MassCyberCenter
at the MassTech Collaborative

Robinson+Cole

Cybersecurity Incident Response Plan Workshops For Municipalities

Workshop 1: Developing the Incident Response Plan Template and Checklist

July 2020

Workshop 1 - Agenda

- Introductions: MassCyberCenter & Robinson + Cole
- Cyber Risks Faced by Municipalities
- Overview: Workshop 1 Developing the Incident Response Plan
- National Institute of Standards & Technology (NIST) Phases for Responding to a Cybersecurity Incident
    - Preparation, Detection & Analysis, Containment, Eradication & Discover, Post-Incident Activity
- Incident Response Plan Checklist
- Maintenance & Going Forward
- Strategies for Municipalities
- Helpful Websites & Links
- What’s Next?
    - Webinar and Workshop 2

MassCyberCenter at the MassTech Collaborative

Robinson+Cole

Current trends: What is the threat landscape?

What are the threats to a municipality's operations, infrastructure and/or data?

- Unintended disclosures by employees; Employee Error
- Hacking/Malware/Ransomware
- Insider Wrong-Doing
- Zero Day Vulnerabilities
- Physical Loss
- Portable Device/Removable Media

Current trends: What is the threat landscape?

(cont'd)

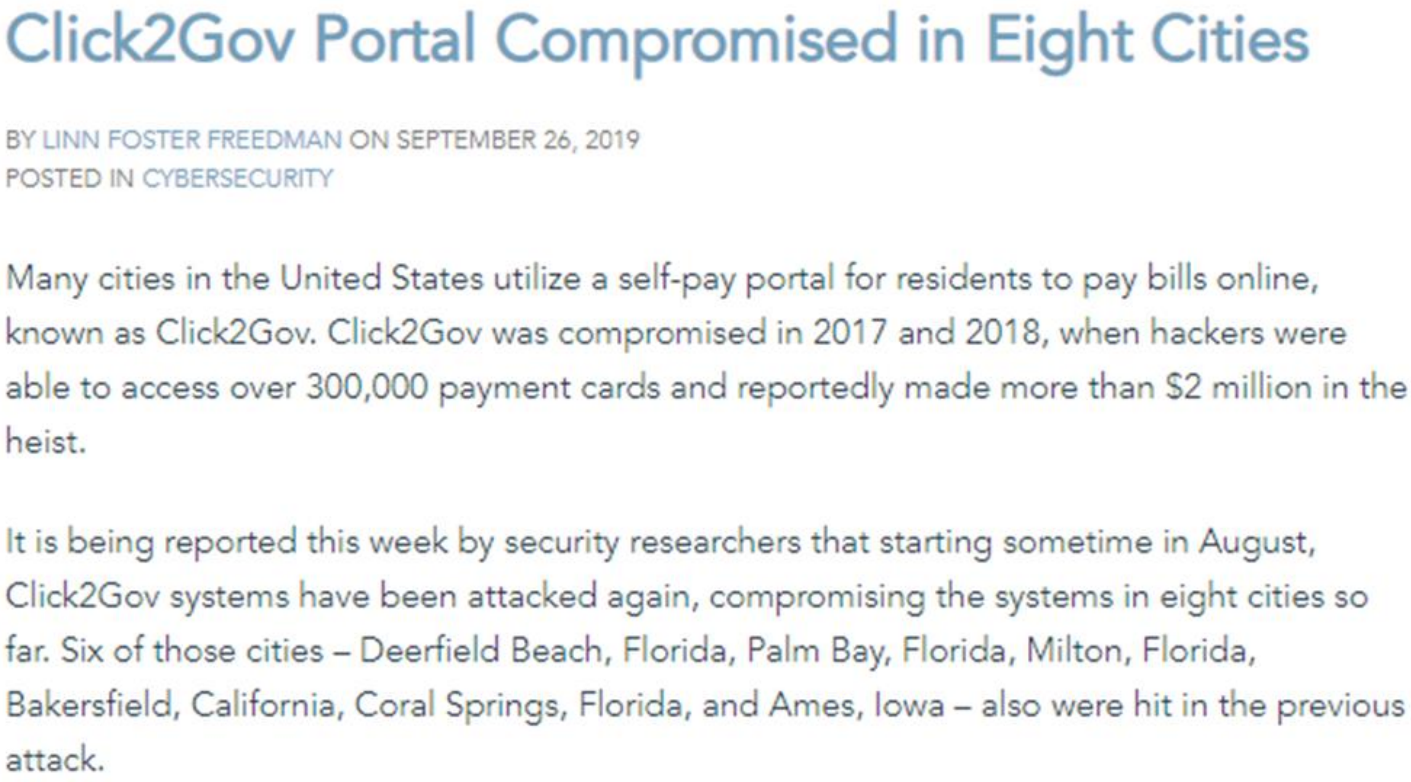
- Technology Intrusions
- Phishing/Spear-Phishing Scheme
- Man-in-the-Middle Attacks
- Wire Transfer Fraud
- Skimming Incidents
- Vendors/Subcontractors –Poor Security
- Protocols/Standards

Recent Attacks on Municipalities

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 and attacks can provide a potent outlet, resulting in a variety of disruptive, public consequences

