Cyber Resilience Challenge

Situation Manual

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

***Sponsored by***



# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Cyber Resilience Challenge (Islanding) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This is a tabletop exercise designed by Cyber Florida to simulate response actions to a cyber-compromise within a controlled environment tailored to the participating critical infrastructure sector/subsector. |
| **Focus Area(s)** | Emphasizes the National Preparedness Goal's mission areas of Protection, Response, and Recovery, applicable to a broad range of critical infrastructure sectors. |
| **Capabilities** | * Cybersecurity Management
* Incident Response and Recovery
* Critical Infrastructure Protection
* Public Information and Warning
 |
| **Objectives** |  1: Evaluate the impact of islanding cyber-compromise that is directly affecting the status of the utility in question, focusing on operational continuity and public safety. 2: Create and assess contingency strategies to maintain or quickly restore essential services, considering a direct cyber intrusion into critical systems, notwithstanding existing defensive measures. |
| **Threat or Hazard** | A hypothetical yet plausible technological/cyberattack targeting the critical systems of [Insert Specific Sector Here], facilitated by an adversary gaining direct network access to those systems. This scenario is designed to challenge assumptions about the invulnerability of existing security measures. |
| **Scenario** | Despite the robust defense mechanisms in place, the Cybersecurity and Infrastructure Security Agency (CISA) uncovers a sophisticated cyber threat, dubbed "Viru3s2.0," capable of breaching the sector's defenses and gaining control over its critical systems. This exercise scenario serves as a stress test for the sector's preparedness, challenging participants to consider and address potential vulnerabilities and response strategies in the face of a direct and formidable cyber intrusion. |
| **Sponsor** | Sponsored by internal department |
| **Participating Jurisdictions/ Organizations** | Tailored to each session, with expected participation from Federal, State, and local agencies, DHS, CISA, and representatives from the focus sector (e.g., electric, water, gas, oil, banking), emergency management agencies, and academic partners. A comprehensive list of participating agencies will be included in Appendix B. |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor)] |

# Exercise Assumptions

For the Cyber Resilience Challenge, certain assumptions have been established to guide the development, execution, and evaluation of the tabletop exercise. These assumptions are designed to provide a common understanding among participants from various critical infrastructure sectors and ensure that the exercise focuses on strategic decision-making and operational coordination rather than technical specifics.

## General Assumptions:

**Generic Incident Response Framework:** This TTX is based on a generic incident response plan applicable across all participating critical infrastructure sectors. Participants are advised to avoid sector-specific technicalities and focus on the broader aspects of incident management and recovery.

**Legal and Governmental Processes:** It is assumed that legal and governmental entities involved in the response to and recovery from the cyber-compromise will act and process information and actions accordingly, in a timely and supportive manner.

**Direct Adversary Access:** Regardless of the existing defense mechanisms within the infrastructure, participants should assume that an outside adversary has gained direct access to the sector's critical systems through the network. This assumption challenges the notion of invulnerability and emphasizes the importance of robust detection, response, and recovery strategies.

**Cross-Sector Impact Consideration:** While the TTX is tailored to the specific sector in question, it is important to consider the potential cross-sector impacts of the cyber-compromise. Participants should assume that their sector's disruption could have cascading effects on other sectors and include this consideration in their response and recovery planning.

## Sector-Specific Assumptions:

**Communication:** Effective communication with the public, stakeholders, and legal team is critical in managing the incident. It is assumed that each sector has established communication channels and protocols to address public concerns and provide accurate, timely information during the crisis.

**Resilience and Adaptation:** Each sector possesses inherent baseline resilience and the capability to adapt to disruptions. The TTX assumes that sectors can identify and deploy workaround strategies to maintain essential services, even under direct cyber threats.

**Interdependency Awareness:** Participants should be aware of the interdependencies within and across sectors, recognizing that disruptions in one sector can significantly impact others. Planning and response efforts should account for these interconnections.

