MAMA GLS Education Conference

Grand Traverse Resort, Acme MI | June 27-28, 2025

Digital Dangers: Protecting Public Data and Managing Cyber Incidents in a Connected World

Starr Kincaid

Director of Claims & Legal Services
MMRMA

Samantha Heraud

Senior Claims Attorney
MMRMA

Dan Bourdeau

Director of IT & Cybersecurity
MMRMA

*The content of this presentation is for informational purposes only and does not constitute legal advice. While it covers topics related to cyber claims, insurance, and related legal considerations, nothing herein should be interpreted as a substitute for professional legal counsel, who should be sought for advice on any specific legal issues or claims.

Growing Cybersecurity Risks to Local Governments in Michigan

53%
have experienced a cybersecurity attack

$80K
is the average ransom payment

28%
from phishing account compromise

53%
increase in incidents since 2020

46%
use unsupported server operating systems

19%
lack an incident response plan

Don’t Press the Panic Button – To Speak or Not to Speak….*and what to say.*

- **Communication Objectives**
  - Ensure that messaging is consistent across various stakeholders.
  - Communicate accurately, proactively, and transparently with employees, constituents and others as appropriate, with an emphasis on “business as usual.”
  - Protect your reputation while ensuring your municipality’s communications strategy is directly aligned with its interests.
  - Mitigate negative reaction from stakeholders by minimizing/containing the story and not unnecessarily amplifying it.
- **Designated Communication Person/Office**

Don’t Press the Panic Button – What to Say, and what NOT to Say

- **DO use words like “incident,” “event,” “issue,” “situation,” and “investigation.”**
- **DO NOT use words like “compromise,” “attack,” “stolen,” “sophisticated,” “nation state,” or “extortion.”**
  - If your consumers or others use these words, do not repeat them in response.
- **NEVER use the word “breach” unless it is legally required.**
  - “Breach” is a word with a specific legal definition and impact.
- **Be mindful of referring to yourself/entity as a “victim”.**
- **Your tone should friendly, serious, and helpful - but not grave.**
- **You are under no obligation to have immediate answers to all questions. If you do not know the information, <u>do not speculate or guess</u>.**

Data Breach – What is it, really?

- **Unauthorized acquisition, disclosure, or loss of personal information stored in a database.**

- **This includes *internal* unauthorized access to information *AND* data leaks ("FREE" versions, over sharing & AI)**

Data Breach – What is it, really?

Personally
Identifiable
Information

&

Protected
Health
Information

Data Breach

- **First-Party Claims**
  - Not always electronic!
  - Data not always stored on your network!
  - Can include regulatory reporting:
    - The State Attorney General's Office
    - Office of Recipient Rights/ Health and Human Services
- **Third-Party Claims**
  - Third parties allege harm from the disclosure of their information
  - Actions taken by regulatory agencies against you stemming from a data breach.

Social Engineering

- **Fraudulent requests for credentials or payments, often disguised as coming from trusted sources.**
- **Relies on the psychological manipulation of human behavior to "trick" a victim into:**
  - disclosing sensitive data, sharing credentials, granting access to a personal device, or otherwise compromising their digital security.
- **Specific examples include:**
  - "Nigerian prince" emails
  - ACH payment fraud
- **Phishing, Smishing, Spear Phishing**
- **Business Email Compromise (BEC)**