Recent Attacks on Municipalities



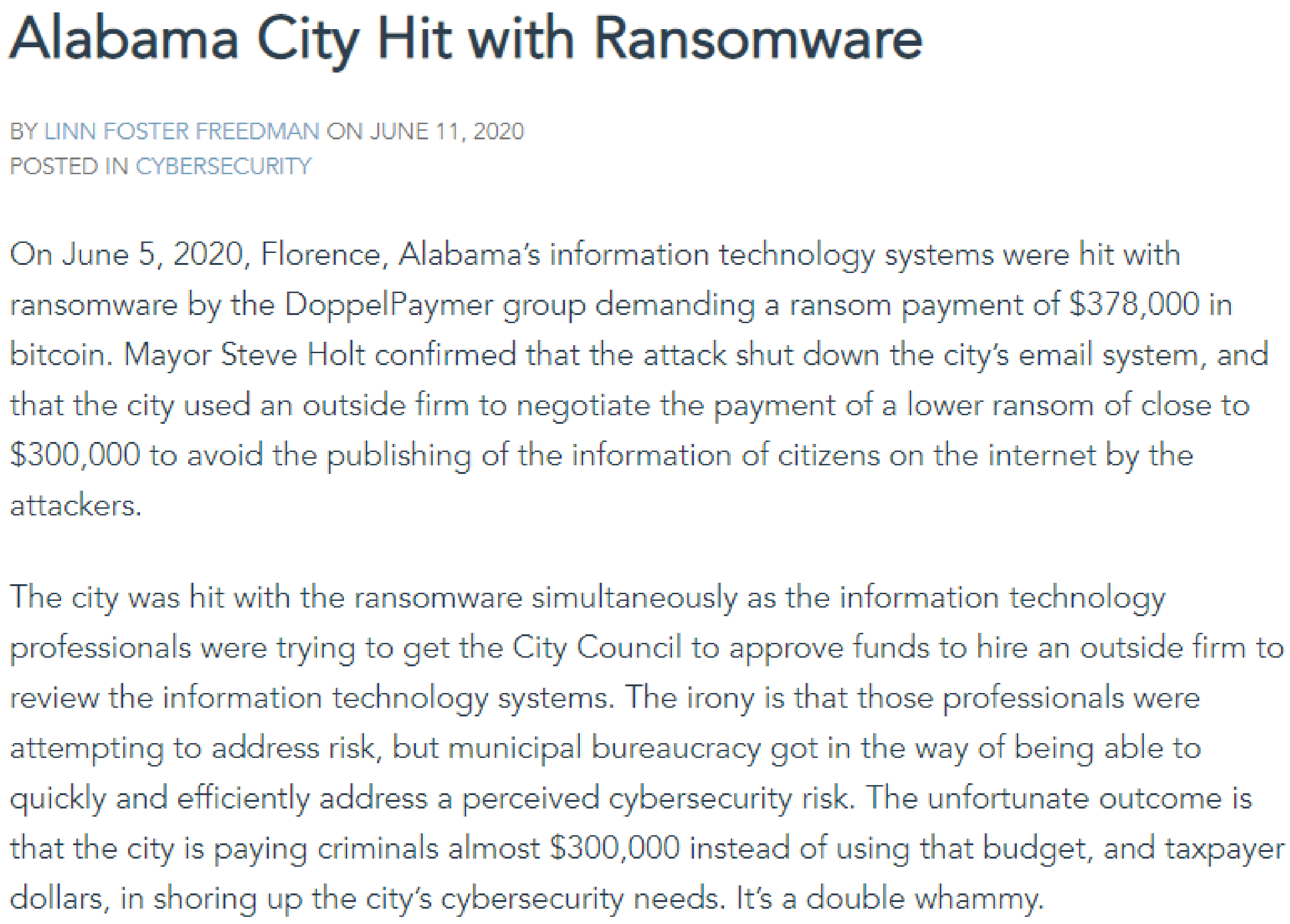
Click2Gov Portal Compromised in Eight Cities

BY LINN FOSTER FREEDMAN ON SEPTEMBER 26, 2019
POSTED IN CYBERSECURITY

Many cities in the United States utilize a self-pay portal for residents to pay bills online, known as Click2Gov. Click2Gov was compromised in 2017 and 2018, when hackers were able to access over 300,000 payment cards and reportedly made more than $2 million in the heist.

It is being reported this week by security researchers that starting sometime in August, Click2Gov systems have been attacked again, compromising the systems in eight cities so far. Six of those cities – Deerfield Beach, Florida, Palm Bay, Florida, Milton, Florida, Bakersfield, California, Coral Springs, Florida, and Ames, Iowa – also were hit in the previous attack.

Recent Attacks on Municipalities



Alabama City Hit with Ransomware

BY LINN FOSTER FREEDMAN ON JUNE 11, 2020
POSTED IN CYBERSECURITY

On June 5, 2020, Florence, Alabama's information technology systems were hit with ransomware by the DoppelPaymer group demanding a ransom payment of $378,000 in bitcoin. Mayor Steve Holt confirmed that the attack shut down the city's email system, and that the city used an outside firm to negotiate the payment of a lower ransom of close to $300,000 to avoid the publishing of the information of citizens on the internet by the attackers.