# General Information

## Exercise Objectives and Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team.

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Assess the impact of a cyber-compromise across critical infrastructure | Operational Coordination and Public Information and Warning |
| Develop sector-specific contingency strategies to maintain essential services | Infrastructure Systems and Cybersecurity |
| Evaluate communication strategies with the public and stakeholders across diverse sectors | Public Information and Warning |
| Enhance incident command system integration for cyber incidents | Operational Coordination |
| Identify recovery and restoration strategies post-incident | Recovery Planning |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise and their respective roles and responsibilities are as follows:

**Players:** Personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.

**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.

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

**Evaluators:** Are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, polices, and procedures.

## Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following [**3**] modules:

* **Module 1:** Incident Notification and Initial Response
(Summary of the cyber threat notification and initial actions taken by the utility and government agencies.)
* **Module 2:** Continuity of Operations and Workarounds
(Discussion on maintaining operations, identifying, and implementing workaround strategies to continue delivering services to the customer.)
* **Module 3:** Communication and Recovery Planning
(Strategies for effective communication with stakeholders and the public and planning for recovery and restoration of services.)

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in functional group discussions of appropriate [focus area] issues. For this exercise, the functional groups are as follows:

* IT and Cybersecurity Team
* Operations and Engineering Team
* Public Relations and Communication Team
* Emergency Management and Legal/Government Liaison Team
* Other related groups or teams

After these functional group discussions, participants will engage in a moderated plenary discussion in which a spokesperson from each group will present a synopsis of the group's actions based on the scenario.

##

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent-setting and may not reflect your jurisdiction's/organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [focus area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned capabilities, capability targets, and critical tasks, which are documented in Exercise Evaluation Guides (EEGs). Evaluators have EEGs for each of their assigned areas. Additionally, players will be asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise, and compile the After-Action Report (AAR)/Improvement Plan (IP).

# Module 1: [Incident Notification and Initial Response]

## Scenario

### [Month, Day, Year]: [9:00 AM]

[The Cybersecurity and Infrastructure Security Agency (CISA) issues an urgent alert to all [Name CI Sector Entity] critical infrastructure sectors nationwide about a newly discovered cyber vulnerability named "Viru3s2.0." This vulnerability has already started to exploit the compromised network in a significant incident affecting the infrastructure's systems. It is confirmed the outside adversary gained control over critical systems, leading to substantial service disruptions.]

**[Month, Day, Year]: [9:30 AM]**

[The affected sector identifies the compromise and initiates its incident response protocol. The sector's cybersecurity team starts an in-depth investigation to assess the extent of the breach and to identify all affected systems and operations. After an extensive review of current cybersecurity systems, it has been determined that [Name CI Sector Entity] has the identified vulnerability. Leadership has decided to isolate entity's critical systems from the internet (islanding) to protect against cyber -attacks and vulnerability. Before islanding can be accomplished, what is the impact of this isolation?]

**[Month, Day, Year]: [10:15 AM]**

[Considering the potential for widespread impact across other sectors with similar vulnerabilities, the senior management team of the affected sector convenes an emergency meeting. The agenda includes deciding on immediate actions to contain the breach, including the isolation of critical systems from the network to prevent further compromise. Breakout teams are to review plans, policies, and procedures to develop possible work arounds to continue delivering services to customers.]
**Key Issues**

* [**Initial Detection and Notification**: The process of detecting the "Viru3s2.0" vulnerability and the urgent alert issued by CISA. Evaluating the effectiveness of current cybersecurity monitoring systems and protocols across different sectors.]
* [**Immediate Response Actions**: The initial response by the [Name CI Sector Entity], including the activation of incident response protocols and communication with internal legal and regulatory liaison teams and external agencies such as CISA and emergency services, to manage the situation.
* [**Impact Assessment**: Conducting an early assessment of the incident's impact on operations, customer service, and public safety across the service area of the affected [Name CI Sector Entity]. This includes considering the potential cascading effects on interconnected and interdependent systems and other critical infrastructure sectors.]

## Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 1. Identify any critical issues, decisions, requirements, or questions that should be addressed now. The following questions are suggested subjects you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

### [IT and Cybersecurity Team]

1. [What are the immediate steps to assess and contain the cybersecurity breach?]
2. [How do we ensure effective communication with CISA and other relevant authorities?]
3. [What measures are in place to quickly isolate affected systems without disrupting essential services?]

### [Operations and Engineering Team]

1. [What measures are in place to quickly isolate affected systems without disrupting essential services?]
2. [What contingency plans can be activated to mitigate the impact on customers?]
3. [How do we prioritize critical services and infrastructure for power supply?]

