

**CISA Tabletop Exercise Package Communications Sector – Rural Broadband**

[Enter Organization Name]

<Exercise Date>

Updated February 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc170288148)

[Exercise Overview 5](#_Toc170288154)

[General Information 6](#_Toc170288155)

[Module 1 8](#_Toc170288156)

[Module 2 10](#_Toc170288157)

[Appendix A: Additional Discussion Questions 12](#_Toc170288158)

[Appendix B: Acronyms 15](#_Toc170288159)

[Appendix C: Case Studies 16](#_Toc170288160)

[Appendix D: Malicious Activity 18](#_Toc170288161)

[Appendix E: Contacts and Resources 20](#_Toc170288162)

# 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 <broadband provider> in response to a significant cyber incident impacting the communications sector. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Discuss organizational resilience to threats and disruptions targeting the communications sector. 2. Examine plans, policies, and procedures in response to a cyber incident. 3. Assess internal/external communications processes. | |
| Threat or Hazard | Cyber Incident | |
| Scenario | A cyber threat actor sends phishing emails to both your personnel and customers, as an entry point into your network/systems. A Distributed Denial of Service (DDoS) attack follows, with an inadvertent Telephony Denial of Service (TDoS) created by customers calling in to report service outages. | |
| 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)  **Communications**  **Sector Risk Management Agency**  CommunicationsSector@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 malicious activity 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 management personnel, human resources personnel, legal personnel, and any other 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, IT/information security personnel, emergency management personnel, legal personnel, and any other personnel without 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 possible phishing attack against both your personnel and your customers, followed by customers calling to complain about service issues.
  + **Module 2:** This module continues the scenario with a DDoS attack followed by an inadvertent TDoS caused by customers calling to report service issues and local media inquiries into the impacts of the attack on the local community.
* 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

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issue a joint alert addressing efforts by state-sponsored cyber actors to disrupt internet access throughout the United States.[[3]](#footnote-4) Methods employed include large-scale Distributed Denial of Service (DDoS) attacks, created using phishing, vishing and smishing campaigns. These messages are created with generative artificial intelligence, making them more difficult to identify as fraudulent. Through these methods, the threat actors gain access to multiple computing devices and create large botnets to mount their attacks. The alert recommends all telecommunications providers ensure they are running the latest releases of software with all applicable patches installed, and that end consumers are made aware of potential phishing, vishing, and smishing attacks.

## 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) like those addressed in the alert?
   2. What risks do you face from end user malware infections?
   3. What are the potential impacts to you and your customers if you were the target of a DDoS attack?
2. What cybersecurity threat information does your organization receive (e.g., information from CISA, FBI, Fusion Center)?
   1. What cyber threat information is most useful?
   2. How is information disseminated throughout your organization?
   3. What actions would your organization take in response to an alert like the one presented in the scenario?

### Day 12

Employees from your organization receive emails from what appears to be your third-party 401k vendor asking them to update their investment selections for the upcoming renewal period. Some employees click on the embedded link and are taken to what appears to be a selection website. They are instructed to download a file for their records upon completing their selections.[[4]](#footnote-5)

1. Describe your organization’s cybersecurity posture.
2. 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?
3. Describe your organization’s cybersecurity training program for employees.
4. How often are employees required to complete this training?
5. What additional training is required for employees with elevated or system administrator-level privileges?
6. What training methods or approaches have you found most beneficial?
7. How are employees trained to recognize and report cyber threats such as phishing scams?
8. What additional training does your organization require for those who fall for a phishing email?
9. What are your network access and authentication controls for users?
10. Does your organization allow users to run document macros? If so, what compensating security controls do you have to mitigate the risk?
11. What cybersecurity controls are present to mitigate the risk of users entering credentials into phishing websites?

### Day 20

One of your network engineers comes across a thread from an online chat group where IT staff from several telecommunications providers state they have experienced an uptick in network outages.[[5]](#footnote-6) Some were attributed to physical issues (storms, broken transmission lines) while others seem to be from cyber related events, including DDoS events.

1. What would you do with this information, if verified?
2. What methods do you have in place for network monitoring?
   1. What services do you use for intrusion detection monitoring?
   2. When was your last penetration test performed and what improvements have you made based on the findings?

### Day 24

Customers call your customer service and technical support lines complaining of service issues. Many state they are unable to reach any websites while others complain of receiving slower access speeds than promised.