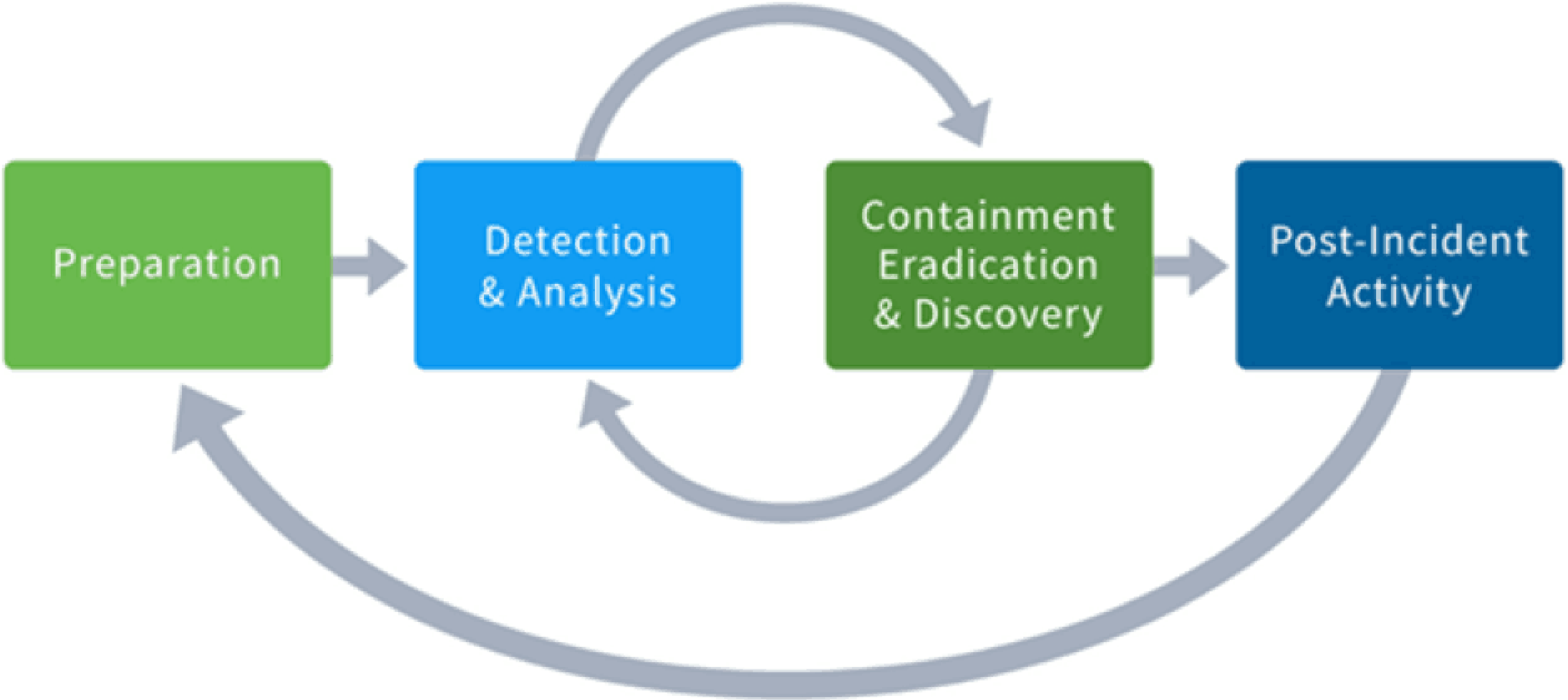
The city was hit with the ransomware simultaneously as the information technology professionals were trying to get the City Council to approve funds to hire an outside firm to review the information technology systems. The irony is that those professionals were attempting to address risk, but municipal bureaucracy got in the way of being able to quickly and efficiently address a perceived cybersecurity risk. The unfortunate outcome is that the city is paying criminals almost $300,000 instead of using that budget, and taxpayer dollars, in shoring up the city's cybersecurity needs. It's a double whammy.

Governor Baker’s Announcement

- In October 2019, Governor Baker announced a series of statewide workshops
- Provide municipalities with the tools to develop or review their cyber incident response plans and facilitate collaboration with neighboring communities.
- Through the planning process cities and towns will:
    - Prioritize the assets they need to protect,
    - Build a cybersecurity team,
    - Create processes to mitigate vulnerabilities, and
    - Raise awareness internally about the importance of cybersecurity.
- Strengthen regional collaboration around cybersecurity.

Incident Response Plan: What is it and why do we need one?

NIST: Recommended phases for responding to a cybersecurity incident



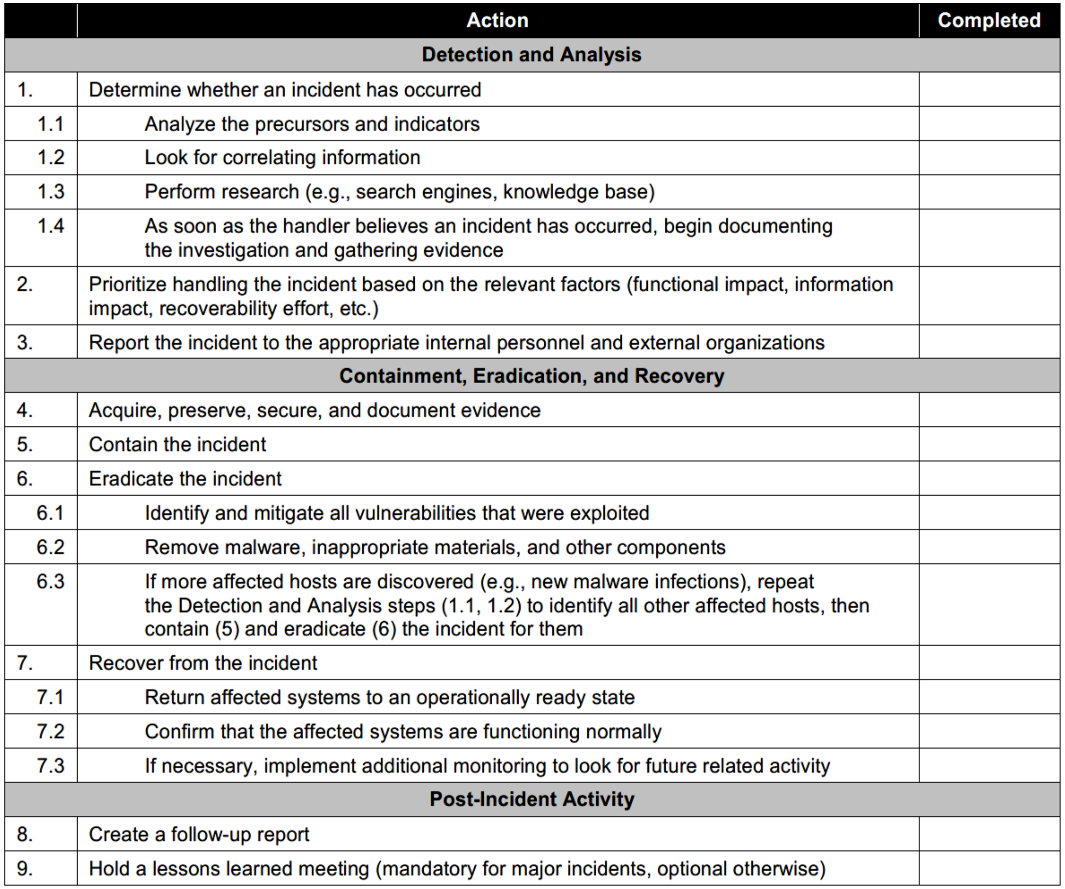
Preparation: Developing the Incident Response Plan (“the Plan”)

