Cybersecurity for Municipalities: A Brief Table Top Exercise

SecureWon

Michelle Stanfield
2/13/2025

Hi. I’m Michelle.

Life-long learner, eternally curious, equity and justice advocate, mom.

Objectives & Outcomes

By the end of our time together participants will:

- understand their roles and the decision-making process during a cybersecurity crisis.
- Highlight the importance of clear communication, pre-established protocols, and backup plans when key contacts are unavailable.
- Evaluate current crisis response procedures through simulated injects to identify potential gaps and areas for improvement.

Scenario Overview

Welcome to Riverbend City!

Date & Time: February 14, 2025, 3:30 PM

Riverbend City is a well-regarded municipality known for its dependable services and strong community engagement. Recently, our city has been navigating significant budget constraints. We've been forced to severely limit overtime, and we urgently need to invest in a new fire truck, as well as address critical upgrades at the high school (new windows and HVAC improvements).

On this February afternoon, senior leadership is suddenly faced with troubling reports that indicate a cybersecurity incident is unfolding—a crisis that will test our decision-making and communication skills from the very start.

Inject #1

At 3:30 PM, municipal leadership in the City Manager's office begins receiving urgent phone calls from several department heads. The calls describe a peculiar email circulating within the city departments. One department reported receiving a message with the subject "Urgent Software Update: Immediate Action Required." Although the email appears to come from the IT Office, subtle irregularities—such as inconsistencies in the sender's details and formatting—raise immediate concerns.

Questions

- What Is your first step In responding to this Information?
- Who should you contact immediately when unusual communications or suspicious emails are reported?
- Is this a cyber incident? Should you activate your CIRT?

