Module 3

September 1, 2023 [Fair Day 8 – Evening]

During a high-profile evening concert, anyone who has downloaded the Champlain Valley Fair smartphone app receives an urgent notification warning of an active shooter in the area. The notification asks everyone to evacuate the premises immediately.

Chaos erupts as word quickly spreads through the crowd. Many begin to panic while searching for exits causing several injuries in their attempt to leave the area.

September 1, 2023 [Fair Day 8 – Continued]

Local media at the fairgrounds begin breaking live news coverage of the incident. Users that were not currently at the fair post screenshots of the notification they received from the app on social media to spread the word.

911 operators receive an influx of callers reporting the active shooter notification they received on their phones. The system quicky becomes overwhelmed as well as cell towers in the area.

September 1, 2023 [Fair Day 8 – Continued]

Law enforcement begins to clear the area and search for an active shooter. Later, the Champlain Valley Fair Marketing Team notifies law enforcement that the smartphone app had been hacked and the active shooter notification was fake. Initial triage indicates 10 casualties and one fatality.

Local media covering the incident are now requesting statements from local law enforcement and Champlain Valley Expo staff at the fairgrounds.

Discussion Questions

1. What are your organization's priorities during this scenario?
   a. How would the false active shooter notification and medical emergencies be managed?
2. How do you manage communications at the Champlain Valley Expo during an incident?
   a. Who would be involved in coordinating messaging?
   b. What information are you sharing internally? (e.g., staff, leadership, volunteers)
   c. What information are you sharing externally? (e.g., law enforcement, public)
3. What additional resources would be required to respond to this scenario?
   a. What is the process for requesting additional resources from the state and/or federal partners?
4. How would you coordinate emergency response if 911 call centers were unavailable?
   a. What backup systems and processes are in place for these incidents?
   b. What are your additional concerns with the overwhelmed 911 system?
5. Discuss if there would be any consideration of the false notification being a cyber incident.
6. Describe your organization's after-action/lessons learned processes for cyber and/or physical incidents.

Please complete the feedback form using the QR code or entering the following link into your phone, tablet, or laptop browser: https://forms.office.com/g/XYLdgRkaGd

For more information about the National Cyber Exercise Program, please contact: CEP@HQ.DHS.GOV

TLP:AMBER

Champlain Valley Exposition Tabletop Exercise

August 15, 2023

Exercise Purpose:

Identify best practices and areas for improvement in incident planning, identification, and response to a significant incident with cyber and physical security impacts.

Objectives:

1. Assess preparedness to mitigate and respond to cyber and physical security incidents impacting events held at the Champlain Valley Exposition.
2. Examine the policies and procedures of cyber and physical incident response plans.
3. Discuss internal and external communication processes and plans to address cyber and physical security incidents that may impact events at the Champlain Valley Exposition.
4. Examine overall organizational information sharing processes and cybersecurity posture.
5. Raise awareness to the complex dependencies and challenges within crisis management.

TLP:AMBER

Module 1

August 18, 2023 [7 Days Before The Fair]

The Cybersecurity & Infrastructure Security Agency (CISA) releases an advisory regarding Distributed Denial of Service (DDoS) attacks targeting State, Local, Tribal, and Territorial (SLTT) government networks. Recent activity by known cyber threat actors indicate additional planned attacks targeting major entertainment events in the United States including concerts, sporting events, and seasonal fairs.

August 20, 2023 [5 Days Before The Fair]

CISA and the Federal Bureau of Investigation (FBI) release and joint advisory warning that a cyber-criminal group is targeting organizations hosting large events. Threat actors conduct sophisticated phishing campaigns via email to infect networks with malware. The emails contain a malicious attachment or link that installs malware on a user's machine without their knowledge when opened.

August 21, 2023 [4 Days Before The Fair]

Employees of the City of Essex Junction and the Town of Essex, receive an email from the Champlain Valley Fair offering two free tickets to local government workers as a thank you for their service to the community.

The email includes a link to a virtual form for the tickets where users are asked to enter their name, email address, and phone number. Several employees from various local organizations complete the form to receive tickets.

August 22, 2023 [3 Days Before The Fair]

A fiber optics line was accidentally cut during a construction project in Essex Junction causing internet outages at Government Offices, Law Enforcement, and Emergency Services. With the loss of internet, emergency service locations quickly become overwhelmed.

August 23, 2023 [2 Days Before The Fair]

The IT Help Desk receives several reports from City of Essex Junction and the Town of Essex employees regarding network latency with their workstations. The latency does not have a major impact on daily operations.