- 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: Developing the Checklist

Example: NIST – Security Incident Checklist – NIST Security Incident Handling Guide



	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Preparation: Who needs to be part of the Plan development team?

- **Determine who are the stakeholders:**
  - Organizational leadership
  - IT & Information Security leadership
  - Audit
  - Finance
  - Human Resources
  - Communications
  - Legal counsel

- **Determine what decisions need to be made:**
  - Obtain or clarify cyber liability insurance information and requirements
  - Determine vendors needed such as forensics, outside legal counsel, mitigation and communications services

Preparation: Goals of the Plan

- Establish the **Incident Response Team** (the “Team”)
- Establish **definitions** –security incident, data breach
- **Assess** the incident and threat level
- **Define** the actions to be taken when an incident occurs
- **Respond** to the incident
- **Restore** - present an orderly course of action for restoring functionality
- **Document** – collect and document the incident
- **Communicate** – specify how information should be communicated, who should communicate and how
- **Mitigate** – implement processes to mitigate the effects of the incident

Preparation: Additional Goals of the Plan

- **Prevention** - Improve processes and procedures to help prevent the security incident or breach from reoccurring

- **Education** – Train and educate employees to prevent future incidents

- **Review** - Review lessons learned, policies, procedures and technology, and update as necessary

- **Communicate** – With Municipal leadership

Preparation: Create 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

Preparation: Determine team members

Incident Response Coordinator or Chief Privacy Officer

- Determines the nature and scope of the incident.
- Contacts members of the Incident Response Team.
- Determines which Incident Response Team members play an active role in the investigation.
- Escalates to executive leadership as appropriate.
- Monitors progress of the investigation.
- Aids in evidence gathering, chain of custody, and preservation as appropriate.
- Prepares a written summary of the incident and the corrective action taken.

Preparation: Roles of the Team (cont'd)

Technology Coordinator or Chief Security Officer

- Determines the system(s) affected by the incident.
- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks.
- Runs tracing tools, port monitors, and event loggers.
- Contacts external Internet service provider for assistance in handling the incident if necessary.
- Updates all service packs and patches on mission-critical computers as necessary.
- Creates backups and that backups are in place for all critical systems.
- Examines system logs of critical systems for unusual activity.
- Monitors business applications and services for signs of attack.
- Reviews audit logs of mission-critical servers for signs of suspicious activity.
- Coordinates with outside IT vendors/forensic analysts.
- Provides recommendations for mitigation or other tools.

Preparation: Roles of the Team (cont'd)

Communications Coordinator

- May assist with contacting appropriate affected individuals to notify them of the incident(s).
- May assist with contacting local, state, federal or other governmental entities if incident is criminal in nature.
- Spearheads communication with media, as necessary.
- Collates all related documentation and data of final assessment of incident for preservation purposes.
- Coordinates internal and external communications and crisis management.

Preparation: Roles of the Team (cont’d)

Internal Audit Coordinator

- Reviews systems for compliance with information security policies and controls.
- Performs appropriate audit tests to keep systems current with service packs and patches.
- Reports any system control gaps to management for corrective action

Preparation: Roles of the Team (cont'd)

Legal Counsel/Outside Legal Counsel

- Serves as Coach for Security Incident.
- Coordinates legal analysis of data breach notification of individuals and/or regulatory authorities.
- Assists with coordination with cyberliability insurance company.
- Coordinates three-way agreement with forensic (and other) vendor(s) and municipality – protects attorney/client privilege
- Point person for government investigations and other government or regulatory communication
- Coordinates any litigation

Preparation: Roles of the Team (cont'd)