Email-Based Red Flags

Suspicious Sender:
- Look-alike domains or subtle misspellings

- **Unexpected Recipients**:
  - Odd CC/BCC lists unrelated to the recipient

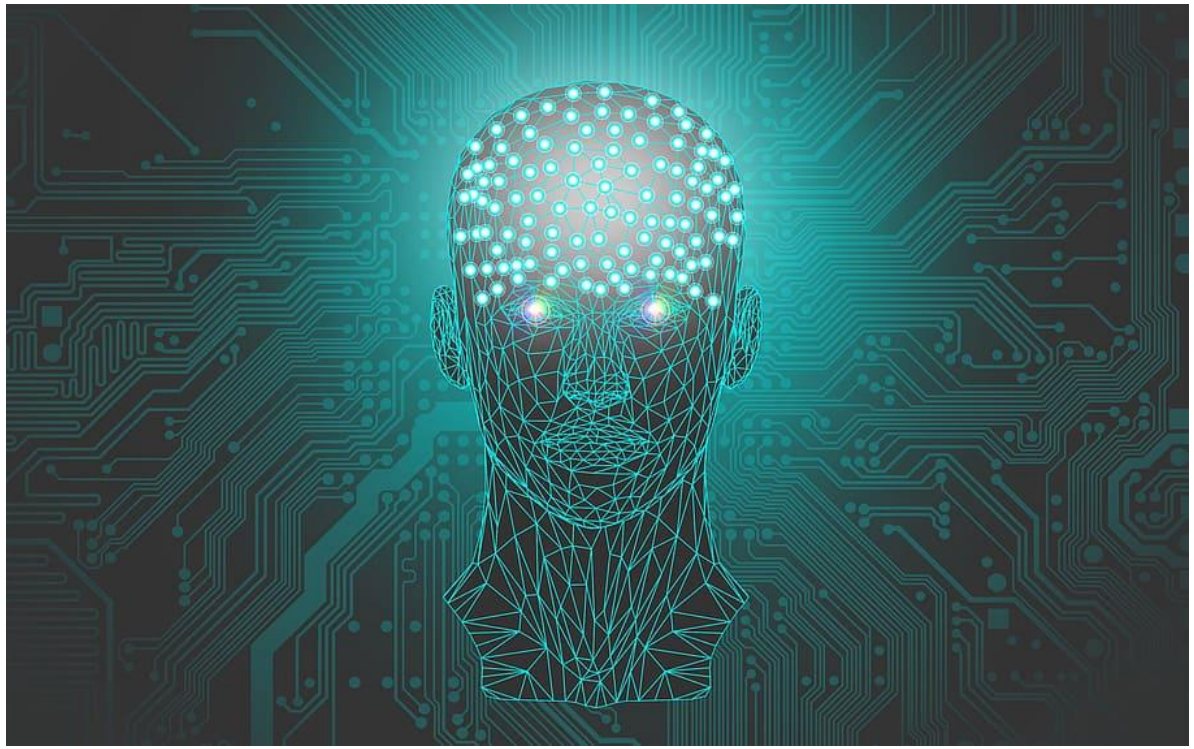
- **Emotional Triggers**:
  - Urgency, fear, or greed invoked in subject lines

- **Odd Timing**:
  - Emails sent at unusual hours

- **Mismatched Links**:
  - Mouse-over URL differs from displayed text

- **Unexpected Attachments**:
  - Unusual file types (.zip, .exe)

Phone or Virtual (Teams/Zoom)



- **Dropping Names**: Referencing authority figures to bolster credibility
- **Evasive Responses**: Avoiding or deflecting direct questions
- **Deliberate Mistakes**: Sympathy ploys (e.g., spilled coffee scenario)
- **Broad Information Requests**: Unusual or overly broad requests for sensitive data
- **No Verifiable Callback**: Refusal to provide a valid callback number

Delete | Respond | Quick Steps | More | Tags | Editing | Zoom

Thu 5/18/2017 2:45 PM

E [redacted] <C67C9010-4EAA-4843-BEC5-67127D13B678-4EAA-67123B67D178@giafl.com>

Email Quarantine: 14 new messages

To [redacted]

You forwarded this message on 5/19/2017 8:11 AM.

If there are problems with how this message is displayed, click here to view it in a web browser.

Office 365

Dear [redacted]

There are 14 new messages in your Email Quarantine since you received your last Notification.

Messages will be automatically removed from the qua

http://www.yanboychuk.com/dc.php
Click or tap to follow link.

To see all quarantined messages view your email quarantine or continue below

Continue

Note: This message has been sent by a notification only system. Please do not reply

Notice that the "From" email address is not from Microsoft and the sender's name that was actually shown was that of the customer (blacked out for security purposes). In fact, the email address doesn't have anything to do with Microsoft at all!

