MULLEN
COUGHLIN LLC

Cybersecurity: What Municipalities Need to Know Now

There's Been a Cybersecurity Incident. Now What?

January 24, 2020

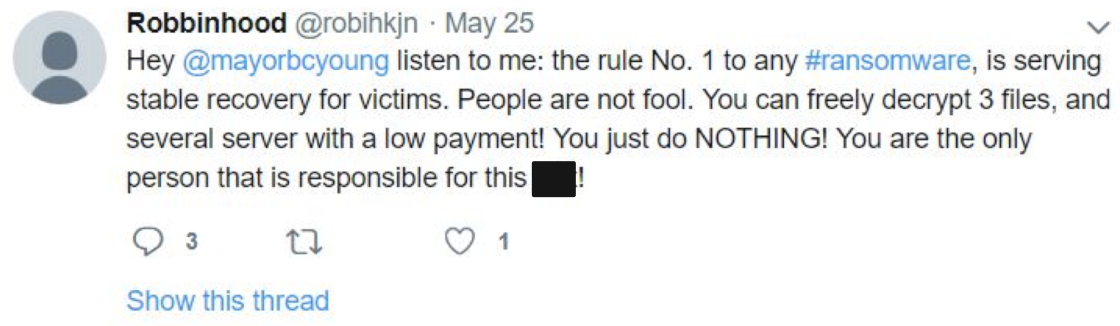
Gregory J. Bautista, Partner, CIPP/US
Michele T. Veltri, Associate

Learning Objectives

- **Trends in Municipal Breaches**
- Responding to a Cybersecurity Incident
- Best Practices

You’ve Seen the Headlines

- Baltimore Maryland
  - May 2019
  - RobinHood
  - $76,000 demand
  - City refused to pay
  - Attackers tweeted at government leaders
  - Posted links to images of documents allegedly stolen
  - Media attention used to promote ransomware-as-a-service
  - City estimates the attack will cost at least $18.2 million



Robbinhood @robihkjn · May 25

Hey @mayorbcyoung listen to me: the rule No. 1 to any #ransomware, is serving stable recovery for victims. People are not fool. You can freely decrypt 3 files, and several server with a low payment! You just do NOTHING! You are the only person that is responsible for this [redacted]!

Municipalities are Targets of Ransomware

- Local governments are increasingly being targeted by ransomware
- Hackers are coordinating attacks against multiple municipalities at once (23 cities in Texas impacted)
- Hackers are also targeting managed service providers (MSPs) to spread ransomware quickly to multiple clients
- Neighboring municipalities using the same MSP may be encrypted by ransomware at the same time
- Hackers are targeting police departments
- Local governments in Massachusetts have been impacted

Not to Mention Other Data Security Events

- Business email compromises
- Social engineering
- Denial of service attacks
- Insider threats
- Phishing emails
- Malware infections
- Website disruptions
- Data theft
- System hacks

What’s the Harm

- Disruption of daily operations
- Potential financial harm
- Risk to individuals with data in your systems
- Notification obligations triggered by law

Data Breaches in the Commonwealth

Massachusetts	2019	2018	2017
Breach Notifications	2,145	1,835	1,889
Residents	tbd	442,941	3,377,646
Equifax (2017) impacted 2,929675 MA residents			

