

The Next 45 Minutes

Cities Association of Santa Clara County Cybersecurity
Table Top Exercise

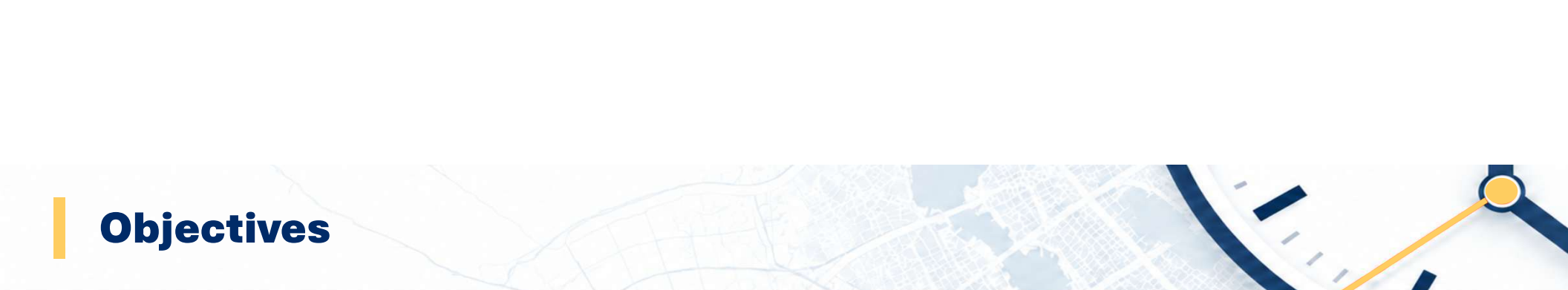


Presented by:

