

**CISA Tabletop Exercise Package Emergency Services**

[Enter Organization Name]

<Exercise Date>

Updated January 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc170301704)

[Exercise Overview 5](#_Toc170301710)

[General Information 6](#_Toc170301711)

[Module 1 9](#_Toc170301712)

[Module 2 11](#_Toc170301713)

[Appendix A: Additional Discussion Questions 13](#_Toc170301714)

[Appendix B: Acronyms 16](#_Toc170301715)

[Appendix C: Case Studies 17](#_Toc170301716)

[Appendix D: Attacks and Threats 18](#_Toc170301717)

[Appendix E: Contacts and Resources 19](#_Toc170301718)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world; there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):GREEN*”: Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

# 

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | Examine the cyber resilience of <emergency services sector organization> in response to a significant cyber incident impacting the emergency services sector. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess the cyber resilience of <emergency services sector organization> before, during, and following a cyber incident impacting emergency services. 2. Review plans, procedures, roles, responsibilities, and capabilities for responding to a cyber incident. 3. Discuss coordination and collaboration across the <emergency services sector organization>. | |
| Threat or Hazard | Cyber Incident | |
| Scenario | A cyber threat actor targets personnel through a phishing email as an entry point into networks/systems, later compromising devices and data using malware. The communications call center also experiences a Telephony Denial of Service (TDoS) attack. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact (POC) | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov)  **Emergency Services**  **Sector Risk Management Agency**  EmergencyServicesSector@cisa.dhs.gov | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

## Using this Situation Manual

This Situation Manual provides a scenario and accompanying discussion questions designed to identify strengths and areas for improvement, including understanding of plans, policies, and procedures. This Situation Manual is intended to be adaptable and editable.

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. The footnotes throughout the modules contain corresponding resources to guide your preparedness efforts, including the CISA Cross-Sector Cybersecurity Performance Goals (CPG). The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An explanation of the threats presented in this scenario.
* Appendix E: Additional cybersecurity preparedness and response resources.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include IT/information security personnel, Emergency Communications Center (ECC)/Public Safety Answering Point (PSAP)/9-1-1 Call Center, law enforcement, fire and rescue, emergency medical services, emergency management, and public works personnel with a role in incident response.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include senior-level leadership and IT/information security personnel, ECC/PSAP/9-1-1 Call Center, law enforcement, fire and rescue, emergency medical services, emergency management, public works, human resources, and legal personnel who do not have a role in incident response.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

**Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces a TDoS attack against a neighboring locality and a possible phishing attempt against your personnel.
  + **Module 2:** This module continues the scenario with a TDoS attack against your communications center, malware, and media inquiries into the impacts of the attacks on operations.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions. The hotwash is held at the end of the exercise discussion. The hotwash is designed to provide an opportunity to discuss strengths and areas for improvement immediately following the conduct of an exercise.[[2]](#footnote-3)

# Module 1

### Day 1

A nearby locality recently suffered a TDoS attack against their ECC/PSAP/9-1-1 call center. The tactics, techniques, and procedures (TTPs) demonstrated in the attack are similar to those detailed in an MS-ISAC alert released two weeks ago and forwarded to you from your [CISA Emergency Communications Coordinator/Statewide Interoperability Coordinator/National Association of State 9-1-1 Administrators]. The alert detailed an increase in malicious actors seeking to disrupt emergency communications systems.[[3]](#footnote-4);[[4]](#footnote-5) Malicious actors use artificial intelligence (AI) and robocall systems to execute a TDoS attack, hindering ECC/PSAP/9-1-1 call center services. The TDoS is used as a distraction mechanism for secondary attacks, with the end goal of accessing computer aided dispatch systems.

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What are the greatest cyber threats to your organization?
   1. What concerns do you have regarding potential threats posed by Artificial Intelligence (AI)?
   2. How would a cyber event at a neighboring PSAP impact you?
2. What cybersecurity threat information does your organization receive (e.g., information from CISA, Federal Bureau of Investigation, Fusion Center, MS-ISAC)?
   1. What cyber threat information is most useful?
   2. How is information disseminated throughout your organization and by whom?
   3. What actions would your organization take in response to an alert like the one presented in the scenario?
3. Are members of the PSAP registered users of Government Emergency Telecommunications Service (GETS)/Wireless Priority Service (WPS) to ensure they have the level of priority needed to communicate during an incident?