Let’s walk through 3 common scenarios…

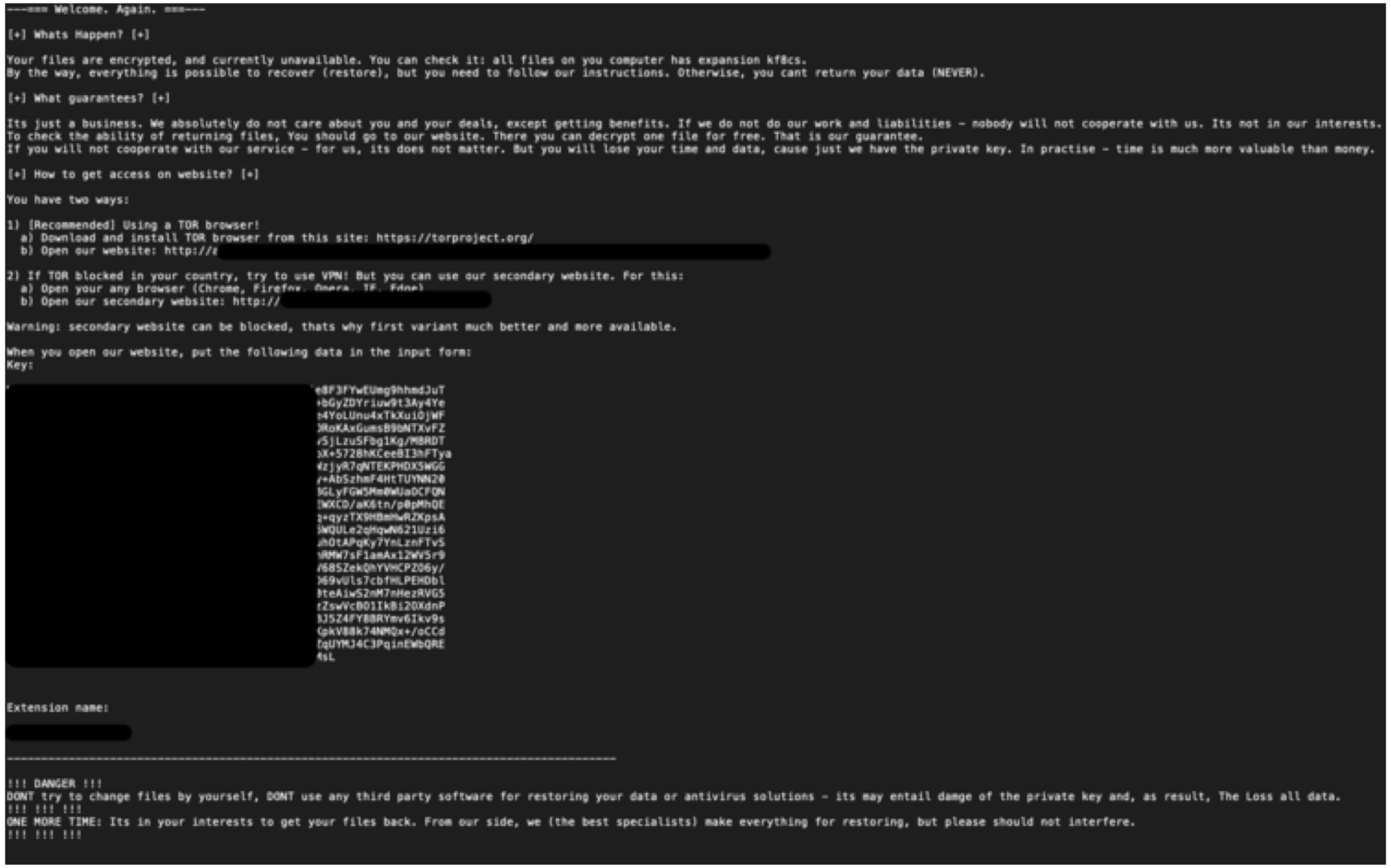
Scenario 1

It's Friday morning and city staff can't log into the computer network. The fire and police departments are now relying solely on radio communications, rather than mobile data systems, to receive incident information. City staff are communicating via text message with the few numbers they have in their personal smartphones because the telephone and email systems are down. It's a payday and most employees rely on direct deposit to receive their paychecks but no one received their electronic check on Thursday night. Residents and business owners who need to conduct business with the municipality are becoming frustrated.

