

# TABLETOP EXERCISES FOR INCIDENT RESPONSE PLANS UNDER NERC RELIABILITY STANDARD CIP-008



Mark Simon – [msimon@encari.com](mailto:msimon@encari.com)



# Agenda

- Introduction
- Preparations for Tabletop Exercise
- Executing a Tabletop Exercise
- Evaluating the Exercise and Lessons Learned
- Checklist
- Questions

# Introduction

- Requirement R1.6 of NERC Reliability Standard CIP-008-2

## B. Requirements

**R1.** Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

**R1.6.** Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

# Introduction

- Test cyber security incidents
  - Cyber security incidents described in OE-417 and NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting
  - Include precursors or warnings
    - Renewal of June 21, 2007 ES-ISAC advisory threat about Aurora
    - Vendor advisories about the Stuxnet worm

# Introduction

- Tabletop Exercise
  - Discussion-based exercise: discuss roles during an incident and responses to a particular scenario or situation. Does not involve deploying equipment or other resources.
  - Objectives:
    - determine if participants can realistically “talk through” their critical functions during an incident response scenario; and
    - help participants become more aware of possible weaknesses and gaps in the incident response plan

# Introduction

- Advantages
  - Can have a broad or narrow focus
  - Economical
  - Presents a real scenario in a non-threatening, non-disruptive format.
- Limitations
  - Tabletop test provides only a high-level estimate of the current potential for success of a cyber security incident response plan. Considerable uncertainty regarding the skills, available resources and actual capabilities necessary for execution of the plan.

# Introduction

- Alternative – Paper Test
  - Subject matter experts review the plan with a critical eye to verifying the facts, as well as making sure the document is clearly written; note, step-by-step, which items are correct and which ones need changing; plan coordinator collects and compares test notes.
  - Paper testing focuses on errors in the plan.

# Introduction

- Alternative – Simulation
  - Shares many characteristics with a walkthrough. A simulation is basically an on-location walkthrough test with props.
  - Highly choreographed/ participants made to experience that events are actually occurring.
  - May take weeks or months to plan.

# Introduction

- Alternative – Parallel Testing
  - CSIRT personnel actually perform steps in a test environment
  - Goal: determine if steps actually work
  - Production systems not involved.

# Introduction

- Alternative – Actual Cyber Security Event
  - CSIRT personnel actually perform steps in production environment
  - Goal: apply plan as required by the event and effect containment, remediation, and recovery.

# Agenda

- Introduction
- **Tabletop Exercise Preparations**
- Executing a Tabletop Exercise
- Evaluating the Exercise and Lessons Learned
- Checklist
- Questions

# Tabletop Exercise Preparations

- Preliminary Preparations
  - Management buy-in
  - Is the incident response plan (IRP) up to date?
  - Are personnel trained to fulfill their roles under the IRP?

# Tabletop Exercise Preparations

- Design Phase
  - Determine objectives, topics, scope, participants - the most time-consuming phase of planning a tabletop exercise.
  - Senior-level tabletop exercises typically range from one to three hours; operational-level tabletop exercises may take longer.
  - Exercise materials.

# Tabletop Exercise Preparations

- Tabletop Exercise Facilitator
  - The facilitator presents the scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making.
  - The facilitator should have the ability to redirect the participants' focus from the scenario to the objectives, should they begin focusing too much on the content of the scenario.

# Tabletop Exercise Preparations

- Data Collector
  - The data collector should be thoroughly familiar with the content of the IRP being exercised and with the exercise objectives.
  - Must know what type of information to capture during the exercise and, ultimately, document in the after action report.

# Tabletop Exercise Preparations

- Tabletop Exercise Materials
  - Agenda and logistics information.
  - Facilitator Guide
    - The purpose for conducting the exercise
    - The exercise's scope and objectives
    - The exercise's scenario(s).
    - A list of questions regarding the scenario that address the exercise objectives
    - A copy of the IRP being exercised.

# Tabletop Exercise Preparations

- Tabletop Exercise Materials
  - Participant Guide. The participant guide includes the same information as the facilitator guide without the facilitator's list of questions. Participant guides contain a list of issues to orient participants to the types of matters that may be discussed during the exercise.

# Tabletop Exercise Preparations

- Scenarios for Tabletop Exercise
  - A scenario is a sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and allow demonstration of the exercise objectives
  - Use multiple short, concise scenarios? With long, detailed scenarios, participants often spend more time dissecting the scenario and discussing its content than they spend on meeting the objectives (e.g., “talk through” critical roles and functions; identify plan weaknesses).

# Tabletop Exercise Preparations

- Common/General Scenario Questions:

- Who decides how many incident response team members would participate in handling this incident?
- Besides the incident response team, what groups within the organization would be involved in handling this incident?
- To which external parties would the incident be reported? When would each report occur? How would each report be made?
- What other communications with external parties may occur?
- What tools and resources are necessary to handle this incident?
- What aspects of the response would be different if the incident occurs at a different day and time (on-hours versus off-hours)?
- What aspects of the response would be different if the incident occurs at a different physical location (onsite versus offsite)?