Auston Davis

City Chief Information Security Officer
Cybersecurity Division
City of San Jose





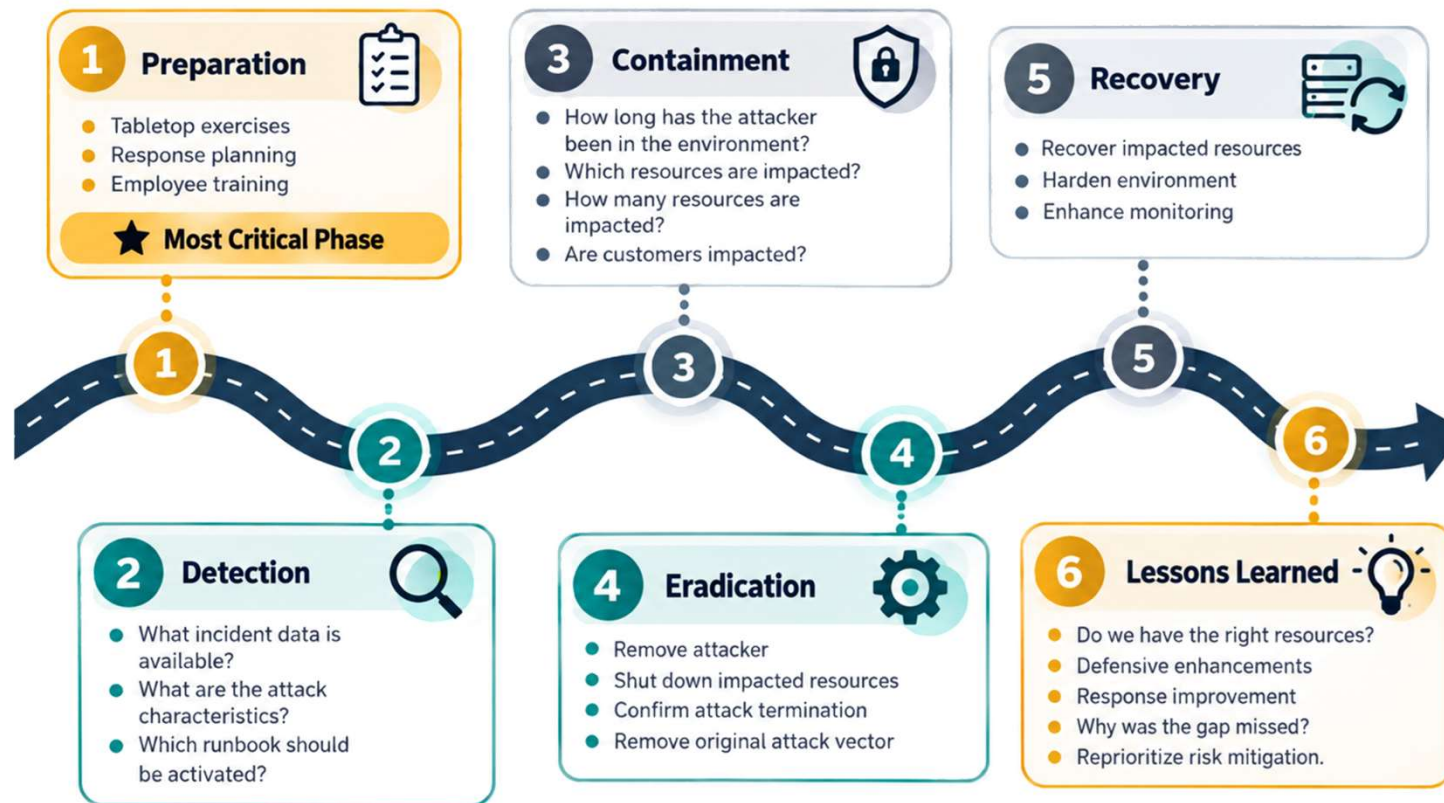
Objectives

- ☒ **Increase** response and recovery **awareness** of the City Council attendees
- ☒ **Self-assess** readiness of tabletop exercise attendees to handle a real-world cybersecurity incident scenario
- ☒ **Improve communication** and readiness should an actual breach be experienced
- ☒ **Identify gaps** in logistics and procedures and **develop** “get well” plans

