

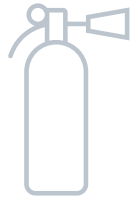


BAY AREA UASI CYBER BRIDGE 2026 Tabletop Exercise

Welcome to today's exercise, we will get started soon.



ADMINISTRATIVE REMARKS



Safety
information



Restrooms



Food / Drinks



Breaks and lunch



Microphones



WIFI

HOST WELCOME MESSAGE



CONTRA COSTA

COUNTY, CALIFORNIA





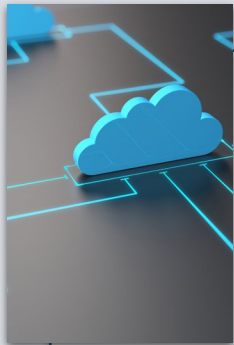
EXERCISE SCHEDULE

Time	Activity
9:30 AM - 10:00 AM	Welcome and Exercise Overview
10:00 AM - 11:00 AM	Module 1-Early Indicators
11:00 AM - 12:00 PM	Module 2-Emerging Regional Impacts
12:00 PM - 1:00 PM	Break/Lunch
1:00 PM - 2:00 PM	Module 3-Information Integrity Crisis
2:00 PM - 2:45 PM	Hot Wash
2:45 PM - 3:00 PM	Closing Comments/Adjourn

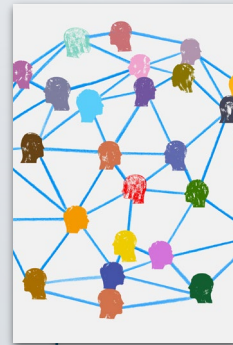


EXERCISE PURPOSE

Cyber Bridge 2026 will evaluate the region's ability to:



Share information
across jurisdictions



Maintain a common
operating picture



Make coordinated
operational decisions



Respond to cascading
cyber impacts

OBJECTIVE #1

Assess the ability of participating jurisdictions and regional stakeholders to identify, validate, and share cyber threat intelligence, indicators of compromise, and situational awareness information across agencies within established coordination processes during an escalating AI-enabled cyber incident affecting multiple Bay Area jurisdictions.

- *Core Capability: Intelligence and Information Sharing*





OBJECTIVE #2

Evaluate the ability of participating organizations to coordinate regional operational response actions, including executive notifications, resource prioritization, cross-jurisdiction coordination, and decision-making processes, in response to cascading cyber impacts affecting critical services, infrastructure, and public operations.

- *Core Capability: Operational Coordination*



OBJECTIVE #3

Evaluate the ability of participating organizations to implement internal and external communications procedures, including leadership notifications, interagency coordination, mission partner engagement, and public information considerations, during a rapidly evolving cyber incident involving AI-enabled threats and operational disruptions.

- *Core Capability: Operational Communications*

OBJECTIVE #4

Assess the ability of participating jurisdictions and regional partners to analyze and implement cybersecurity response, continuity, and recovery actions aligned with the NIST Cybersecurity Framework functions of Identify, Protect, Detect, Respond, and Recover during a coordinated cyberattack targeting regional systems, infrastructure, and public services.

- *Core Capability: Cybersecurity*



EXERCISE GUIDELINES



This is an open no-fault environment. Varying viewpoints are expected and open discussion is encouraged.



Base your responses on the existing plans and capabilities of your agency, organization or group.

EXERCISE GUIDELINES



Decisions are not precedent setting; consider different approaches and suggest improvements.



Issue identification is not as valuable as suggestions and recommended actions that could improve regional coordination.

EXERCISE ROLES

Facilitators

Evaluators

Support
Staff

Players

Observers





EXERCISE DOCUMENTATION

- Exercise materials are available digitally.
- During check-in you were sent an email with a link to an exercise page for you.
 - *Check your junk folder if you did not get it.*
 - *There is also a link to that page in the printed Sitman.*
- On that webpage you can find the following documents:
 - Situation Manual (Sitman).
 - Scenario Inject Cards.
 - Pre-Exercise read-ahead materials.



EXERCISE INSTRUCTIONS

- Facilitators will deliver scenario cards and video injects; you can also find them on DrillDeck through the link.
- The exercise room has been divided into county groups and regional "pods" to promote neighbor-to-neighbor discussions.
- You are encouraged to discuss issues and impacts with your neighboring or similarly impacted groups.



