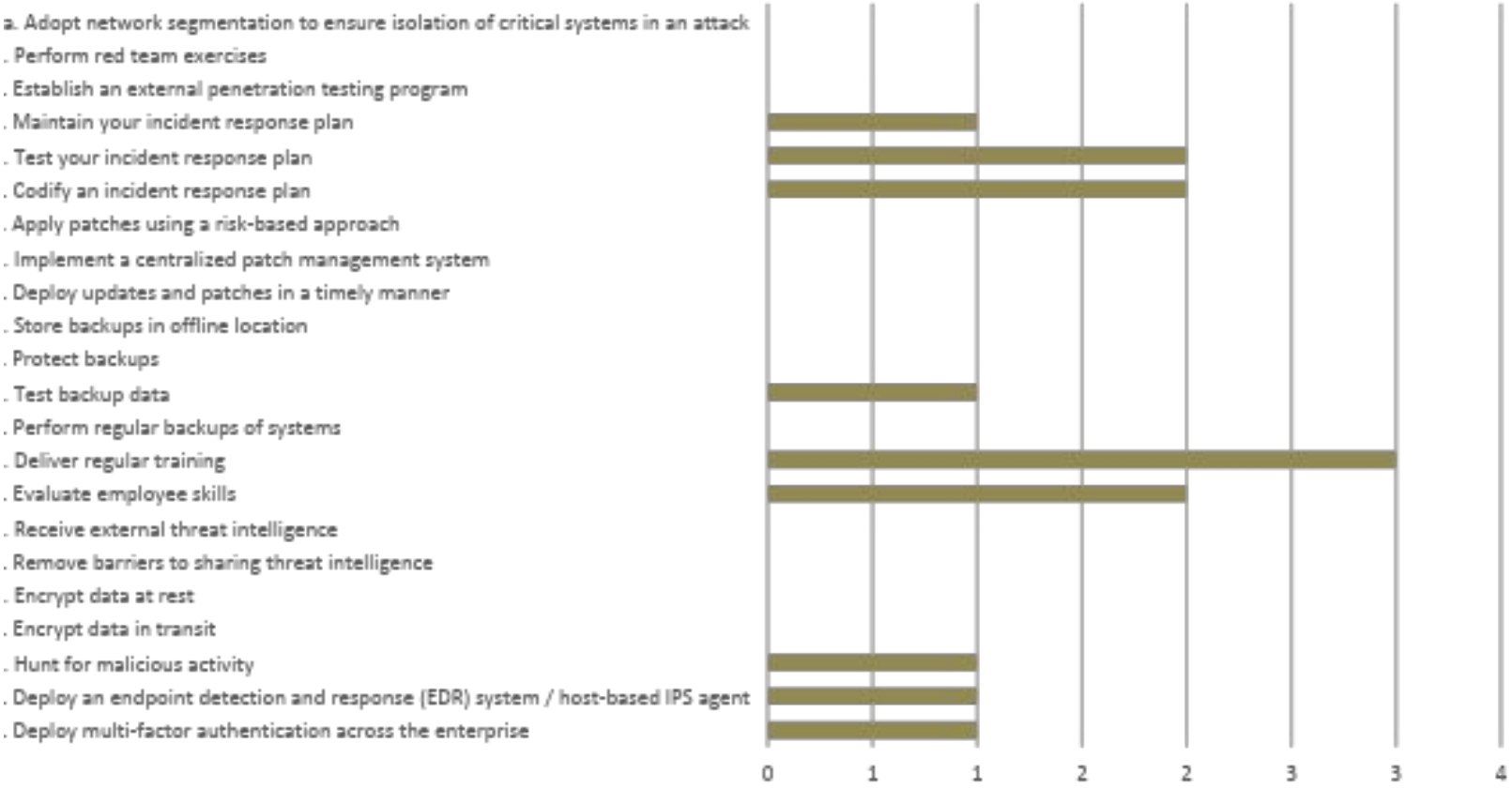
SCRAM
Secure Cyber Risk Aggregation and Measurement

Losses from failures, by control, total, USD



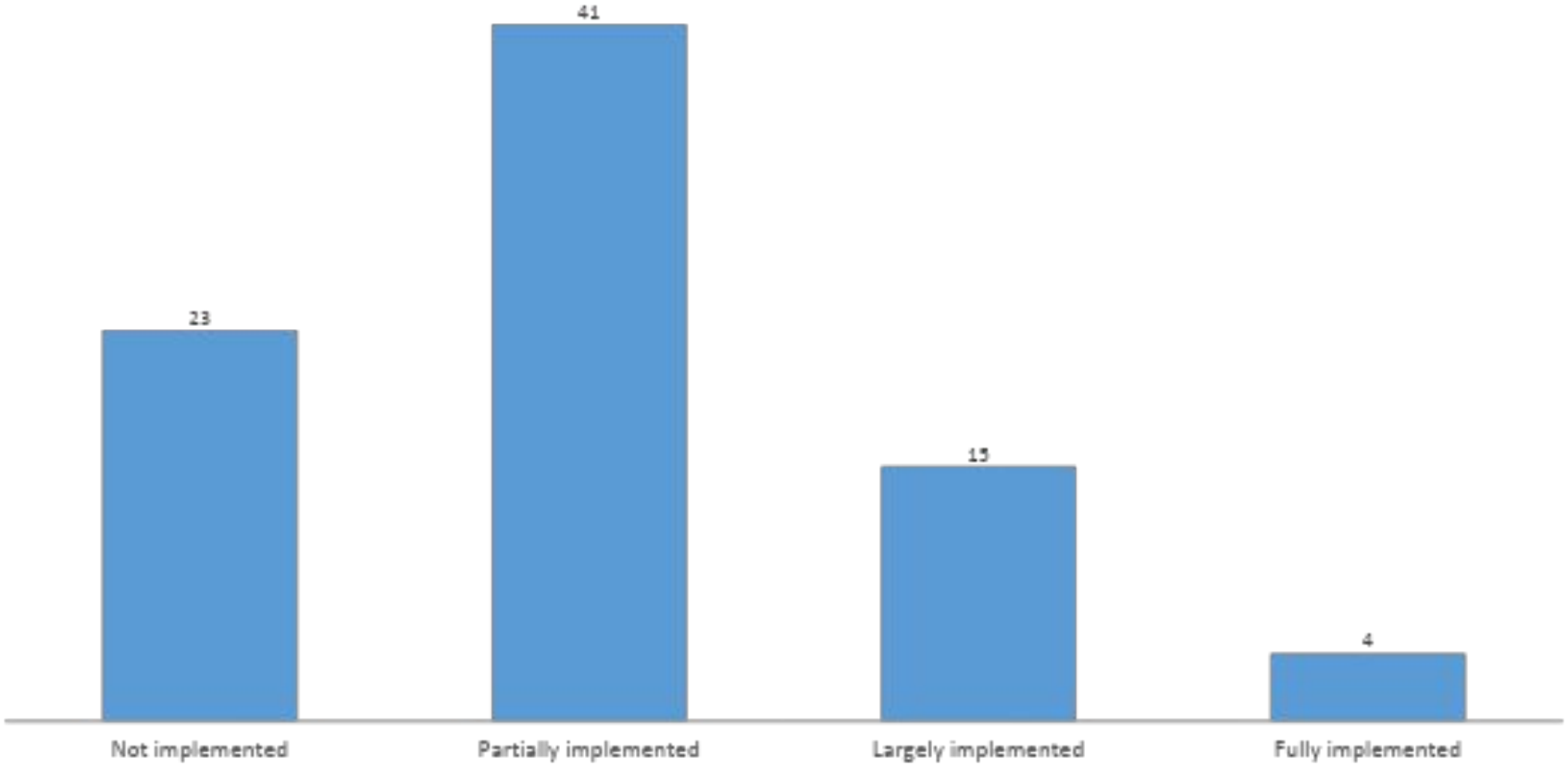
SCRAM
Secure Cyber Risk Aggregation and Measurement