Notice the sense of urgency: "If you don't take action soon, your messages will be deleted". A typical phishing ploy to get action.

If you hover your mouse over the link (be careful not to click it!), you'll notice that the link's URL is not going to the Microsoft 365 site

The URL connected to this button goes to the same bogus site as the link. Again, hovering your mouse over the button will reveal the link

How business email compromise works

The start

Attackers see if they can spoof your domain and impersonate the CEO or other important people.

The phish

Spoofed emails are sent to high-risk employees in the organization.

The response

The targets receive the emails and act without reflecting or questioning the source.

The damage

Social engineering is successful, giving hackers access to what they are after.

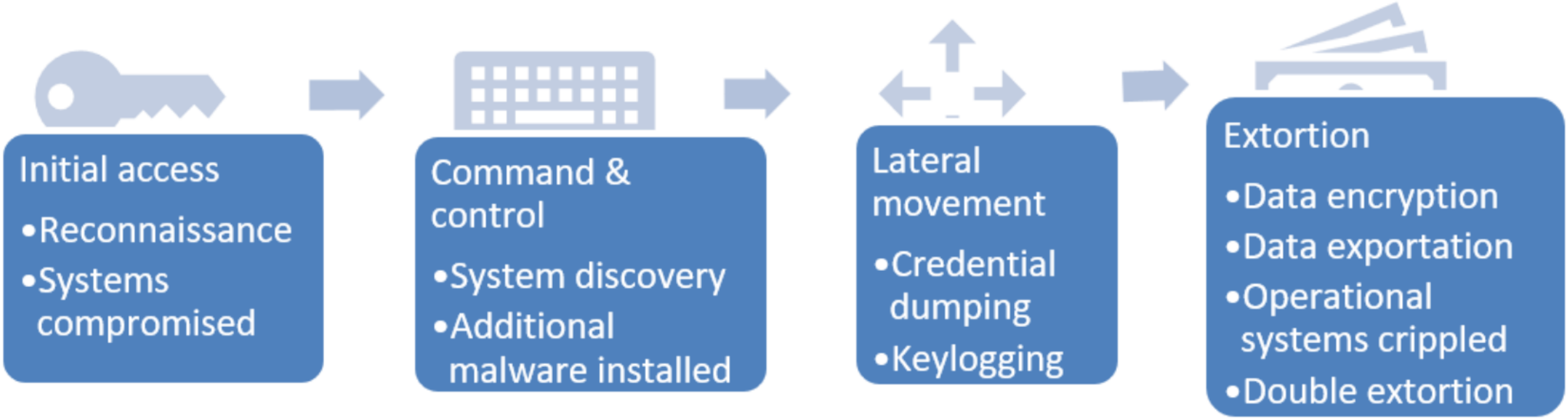
The result

Fallout may include monetary loss, data theft, lawsuits, leadership dismissals or reputational damage.

MALWARE v. RANSOMWARE

Malware is a computer virus designed to replicate and copies itself from file to file or program to program.	Ransomware is a sub-type of malware from cryptovirology that blocks access to the system unless ransom is paid.
Malware typically piggybacks on malicious links, fraudulent email attachements, social media messages, etc.	Ransomware are spread through phishing emails containing malicious attachments or web-based messaging applications.
Malware is also referred to as virus, worm, Trojan horses, spyware, adware, and ransomeware.	It's a new type of malware that presents itself in many ways to hold data to ransom.
The best way to protect the system from malware is to install antimalware programs.	The only way to protect your systems is to pay the ransom to the attackers.
It's a broad term that refers to all types of malicious programs.	Crypto and Locker are the two main types of ransomware.