### [Public Relations and Communication Team]

1. [What is the strategy for communicating with the public, regulators, and stakeholders about the incident and its impact?]
2. [How do we address concerns about safety and service restoration?]
3. [What channels will be used to provide updates and information to customers?]

### [Emergency Management and Government Liaison Team]

1. [How do we coordinate with local and state emergency management agencies to support response and recovery efforts?]
2. [What information do government partners need, and how will it be shared?]
3. [How can we leverage government resources and support during this incident?]

# Module 2: [Continuity of Operations and Workarounds]

## Scenario

### [Month, Day, Year]: [12:00 PM]

[Following the initial response to the cyber incident, the leadership and technical teams across the affected critical infrastructure sector begin assessing the feasibility of continuing operations while the primary systems are isolated for thorough inspection and remediation. They start exploring alternative operational methods and manual overrides to maintain essential services.]

### [Month, Day, Year]: [1:30 PM]

[The Name CI Sector Entity engages with partners, including other entities within the same sector, and relevant support services are initiated to discuss mutual aid and support options. This could include rerouting services or leveraging shared resources to offset any deficits in service provision resulting from the compromised systems.]

### [Month, Day, Year]: [3:00 PM]

[Technical teams evaluate the potential for deploying secondary systems unaffected by "Viru3s2.0" and the viability of manual operations in certain areas. Discussions emerge regarding the long-term implications of operating under modified conditions and the urgent need for enhancing system security and resilience against future cyber threats.]

## Key Issues

* [**Operational Continuity**: Identifying immediate steps to continue the provision of essential services across the [Name CI Sector Entity] service area despite the cyber incident's impact on critical systems.]
* [**Alternative Control Strategies**: Evaluating the feasibility of adopting manual controls, activating secondary systems, and seeking mutual aid to ensure uninterrupted service delivery.]
* [**Long-term System Resilience**: Reflecting on the incident's broader implications for future operations within the [Name CI Sector Entity] service area, including identifying necessary system upgrades and implementing robust cybersecurity protocols to prevent similar vulnerabilities.]

## Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 2. Identify any critical issues, decisions, requirements, or questions that should be addressed now. The following questions are suggested subjects you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

### [Operations and Engineering Team]

1. [What are the overarching challenges of shifting to manual operations or activating secondary systems at [Name CI Sector Entity]]
2. [How can we validate the safety and reliability of operations when employing alternative control methods?]
3. [What are the general requirements and expected timelines for deploying these workaround strategies?]

### [IT and Cybersecurity Team]

1. [How can we quickly secure secondary systems against "Viru3s2.0" and other potential vulnerabilities?]
2. [What measures are needed to enhance system resilience against future cyber threats while maintaining operational capabilities?]
3. [In the context of various critical infrastructures, how can the recovery of compromised systems be accelerated with minimal impact on service delivery?]

### [Public Relations and Communication Team]

1. [How do we communicate the continuity of operations and workaround strategies to reassure the public, regulators, and stakeholders?]
2. [What type of information about the security measures and recovery efforts should be disseminated, and how can this be tailored to the needs and concerns of diverse audiences?]
3. [How can public expectations regarding service disruptions or changes in service delivery be managed effectively across a variety of critical services?]

### [Emergency Management and Government Liaison Team]

1. [How do we coordinate with local, state, and federal emergency management agencies to support continuity of operations?]
2. [What role can government partners assume in providing regional or national support and resources to sustain operations across affected critical infrastructures?]
3. [Are there regulatory or legal considerations to address when implementing workaround strategies or seeking mutual aid.]

# Module 3: [Communication and Recovery Planning]

## Scenario

### [Month, Day, Year]: [4:30 PM]

[Following the implementation of temporary strategies to maintain service continuity, the focus shifts towards communicating with stakeholders, regulators, and the public about the ongoing response efforts and plans for recovery. Communication is critical across all sectors to manage perceptions and ensure informed public awareness.]

### [Month, Day, Year]: [5:00 PM]

[The Public Relations team launches a comprehensive communication campaign, employing a variety of channels. including social media, press releases, and community meetings. The objective is to keep the public and stakeholders well-informed about the incident's status, the interim measures in place to secure services, and the preparatory steps for the sector's recovery phase.]