Frequency of control failure, by control, total



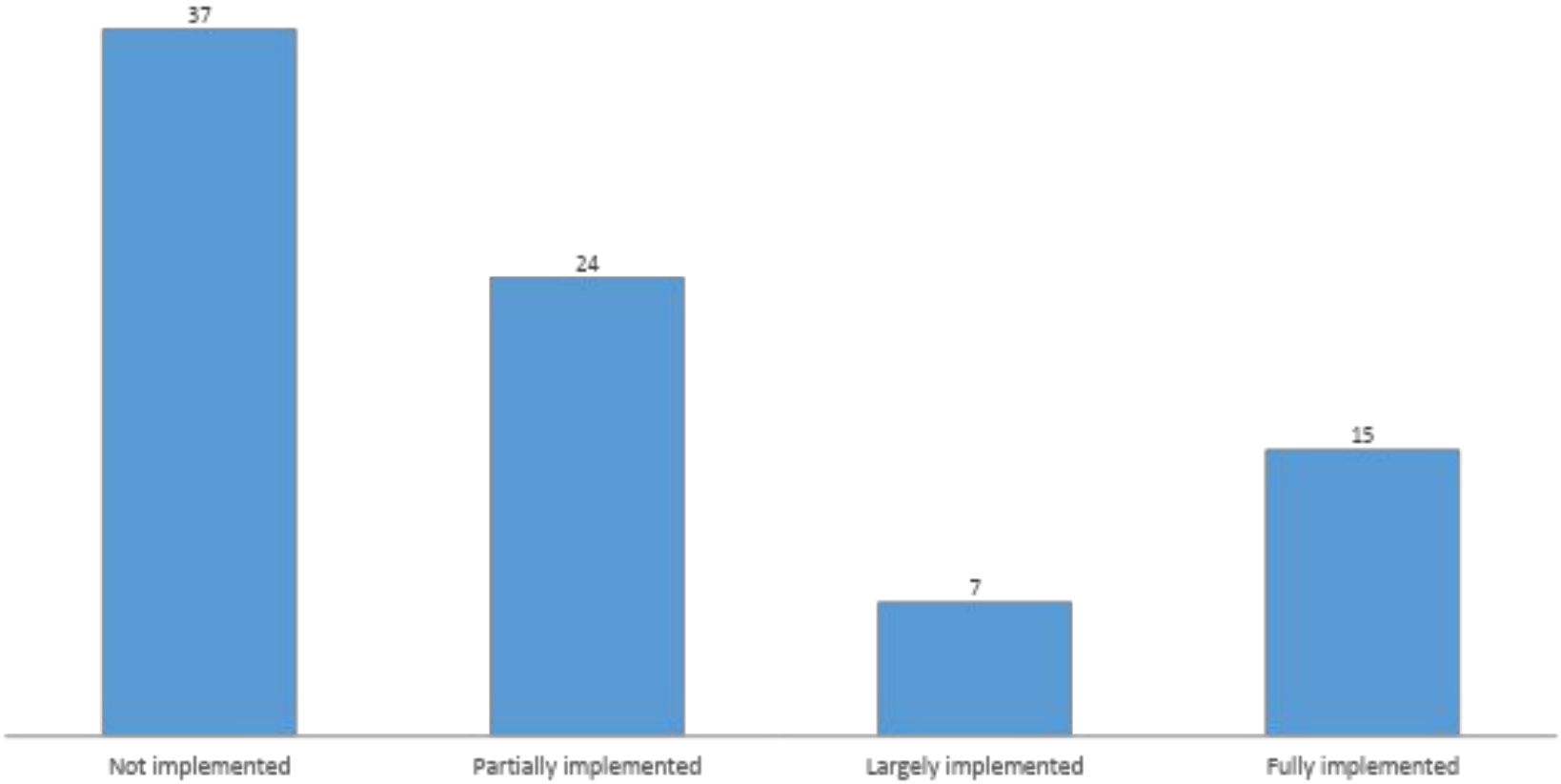
SCRAM
Secure Cyber Risk Aggregation and Measurement