# Tabletop Exercise Preparations

- Scenario Questions – Preparation
  - Would the organization consider this activity to be an incident?
  - What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?

# Tabletop Exercise Preparations

- Scenario Questions – Detection and Analysis:
  - What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to attempt to take action before the incident occurred?
  - How is this incident be recognized?
  - How would the incident response team analyze and validate this incident?
  - To which people and groups within the organization would the incident be reported?
  - How would the incident response team prioritize the handling of this incident?

# Tabletop Exercise Preparations

- Scenario Questions – Containment, Eradication, and Recovery:
  - What strategy should the organization take to contain the incident? Why is this strategy preferable to others?
  - What could happen if the incident were not contained?
  - What sources of evidence, if any, should the organization acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained? How is a chain of custody maintained?

# Tabletop Exercise Preparations

- Scenario Questions – Post-Incident Activity:
  - Who should attend the lessons learned meeting regarding this incident?
  - What could be done to prevent similar incidents from occurring in the future?
  - What could be done to improve detection of similar incidents?

# Tabletop Exercise Preparations

- Sample Scenario (all pertaining to the same site)
  - At 8:15 a.m., power management reports that it cannot establish a remote desktop connection to an historian for a SCADA system at a remote hydro plant.
  - At 8:30 a.m., a SCADA operator reports signs of a break-in at the hydro plant's generation powerhouse.
  - At 11:00 am., a SCADA operator reports from the hydro plant that a key configuration file in the SCADA system has been inexplicably altered.

# Agenda

- Introduction
- Tabletop Exercise Preparations
- Executing a Tabletop Exercise
- Evaluating the Exercise and Lessons Learned
- Checklist
- Questions

# Executing the Exercise

- Facilitator
  - Welcome participants.
  - Request that participants introduce themselves and describe their roles and responsibilities under the IRP.
  - Review scope, objectives and logistics of exercise.
  - Walk participants through scenario.
  - Pose questions designed to prompt role recognition, decision-making or coordination among participants.

# Executing the Exercise

- Data Collector

- The data collector should record observations to be included in the after action report.

- | Observation or Problem | Affected Role(s) | Resolution or Recommendation |
|------------------------|------------------|------------------------------|
|                        |                  |                              |
|                        |                  |                              |
|                        |                  |                              |

# Agenda

- Introduction
- Tabletop Exercise Preparations
- Executing a Tabletop Exercise
- Evaluating the Exercise and Lessons Learned
- Checklist
- Questions

# Evaluating the Exercise

- Hotwash
  - Immediately following the facilitated discussion, the facilitator and data collector should conduct an exercise debrief (referred to as a hotwash).
  - During the debrief, the facilitator asks participants in which areas they felt they excelled, in which areas they could use additional training, and which areas of the plan should be updated.

# Evaluating the Exercise

- After Action Report.
  - Provides a means to evaluate how well exercise objectives were met and identify areas where additional exercises might be necessary.
  - Should contain hotwash comments and documented observations made by the facilitator and data collector during the exercise.

# Evaluating the Exercise

- Incident Response Plan Owner
  - Uses after action report to enhance the IRP.
  - Follows established process for communicating IRP change within thirty calendar days of any change.

# Agenda

- Introduction
- Tabletop Exercise Preparations
- Executing a Tabletop Exercise
- Evaluating the Exercise and Lessons Learned
- Checklist
- Questions

# Tabletop Exercise Checklist

Logistics	Target Date	Completed Date
Obtain management buy-in		
Select a date for the exercise		
Reserve a conference room to accommodate participants		
Determine need for audio/visual equipment		
Identify facilitator and data collector		
Identify participants		
Invite participants		
Develop exercise materials		
Arrange printing of exercise materials		
Advance distribution of participant guide		
Ensure conference room is available insufficient time to allow for setup		
Arrange for refreshments, if appropriate		
Create attendance record		
Conduct exercise		
Prepare after action report		
Obtain management approval and update plan for changes		
Communicate plan changes within thirty calendar days of plan update.		
Retain record of exercise materials, attendance record, after action report, update communications and modified plan.		
Schedule next test		

# Resources

- Computer Security Incident Handling Guide, NIST SP 800-61 (rev1) (March, 2008)
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, NIST SP 800-84 (Sept. 2006)
- Developing an Industrial Control systems Cybersecurity Incident Response Capability, DHS (October 2009)
- Creating Cyber Forensics Plans for Control Systems, DHS (August 2008)

# Q&A and Contact Information

- Mark Simon, JD, CISSP – Sr. NERC CIP Compliance Specialist
  - +(001) 224-612-3101
  - [msimon@encari.com](mailto:msimon@encari.com)