Human Resources

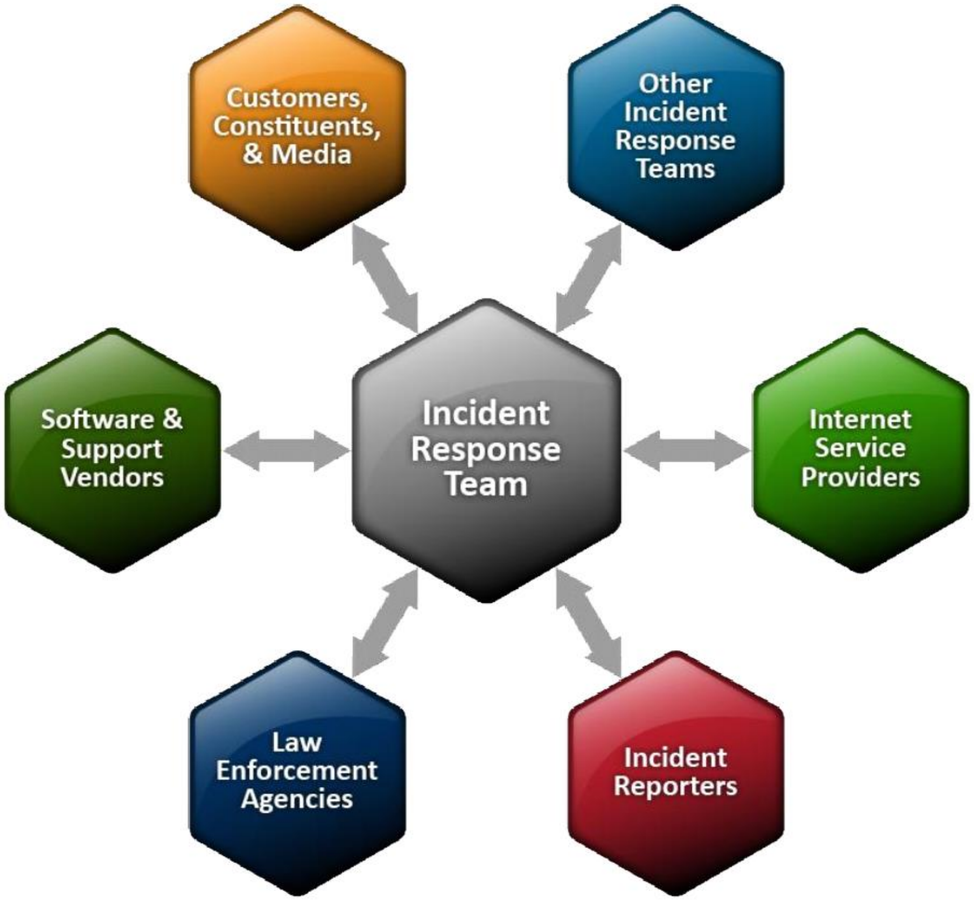
- Oversees employee discipline, as necessary
- Assists with communication and employee relations in the event of an incident that affects employee data

Preparation:

- **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 Department of Attorney General
    - Information sharing entities

Preparation: Manage Communications

NIST Model


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Detection & Analysis:

- Review information received from the individual(s) reporting the security incident
- Work with other departments and information technology staff, as appropriate, to determine the risk of continuing operations
  - E.g. deciding whether to shut down system, disconnect from network, continue operation, etc.;
  - however, any decision to delay the containment should be discussed with legal counsel based on the liability
- Coordinate with incident response services of a third-party security firm and outside legal counsel as appropriate
- Implement processes to prevent alteration to the system(s) until a backup has been completed
- Implement processes to change passwords or other security safeguards on any compromised systems
- Maintain detailed documentation on all actions taken

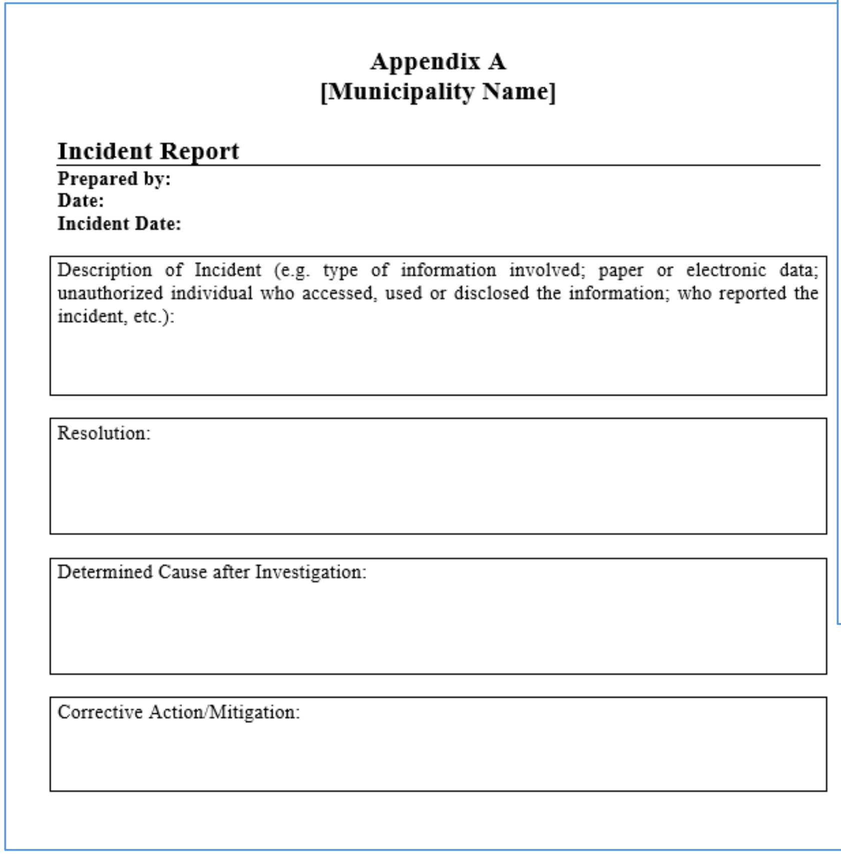
Detection & Analysis: Checklist (cont'd)

- ❑ **Incident handling and investigation**
  - ❑ Low risk level vs. high risk level incident
- ❑ **Coordination of engaging legal counsel and other third parties to establish protections of documents and communication**
- ❑ **Notification to insurance broker, as applicable**
- ❑ **Coordination of responses to incidents**
- ❑ **Communication with employees & affected individuals**
- ❑ **Determination if there is a reportable data breach**

Detection & Analysis: Checklist (cont'd)