Trends in Ransomware

- Hackers are spreading malware that steals passwords before encrypting files during a ransomware attack
- Hackers are threatening to release private data if ransoms are not paid
- Ransom demands are increasing
- Hackers are encrypting or deleting backups
- Hackers are disabling antivirus to move undetected in environments for weeks or months before an attack
- Hackers are targeting municipalities

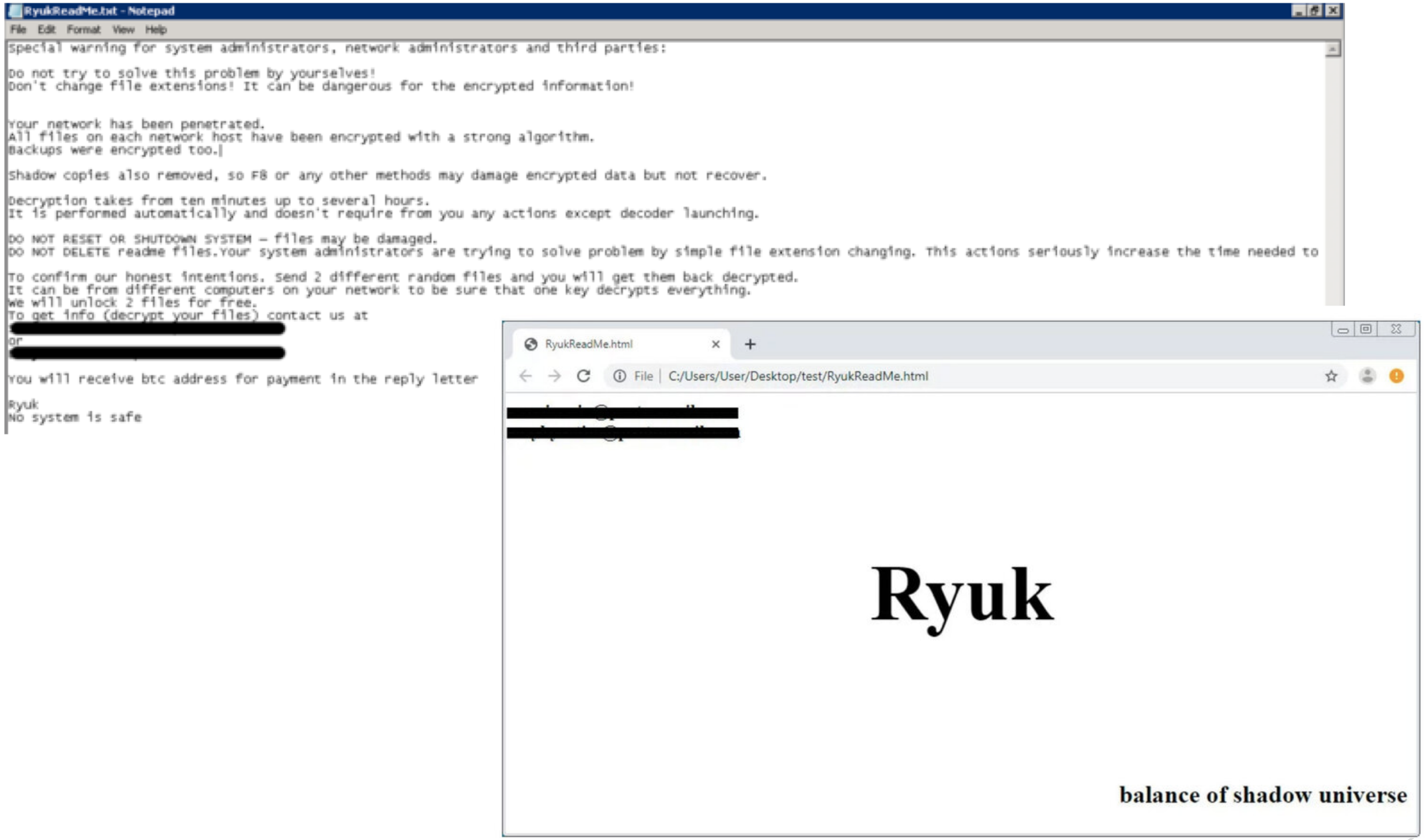
Ransom Note on Infected Computers



```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion kf8cs.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://[redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://[redacted]

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

[redacted]e8F3FYwEUmg9hhmdJuT
bGyZDYriuw9t3Ay4Ye
4YoLUnu4xTkXui0jWF
RoKAxGumsB9bNTXvFZ
5jLzuSFbg1Kg/M8RDT
X+S728hKCeeBI3hFTya
zjyR7qNTEKPHDXSWGG
+AbSzhmF4HtTUYNN20
GLyFGW5Mm0WUaDCFQN
WXCD/aK6tn/p0pMhQE
+qyzTX9HBmHwRZKpsA
WQULe2qHqwN621Uzi6
hOtAPqKy7YnLznFTvS
RMW7sF1amAx12WVSr9
/68SZekQhYVHCPZ06y/
69vUls7cbfHLPEHDbl
teAiwS2nM7nHezRVGS
ZswVcB01IkBi2OXdnP
J5Z4FY88RYmv6Ikv9s
pkV88k74NMQx+/oCCd
qUYMJ4C3PqinEWbQRE
sL


Extension name:

[redacted]

-----------------------------------------------------------------------------------------

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.
!!! !!! !!!
```