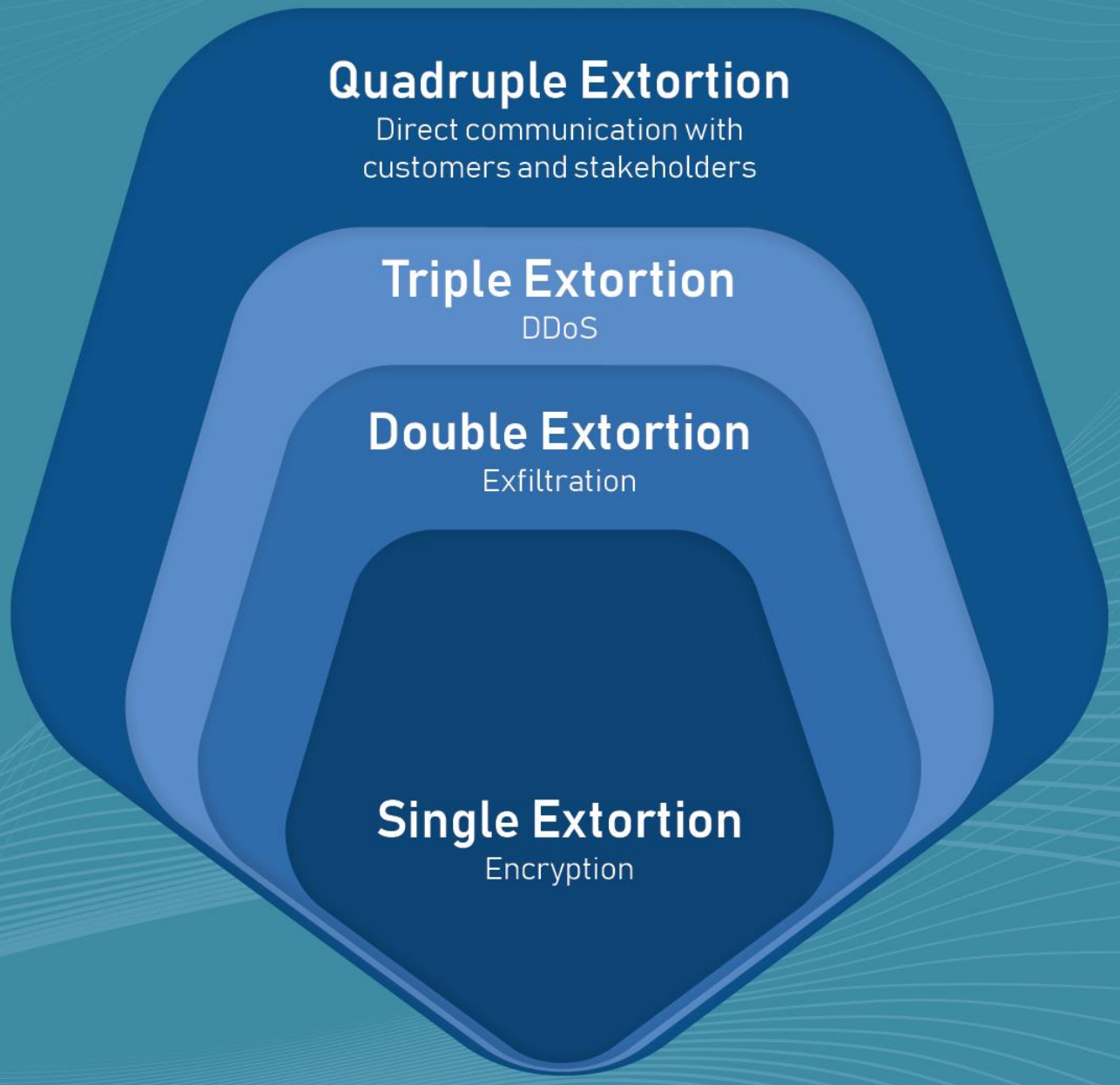
Ransomware


Initial access
•Reconnaissance
•Systems compromised
Command & control
•System discovery
•Additional malware installed
Lateral movement
•Credential dumping
•Keylogging
Extortion
•Data encryption
•Data exportation
•Operational systems crippled
•Double extortion

Ransomware –

One and done?