Assumptions



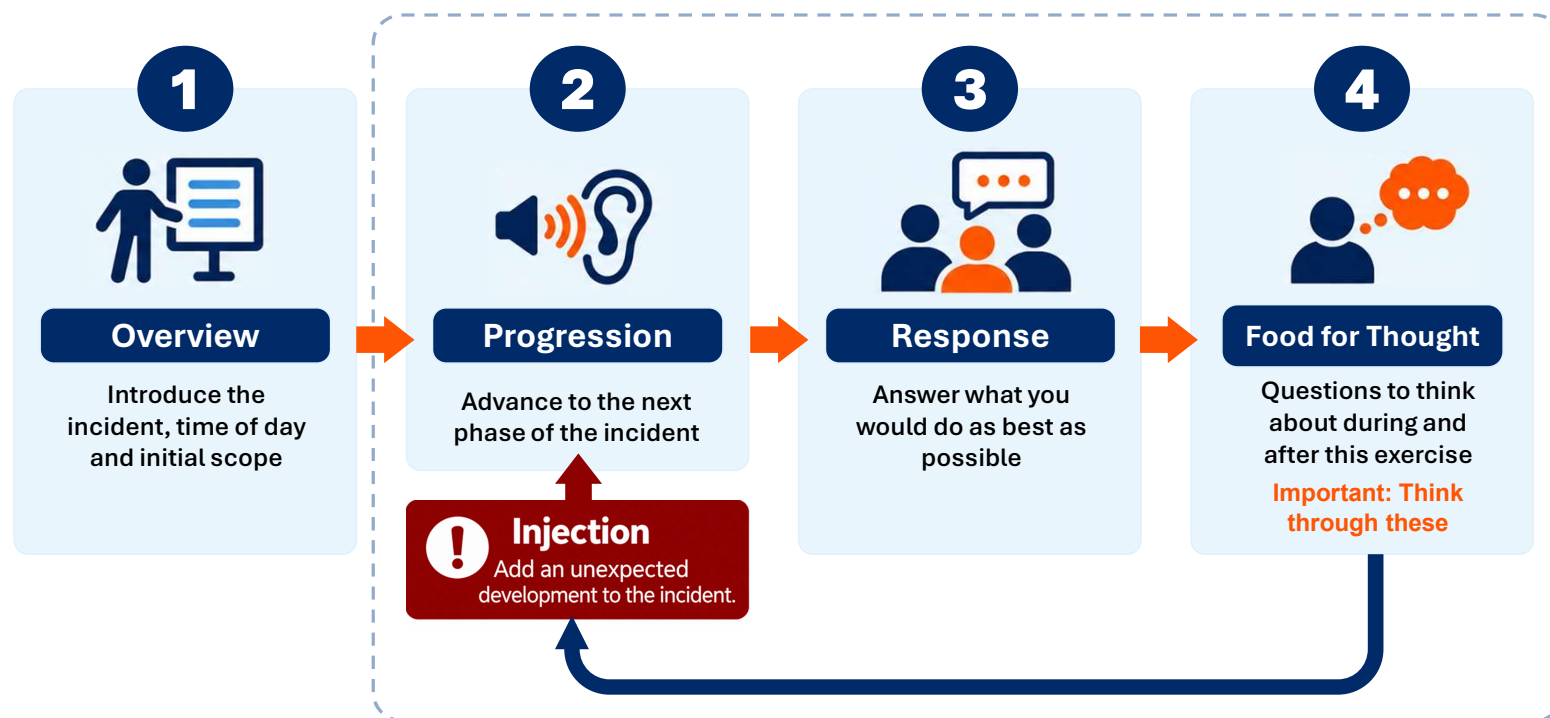
Typical Response Process



Typical (Major) Response Team



Sequence of Events





“

In any moment of decision, the best thing you can do is the **right thing**, the next best thing is the **wrong thing**, and the worst thing you can do is **nothing**

”

- Theodore Roosevelt

Let's Begin!



9:14am Thursday

**A staff member
entered their
credentials**



**How should this
request be verified?**



**What should
happen next?**

Urgent: Briefing materials needed



City Manager

citymanager@city-office.example

To: Councilmember

Councilmember,

I need the confidential briefing packet and your constituent contact list for an urgent meeting. Please upload them through this secure link within the next 20 minutes. I'm in a meeting and cannot take calls.

[Upload briefing materials securely](https://secure-city-files.example/upload)

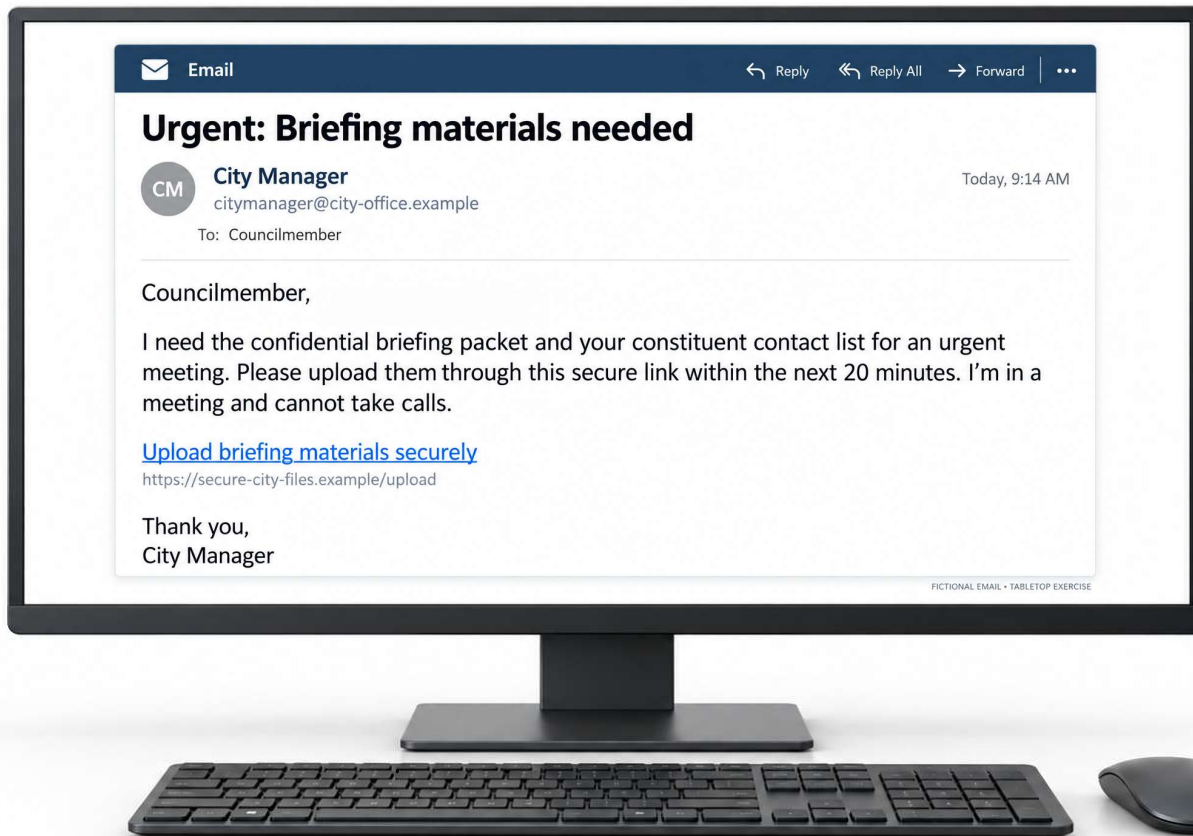
https://secure-city-files.example/upload