Image from Coveware - example of Sodinokibi ransomware note.

Ransom Notes Can Take Many Forms



```
Special warning for system administrators, network administrators and third parties:

Do not try to solve this problem by yourselves!
Don't change file extensions! It can be dangerous for the encrypted information!


Your network has been penetrated.
All files on each network host have been encrypted with a strong algorithm.
Backups were encrypted too.

Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

Decryption takes from ten minutes up to several hours.
It is performed automatically and doesn't require from you any actions except decoder launching.

DO NOT RESET OR SHUTDOWN SYSTEM – files may be damaged.
DO NOT DELETE readme files.Your system administrators are trying to solve problem by simple file extension changing. This actions seriously increase the time needed to

To confirm our honest intentions. Send 2 different random files and you will get them back decrypted.
It can be from different computers on your network to be sure that one key decrypts everything.
We will unlock 2 files for free.
To get info (decrypt your files) contact us at
[redacted]
or
[redacted]

You will receive btc address for payment in the reply letter

Ryuk
No system is safe
```

[redacted]

Ryuk

balance of shadow universe

Images from Coveware - examples of Ryuk ransomware note.

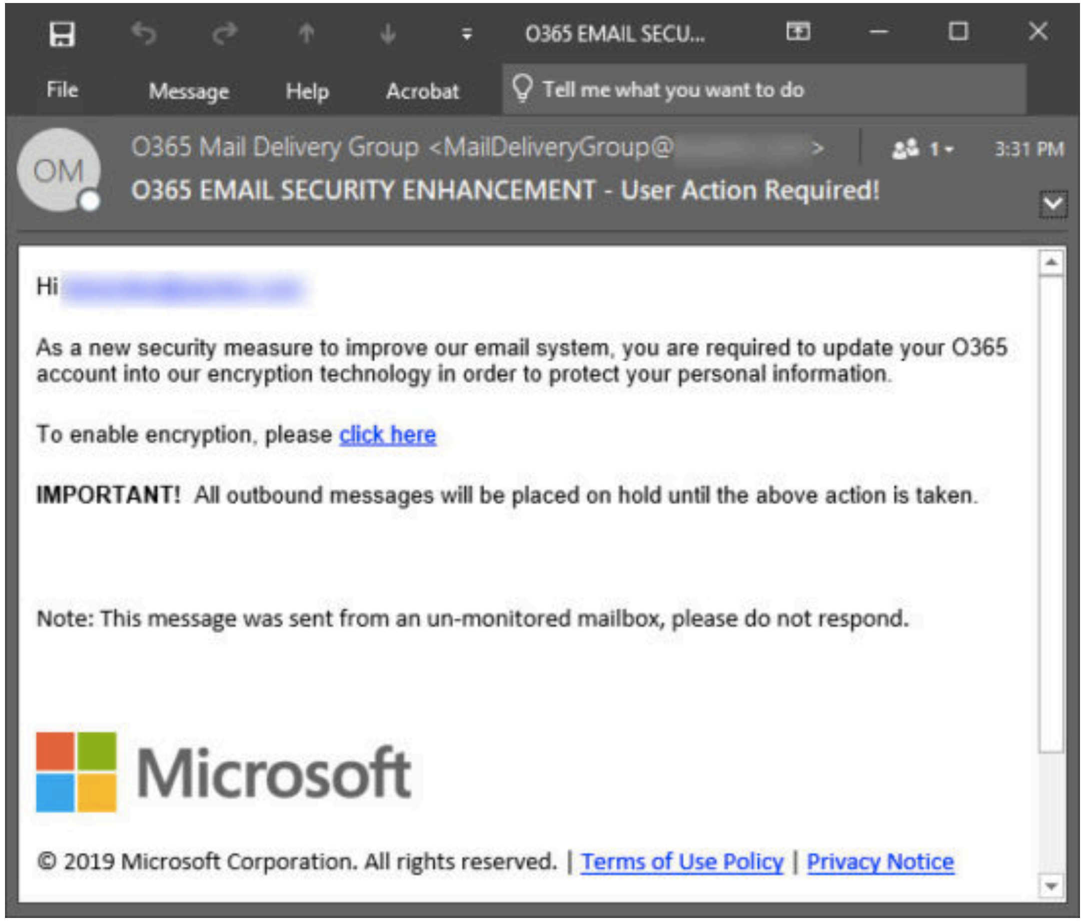
Scenario 2

You receive a call from a representative at your bank about unusual activity that was flagged in connection with one of your municipal bank accounts. Upon further review, you realize that an unknown third party has been slowly withdrawing funds from the bank account. Only limited personnel can access the bank account and you are concerned that one of their computers or accounts has been compromised.