### Day 11

Employees across your organization receive an email from your human resources (HR) office requesting employees click a link to confirm or update their direct deposit data. Some employees click the link, provide their login credentials, and are met with a 404 – error screen. Other employees report the email as suspicious.[[5]](#footnote-6)

### Day 12

Employees who attempted to perform the HR task contact the help desk stating they are unable to log into their computers. The help desk resets user passwords for several employees, who are then able to access their computers.

1. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?[[6]](#footnote-7)
   1. What information technology (IT) systems or processes are the most critical to your organization?
   2. Describe your organization’s asset management plan and how you prioritize critical assets.
   3. What improvements were implemented to enhance cyber resilience following recent risk assessments?
   4. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
2. Describe your organization’s cybersecurity training program for employees.
3. How often are employees required to complete this training?
4. What additional training is required for employees who have system administrator-level privileges?
5. What type of training methods or approaches have you found most beneficial?
6. How are employees trained to recognize and report cyber threats such as phishing scams?
7. What additional training does your organization require for those who fall for a fake phishing campaign?
8. How do users report suspicious emails?
9. What procedures or plans would be followed once a suspicious email is reported?
10. Describe your organization’s cybersecurity posture.
11. How frequently are users required to change their passwords?
12. Does your organization use multi-factor authentication (e.g., something you know, something you have, something you are) to mitigate the potential effects of phishing?
13. What are your network access and authentication controls for users?[[7]](#footnote-8)
14. Does your organization allow users to run document macros? If so, what compensating security controls do you have to mitigate the risk?
15. What cybersecurity controls are present to mitigate the risk of users entering credentials into phishing websites?
16. How is your network segmented/configured to protect yourself from the threats described?

# Module 2

### Day 14 – 1:00 a.m.

ECC/PSAP/9-1-1 telecommunicators are inundated with calls. Most are recorded voices mentioning used car warranties, however there are also citizens reporting emergencies who state they had to call numerous times as they keep getting an “all-circuits busy” message.

Later, call volume suddenly returns to normal for this time of day.

### Day 25 – 7:30 a.m.

ECC/PSAP/9-1-1 call takers are busy taking calls at the communications center when all computers enter a reboot sequence. Once they reboot, all screens turn red and then shut down. Users are unable to reboot them.[[8]](#footnote-9)

### Day 25 – 7:35 a.m.

The communications center receives calls from area law enforcement, fire departments and emergency medical services stating they are locked out of their systems.[[9]](#footnote-10)

### Day 26 – 7:00 a.m.

ECC/PSAP/9-1-1 volume is so high that legitimate calls are not getting through. Citizens show up at local fire and police stations reporting fires and accidents, and demanding help because they can’t reach 9-1-1.[[10]](#footnote-11)

### Day 26 – 8:30 a.m.

Local news reports the issues with local emergency lines. The public is demanding to know when services will be back to normal.