1a. Deploy multi-factor authentication across the enterprise



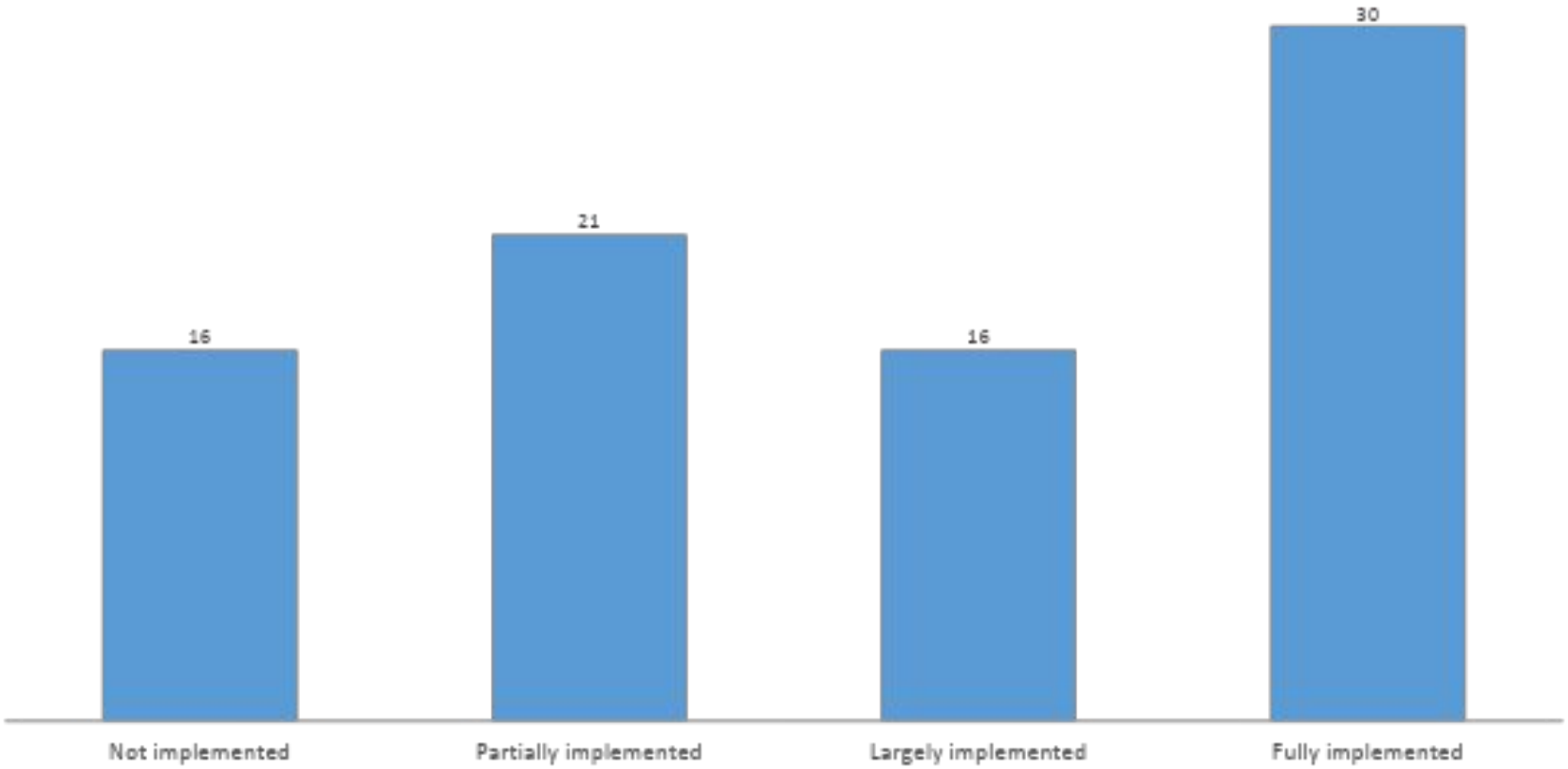
SCRAM
Secure Cyber Risk Aggregation and Measurement

3b. Encrypt data at rest



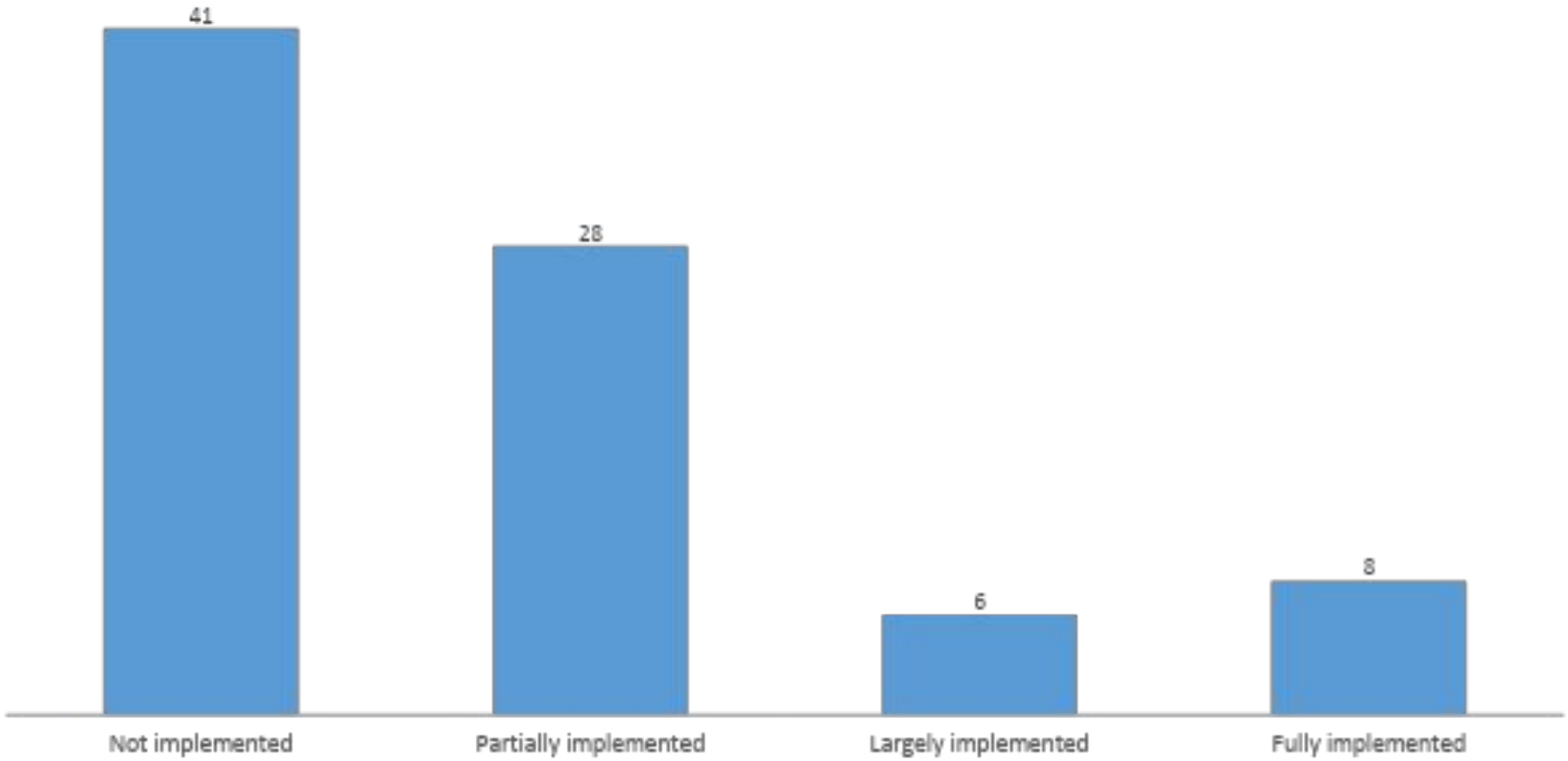
SCRAM
Secure Cyber Risk Aggregation and Measurement