Trends in Business Email Compromise Events

- Hackers can send emails from spoofed email accounts or legitimate compromised accounts
- Emails often include malicious attachments (hackers might say they are invoices)
- Emails will direct someone to a web page that looks legitimate (often a fake Microsoft log in page)
- Hackers are after passwords that they can use to access other accounts or systems on your network
- Emails may contain spyware that give hackers remote control of a computer or allow them to track online activities

Sample Phishing Email



OM O365 Mail Delivery Group <MailDeliveryGroup@[redacted]> 1 3:31 PM

O365 EMAIL SECURITY ENHANCEMENT - User Action Required!

Hi [redacted]

As a new security measure to improve our email system, you are required to update your O365 account into our encryption technology in order to protect your personal information.

To enable encryption, please click here

IMPORTANT! All outbound messages will be placed on hold until the above action is taken.

Note: This message was sent from an un-monitored mailbox, please do not respond.

Microsoft

© 2019 Microsoft Corporation. All rights reserved. | Terms of Use Policy | Privacy Notice

Image from Cisco.

Scenario 3

It’s a Friday before a Monday holiday and the office is closing early. Some employees have taken the day and those that are in the office are anxious to start the long weekend. An employee receives an email that appears to be from a manager. The email includes instructions to issue a payment before the end of the day because banks are also closed on Monday. Typically, your employees follow protocols to confirm a financial transaction. Today, with many out of the office, the employee initiates the transaction without calling the manager to verify the email. Two hours later, the employee realizes the email was from a fake email address.