- ❑ **If it is determined there is a reportable data breach:**
  - ❑ Determine notification requirements to regulatory authorities, as applicable
  - ❑ Notification to law enforcement, as applicable
  - ❑ Determine notification requirements to affected individuals, as applicable

Detection & Analysis: Checklist (cont'd)



Appendix A
[Municipality Name]

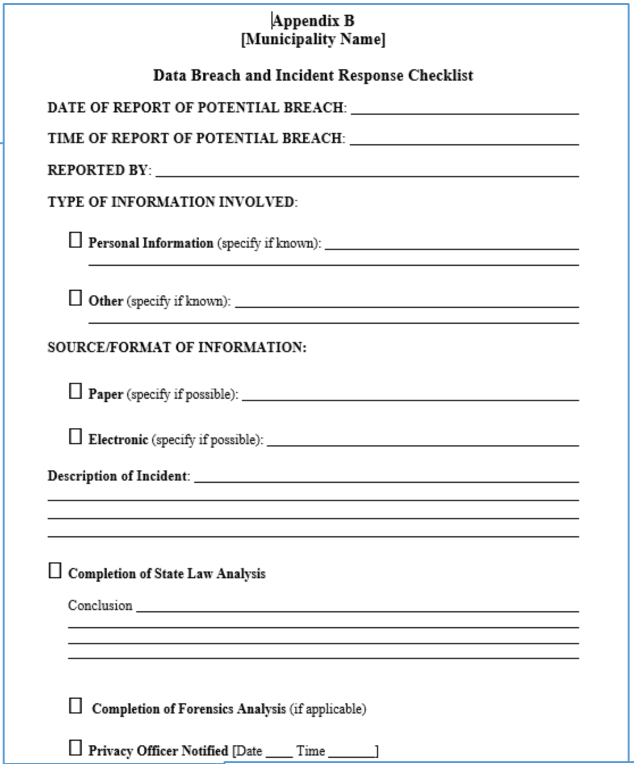
Incident Report
Prepared by:
Date:
Incident Date:

Description of Incident (e.g. type of information involved; paper or electronic data; unauthorized individual who accessed, used or disclosed the information; who reported the incident, etc.):

Resolution:

Determined Cause after Investigation:

Corrective Action/Mitigation:



Appendix B
[Municipality Name]

Data Breach and Incident Response Checklist

DATE OF REPORT OF POTENTIAL BREACH: ______________________

TIME OF REPORT OF POTENTIAL BREACH: ______________________

REPORTED BY: ______________________

TYPE OF INFORMATION INVOLVED:

□ **Personal Information** (specify if known): ______________________

□ **Other** (specify if known): ______________________

SOURCE/FORMAT OF INFORMATION:

□ **Paper** (specify if possible): ______________________

□ **Electronic** (specify if possible): ______________________

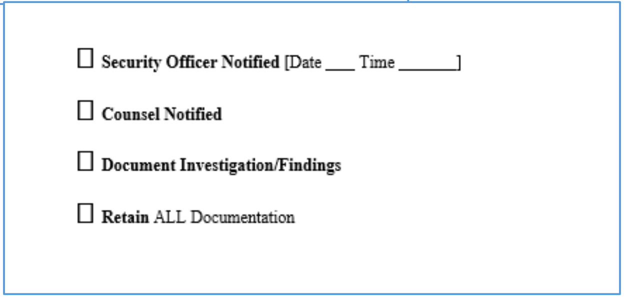
Description of Incident: ______________________

□ **Completion of State Law Analysis**

Conclusion ______________________

□ **Completion of Forensics Analysis** (if applicable)

□ **Privacy Officer Notified** [Date ____ Time ______]



□ **Security Officer Notified** [Date ___ Time _______]

□ **Counsel Notified**

□ **Document Investigation/Findings**

□ **Retain** ALL Documentation

Detection & Analysis: Checklist (cont'd)

- ❑ Coordinate with incident response services of a third-party forensic firm, outside legal counsel, and others, as applicable
- ❑ Review information received from the individual(s) reporting the security incident or breach

Containment, Eradication & Discovery: Checklist (cont'd)

❑ Implement processes to prevent alteration to the system(s) until a backup has been completed

❑ Implement processes to perform a full backup of the system(s) to forensically sterilize media (i.e. disk imaging) and store the backup in a secure area as an important part of the chain of custody (as applicable)

❑ Work with other departments and information technology staff, as appropriate, in determining the risk of continuing operations

(e.g. deciding whether to shut down system, disconnect from network, continue operation, etc.);
however, any decision to delay the containment should be discussed with legal counsel based on the liability

Containment, Eradication & Discovery: Checklist (cont'd)

- ❑ Implement processes to change passwords or other security safeguards on any compromised system
- ❑ Maintain documentation on all actions taken

Post-Incident Activity: Checklist

❑ Responsibilities of the Team – Post Incident:

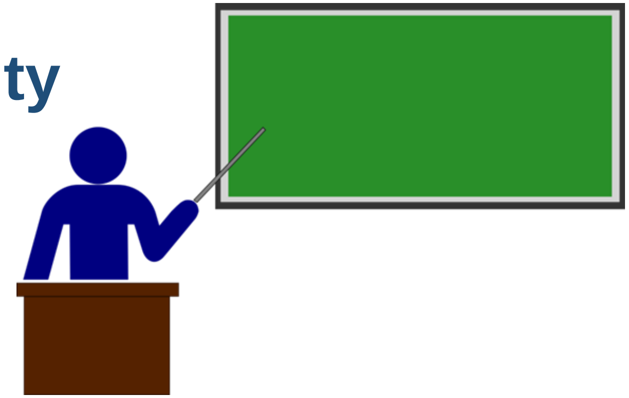
- Assess damage and cost; assess the damage and estimate both the damage cost and the cost of the containment efforts.
- Review response and update policies, procedures, plans and guidelines; plan and take preventative steps so the intrusion will not recur.
- Consider whether a procedure or policy was not followed which may have led to the intrusion.
- Determine whether additional user education is warranted.
- Was the incident response appropriate? How could it be improved?