5b. Deliver regular training



SCRAM
Secure Cyber Risk Aggregation and Measurement

8a. Codify an incident response plan



SCRAM
Secure Cyber Risk Aggregation and Measurement

Cybersecurity Incident Response – An Insurance Perspective

- Incident response statistics
- Updates for next year's policies are informed by previous incidents
- Common mistakes
- Best practices

MULLEN COUGHLIN LLC

Cybersecurity Incident Response – An Insurance Perspective

Gregory Bautista, Partner – Mullen Coughlin

MMA Annual Meeting

January 20, 2023

Brief Cybersecurity Overview

Common cybersecurity threats and attacks:

- Ransomware
- Data theft (exfiltration)
  - Confidential information
  - Personal information
  - Intellectual property
- Malicious software (malware)
  - Viruses
  - Worms
  - Trojans
  - Bots
  - Spyware and keystroke loggers
  - Adware
  - Cryptominers
- Phishing
  - Social engineering
- Denial-of-service and distributed denial-of-service (DDoS) attacks
- Insider threats
  - Systems misuse
  - Fraud

Why cyber incidents happen:

- Attackers dupe people with phishing and other social engineering attacks
- Unpatched vulnerabilities
- Unsecure software or hardware configurations
- Outdated anti-malware controls
- Weak network controls
- Unsecure vendor environments or supply chain compromises
- Lack of monitoring

Cyber Incident Statistics Government

Incident Type

2019

Incident Type	Count
Other/Unknown	46 (29%)
Ransomware	44 (28%)
Business Email Compromise (BEC) – Total	34 (21%)
BEC – Other	26
BEC – Wire Fraud	8
Network Intrusion	16 (10%)
Inadvertent Disclosure	14 (9%)
Third-Party Breach	6 (3%)
Total	**160 (100%)**

2020

Incident Type	Count
Ransomware	76 (38%)
Other/Unknown	50 (25%)
Business Email Compromise (BEC) – Total	28 (15%)
BEC – Other	23
BEC – Wire Fraud	5
Network Intrusion	20 (10%)
Third-Party Breach	13 (6%)
Inadvertent Disclosure	13 (6%)
Total	**200 (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/Unknown	11 (5%)
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%)
Third-Party Breach	15 (12%)
Other/Unknown	7 (6%)
Total	**122 (100%)**

Ransomware-Specific

2019	
Number of RW Incidents	44 (28%)
Number of RW Incidents Paid	12 (27%)
Ransom Payment Reason	Delete Only – 0 (0%) Key and Delete – 0 (0%) Key Only – 12 (100%)
Average Ransom Demand	$661,176
Average Ransom Payment	$213,329
Median Ransom Payment	$82,443

2020	
Number of RW Incidents	76 (38%)
Number of RW Incidents Paid	15 (20%)
Ransom Payment Reason	Delete Only – 0 (0%) Key and Delete – 2 (13%) Key Only – 13 (87%)
Average Ransom Demand	$473,090
Average Ransom Payment	$221,387
Median Ransom Payment	$125,000

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

Business Email Compromise-Specific

2019	
Number of BEC Incidents	34 (21%)
Number of BEC-WF Incidents	8 (24%)
Average Amount Fraudulently Wired	$369,095
Median Amount Fraudulently Wired	$146,500

2020	
Number of BEC Incidents	28 (14%)
Number of BEC-WF Incidents	5 (28%)
Average Amount Fraudulently Wired	$356,735
Median Amount Fraudulently Wired	$103,470

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

Anatomy of a Breach Response

BREACH DISCOVERY

EXPERTS

- Breach coach
- Forensics
- Public relations

INVESTIGATION - internal/forensic/criminal

- How did it happen?
- When did it happen?
- Is it still happening?
- Who did it happen to?
- What was accessed/acquired? (What wasn't?)