Trends in Phishing Emails

- Hackers identify personnel with access to sensitive information or accounts
- They're looking for tax information, payroll information, bank account information, or other financial information
- Scammers may impersonate management and use a fake email address to request that employees send sensitive documents or make wire transfers
- They'll take advantage of vulnerable times like Fridays before long weekends
- Employees often realize their mistakes once the documents or money has been sent…

Learning Objectives

- Trends in Municipal Breaches
- **Responding to a Data Incident**
- Best Practices

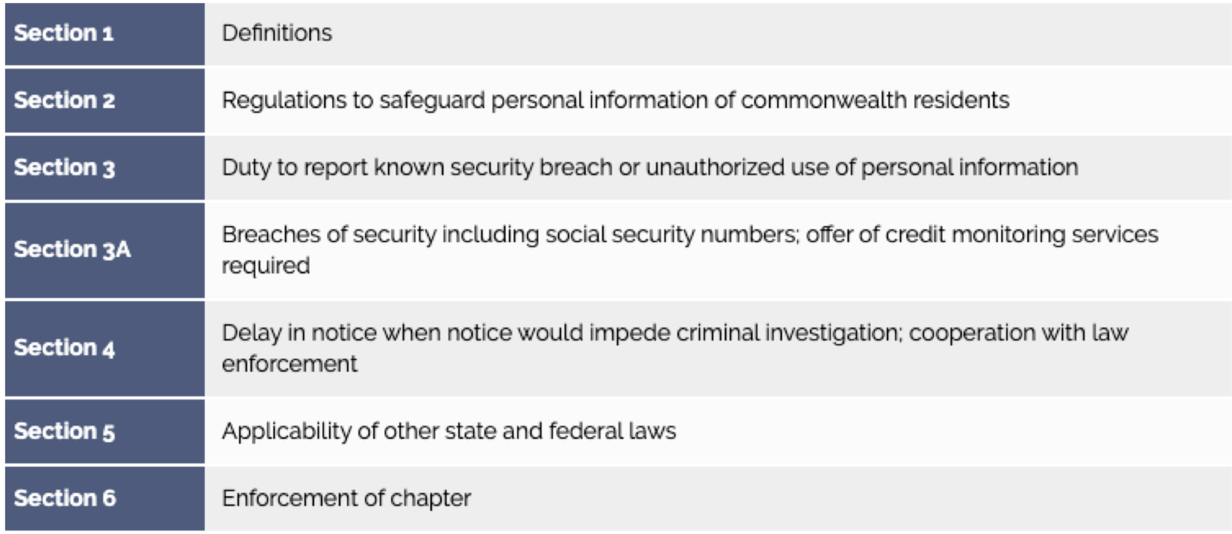
What Makes an Incident a Breach

- Definition
  - Access v. Acquired – what does that really mean?
  - Confidentiality, integrity, and security of personal information
  - “Risk of harm”
  - Encryption “safe harbor” – or is it?

- And don’t call it a “breach”
  - Legal impact of a “breach”
  - So what do you call it?

Data Breach Response is Regulated

- Massachusetts has regulations regarding security breaches
- Regulations for safeguarding resident information
- Requirements for reporting known security breaches or unauthorized use of personal information



Section 1	Definitions
Section 2	Regulations to safeguard personal information of commonwealth residents
Section 3	Duty to report known security breach or unauthorized use of personal information
Section 3A	Breaches of security including social security numbers; offer of credit monitoring services required
Section 4	Delay in notice when notice would impede criminal investigation; cooperation with law enforcement
Section 5	Applicability of other state and federal laws
Section 6	Enforcement of chapter

Notification to Residents vs. Regulators

REGULATORS

- Nature of breach
- Number of residents affected
- Type of government agency
- Type of personal information
- Whether the agency maintains a written information security plan
- Steps taken in response

RESIDENTS

- Very specific requirements about what can and cannot be included in notification
- Cannot include the nature of the breach or include the number of residents affected
- Must include information about rights of residents and mitigation steps residents should take
- If SSNs are involved, 18 months of credit monitoring services

Notification to Impacted Individuals

- Breach counsel can assist you in determining if notification is required under state data breach notification regulations in Massachusetts
- You may be required to notify residents whose personal information is at risk
- If even one resident is notified, you also need to notify the Attorney General's Office and the Office of Consumer Affairs and Business Regulation
- Notification is required as soon as practicable and without unreasonable delay and cannot be delayed because the number of residents affected is not known

You May Have More Data Than You Think

- Financial data (water bills, taxes, parking fines)
- Personnel files (SSNs, bank accounts for direct deposit)
- Sensitive records (mortgage, birth and death certificates, divorce decrees, medical records, military discharge)
- Police data (SSNs, driver’s license numbers, finger prints)
- Dispatch or EMT data (medical information)
- Court system (confidential files)

You suspect a breach. Now what?