## Discussion Questions

1. Using your organization’s existing incident response plan/cyber incident response plan (CIRP), describe the actions your organization would take at this time.
   1. Describe the training your employees receive on this plan.
   2. What guidance does the plan include on assessing the severity of an incident?
   3. How does incident severity level dictate response?
   4. How are critical systems and processes incorporated within your CIRP?
2. What essential functions are impacted by the incidents described in the scenario?
3. What backup or redundant systems exist for when primary systems are compromised?
4. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
5. Who can authorize use of backup systems or manual procedures?
6. How long can you perform manual or alternate processes?
7. What additional resources are required to operate with manual processes?
8. Does your organization have backups of call logs, vital maps and call voice recordings stored in a location separate from your primary working files/copies?[[11]](#footnote-12)
   1. How frequently do you run backups?
   2. How long do you keep copies of archived files backed up?
   3. How long would it take to restore primary files from backups and has this been tested?
9. Do you employ a TDoS mitigation solution?
10. What additional resources outside of <local government> are necessary for responding to the cyber incident?
11. What procedures does your organization have to supplement staffing?
    1. Do you have any agreements with other Emergency Communications Centers/PSAPs to provide backup call capabilities?
12. What are the processes or procedures for requesting additional resources and are these documented in your incident response plan?
13. Would these incidents trigger the activation of the Emergency Operations Center (EOC)?
14. Describe your crisis communication plan.
    1. If primary communications are compromised, how do you provide information to internal and external entities?
15. Describe your organizational processes to respond to the media reports and inquiries.
    1. What pre-scripted messages have been developed for cyber incidents?
    2. How is public messaging coordinated and disseminated during a cyber incident?
    3. How would you preserve and reinforce the public’s confidence and trust in your organization during a significant cyber incident?
    4. What are the short term and long-term challenges you expect to face?
16. Based on discussion, what changes would you implement to increase the resilience of your organization?

# 

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Questions are aligned with the NIST functional areas and organizational roles and responsibilities. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. *This instructional paragraph, as well as undesired discussion questions, should be deleted.*

## Cyber Resilience

1. Discuss how cyber preparedness is integrated with your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
3. Discuss your risk management strategy.
4. How is it developed/maintained?
5. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
6. Describe your organization’s review process for your cyber incident response plan (CIRP).
7. How is your CIRP integrated with other incident or emergency response/management plans?
8. How often is the CIRP reviewed?
9. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
10. How are updates to the plan communicated to department or agency employees?
11. What cybersecurity language is included within third-party vendor contracts?
12. How do you evaluate the cybersecurity posture of your vendors?
13. How often are contracts reviewed?
14. How do your service level agreements address cyber incident notification?
15. How is the integrity of your critical data protected and validated?
16. What external entities have access to your data?
17. How would those entities report a breach of their systems to your office?
18. What essential functions are impacted by the incidents described in the scenario?
19. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. What are your organization’s policies or procedures for IT account management?
2. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?
3. Describe your organization’s bring your own device (BYOD) policy.
4. Describe your organization’s employee off-boarding process.
5. Is this process coordinated with IT and Human Resources (HR)?
6. What additional actions are taken if the employee’s termination is contentious?
7. How does your organization retrieve all information system-related property during the employment termination process (e.g., authentication token, system administrator’s handbook/manual, keys, identification cards, etc.)?

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by regulation, state law, and/or organization policy?
3. What training do employees receive regarding reporting requirements and your cyber incident response plan?
4. What cybersecurity incident escalation criteria is defined in your cyber incident response plan?
5. Who is responsible and what actions would they take based on the scenario?
6. Who needs to be notified internally and externally according to the plan?
7. When would leadership be notified?
8. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
10. How often is your organization’s data reviewed?
11. How would you determine whether unauthorized manipulation of data occurred?

## Incident Response

1. How is information recorded if CAD/call triage is unavailable?
2. How do you identify the primary and secondary rollover PSAP?
   1. Do those PSAPs have access to your CAD?
   2. Do they have access to dispatch your emergency services?
3. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
4. At what point in the scenario would you contact law enforcement?
   1. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
5. What are the processes for contacting critical personnel outside of core hours?
6. How do you proceed if critical personnel are unreachable or unavailable?
7. How would a breach of vendor(s) affect your organization if they have access to your information?
8. What are the notification requirements to your organization for breaches?

## Recovery

* 1. When does your organization determine a cyber incident is resolved?