NOTICE OBLIGATIONS

- State
- Federal
- Other (i.e., PCI, Contract)
- Deadlines – Can be 48/72 hours

NOTIFICATION

PROCESS

- Written
- Electronic
- Substitute
- To Media

VENDORS

- Printing, Mailing and Call Center
- Credit Monitoring

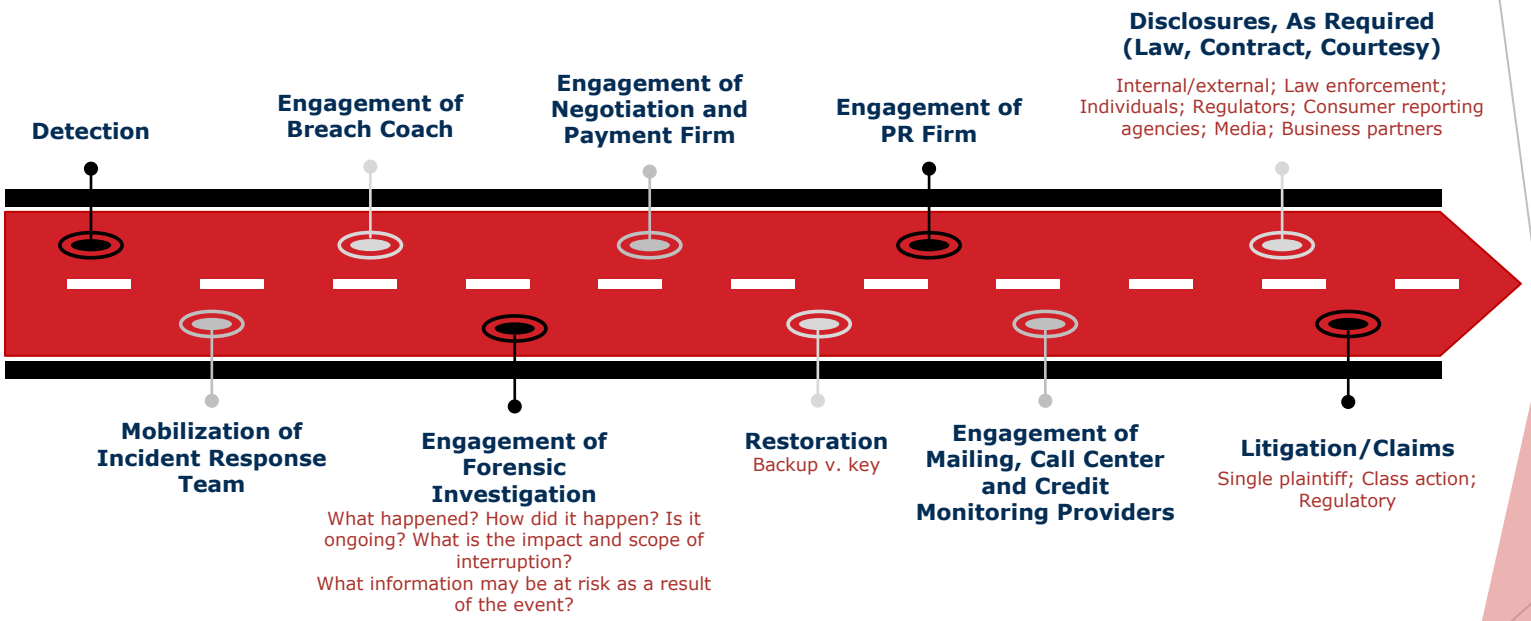
INQUIRIES

- State Regulators (i.e., AG, PD)
- Federal Regulators (i.e., OCR)
- Federal Agencies (i.e., SEC, FTC)
- State Insurance Commissioners
- Consumer reporting agencies
- Potential Plaintiffs

LITIGATION

- Government Entities
- Class Action
- Indemnification

The (Potential) Roadmap



Understand the Incident Response Process– Before You Have an Event

- Understand your policy
  - What is the process? How to alert necessary parties?
- Understand customer contracts and legal duties
  - What are your immediate deadlines?
  - Where are contracts and licenses stored?
- Get vendors lined up
  - Meet your forensic, PR, and notice options
    - Understand their role and information they may need

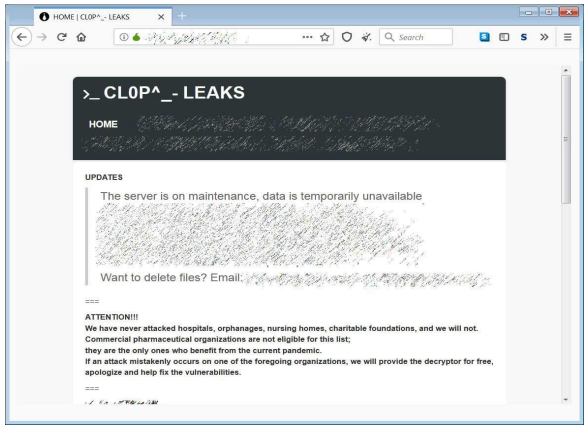
Best Practices Post Incident

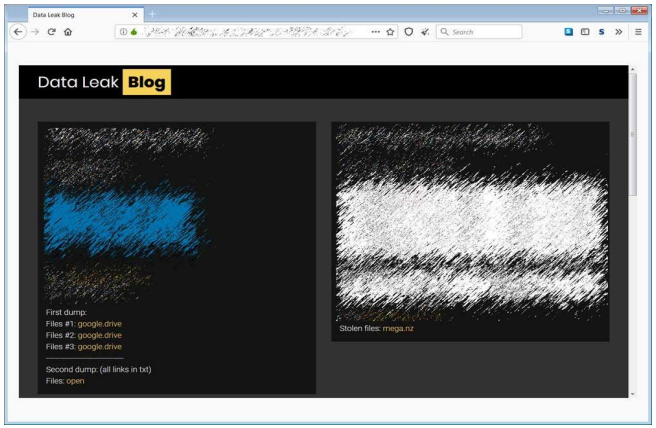
- Do **not rush** to go public
  - Tremendous desire to go public fast, but an inability to answer questions that will inevitably follow can be devastating
  - **If your notice goes out 4 hours after discovery, there will be people who charge you with delay, so "delay" is unavoidable**
- **Prepare for litigation** and regulatory investigation — Preserve all relevant documents
- Conduct **risk assessment** and implement **data security improvements** prior to being asked by a regulator
- Do not use terms "Breach" or "PII" lightly — these are statutorily defined legal terms the use and admission of which have consequences

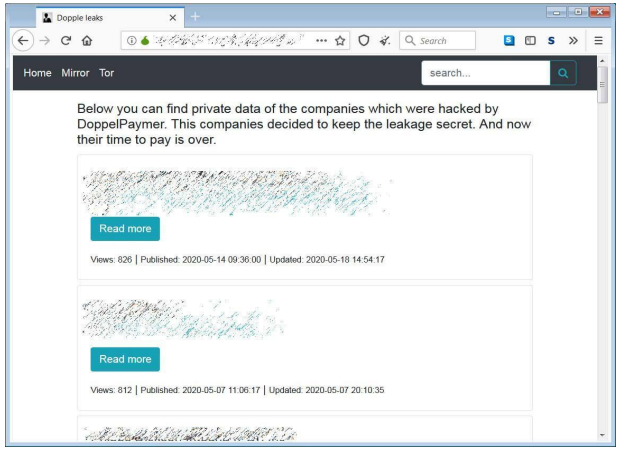
Ransomware Procedure Summary

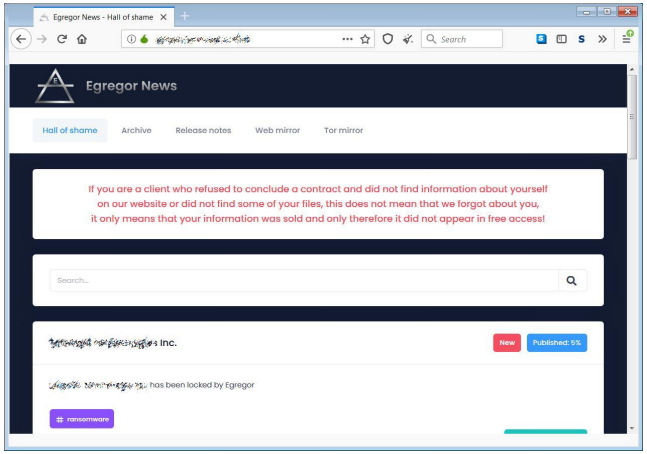
- Notify cyber insurance carrier
- Engage counsel immediately
- Engage forensics immediately (through counsel)
  - Parallel track of getting organization operational in a secure and timely fashion, and conducting forensic investigation into nature and scope of event
- Contact law enforcement/ File IC3 report with FBI
- Determine legal notice obligations based on findings of forensic investigation
  - Prepare compliant notice deliverables to individuals, regulatory agencies, media, etc., as needed