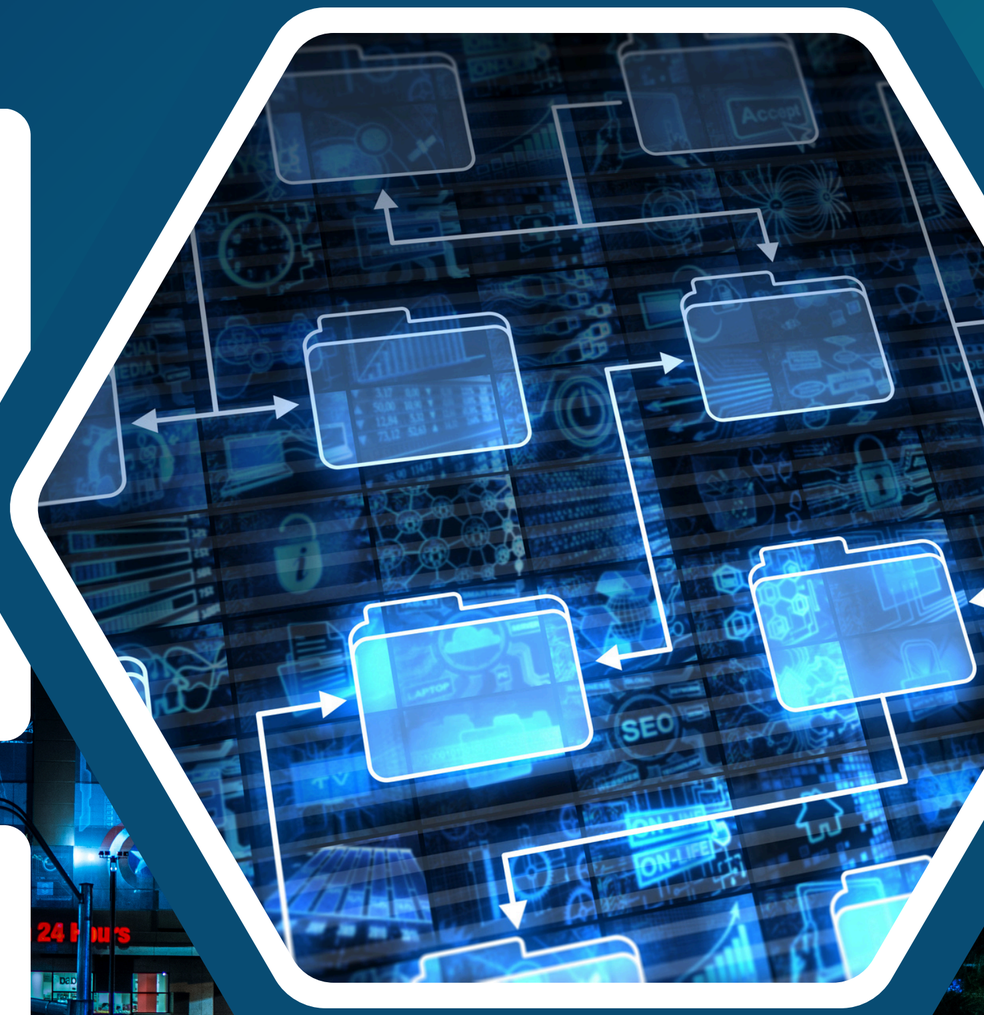
Inject #2

Time: 3:40 PM
Moments after the initial reports, leadership attempts to reach the designated cybersecurity liaison—the person responsible for coordinating the city's digital response. To their surprise, they learn that this key contact is on vacation and unreachable for the next several days. With the primary point of contact unavailable, leaders must quickly decide on an alternative course of action to manage the emerging crisis.

Questions
What contingency plans are in place for situations when the primary cybersecurity liaison is unavailable?
• How do you ensure that all senior leaders are aware of alternative contacts and escalation paths?
• What immediate steps should be taken to designate an interim leader or team to handle the incident?
• How might this unavailability influence your overall crisis management strategy, and what can be done to prevent such gaps in the future?

Inject #3

Time: 3:55 PM
By 3:55 PM, additional reports indicate that an employee in the Public Works Department inadvertently opened the suspicious email's attachment. Instead of a routine software update, her action appears to have triggered unexpected behavior on her computer. While the technical details are being investigated by IT, it becomes clear that this incident may be the entry point for a broader problem affecting multiple city systems, including email and phone systems.



Questions

- What is your immediate priority?
- How do you plan to communicate with fellow members of leadership?
- What does your Incident Response Plan advise, and can you easily access the plan?

Inject #4

At 4:10 PM, the situation escalates. Reports confirm that the incident is now affecting systems that manage essential services. Critical systems—including those responsible for water treatment and emergency response—are under threat as the attackers begin moving within the network. Leadership is informed that the integrity of public safety services is at risk.

Questions

- Which essential services must be prioritized immediately, and what criteria should be used to decide this?
- How will you coordinate with department heads to ensure that critical services remain operational?
- What measures should be in place to protect or isolate vital systems while the incident is being addressed?
- How can municipal leadership prepare to make rapid, high-stakes decisions when public safety is potentially compromised?

Inject #5

Time: 4:25 PM
At 4:25 PM, a dramatic twist occurs: a ransom note appears on several municipal workstations with the message: "Your City's Critical Services Are in Our Hands. Pay 50 Bitcoin within 72 hours or watch your systems go dark." This alarming message is accompanied by confirmation that key data and systems have been locked down. Now, the leadership team faces a high-stakes decision that could affect the future of the city's operations.

Questions

- What internal protocols should be immediately activated when a ransom note is detected?
- How do you rapidly escalate the incident to involve senior leadership and external partners, such as law enforcement?
- What factors must be considered when deciding whether to negotiate with attackers versus relying on pre-established recovery plans?

Inject #6

Time: 4:40 PM

By 4:40 PM, the incident has spilled beyond internal channels. Local media outlets and social media platforms are buzzing with rumors, and worried citizens are calling the City's 311 hotline for information. The municipal spokesperson is preparing to issue a public statement, and leadership must quickly develop a coordinated communication strategy.

Questions

- What are the key messages you need to convey to maintain public trust and prevent panic?
- How should you coordinate with local media and law enforcement to ensure a unified response to the public?
- What communication channels are most effective for updating citizens during a rapidly evolving crisis?
- How can you ensure that the public receives timely and accurate information while internal crisis management is still underway?

Inject #7

Time: 4:55 PM
At 4:55 PM, the recovery team presents two challenging options. One option is to negotiate with the attackers, risking the possibility of setting a precedent for future incidents. The other is to restore systems from backups—a process that may lead to service delays and data loss. Each path carries significant risks, and the leadership team must decide quickly under intense pressure.