# Module 2

### Day 43 – Early Morning

Your organization receives several million illegitimate web requests per second (RPS), preventing your servers from authorizing legitimate requests. The resulting DDoS limits the ability to provide services to your customers, including local Emergency Communications Centers (ECCs)/Public Safety Answering Points (PSAPs)/9-1-1 Call Centers and other critical infrastructure owners.

## 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 methods does your organization have to sustain operations during a DDoS?
   1. Do you employ a DDoS mitigation solution?
3. Describe your crisis communication plan.
   1. If primary communications are compromised, how do you provide information to internal and external entities?
4. Are your responders and support personnel 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?
5. How do you maintain services for critical infrastructure customers?
   1. What methods are referenced in your CIRP/Continuity of Operations Plan (COOP) for restoring these services?

### Day 43 – Mid Morning

Customers cannot access the internet because of the DDoS attack and inundate your call center with complaints. Many customers refuse to hang-up until their service is restored. The volume of customer calls overwhelms the call center and results in a Telecom Denial of Service (TDoS).

1. What steps within your CIRP/COOP might help mitigate the TDoS?[[6]](#footnote-7)
2. What capabilities do you have to get messages out to your customers to inform them of outages and restoration efforts?
3. Given the scenario, what are the broader impacts to your community?
4. What essential services are dependent upon your organization providing telecommunications services?

### Day 43 – Evening

The DDoS subsides; however, the issues your organization and customers faced gain media attention. Local news outlets reach out to multiple customers and the local emergency management agency director. All customers interviewed voice concern over the service disruption the community faced during the event.[[7]](#footnote-8)

1. Describe your organizational processes to respond to the media reports and inquiries.
   1. What pre-scripted messages exist 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?

### Day 60

An investigation reveals the threat actor(s) used a botnet consisting of approximately 1,000,000 devices, including company laptops/desktops, to initiate the attack.

1. How do you determine a cyber event/incident is over?
2. 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. If primary communications are compromised, how do you provide information to internal and external entities?
20. 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. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
2. At what point in the scenario would you contact law enforcement?
   1. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
3. What are the processes for contacting critical personnel outside of core hours?
4. How do you proceed if critical personnel are unreachable or unavailable?
5. How would a breach of vendor(s) affect your organization if they have access to your information?
6. What are the notification requirements to your organization for breaches?
7. Have considerations been made for out-of-band (OOB) communications?

## 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 do 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 |
| COOP | Continuity of Operations Plan |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| DDoS | Distributed Denial of Service |
| ECC | Emergency Communications Center |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| IT | Information Technology |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| OOB | Out of Band Communications |
| POC | Point of Contact |
| PSAP | Public Safety Answering Point |
| RPS | Requests Per Second |
| TDoS | Telephony Denial of Service |
| TLP | Traffic Light Protocol |
| TTP | Techniques, Tactics, and Procedures |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Unsuccessful DDoS Attack Against U.S. Internet Services Companies

In October 2023 one of the largest distributed denial of service attacks of its kind was launched against three U.S. based internet services companies. The attack targeted an undisclosed vulnerability in Hypertext Transfer Protocol (HTTP)/2 protocol. HTTP is used to load webpages. The two-minute attack launched a high volume of illegitimate web requests designed to overwhelm a web server’s ability to respond to legitimate client requests. While the attack was unsuccessful against the three companies, any vendor who implemented HTTP/2 could be subject to a similar attack.

One of the impacted internet organizations said this attack was three and a half times bigger than its previous largest attack on record. Another organization stated the attack was seven and a half times larger than their previous record. No group claimed responsibility and law enforcement could not attribute the attack.[[8]](#footnote-9)

## Malware Attack Against Ukrainian Internet Provider

On February 24, 2022, a cyberattack was launched against a Ukrainian internet organization. The attack against broadband satellite internet access disabled modems that communicate with satellites to provide internet access to Ukraine and Europe.[[9]](#footnote-10) The attack was the result of a new strain of wiper malware called “Acid Rain” designed to remotely erase vulnerable modems and routers with the intent to disrupt service rather than access data or systems.[[10]](#footnote-11)