1. Who makes this decision?
2. What post-incident activities would your organization conduct?
   1. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
3. What is the risk associated with reactivating critical business processes and systems?
4. Describe the process to completely rebuild these systems.
5. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. What additional training and/or exercise requirements do you require for your incident response staff?
3. How often does your organization exercise its CIRP?
4. Who is involved in the exercises?
5. What external agencies are involved in the exercises?
6. How does your organization’s training and exercise efforts address both physical and cyber risks?
7. How often do senior staff/leadership participate in cybersecurity exercises?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
2. How do these goals align with organizational objectives?
3. Describe your organization’s cybersecurity culture.
4. What cybersecurity training is required for senior leadership?
5. At what point would you activate your organization’s Security Operations Center/EOC?
6. What is your role during a cyber incident?
7. What information do you need to support your decision-making process?
8. What are the gaps in your cybersecurity workforce?
9. How does your organization recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. What training do employees receive on reporting contact with the media?
      2. How do you build and maintain trust with the public?

## Legal

1. What is the role of the legal department during a cyber incident?
2. What issues need to be addressed based on the scenario?
3. What legal documents does your organization have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| ECC | Emergency Communications Center |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| IT | Information Technology |
| MOA/MOU | Memorandum of Agreement/Memorandum of Understanding |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| POC | Point of Contact |
| PSAP | Public Safety Answering Point |
| TDoS | Telephony Denial of Service |
| TLP | Traffic Light Protocol |
| TTP | Techniques, Tactics, and Procedures |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Ransomware Attack Against County 911 Center

A county 911 center lost many of its systems following a ransomware attack in April 2020. The operations manager responded to a network login alert and went to the center on Sunday evening, shutting down and isolating affected systems upon arrival to halt the spread. This prevented the attack from spreading to radio and telephone communication systems, but computer-aided dispatch systems went completely offline. Dispatchers then hand-wrote all communications and information from emergency calls to communicate to responding emergency services. The system also dealt with automating the transfer of license plate and criminal record information to officers on patrol, forcing dispatchers to manually collect and disseminate the information. The county rebuilt its system, spending approximately $20,000 on recovery efforts to bring the system back online.[[12]](#footnote-13)

## Royal Ransomware Attack

The Royal ransomware group launched a ransomware attack against a large U.S. city in May 2023. The computer systems used by the police, fire department, courts, and libraries were compromised. The IT team immediately disconnected systems, services, and devices from the network to prevent the spread of the ransomware.[[13]](#footnote-14) The ransomware note sent to the city’s printers stated the group downloaded sensitive data from the city’s servers and promised to restore network access and keep the attack confidential if they paid the ransom. The investigation showed the ransomware group accessed the servers for three weeks prior to the ransomware attack and downloaded the personal information of over 27,000 people. The City Council approved over $8 million to cover hardware, software updates, and incident response.[[14]](#footnote-15)

## Local Government Impacted by Ransomware Attack Against Water Utility

The operations of a county and its largest city were impacted for almost a year following a ransomware attack that originated at the local water utility in December 2020. The attack impacted a number of city and county organizations, including the Sherriff’s Office, the Police Department, the District Attorney’s Office, the District Clerk’s Office, and the Justices of the Peace. For months, the city and county reverted to manual processes: city employees were paid based upon the last check they received before the attack, regardless of actual hours worked; customers of the water utility were told to estimate their own water usage and pay based upon that and the city issued hand-written receipts for invoice payments. The government permanently lost data prior to the incident, and data for the 2021 year is incomplete, without the ability to record and store it. The city implemented more resilient backups and user account controls as a result of the incident.[[15]](#footnote-16)

# Appendix D: Attacks and Threats

## Social Engineering and Phishing

One of the most prominent tactics cyber threat actors use to exploit network and system vulnerabilities is social engineering, the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. A common social engineering technique involves the use of phishing. Phishing uses email, text messaging, and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. Social engineering is effective for compromising networks, and evading intrusion detection systems without leaving a log trail. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, providing instruction on where to forward them, and keeping software and systems up to date. Organizations can also implement software designed to safeguard sensitive information, detect unsafe URLs, block phishing websites, detect known phishing and malware, and implement Multi-Factor Authentication (MFA) to guard against the use of stolen credentials.