### [Month, Day, Year]: [6:00 PM]

[The Recovery Planning team starts to draft a detailed plan for the full restoration of all systems to their operational capacity. This plan outlines the timelines for necessary repairs and system enhancements, strategies for enhancing cybersecurity measures to avert future incidents, and methods to phase out the reliance on temporary workaround strategies.]

## Key Issues

* [**Effective Communication:** The necessity for accurate, timely, and clear communication to stakeholders, regulators, and the public regarding the incident's impact, ongoing response, and recovery plans. This communication should aim to reassure all parties about the steps being taken to secure and restore services.]
* [**Public Trust and Confidence:** The importance of maintaining or restoring public trust through transparent, consistent updates on the recovery process and future prevention strategies. Demonstrate a commitment to learning from the incident and strengthening systems against future threats.
* [**Recovery and Restoration Planning:** The challenge of developing a concise, actionable recovery plan that not only addresses the immediate restoration of services but also incorporates long-term cybersecurity enhancements based on lessons learned from the incident. The plan should be adaptable to various sectors, focusing on restoring full operational capacity and bolstering defenses.]

## Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 3. Identify any critical issues, decisions, requirements, or questions that should be addressed now. The following questions are suggested subjects you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

### [Public Relations and Communication Team]

1. [What key messages need to be communicated to the public, regulators, and stakeholders regarding recovery efforts and timelines?]
2. [How can we maintain consistency and accuracy of information across all communication channels, tailored to the specific needs and concerns?]
3. [What proactive strategies can be employed across sectors to manage and mitigate misinformation or public concerns during the recovery phase?]

### [IT and Cybersecurity Team]

1. [What are the overarching priorities for system recovery and cybersecurity enhancements to prevent future incidents?]
2. [How can technical aspects of the recovery process be communicated effectively to non-technical stakeholders in a way that is easily understandable and sector-specific?]
3. [What general lessons learned from the incident can be shared industry-wide to bolster cybersecurity resilience across all sectors?]

### [Operations and Engineering Team]

1. [What steps are being taken to restore systems to full operational capacity?]
2. [How will the transition from workaround strategies back to normal operations be managed to ensure a smooth, safe restoration of services?]
3. [What improvements or upgrades are planned to prevent future vulnerabilities or to enhance system resilience?]

### [Emergency Management and Government Liaison Team]

1. [How do we coordinate recovery efforts with local, state, and federal emergency management agencies?]
2. [What role will government partners play in the recovery phase, especially regarding regulatory compliance and support for cybersecurity initiatives?]
3. [How can we leverage this incident to advocate for more resources or changes in policy to better protect critical infrastructure?]

# Appendix A: Exercise Schedule

**Note:** Because this information is updated throughout the exercise planning process, appendices may be developed as stand-alone documents rather than part of the SitMan.

|  |  |
| --- | --- |
| Date | [Insert Date] |
| [Time] | Registration |
| [Time] | Welcome and Introductions |
| [Time] | Module 1: [Incident Notification and Initial Response] |
| [Time] | Break |
| [Time] | Module 2: [Continuity of Operations and Workarounds] |
| [Time] | Break |
| [Time] | Module 3: [Communication and Recovery Planning] |
| [Time] | Break |
| [Time] | Hotwash |
| [Time] | Closing Comments |

# Appendix B: Exercise Participants

| **Participating Organizations** |
| --- |
| **Federal** |
| [Federal Participant] |
| [Federal Participant] |
| [Federal Participant] |
| **State** |
| [State Participant] |
| [State Participant] |
| [State Participant] |
| **[Jurisdiction A]** |
| [Jurisdiction A Participant] |
| [Jurisdiction A Participant] |
| [Jurisdiction A Participant] |
| **[Jurisdiction B]** |
| [Jurisdiction B Participant] |
| [Jurisdiction B Participant] |
| [Jurisdiction B Participant] |

# Appendix C: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

# Appendix D: Acronyms

| Acronym | Term |
| --- | --- |
| CI | Critical Infrastructure |
| CISA | Cybersecurity and Infrastructure Security Agency |
| DHS | Department of Homeland Security |
| HSEEP | Homeland Security Exercise and Evaluation Program |
| ICS | Industrial Control Systems |
| IT | Information Technology |
| PR | Public Relations |
| SitMan | Situation Manual  |
| TTX | Tabletop Exercise  |
| USF | University of South Florida |
| [Acronym] | [Term] |
| [Acronym] | [Term] |