Service impacts lasted over two weeks and spread beyond Ukraine. A major German energy company lost remote monitoring access to over 5,800 wind turbines, and in France nearly 9,000 subscribers of a satellite internet service provider experienced an internet outage. Additionally, approximately 13,000 subscribers were impacted from another satellite internet service provider to multiple European countries.[[11]](#footnote-12)

## Ukraine Mobile Provider Cyber Attack

In December 2023, a Ukrainian mobile provider was attacked by the Sandworm Group, a threat actor with ties to the Russian intelligence community.[[12]](#footnote-13) The impacts included loss of mobile service, banking services, damaged IT infrastructure and malfunctions in the air raid alert system. Additionally, the attack caused a surge in traffic with other mobile and internet providers as people turned to other forms of communication.[[13]](#footnote-14) Investigation revealed the hackers were inside the organization’s IT infrastructure since May 2023.

As of January 5, 2024, investigators are still working to establish how the organization was penetrated or what type of trojan horse malware was used to break into the systems. Investigators found samples of malware used to steal large numbers of passwords at a time in the impacted system.[[14]](#footnote-15)

# Appendix D: Malicious Activity

## Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of devices (e.g., computers, cellphones, Internet of Things, etc.) making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the “master” because it controls any subsequent devices that become infected. The other infected devices, known as “bots” or “zombies” carry out the actual attack and create what is known as a “botnet”. The “bots” receive a command from the “master” which includes the address of the target. Extremely high volumes (floods) of data are sent to the target which slows down web server performance and prevents acceptance of legitimate network traffic.

### Additional Resources

* Understanding and Responding to Distributed Denial-of-Service Attacks

(<https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf>)

* CISA Understanding Denial-of-Service Attacks (<https://www.cisa.gov/news-events/news/understanding-denial-service-attacks>)

## 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, vishing, and smishing. Phishing uses email, text messaging, and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. Vishing uses voice communication to convince a victim to call a certain number and share sensitive information. Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed. Smishing uses SMS/text messages to send malicious links, email addresses, and phone numbers.

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 emergency communication centers (ECC) and/or public safety answering points (PSAP) 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/safecom/next-generation-911>)

# Appendix E: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.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)

Communications Sector Resources

* CISA Communications Sector (<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector>)
* Communications Sector Coordinating Council (<https://www.comms-scc.org/>)
* 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 GETS/WPS Resources (<https://www.cisa.gov/resources-tools/resources/getswps-documents>)
* CISA Emergency Communications Coordination Program (<https://www.cisa.gov/resources-tools/programs/emergency-communications-coordination-program>)
* National Cable and Telecommunications Association (NCTA) – The Internet and Television Association (<https://www.ncta.com/>)
* National Telephone Cooperative Association (NTCA) – The Rural Broadband Association (<https://www.ntca.org/>)

Preparedness Resources

* 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. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-02>. [↑](#footnote-ref-4)
4. NIST CSF 2.0 via 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-5)
5. NIST CSF 2.0 via CPRT, “ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-02>. [↑](#footnote-ref-6)
6. NIST CSF 2.0 via 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-7)
7. NIST CSF 2.0 via CPRT, “RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.CO-04>. [↑](#footnote-ref-8)
8. Tim Starks and David DiMolfetta, “The largest cyberattack of its kind recently happened,” *The Washington Post,* October 11, 2023, <https://www.washingtonpost.com/politics/2023/10/11/largest-cyberattack-its-kind-recently-happened-heres-how/>. [↑](#footnote-ref-9)
9. CyberPeace Insitute, “Case Study: Viasat,” June 2022, [https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat%20](https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat). [↑](#footnote-ref-10)
10. Gordon Corera, “Russia Hacked Ukrainian satellite communications, officials believe,” *BBC,* March 25, 2022, <https://www.bbc.com/news/technology-60796079>. [↑](#footnote-ref-11)
11. CyberPeace Insitute, ibid. [↑](#footnote-ref-12)
12. Tom Balmforth, “Exclusive: Russian hackers were inside Ukranian telecoms giants for months,” *Reuters,* January 5, 2024, <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/>. [↑](#footnote-ref-13)
13. Max Hunder, Jonathan Landay, and Stefaniia Bern, “Ukraine’s top mobile operator hit by biggest cyberattack of war,” *Reuters,* December 12, 2023, <https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/>. [↑](#footnote-ref-14)
14. Balmforth, ibid. [↑](#footnote-ref-15)