### Additional Resources

* Avoiding Social Engineering and Phishing Attacks

(<https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>)

* Phishing Guidance: Stopping the Attack Cycle at Phase One (<https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>)

## Telephony Denial of Service

Telephony Denial of Service (TDoS) is a type of attack where a large volume of telephone calls overloads a communications network, overwhelming call capacity. The chokepoint may occur in any part of the network, from the service provider’s infrastructure to the equipment of the end user. Malicious TDoS methods include using botnets of mobile phones, voice over internet protocol (VoIP) services that allow users to target any geographic area with a large number of quickly generated phone numbers, and compromised networks of phones from a large organization or a compromised phone exchange. TDoS mitigation best practices include having a large overflow reserve for call centers, the ability to scale call response personnel levels, TDoS filters that detect and deal with malicious call flooding, and coordination with surrounding area ECCs/PSAPs to provide a networked call-handling capability. See the resource list below for more detail on mitigation and best practices.

*Additional Resources*

* Cyber Risks to 911: Telephony Denial of Service (<https://www.cisa.gov/sites/default/files/2023-02/Cyber%20Risks%20to%20911%20TDoS_6.4.2020%20-%20%28508c%29_1.pdf>)
* Cybersecurity Resources for 911 Centers

(<https://www.cisa.gov/sites/default/files/2023-03/cybersecurity_resources_for_9-1-1_centers-032023-508.pdf>)

* Cyber Risks to Next Generation 911 (<https://www.cisa.gov/sites/default/files/2023-02/NG911%20Cybersecurity%20Primer.pdf>)

# Appendix E: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
  + CISA Emergency Communications Division (contact: [ECD@cisa.dhs.gov](mailto:ECD@cisa.dhs.gov))
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact: <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)
* Federal Bureau of Investigation (FBI)
* Field Offices (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)

Emergency Services Sector Resources

* CISA Emergency Services Sector Cybersecurity Initiative (<https://www.cisa.gov/resources-tools/programs/emergency-services-sector-cybersecurity-initiative>)
* Cybersecurity Resources for 9-1-1 Centers (<https://www.cisa.gov/resources-tools/resources/cybersecurity-resources-9-1-1-centers>)
* Cyber Risks to Next Generation 9-1-1 (<https://www.cisa.gov/sites/default/files/2023-02/NG911%20Cybersecurity%20Primer.pdf>)
* Two Things Every 911 Center Should Do To Improve Cybersecurity (<https://www.cisa.gov/sites/default/files/2023-02/22_0913_ecd_ng911wg_two_things_911centers_508C.pdf>)
* Emergency Services Sector Roadmap to Secure Voice and Data Systems (<https://www.cisa.gov/resources-tools/resources/emergency-services-sector-roadmap-secure-voice-and-data-systems>)
* Cyber Resiliency Resources for Public Safety (<https://www.cisa.gov/resources-tools/resources/cyber-resiliency-resources-public-safety-fact-sheet>)
* Emergency Services Sector Cyber Risk Assessment (<https://www.cisa.gov/resources-tools/resources/emergency-services-sector-cyber-risk-assessment>)
* CISA SAFECOM (<https://www.cisa.gov/safecom>)
* Communications and Cyber Resiliency Toolkit (<https://www.cisa.gov/resources-tools/resources/communications-and-cyber-resiliency-toolkit>)
* CISA Emergency Communications Coordination Program (<https://www.cisa.gov/resources-tools/programs/emergency-communications-coordination-program>)
* CISA GETS/WPS Resources (<https://www.cisa.gov/resources-tools/resources/getswps-documents>)
* CISA Shared Resources High Frequency Radio Program (<https://www.cisa.gov/resources-tools/programs/shared-resources-shares-high-frequency-hf-radio-program>)

Preparedness Resources

* State and Local Cybersecurity Grant Program (<https://www.cisa.gov/state-and-local-cybersecurity-grant-program>)
* CISA CDM Program (<https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program>)
* CISA Find Help Locally (<https://www.cisa.gov/audiences/find-help-locally>)
* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>)
* NIST Cybersecurity Framework Tools ([<https://www.nist.gov/cyberframework>](https://www.nist.gov/cyberframework))