Thank you,
City Manager



**Is anything concerning
about this email?**

9:14am Thursday

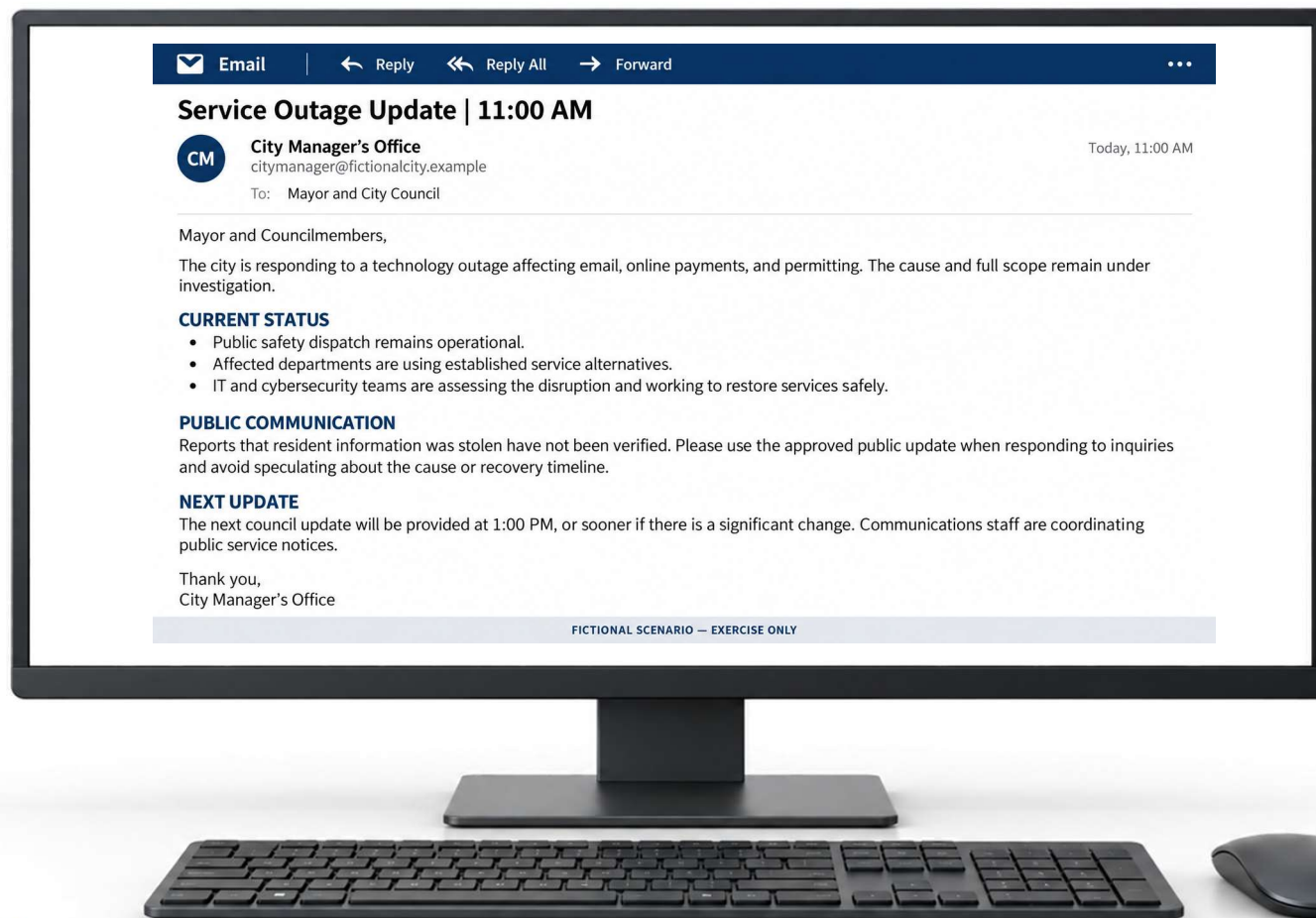



Do you have the email and/or phone number for reporting Cybersecurity emergencies?