EXERCISE INSTRUCTIONS

- Collecting information from all players is a critical component of the exercise.
- Each group should identify a data entry player; you can rotate this position if you wish.
- Data entry is VERY subjective; don't stress over details about the nature of the cyber incidents, it might change overtime.

ArcGIS Survey123



- We are using Survey123 as a data collection tool for exercise play.
- The data entered by each county group can be viewed via the live dashboard during the exercise and will be captured afterward for follow-up.
- Links to both the survey and the dashboard are in the Sitman.



Display Dashboard



Bay Area Cyber Incidents

Filter

Region
South

☐ Select all

☐ East

☐ North

☒ South

☐ West

Counties
No data

Select a Day
No day selected

Total Incidents
 8

Jurisdictions Affected
 5

Latest Incidents

36 : San Jose Denial of Service / Service Disruption

34 : San Benito County Website Defacement / Web Spoofing

32 : San Jose Denial of Service / Service Disruption

31 : Monterey County Operational Technology / ICS / SCADA Disruption

28 : Santa Clara County Fraud / Payment Redirection

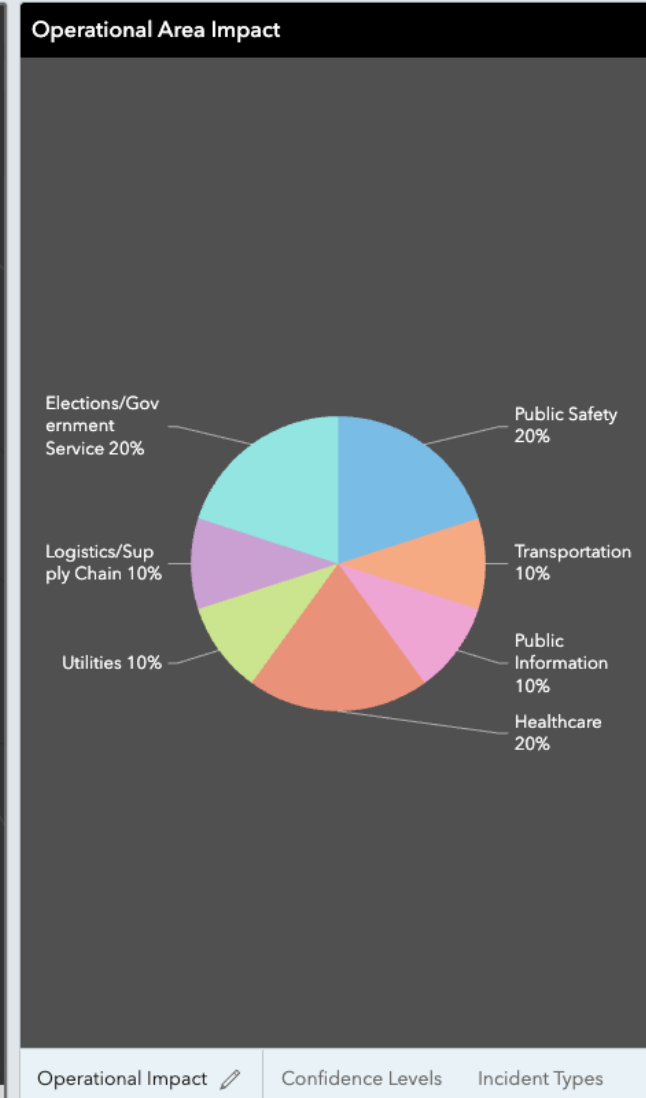
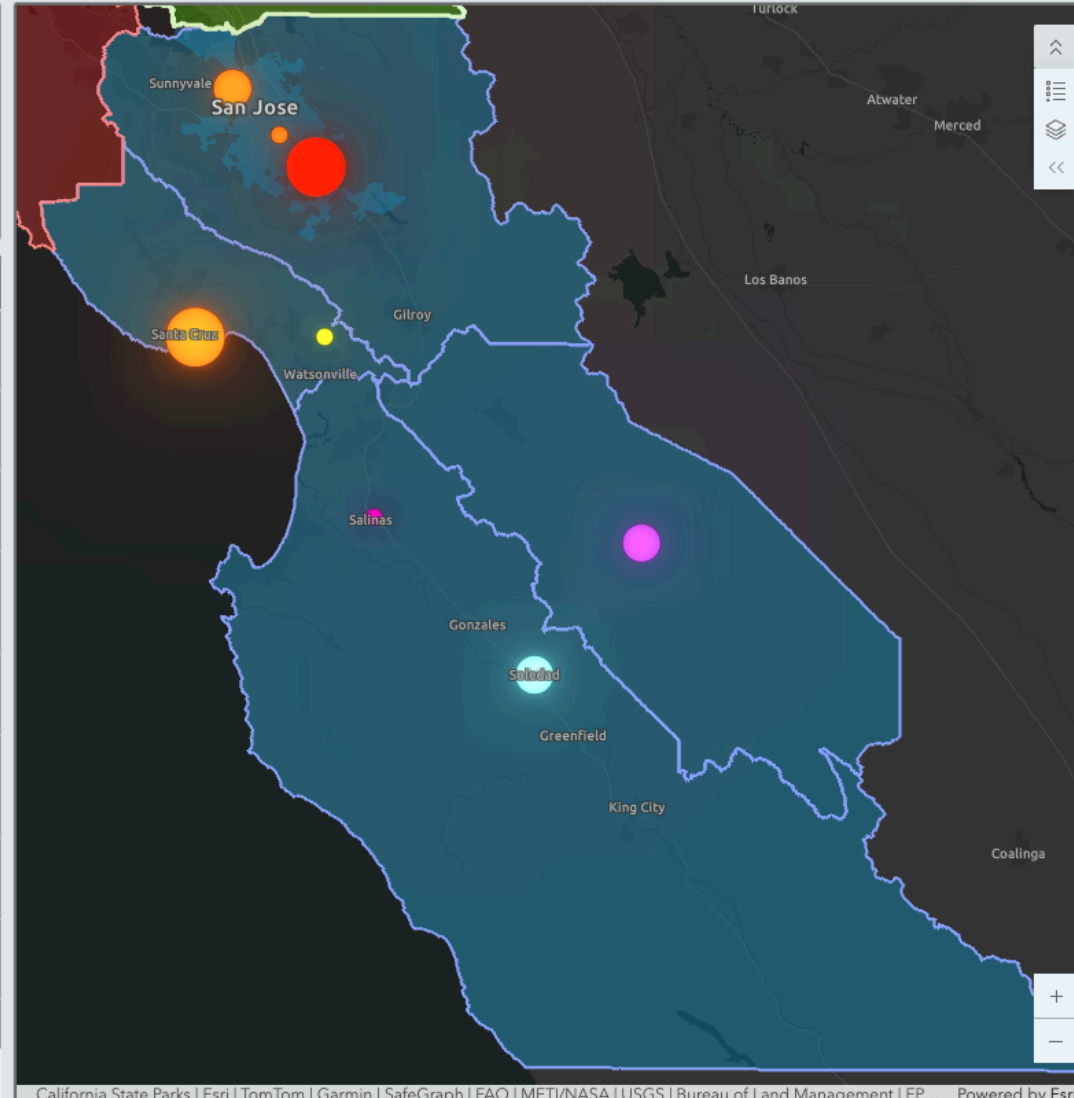
26 : Monterey County Business Email / Communications Compromise