Ransomware Leak Sites







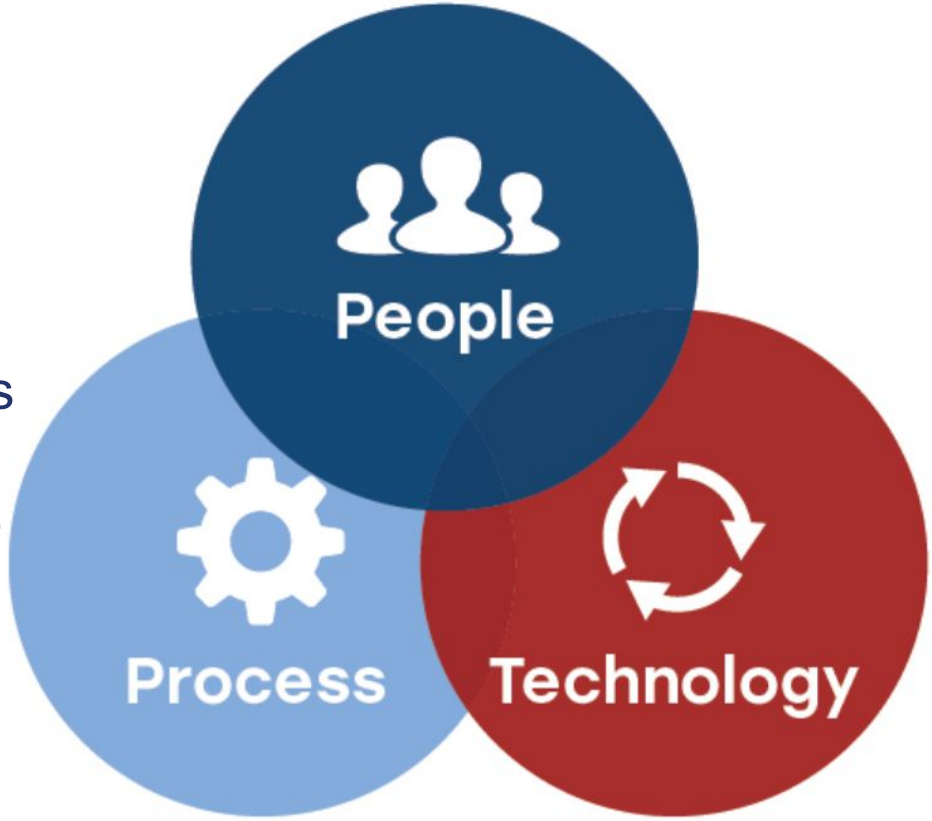


Thank you.

Gregory J. Bautista
Partner
Mullen Coughlin LLC
gbautista@mullen.law
(267) 930-1509 - Office
(516) 356-8853 - Mobile
www.mullen.law

What is cybersecurity?

- Leadership Talent/employment
- Training/education
- Citizens



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

- Sensors
- Decision aids
- Defense tools

MassCyberCenter
at the MassTech Collaborative

Commonwealth Resources for Municipalities

EOTSS

Office of Municipal and School Technology (OMST)

Municipal Cybersecurity Awareness Grant Program

Cyber Health Checks

MassCyberCenter at the MassTech Collaborative

MassCyberCenter

Minimum Baseline of Cybersecurity

Cyber Incident Response Planning Materials

Community Compact Cabinet

Community Compact Program

Best Practices Program

IT Grant Program

EOPSS

Office of Grants & Research (OGR)

Homeland Security Grant Program (HSGP)

CFC

Massachusetts State Police – Commonwealth Fusion Center

Massachusetts Cybersecurity Program (MCP)

OSD OPERATIONAL SERVICES DIVISION

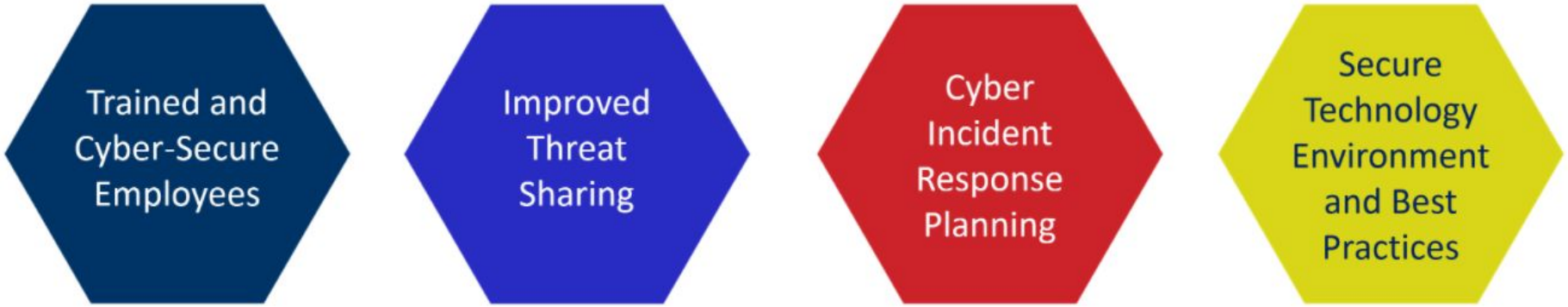
Operational Services Division (OSD)

ITS78: Statewide Contract for Cybersecurity and Incident Response Services

Minimum Baseline of Cybersecurity for Municipalities

A framework for helping Massachusetts municipalities improve their cybersecurity posture and protect their municipality from cyberattacks using people, process, and technology.

There are 4 goals:



MassCyberCenter at the MassTech Collaborative

Cyber Incident Response Plan:

What is it and why do we need one?

Preparation:
Developing the Incident Response Plan ("the Plan")

- The **Plan** is designed to provide a well-defined, organized approach for handling any potential security breaches, or threats to a Municipality's data, systems, and infrastructure.

- The **Plan** defines what constitutes a security incident, identifies the areas of responsibility, establishes a process for documenting the incident and includes assessment procedures.

Preparation:
Who needs to be part of the Planning Team?

Preparation:
Who needs to be part of the Planning Team?

- **Determine who are the stakeholders:**
  - Organizational leadership
  - IT & Information Security leadership
  - Legal counsel
  - Audit
  - Finance
  - Human Resources
  - Communications
- **Determine what decisions need to be made:**
  - When does the Response Plan get activated and who decides
  - Obtain or clarify cyber liability insurance information and requirements
  - Determine vendors needed such as forensics, outside legal counsel, mitigation and communications services

Preparation:
Who needs to be part of the Cyber Incident Response Team?

Preparation:
Who needs to be part of the Cyber Incident Response Team?