Think again…



Media Injury

- **What is Media Injury?**
  - In the Data Breach and Privacy world, this generally means the unauthorized use- often characterized as copyright infringement- of images on an entity's network, i.e., website or other digital publication.
- **How does it Happen?**
  - Someone searches the internet for an image, copies it, and uses it on a website page, cover of a report, etc. The image happens to be copyrighted.
- **The Use of AI has Increased these Claims Exponentially.**
  - Watch your interns!

Incident Response – Immediate Actions

- **Containment**
  - Isolate affected systems
  - Notify key personnel (IT, legal, leadership)
  - Change all relevant passwords
  - If applicable, contact financial institutions
- **Begin evidence preservation**
  - NEVER DELETE! NEVER POWER OFF!
- **Notify Insurer Immediately**
  - Provide initial notice per policy requirements
  - Include known details: type of incident, estimated impact
  - Provide best UNCONNECTED contact information and alternate contacts

Incident Response – Ask (and trust) the Experts

- **Depending on the incident, multiple experts may be utilized. This includes:**
  - Information Technology
  - Breach Counsel
  - Forensics
  - Human Resources
  - Communications / Public Relations
  - Ransomware Negotiator
  - Cyber coverage claims personnel
- **TRUST the experts – FEAR is a LIAR**
  - Fear may lead you to resist expert guidance or obfuscate the facts.
  - Don't fear your experts. Don't fear past technical/operational deficiencies.
- **Instead, use this as a foundation for improvement and sustained investment**

Incident Response - Business Email Compromise

- ✓ You've contained
- ✓ You've preserved
- ✓ You've called your insurer

- **Why should I spend time and money on forensics when my network is already secure?**
  - How did the Threat Actor access your environment?
  - What did the Threat Actor do in your environment?
  - Did they acquire any PII or PHI?

Incident Response for Ransomware – *A Three Track Approach*

SECURITY	RESTORATION	FORENSIC INVESTIGATION
• Using "offline accounts" • Deploy monitoring software • Wait for "all clear" before utilizing your network	• Backups • Third-party providers • Other data points • Encryption key	• Threat Actor access point • Was there a data breach?

Incident Response and Notification – *When* am I required to notify?

- **PHI (Personal Health Information)**
  - HIPAA generally requires notification within 60 days of discovery
  - Exceptions may be granted if requested by law enforcement

- **PII (Personal Identifiable Information)**
  - Michigan generally requires notification within 45 days

*Date of discovery is generally recognized as discovery that data was acquired not that there was unauthorized access to a network.