24 : Santa Cruz County Denial of Service / Service Disruption

18 : San Jose Credential Harvesting / Phishing

Incidents

Details





IMPORTANT SURVEY123 FIELDS



Operational Impact Areas



Impact Severity



Action Taken



Resource Requests

QUESTIONS

Are there any questions
before we get started?





STARTEX





SCENARIO BACKGROUND

Tensions have been increasing between the United States and China following American restrictions on semiconductor exports, advanced computing technologies, and artificial intelligence systems.

A Chinese government-sponsored cyber group, **APT Dragon Typhoon**, has quietly embedded itself within Bay Area government and industry networks.





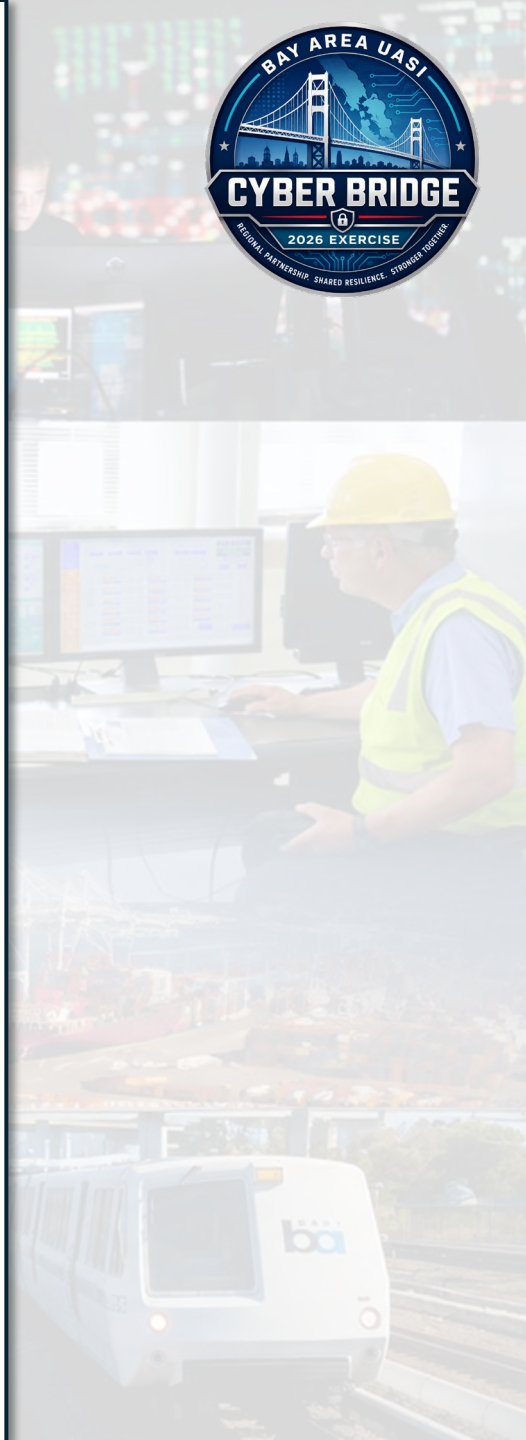
SCENARIO BACKGROUND

APT Dragon Typhoon seeks multiple goals against the United States:

- Demonstrate U.S. IT systems vulnerabilities
- Undermine public cybersecurity confidence
- Create political pressure and influence
- Gather intelligence to steal models and advancements
- Leverage and exploit AI as a force multiplier







VIDEO INJECT #1





MODULE 1 – EARLY INDICATORS



The items presented in the first grouping occurred in the days and weeks prior to today.



Location-specific scenario updates will now be provided to you by your facilitators.



The Situation Manual has some group discussion questions for Module 1 on page 10.



MODULE 1 – GROUP DISCUSSIONS



Spend the next 10-15 minutes discussing the situation and module discussion questions.



Group facilitators will be available to guide you if necessary.

MODULE 1 – POD DISCUSSIONS



With your POD groups,
discuss the current
situational impacts you are
dealing with.



Discuss any issues that
might have regional
impacts and how they can
be coordinated together.

MODULE 1 – DAY 1 UPDATE

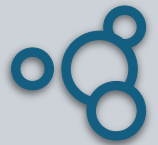


Group facilitators will provide a scenario update when your groups are ready.



Discuss the module 1 questions with the updated scenario information presented.

MODULE 1 – POD REPORTS



North Bay



South Bay



East Bay



West Bay





10 MINUTE BREAK





MODULE 2



VIDEO INJECT #2



PACIFIC REPORT

REGIONAL IMPACT

Food Supply Critical as Cyberattacks Disrupt Ports, Farms and Assistance Programs