Do members of my staff know what to do in the event of a situation like this? If not, what can I do to better prepare them?

What reporting guidance should every elected official have?

11:05am Thursday



12:01pm Thursday

Several city services are unavailable. What is going on?



What steps should council take as a result of this phone call?



What can be responsibly communicated? (At this stage of the incident)

12:01pm Thursday



Has my council been part of a cybersecurity exercise recently?

Does my counsel have its own incident response plan and call tree?

How should I expect to be notified about cybersecurity incidents that could affect my constituents?

1:01pm Thursday



**Does your City already
have a Return to Service
Priority and Plan?**

Email | Reply | Reply All | Forward

Cybersecurity Incident Update | 1:00 PM

City Manager's Office

Today, 1:00 PM

and the systems identified earlier and is now affecting additional criti

aintenance scheduling are disrupted.

affected. Water delivery and treatment remain operational.
onal; some supporting administrative systems are disrupted.

ective measures to contain the attack. Additional systems may be t
edures and prioritizing life safety and essential services. The full sc

ATION

anager's Office when responding to inquiries. Claims that resident
ing public service notices and alternatives.

The next council update will be provided at 3:00 PM, or sooner if there is a significant change.

Thank you,
City Manager's Office

FICTIONAL SCENARIO — EXERCISE ONLY



**Which city services should
take priority during this
outage, and what factors
should determine that order?**

*(i.e. life and safety, basic needs,
resident impact, etc.)*

3:00pm Thursday

We received a claim that resident information was stolen. Care to comment?



What can be responsibly communicated?



What internal questions should be asked to respond to this inquiry?

3:00pm Thursday

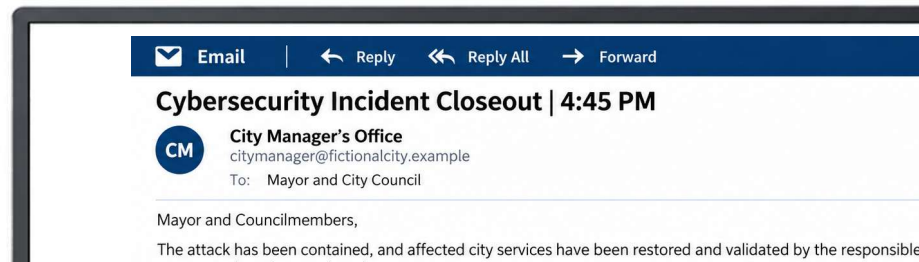



Who should I be coordinating with to respond to media inquiries about an ongoing cybersecurity incident investigation?

What information should a useful council update from the investigations team contain? Do my City colleagues know my expectations? How?

How should I expect to be notified about cybersecurity incidents that could affect my constituents?

4:45pm Thursday



What if the incident continued for several days?



Should council keep track of the incident through remediation?

ting, public works, and utility customer service systems are operational. r delivery and treatment remained operational throughout the incident. layed transactions and addressing service backlogs.

ompleted recovery checks, addressed the identified compromise, and increased monitoring for signs of renewed

exposure continues; no conclusion has been reached. Any requ n review will document lessons learned and corrective actions,

ction report will be provided to council within five business d

FICTIONAL SCENARIO — EXERCISE ONLY



What if there was a demand for the city to pay a ransom?

Suggested Takeaways

- ☒ **Request** to participate in a **tabletop exercise** on a recurring basis with the larger response team
- ☒ **Clarify** the role you are expected (and you expect to play) in response to a major cybersecurity incident
- ☒ **Develop** call trees and **communications plans** with your staff, council members and City leaders
- ☒ **Think through** the “food for thought” questions and take time to **develop** “get well” plans

A grayscale photograph of an audience of people clapping their hands, overlaid with a semi-transparent blue filter. The text 'THANK YOU!' is centered in large white letters.

THANK YOU!



Presented by:

Auston Davis
City Chief Information Security Officer
Cybersecurity Division
City of San Jose