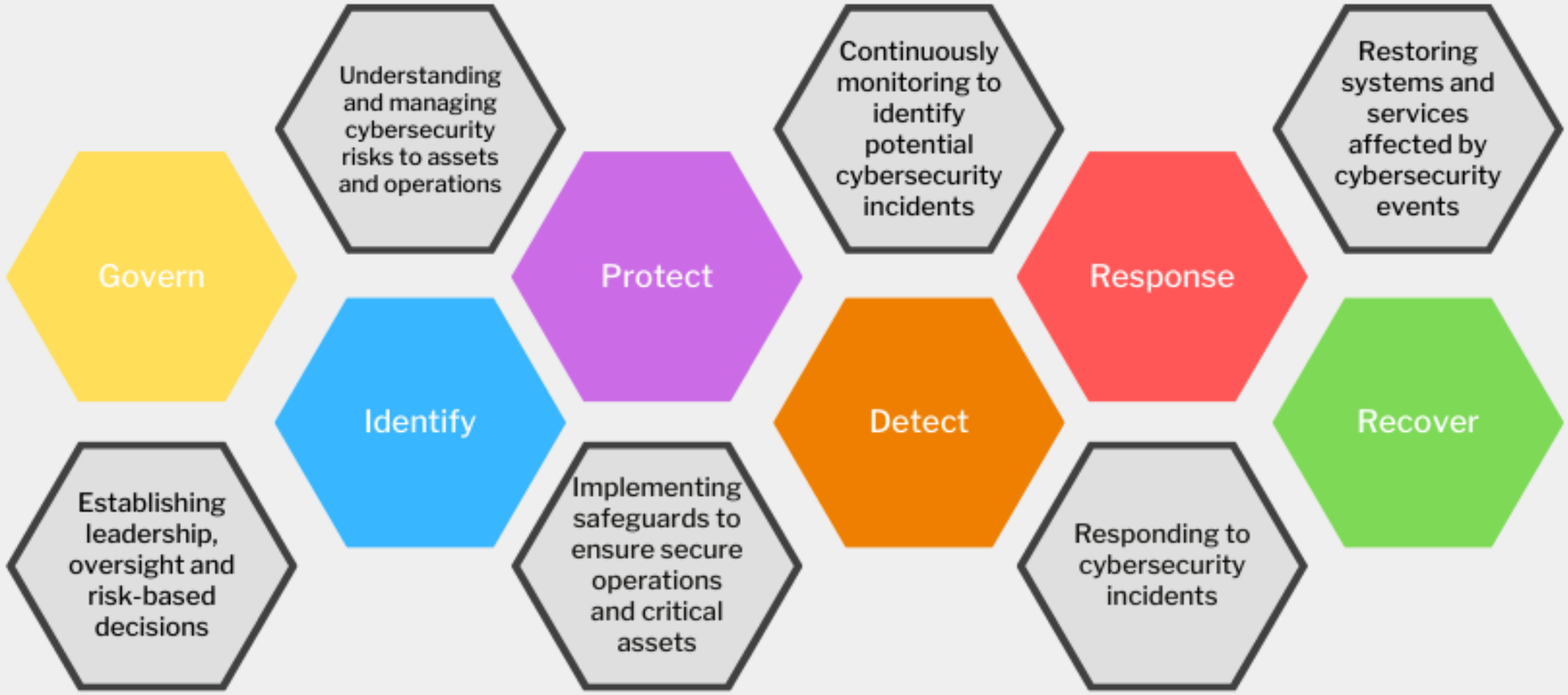
Incident Response and Notification – *Who* do I notify?

- Individuals
- Regulatory Agencies/Government
- Business Partners/Contractual Obligations

Incident Response and Notification – *How* do I notify?

- **Direct Mailings**
  - Often come with an "opt in" to credit monitoring services
  - Complicated when the person is a minor or deceased
- **Alternate Publications**
  - Website
  - Local/National Newspapers
- **Considerations**
  - Do you have a third-party provide the notifications?
  - Do you provide credit monitoring; if so, how long?
  - Do you utilize a call center?

Cyber Risk Assessment



Data Breach and Cyber Coverage

- **It's not WHETHER an incident will occur, it's <u>WHEN.</u>**
- **<u>Secure appropriate coverage to protect your municipality.</u>**

- **Data Breach Response Costs:**
  - Including legal fees, public relations, notification costs, and credit monitoring.
- **Business Interruption Losses:**
  - Covers income lost due to a cyberattack disrupting normal operations.
- **Cyber Extortion & Ransomware:**
  - Covers payments and negotiation services related to ransomware or other cyber extortion attempts.

Data Breach and Cyber Coverage

- **Third-party Liability:**
  - Protects against lawsuits due to data loss or privacy breaches affecting external parties.
- **Network Security Liability:**
  - Coverage for failure to prevent unauthorized access, malware, or denial of service attacks.
- **Regulatory Fines & Penalties:**
  - Protection against penalties arising from non-compliance with data protection laws (like GDPR or state laws).

Data Breach and Cyber Coverage Considerations

- **Experience In Public Entity Coverage**
- **Customizable Limits and Sub-limits:**
  - Tailor to entity size, data sensitivity, and budget.
- **Aggregate vs. Per Incident Limits:**
  - Understand whether limits apply per claim or across all claims in a year.
- **Retroactive Coverage:**
  - Ensure coverage applies to breaches that may have occurred before the policy was purchased.
- **Breach Response Panel:**
  - Opt for insurers that offer access to experienced breach counsel and expert teams.
- **Review and Understand Exclusions**

Questions?