THE BAY CHRONICLE

PUBLIC SAFETY

False Evacuation Orders and



COMMUTE CRISIS

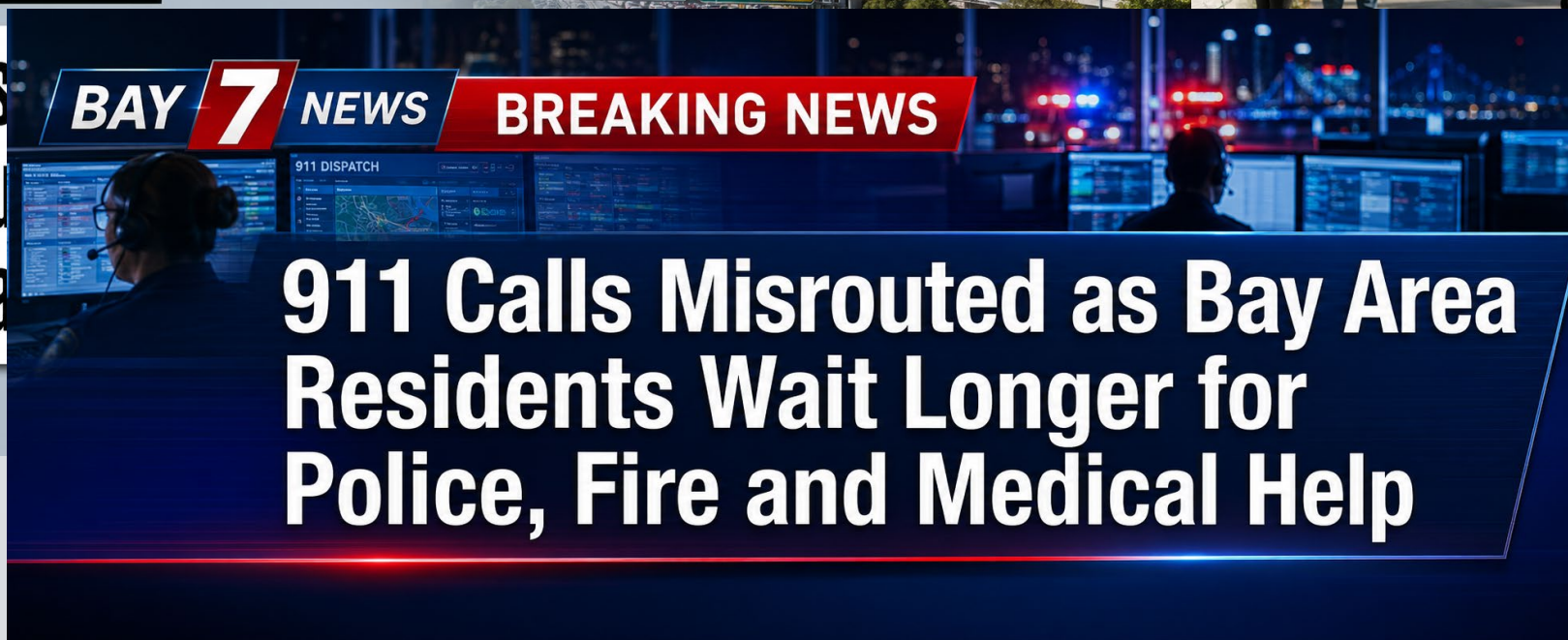
**METRO
NOW**

Trans
Detour
Spread

BAY 7 NEWS

BREAKING NEWS

**911 Calls Misrouted as Bay Area
Residents Wait Longer for
Police, Fire and Medical Help**





MODULE 2 – REGIONAL IMPACTS



Facilitators will present your group with the Day 3 scenario update.



Discuss among your groups and review the Module 2 discussion questions.



Enter all updated impacts and resource needs into Survey123



MODULE 2 – DAY 5 UPDATE



Facilitators will provide your groups with Day 5 scenario updates.



Continue to discuss this update with your group.



Remember to update your Survey123 with any additional issues or impacted locations.



LUNCH BREAK

VIDEO INJECT – Deep Fake

- Play BART Disruption video
- Play Contra Costa Cyber-AI incident video





MODULE 3



BREAKING NEWS

**BAY AREA'S DIGITAL BREAKDOWN REACHES DAY SEVEN,
DISRUPTING NEARLY EVERY PART OF DAILY LIFE LINES**



BREAKING NEWS

**FROM EMPTY SHELVES TO STOLEN IDENTITIES,
PROLONGED CYBERATTACK TAKES GROWING TOLL ON BAY AREA FAMILIES**

BREAKING NEWS

**CYBER CRISIS THREATENS EMERGENCY CARE AS 911 CENTERS
AND HOSPITALS STRUGGLE THROUGH A SECOND WEEK**

BREAKING NEWS

**BAY AREA COMMUTE GRINDS TO A HALT AS
DIGITAL SABOTAGE STRANDS DRIVERS AND TRANSIT RIDERS**

BREAKING NEWS

**"WE DON'T KNOW WHAT TO TRUST": FALSE ALERTS AND OFFICIAL
OUTAGES LEAVE MILLIONS WITHOUT RELIABLE INFORMATION**



MODULE 3 – DAY 7 UPDATE



Facilitators will provide your groups with Day 7 scenario updates.



Discuss the Module 3 questions with your groups.



Update Survey123 as needed.

MODULE 3 – DAY 12 UPDATE



Facilitators will provide your groups with the day 12 scenario updates.



Update Survey123 as needed.

VIDEO INJECT #3





INDEX



Group Hotwash



Strengths

Areas for
Improvement

Closing Comments & Remarks



**CONTRA
COSTA**

COUNTY, CALIFORNIA



*Thank
you!*