State Level Resources

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) (<https://www.nga.org/>)
* NGA Center for Best Practices (<https://www.nga.org/bestpractices/divisions/hsps/>)
* DHS Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)
* National Association of State Chief Information Officers (NASCIO) (<https://www.nascio.org/>)

Additional Resources

* InfraGard (<https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>)
* Internet Security Alliance (<https://isalliance.org/>)
* Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (<https://www.isao.org/information-sharing-groups/>)
* International Association of Certified ISAOs ([http://www.certifiedisao.org](http://www.certifiedisao.org/); contact: [operations@certifiedisao.org](mailto:operations@certifiedisao.org))
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. FEMA, “Homeland Security Exercise and Evaluation Program,” January 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-3)
3. CISA, “Cybersecurity Alerts & Advisories,” <https://www.cisa.gov/news-events/cybersecurity-advisories>. [↑](#footnote-ref-4)
4. CISA SAFECOM Case Study, “Cyber Incident Response to Public Safety Answering Points: A States Perspective,”

   <https://www.cisa.gov/sites/default/files/publications/22_0414_cyber_incident_case_studies_state_final_508c.pdf.> [↑](#footnote-ref-5)
5. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AT-01>. [↑](#footnote-ref-6)
6. NIST CSF 2.0 via CPRT, “ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-04>. [↑](#footnote-ref-7)
7. NIST CSF 2.0 via CPRT, “Identity Management, Authentication, and Access Control (PR.AA),” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA>. [↑](#footnote-ref-8)
8. NIST CSF 2.0 via CPRT, “DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.CM-09>. [↑](#footnote-ref-9)
9. NIST CSF 2.0 via CPRT, “DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.CM-03>. [↑](#footnote-ref-10)
10. NIST CSF 2.0 via NIST’s CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04>. [↑](#footnote-ref-11)
11. NIST CSF 2.0 via CPRT, “PR.DS-11: Backups of data are created, protected, maintained, and tested,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-11>. [↑](#footnote-ref-12)
12. Andy Cordan, “How the Lawrence Co. 911 center hit by a ransomware attack, amid the COVID pandemic, handled the threat,” November 23, 2021, [https://www.wkrn.com/special-reports/how-the-lawrence-co-911-center-hit-by-a-ransomware-attack-amid-the-covid-pandemic-handled-the-threat/](https://urldefense.us/v3/__https:/www.wkrn.com/special-reports/how-the-lawrence-co-911-center-hit-by-a-ransomware-attack-amid-the-covid-pandemic-handled-the-threat/__;!!BClRuOV5cvtbuNI!DTzfGqthX_jMA46-IwwhwIQrshptU3833sFK7bc-OjP76sOoYLFxTcnpA05TVPfL_9buMMPs7Cx5RilqRvkJBt5X1QWVP35NFKw$). [↑](#footnote-ref-13)
13. Alanna Quillen, Larry Collins and Lili Zheng, “Dallas releases technology accountability report following ransomware attack,” *NBC DFW,* June 9, 2023, <https://www.nbcdfw.com/news/local/dallas-to-release-technology-accountability-report-following-ransomware-attack/3274570/>. [↑](#footnote-ref-14)
14. Ken Kalthoff, “Dallas pays millions for ransomware expenses after May attack,” *NBC DFW*, June 9, 2023, <https://www.nbcdfw.com/news/local/dallas-pays-millions-for-ransomware-expenses-after-may-attack/3313643/>. [↑](#footnote-ref-15)
15. Karl Richter, “Cyberattack cripples city, county government computer systems,” *Texarkana Gazette*, December 30, 2021, [https://www.texarkanagazette.com/news/2021/dec/30/cyberattack-cripples-city-county-government/](https://urldefense.us/v3/__https:/www.texarkanagazette.com/news/2021/dec/30/cyberattack-cripples-city-county-government/__;!!BClRuOV5cvtbuNI!DTzfGqthX_jMA46-IwwhwIQrshptU3833sFK7bc-OjP76sOoYLFxTcnpA05TVPfL_9buMMPs7Cx5RilqRvkJBt5X1QWVF0-esos$). [↑](#footnote-ref-16)