Life Cycle of Data Breach Response

- IDENTIFICATION
  - Identify that an event has occurred
  - Determine who should be involved
  - Trigger your Incident Response Plan
- CONTAINMENT
  - Stop the bleeding – but don't damage the wound!
- REMEDIATION
  - Take steps to prevent a similar event from occurring in the future
- NOTIFICATION
  - Who do you tell? How? When?

Who You Gonna Call?

- Breach Counsel
- Cyber Insurance
- IT Support
- Forensic Experts
- Public Relations

Preserve, Protect and Prevent

- Take affected equipment offline immediately
- Don’t turn machines off until forensics are engaged
- Change account passwords, especially sensitive ones
- Notify banks of fraudulent financial transactions
- Do not destroy evidence by wiping systems prematurely
- IT should monitor your network for suspicious activity

Get Back to Work

Forensic experts and Information Technology providers may be engaged to help resume daily operations:

- Recover lost or encrypted data
- Rebuild servers or computers
- Clean infected devices
- Set up a clean, segmented network
- Monitor your computers and servers
- Reconnect phones or printers

You Stopped the Bleeding, Now What?

You may need to engage forensic experts for an investigation to determine if notification is required and help you protect yourself going forward.

Forensic experts will focus on:

- Identifying the attack vector
- Investigating if there has been any access to or exfiltration of sensitive information
- Discovering ongoing vulnerabilities related to the incident
- Determining number of people affected (with counsel)

Prepare for Public Attention

- Breach counsel or public relations firms may be brought in to assist you in crisis communication response
- Media may learn of the incident quickly
- Residents and businesses may ask questions if they notice a change in daily operations
- Law enforcement may reach out
- Regulators could learn of the incident and ask questions
- Public record requests could be made

Think about how this incident is discussed during any public meetings!

Learning Objectives

- Trends in Municipal Breaches
- Responding to a Data Incident
- **Best Practices**

Lead By Example

- Understand what sensitive information you store
- Think strategically
- Cybersecurity can be low-budget and still be effective
- Plan ahead
- Hold third parties accountable
- Adopt best practices with personnel
- Ensure you have backups

At your next meeting, ask what would happen if computer systems went down for two hours, one day, one week?

Personnel Can Be Your Greatest Weakness

- Data breaches may occur due to intentional hacking
- Even then, users can become the entry point
  - User clicks on a malicious link or opens an attachment
- Data breaches can be due to inadvertent disclosure
  - Email sent to the wrong person
  - Personnel loses a laptop
- Security organizations offer end-user security awareness videos at relatively low costs
- Continually remind your workforce about best practices
- Use phishing emails received as learning opportunities

Implement Best Security Practices with IT

- Educate users on strong password hygiene
- Restrict access to data and regularly review user access
- Hold IT accountable for keeping systems up to date
- Create an incident response plan if you don't have one
- Keep multiple back-ups, including offline back-ups
- Require multi-factor authentication where available
- Train employees on phishing emails
- Consider encrypting or de-identifying sensitive data

Avoid Being Phished

- Emails that have to do with money
- Emails making an offer that is too good to be true
- Emails that bring up urgent issues
- Emails that request personal information
- “To” lines that are not address to the user specifically
- Misspelled words and bad grammar
- Changes in the color or type of font
- Text that looks copied and pasted into the email
- Plain text or absence of logos and signatures

Always obtain verbal confirmation for requests for personal information!

Contact

Gregory J. Bautista, J.D., CIPP/US

Mullen Coughlin LLC

Partner

gbautista@mullen.law

Michele T. Veltri, J.D.

Mullen Coughlin LLC

Associate

mgrenier@mullen.law