Post-Incident Activity: Checklist

❑ **Responsibilities of the Team – Post Incident: (cont'd)**

- Was every appropriate party informed in a timely manner?
- Were the incident response procedures followed appropriately? How can they be improved?
- Are all systems patched, systems locked down, passwords changed, anti-virus updated, and appropriate procedures, guidelines and policies in place, etc.?
- Have changes been made to prevent a new and similar incident?
- Should any security measures be updated?
- What lessons have been learned from this experience?

Maintenance & Going Forward



- ❑ 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 tabletop exercises at least annually
- ❑ Conduct regular staff, user and employee education and training in privacy and security

Strategies for Municipalities

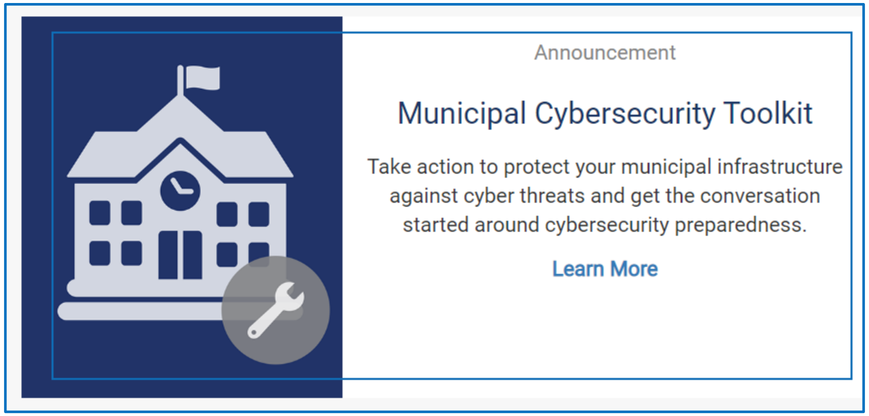
- Cybersecurity risk assessment – determine security gaps in systems and networks
- Implement prevention strategies – strong passwords multi-factor authentication, encryption for laptops, thumb drives, mobile device policies, including BYOD,
- Update software and implement regular patches
- Educate and train employees
- Vendor management
- Back up data
- Incident Response Plan
- Update IT/computer/cybersecurity policies and procedures
- Obtain/update cyber liability insurance

Helpful Websites and Links

- **US-CERT resources for State, Local, Tribal, and Territorial Governments:**
  https://www.us-cert.gov/resources/sltt#geo
- **US-CERT Alerts** up-to-date information on threats, hoaxes, and safety that you can subscribe to:
  https://www.us-cert.gov/ncas/tips
- **STOP.THINK.CONNECT.™** 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/stopthinkconnect
- **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

Cybersecurity Toolkit for Municipalities

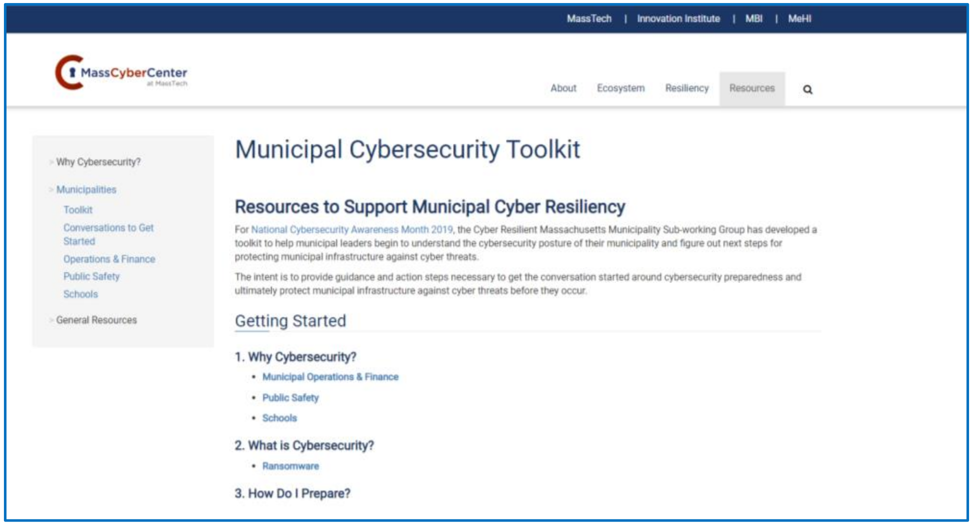
https://masscybercenter.org/municipal-toolkit



Announcement

Municipal Cybersecurity Toolkit

Take action to protect your municipal infrastructure against cyber threats and get the conversation started around cybersecurity preparedness.