Objectives:

- Conduct investigation into incident
- Coordinate response to incident
- Establish communication protocols
- Provide notice to appropriate regulatory authorities
- Coordinate with third-party service providers
- Act as liaison to law enforcement or information sharing agencies, including state and federal
- Determine notice requirements – to any affected individuals

Recommended Team Members:

- Incident Response Coordinator or Chief Privacy Officer
- Technology Coordinator or Chief Security Officer
- Communications Coordinator
- Internal Audit Coordinator
- Legal Counsel | Outside Legal Counsel
- Human Resources
- Finance
- Operations
- First Responders

Preparation:
Value of Planning

- **Create the team approach before an incident**
  - Names, contact information and responsibilities
  - Team meetings to study threats, review plans and update each other on issues
  - Understand the roles of third-party vendors before an incident
  - Establish communications pathways and trust
- **Prioritize key systems in advance**
  - “Critical” systems should be at the top of the list
  - Establish restoral priorities and authorities to modify
- **Exercise the plan to set you up for success**
  - Time for training and testing of response plan is important to promote a culture of cybersecurity preparedness
  - Visibility with your employees – walk the cybersecurity walk

Preparation:
Building the Plan

- **Compile the following information NOW:**
  - Obtain and select insurance approved vendors, as appropriate, and maintain updated contact information for:
    - Forensic vendors
    - Credit monitoring/call center/identity theft mitigation services vendors
    - Outside legal counsel
    - Cyber insurance broker and insurance company contact information to report a breach/security incident
    - Law enforcement officials, including state and federal officials
    - Applicable regulatory body - such as the Office of the Attorney General
    - Information sharing entities

Preparation:
Building the Plan – Ransomware issues

- **Be prepared to address these questions during a ransomware incident:**
  - What is happening technically and what systems are impacted? How long will the systems be down?
  - What revenue streams or business operations are impacted due to the technical attack? Characterize the impact
  - Has any data been exposed or stolen? What type?
  - What legal requirements or regulatory requirements are in play due to the impact of business operations or loss of data?
  - What does our insurance policy cover? (payment of ransom? use of pre-approved vendor for incident response? Negotiator?)
  - Is it legal to pay the ransom? Does your oversight organization have a ransomware policy?

Preparation:
Manage Communications

Build a communications plan in advance:

- Internal
- External

MassCyberCenter at the MassTech Collaborative

Reporting to Law Enforcement – When?

- A cyber incident is an event that could risk the confidentiality, integrity, or the availability of information systems. Cyber-incidents could lead to a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Victims are encouraged to report cyber incidents that may:
- Indicate unauthorized access to, or malicious software present on system and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, economic security, public health or safety, or any combination of those matters.
- Result in a significant loss of data, system availability, or control of systems.
- Impact a large number of victims.
- There are no minimum monetary loss thresholds for reporting.

Reporting to Law Enforcement – How?

- Report the incident to your local police department of jurisdiction in accordance with your organization's existing notification policies, and request they notify the Commonwealth Fusion Center by telephone or email. It is important to establish a working relationship and protocols with these law enforcement points of contact and incorporate them into your incident response plan well in advance of a crisis.
- If you do not have an existing notification process that includes your local police department, you may contact the Commonwealth Fusion Center directly via telephone at **508-820-2233**.
- Once notified, someone from the Commonwealth Fusion Center will contact your organization's designated point of contact.
- Report the incident to other regulatory entities and Federal Law Enforcement in accordance with your organization's policies. Reporting a Cyber Incident to Law Enforcement **does not** fulfill regulatory data breach reporting requirements.

Reporting to Law Enforcement – What to Expect?

Law Enforcement 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.

Law Enforcement 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.

Best Practices

- ❑ Determine who has responsibility for maintaining the Plan
- ❑ Make sure the Plan is distributed as appropriate, within the organization
- ❑ Review Plan at least annually
- ❑ Conduct regular staff, user and employee education and training in privacy and security
- ❑ Conduct tabletop exercises at least annually

MassCyberCenter
at the MassTech Collaborative

Cybersecurity Tabletop Exercises

An Important Part of Goal 3

Cyber Incident Response Planning

A Cybersecurity tabletop exercise (TTX) is a discussion-based event, in an informal setting, to assess response plans, policies, and procedures and understand people's roles and responsibilities when a Cyber incident or crisis occurs.

TTXs can be just a 15-minute discussion at a regular meeting, focused on one aspect of your plan; or day-long off-site events.

Make it work for your organization!

Tabletop Exercise

Cyber Incident Response Planning

Here's the scenario:

8:32 a.m. You receive a phone call from an employee who has arrived at the office and attempted to log into the city's systems. However, the employee says that the system appears "locked" and they are unable to access the network or any city data.

8:35 a.m. IT staff confirms that the system has been attacked by ransomware.

Two days later: IT staff migrates to the City's backup system and does not pay the ransom. However, the hackers provide *proof of life* that all of the city's HR data has been copied and will be published on the internet unless you pay them $500,000.

What do you do?

Incident Response Plan Checklist*

- ❑ **Preparation**
  - ❑ Determine stakeholders that need to be involved with development of the cyber incident response plan
  - ❑ Obtain or clarify cyber liability insurance information and requirements and vendors needed for response
  - ❑ Establish the cyber incident response team
  - ❑ Establish goals for the cyber incident respone team
  - ❑ Compile key contact information
- ❑ **Detection & Analysis**
  - ❑ Review Information of incident
  - ❑ Determine risk of continuing operations – review decision with legal counsel
  - ❑ Coordinate with incident response services and outside legal counsel, as appropriate
  - ❑ Implement processes to prevent alteration to system(s) until backup has been completed
  - ❑ Implement security safeguards and processes to change passwords on compromised systems
  - ❑ Maintain documentation of all actions
  - ❑ Coordinate outside counsel and third-party vendors
  - ❑ Notify insurance broker/company and coordinate responses to incident
  - ❑ Communicate with all affected parties
  - ❑ Determine if reportable breach & notify, as required

* The complete Checklist may be found at https://masscybercenter.org/Response-Plan-Materials

Incident Response Plan Checklist* (cont.)

- ❑ **Containment, Eradication & Discovery**
  - ❑ Implement processes to perform full backup of system(s) to forensically sterilize media and store backup in secure area as an important part of the chain of custody (if applicable)
  - ❑ Coordinate to determine when containment is complete
  - ❑ Implement security safeguards and processes to change passwords on compromised systems
  - ❑ Maintain documentation on all actions taken
- ❑ **Post-Incident Activity**
  - ❑ Assess damage and cost
  - ❑ Review response to determine what led to incident and whether procedures or policies need to be created or modified.
  - ❑ Update policies, procedures, plans and guidelines, as appropriate
- ❑ **Maintenance & Going Forward**
  - ❑ Determine who is responsible for maintaining the cyber incident response plan
  - ❑ Make sure plan is distributed across the municipality
  - ❑ Review and exercise the plan annually
  - ❑ Conduct regular staff, user, and employee education and training annually, and include a review of the plan

* The complete Checklist may be found at https://masscybercenter.org/Response-Plan-Materials

Cybersecurity Considerations for Leaders

- **Have a Plan**
  - Address all aspects of key operations based on risk assessments
  - Prioritize key cybersecurity operations for protection and restoration
  - Include IT, HR, operations, admin managers, finance, risk management, and legal experts in the planning process
- **Have an Incident Response Team with strong leadership**
  - Ensure the team meets before a crisis
  - Incorporate non-IT leadership in cybersecurity discussions
- **Make it a priority**
  - Time for training, planning, and testing of cybersecurity practices
  - Resources to support good IT architecture, back up management, and employee training
  - Visibility with your employees – walk the cybersecurity walk

Thank you!