Discussion Questions

1. What is the greatest cybersecurity threat to your organization?
2. What were the results of cyber risk assessment(s) your organization has conducted to identify threats and vulnerabilities?
3. What types of cyber threat information/alerts does your organization receive?
   a. Who is responsible for receiving and disseminating this information?
   b. What actions would your organization take based on the alerts presented in the scenario?
   c. What cybersecurity threat information does your organization share externally? (e.g., state, federal, vendors, etc.)
4. How would your organization's employees report suspected phishing attempts or other cybersecurity incidents?
   a. What actions does your IT Department take when suspicious emails are reported?
   b. What are some of the challenges your organization encounters with phishing?
   c. How effective are your methods to protect against phishing?
5. Describe your organization's cybersecurity training program for employees.
   a. How often are employees required to complete this training?
   b. What are the ramifications for incomplete cybersecurity training?
   c. What additional training is required for employees/vendors with system-level software access?
6. What actions would be taken in response to the internet outage?
   a. What policies/plans define these actions?
   b. Which external agencies would need to be notified about the internet outage?
   c. How would an outage impact the services your department provides?
7. What actions would the IT Help Desk take after receiving several reports of network latency?
   a. What is the threshold of similar issues being reported that would require further investigation?

TLP:AMBER

Module 2

August 24, 2023 [1 Day Before the Fair]

The City of Essex Junction and Town of Essex websites are altered without IT's authorization. Logos have been modified in color and/or flipped, and listed contact details (e.g., phone numbers, email addresses, etc.) have been changed.

Unauthorized changes also occur on the Champlain Valley Fair website. Upcoming event information and times for the Fair are incorrect and parking information has been altered.

August 24, 2023 [1 Day Before the Fair – Evening]

A well-known hacktivist group makes posts on the dark web about the Champlain Valley Fair. A security researcher informs your organization of these posts claiming the group is planning a wide-spread attack during the Fair.

August 25, 2023 [Fair Day 1 – 7:30 a.m.]

911 receives several calls reporting car accidents at multiple intersections in the City of Essex Junction and Town of Essex. When police officers respond to the scenes, they notice all the traffic lights are displaying green lights. Upon further investigation, several police officers report seeing a flashing USB device plugged into the traffic light's control panel at the scene of their accident.

August 25, 2023 [Fair Day 1 – Morning]

The Champlain Valley Expo begins to receive phone calls from customers who claim they are not able to purchase tickets through the website. After submitting their payment information, the page states there was an error with completing their purchase. However, customers claim their cards were still charged for the tickets even though they never received them.

After an investigation, it is discovered that valid tickets were issued but were sent to a different email address than the ones entered by the customers.

August 25, 2023 [Fair Day 1 – Opening]

Champlain Valley Fair staff report attendees are having a difficult time navigating with the smartphone app and the daily event schedule is not loading. Many staff assume this issue is due to the overwhelming number of people using the app at once.

August 25, 2023 [Fair Day 1 – Afternoon]

Towards the end of the workday, employee computers at the City of Essex Junction and Town of Essex lock-up and display a ransom note. The note demands $100,000 dollars in Bitcoin be paid in the next 24-hours or "chaos will be unleashed." This same ransomware is also discovered on local onsite backups.

Discussion Questions

1. What actions would your organization take in response to the website defacement?
   a. What plans or processes do you have to communicate to the public when primary sources of information are compromised?
   b. What backup systems for websites are available and how quickly can they be deployed?
2. At what point in the scenario would you activate your Cyber Incident Response Plan (CIRP)?
   a. Discuss your notification processes following activation of your CIRP.
   b. What other plans would be activated based on the scenario?
3. How would your organization respond to the security researcher's notification of threats against the Champlain Valley Fair?
4. What actions would your origination take based on customer reports of ticketing issues on the Champlain Valley Fair site?
   a. What internal and/or external notifications would need to be made?
5. What would be done to address the malfunctioning traffic lights?
   a. What additional resources would be needed to direct traffic at multiple intersections and manage wide-spread vehicle accidents?
   b. What further investigation would be conducted on the USB devices?
6. How would Champlain Valley Expo staff respond to the issues with the smartphone app?
7. Describe your organization's decision-making process for ransomware payment.
   a. What discussions have your organizational leadership had regarding ransomware?
   b. How are your cyber insurance providers involved in your response procedures?
   c. What are the advantages/disadvantages to agreeing/refusing to pay?
   d. What are the potential legal and reputational ramifications?
8. What business continuity concerns would your organization have at this point? (e.g., City, Junction, Town, Fair operations)

TLP:AMBER