Municipal Cybersecurity Toolkit

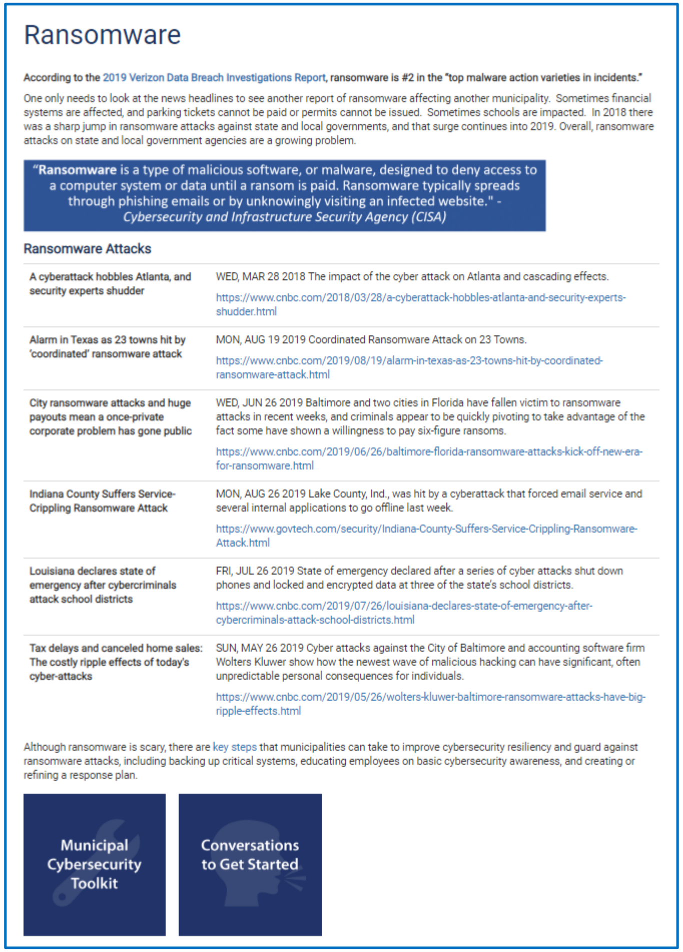
Resources to Support Municipal Cyber Resiliency

For National Cybersecurity Awareness Month 2019, the Cyber Resilient Massachusetts Municipality Sub-working Group has developed a toolkit to help municipal leaders begin to understand the cybersecurity posture of their municipality and figure out next steps for protecting municipal infrastructure against cyber threats.

The intent is to provide guidance and action steps necessary to get the conversation started around cybersecurity preparedness and ultimately protect municipal infrastructure against cyber threats before they occur.

Getting Started

1. Why Cybersecurity?
   - Municipal Operations & Finance
   - Public Safety
   - Schools
2. What is Cybersecurity?
   - Ransomware
3. How Do I Prepare?



Ransomware

According to the 2019 Verizon Data Breach Investigations Report, ransomware is #2 in the "top malware action varieties in incidents."

One only needs to look at the news headlines to see another report of ransomware affecting another municipality. Sometimes financial systems are affected, and parking tickets cannot be paid or permits cannot be issued. Sometimes schools are impacted. In 2018 there was a sharp jump in ransomware attacks against state and local governments, and that surge continues into 2019. Overall, ransomware attacks on state and local government agencies are a growing problem.

> "**Ransomware** is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website." - *Cybersecurity and Infrastructure Security Agency (CISA)*

Ransomware Attacks

A cyberattack hobbles Atlanta, and security experts shudder	WED, MAR 28 2018 The impact of the cyber attack on Atlanta and cascading effects. https://www.cnbc.com/2018/03/28/a-cyberattack-hobbles-atlanta-and-security-experts-shudder.html
Alarm in Texas as 23 towns hit by 'coordinated' ransomware attack	MON, AUG 19 2019 Coordinated Ransomware Attack on 23 Towns. https://www.cnbc.com/2019/08/19/alarm-in-texas-as-23-towns-hit-by-coordinated-ransomware-attack.html
City ransomware attacks and huge payouts mean a once-private corporate problem has gone public	WED, JUN 26 2019 Baltimore and two cities in Florida have fallen victim to ransomware attacks in recent weeks, and criminals appear to be quickly pivoting to take advantage of the fact some have shown a willingness to pay six-figure ransoms. https://www.cnbc.com/2019/06/26/baltimore-florida-ransomware-attacks-kick-off-new-era-for-ransomware.html
Indiana County Suffers Service-Crippling Ransomware Attack	MON, AUG 26 2019 Lake County, Ind., was hit by a cyberattack that forced email service and several internal applications to go offline last week. https://www.govtech.com/security/Indiana-County-Suffers-Service-Crippling-Ransomware-Attack.html
Louisiana declares state of emergency after cybercriminals attack school districts	FRI, JUL 26 2019 State of emergency declared after a series of cyber attacks shut down phones and locked and encrypted data at three of the state's school districts. https://www.cnbc.com/2019/07/26/louisiana-declares-state-of-emergency-after-cybercriminals-attack-school-districts.html
Tax delays and canceled home sales: The costly ripple effects of today's cyber-attacks	SUN, MAY 26 2019 Cyber attacks against the City of Baltimore and accounting software firm Wolters Kluwer show how the newest wave of malicious hacking can have significant, often unpredictable personal consequences for individuals. https://www.cnbc.com/2019/05/26/wolters-kluwer-baltimore-ransomware-attacks-have-big-ripple-effects.html

Although ransomware is scary, there are key steps that municipalities can take to improve cybersecurity resiliency and guard against ransomware attacks, including backing up critical systems, educating employees on basic cybersecurity awareness, and creating or refining a response plan.

What’s Next?

- **Webinar: Workshop 1 Follow up**
  - Questions, discussion of issues, areas of difficulty

SAVE THE DATE!

AUGUST 6, 2020 10:00 am – 12:00 p.m.

- **Workshop 2: Putting the Plan into action**
  - Establishing an Enterprise Wide Security Program Including:
    - Cyber hygiene
    - Education
    - Tabletop exercises for Municipalities
    - Discussion of policies and procedures for legal compliance
    - Tips on how to get municipal leadership engaged and supportive

Thank you! Questions?

Linn Foster Freedman
lfreedman@rc.com
Robinson + Cole

One Financial Plaza
Suite 1430
Providence, RI 02903
401-709-3353

https://www.dataprivacyandsecurityinsider.com/