For more information on Cyber Incident Response Planning and resources, go to

MassCyberCenter.org

MassCyberCenter
at the MassTech Collaborative

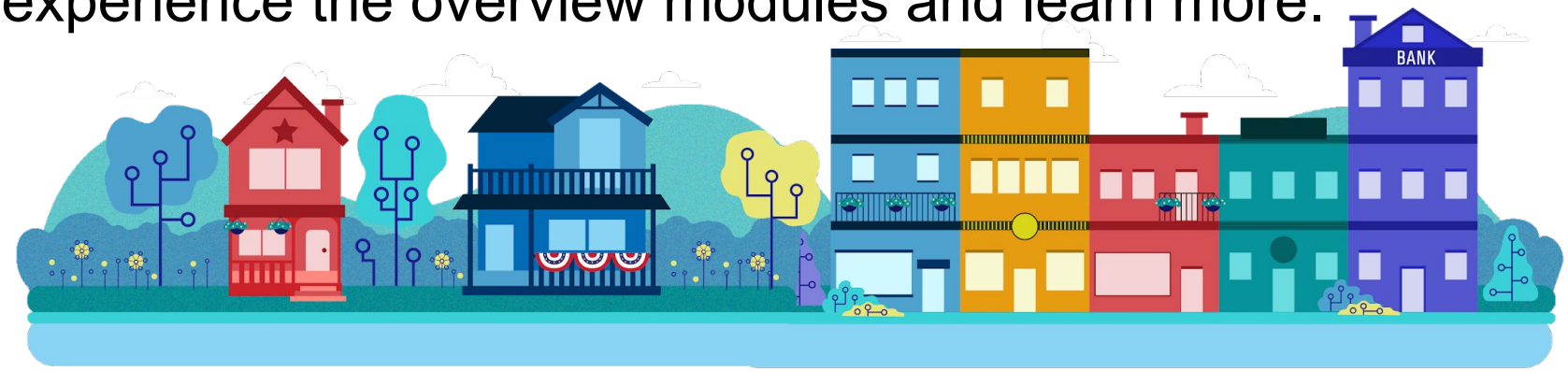
ADDENDUM SLIDES

Minimum Baseline Overview Modules

A fun way to introduce the framework and goals.

Using a notional cyberattack occurring in the fictional town of Massboro as an example to explain the Minimum Baseline of Cybersecurity, the first module introduces the Minimum Baseline, and the other four modules explain each of the four goals.

Go to MassCyberCenter.org and look under Resiliency to experience the overview modules and learn more.



MassCyberCenter
at the MassTech Collaborative

Helpful Massachusetts Websites and Links

- **Mass.gov | Cybersecurity and Enterprise Risk Management Program**
  https://www.mass.gov/orgs/cybersecurity-and-enterprise-risk-management
  Program that focuses on protecting citizen data, ensuring the availability of the Commonwealth's networks and systems, and maintaining the continuity of government operations and services.
- **Mass.gov | Report a cybersecurity incident**
  - Report to your local police department and request they notify the Commonwealth Fusion Center
  - Other resources for reporting incidents:
    https://www.mass.gov/info-details/report-a-cybersecurity-incident

Helpful Federal Websites and Links

- **Multi State Information Sharing and Analysis Center (MS-ISAC) and the Center for Internet Security**
  Alerts and Advisories sent from MS-ISAC on a regular basis about threats that may impact state, local, tribal, and territorial government, plus valuable tools, resources, and services. Membership is free for municipalities: https://www.cisecurity.org/ms-isac/
- **Cybersecurity & Infrastructure Security Agency (CISA)**
  - Resources and guildance for State, Local, Tribal, and Territorial Governments: CISA.gov
  - **CISA's Cyber Essentials**—a guide for leaders of small businesses and small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices: https://www.cisa.gov/cyber-essentials
  - **CISA STOP Ransomware:** https://www.cisa.gov/stopransomware
  - **CISA CYBERSECURITY AWARENESS PROGRAM** is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online: https://www.cisa.gov/cisa-cybersecurity-awareness-program
- **US-CERT Alerts** that you can subscribe to for up-to-date information on threats, hoaxes: https://www.us-cert.gov/ncas/tips
- **Federal Bureau of Investigation (FBI)**
  - **FBI Incident Response Policy:** https://www.fbi.gov/file-repository/incident-response-policy.pdf/view
  - **FBI Fact Sheet** – When to report cyber incidents to the federal government, what and how to report, and types of federal incident response: https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view

Additional Resources for Cybersecurity – Frameworks, Best Practices, Training

- **National Institute of Standards and Technology (NIST)**
  https://www.nist.gov/
  In particular, the **Computer Security Resource Center (CSRC)** (http://csrc.nist.gov) holds a collection of papers that describe security best practices, called NIST Special Publications. They also create security assessment tools.

- **Cybrary**
  https://cybrary.it/
  Cybrary is possibly one of the best IT Security education sites on the internet. It contains full-length college course videos for everything from basic networking up to and including training for certifications, explanations of secure coding, penetration testing and everything else security related.

Additional Resources for Cybersecurity – Blogs & Podcasts

- **Krebs on Security**
  https://krebsonsecurity.com/about/
  Brian Krebs, author of Spam Nation is also one of the better-known security bloggers in the world, having written over a thousand articles on security.
- **Security Nation Podcast**
  https://www.rapid7.com/blog/series/security-nation/security-nation-season-5/
  Security Nation is a podcast dedicated to celebrating the champions in the cybersecurity community who are advancing security in their own ways.
- **Security Now! Podcast**
  https://www.grc.com/securitynow.htm
  A weekly security-focused podcast that covers all topics from law, current events, to conference reviews and explanations of specific exploits as they are discovered in the world.
- **Robinson + Cole Blog - Data Privacy Security Insider**
  www.dataprivacyandsecurityinsider.com
  Weekly posts on cybersecurity and risk management.