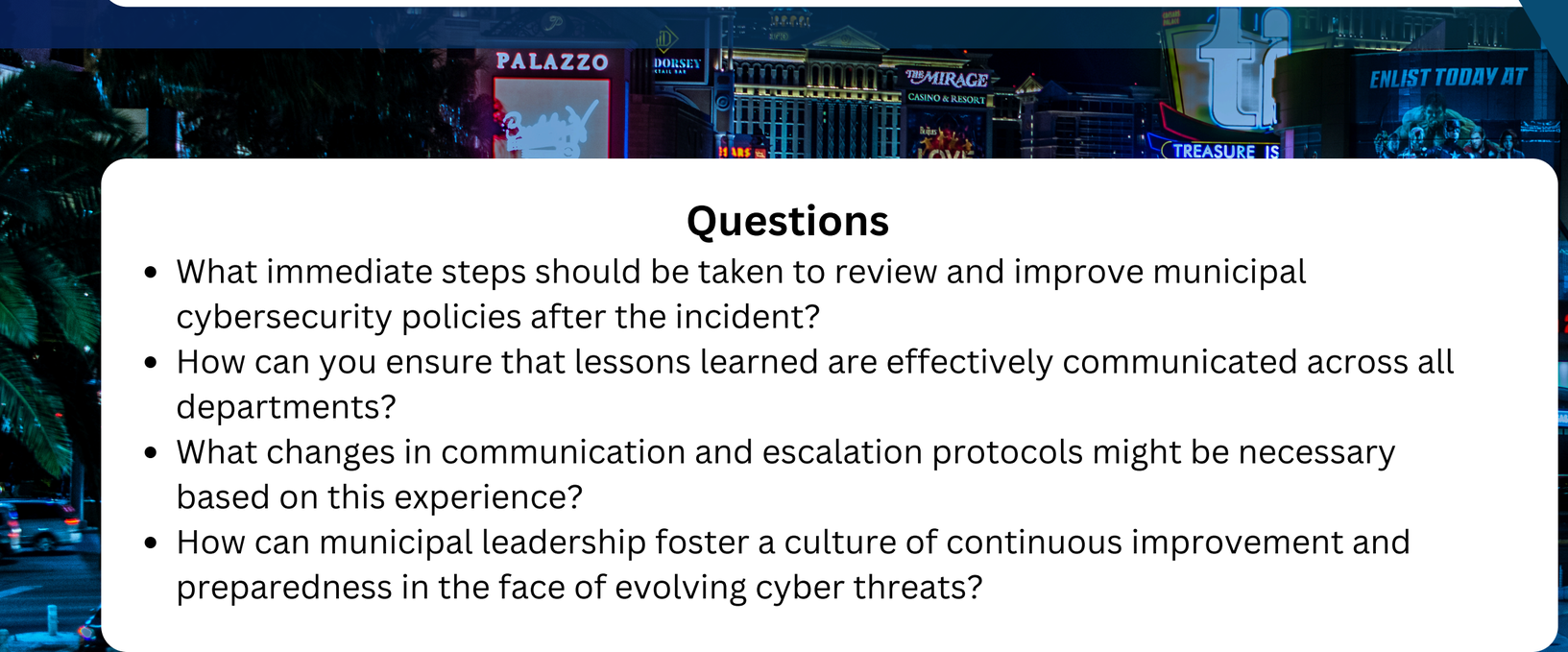
Questions

- What criteria should guide your decision between negotiating with attackers and restoring from backups?
- How do you assess the risks and benefits of each option given the potential impact on municipal services?
- In what ways should your decision be communicated to department heads, staff, and the public?
- How can leadership ensure that this decision is made collaboratively and reflects the long-term interests of the community?

Inject #8

After the immediate threat is contained, the focus shifts to recovery and reflection. In the days following the incident, leadership will coordinate a thorough review of the response, identify lessons learned, and update protocols. This post-incident analysis is essential to strengthen the city's preparedness for future crises.

WHAT'S NEXT?



Questions

- What immediate steps should be taken to review and improve municipal cybersecurity policies after the incident?
- How can you ensure that lessons learned are effectively communicated across all departments?
- What changes in communication and escalation protocols might be necessary based on this experience?
- How can municipal leadership foster a culture of continuous improvement and preparedness in the face of evolving cyber threats?

Share Out

- Key takeaways
- Shout outs

Thank You!

Michelle Stanfield
mstanfieldadams@gmail.com
stanfieldm@bridgew.edu
LinkedIn: michellestanfield

Cybersecurity Strategy

- Risk Assessment
- Employee Education and Training
- Use of Security Software
- Incident Response Plan