

Tabletop Experience: Incident Response



Total Time
Two hours



Maximum Participants
30

Target

Corporate employees who participate in their organization's incident response plan, regardless of technical background or education level.

Overview

A tabletop exercise is a guided simulation in which participants role-play scenarios. It identifies team alignment gaps and weak spots during calm periods, building resilience for actual crises when real-time coordination is essential. The goal isn't perfect execution but preparation through practical scenario testing.

Learning Objectives

By the end of this experience, participants will be able to:

- Explain the importance of an incident response plan in a workplace setting.
- Identify roles and responsibilities during a security incident.
- Apply quick thinking and effective decision-making during incident scenarios.

Materials

- Incident Response checklist handouts
- Timer or stopwatch
- Participant cards (IT Security Lead, Incident Commander, Communications Lead, Legal Counsel, HR Representative, and Department Manager)
- Scenario cards for role-play
- Whiteboard or flipchart
- Markers
- Pens and notepads

Roles in the Tabletop Exercise

Facilitator: Controls exercise pace, guides discussions, updates scenarios, ensures full participation, and introduces information to test team focus.

Participants: Engage in their roles during the simulation, openly discuss their thought processes, support teammates, and respond to scenarios according to the role responsibilities.

Evaluator: Assesses strengths and weaknesses, develops after-action reports, and evaluates alignment with existing plans and procedures.

Observer: Provides subject matter expertise without direct exercise participation, and supports participants by asking relevant questions and providing guidance when needed.

Note-taker: Documents all exercise activities, discussions, identified gaps, alignment with the organization's official procedures, and suggested improvements.

Introduction

Duration: 10 minutes

Effective incident response requires clear communication, defined roles, and adaptability. Tell participants that the activities will simulate real-world scenarios and challenges, helping them develop essential skills for managing security incidents. Remember that successful incident response depends on both **team coordination** and **quick thinking**.

Activity 1: Rapid Response Checklist

 **Duration: 30 minutes**

Materials

- Timer or stopwatch
- Pens and notepads
- Incident Response checklist handouts (See Activity 1 Attachment)

Activity

This activity tests the participant's incident response plan, communication strategy, and decision-making process.

Introduce the following scenario for participants:

"A critical server within your organization is encrypted by ransomware, and the attackers demand a large sum of cryptocurrency to decrypt the files."

With the context established:

1. Distribute Incident Response checklist handouts to each participant. The checklist contains common steps in incident response in random order
2. Give participants 10 minutes to individually prioritize the steps on their checklist in the order they think is most appropriate for the ransomware scenario
3. Have participants form small groups of 3-4 members and discuss their prioritizations for 10 minutes, while ensuring each person completes their own checklist separately
4. Spend the final 10 minutes reviewing effective response sequences as a class, discussing why certain steps should come before others

Answer Key

Based on industry best practices, these are the key checklist items to include:

1. Report the incident immediately (following organizational escalation policy)
2. Mobilize the incident response team
3. Isolate affected systems
4. Document incident timeline
5. Assess data backup status
6. Activate the organization's communication plan for stakeholders
7. Follow established notification procedures for regulatory requirements
8. Engage legal counsel
9. Execute the organization's ransom response policy
10. Contact law enforcement (per organizational policy)

Activity 2: Incident Response Simulation

 **Duration: 35-60 minutes**

Materials

- Organizational participant reference cards (See Activity 2 Attachment)
- Scenario cards with complications (See Activity 2 Attachment)
- Timer or stopwatch
- Whiteboard or flipchart
- Markers
- Pens and notepads
- Organization's actual incident response plan

Activity

This activity tests cross-functional response capabilities using participants' real organizational roles, internal and external communication strategies, and decision-making processes when facing incidents with complications.

Divide participants into groups representing actual organizational incident response teams. Each participant assumes their real role in incident response or the closest equivalent participant card provided.

Instructions:

1. Provide each group with a scenario card describing a security incident with complications
2. Give groups 20 minutes to discuss and formulate a response strategy using their designated roles and the organization's procedures
3. Each group presents their plan (5 minutes per group)
4. Introduce an additional complication to each scenario (e.g., "Media has learned of the incident from a leak")
5. Give groups 10 minutes to adjust their plans based on the new information using established procedures
6. Groups present their adjusted plans and discuss how they adapted within organizational frameworks

Additional Instructions for Groups:

- Reference your organization's actual IR plan during discussions
- "Think out loud" to make decision-making visible
- Ensure all participants contribute based on their real responsibilities
- Focus on realistic actions you would actually take in your role

Discussion

 **Duration: 15 minutes**

Questions

- How did the sequencing exercise in Activity 1 prepare you for the role simulation?
- What challenges did you face in applying your organization's actual procedures?
- What gaps did you identify in your current incident response procedures?
- How well did cross-departmental communication work during the exercises?
- What additional training or resources would help you feel more prepared for these scenarios in your actual role?

Possible answers/prompts

- Challenges: coordinating across departments, accessing real contact information, clarifying actual authorities and decision-making power
- Gaps: unclear escalation paths, outdated contact information, undefined decision authorities, missing notification templates
- Improvements: regular cross-training, updated contact lists, clearer decision trees, role-specific quick reference guides
- Resources: role-specific response cards, regular drills with actual team members, updated IR plan training

Conclusion

 **Duration: 5 minutes**

Summarize key takeaways from both exercises:

- The sequencing exercise built understanding of organizational incident response procedures, while the role simulation emphasized real-world coordination challenges
- Both individual preparation and coordinated team response using actual organizational roles are essential for effective incident response
- Complications will always arise — success depends on adaptability within established frameworks

Next Steps

- Update your organization's incident response plan based on identified gaps
- Refresh contact lists and communication protocols
- Address any identified gaps in role clarity or decision-making authority
- Schedule regular tabletop exercises with actual incident response team members for continuous improvement

Activity 1 Attachment – Incident Response Checklist Handouts

Print one copy of this page for every six participants. Cut along the solid lines to create individual cards, providing one card to each participant. For greater durability, print on card stock or heavyweight paper.



Rapid Response Checklist

- ☐ Isolate affected systems
- ☐ Report the incident immediately (following organizational escalation policy)
- ☐ Assess data backup status
- ☐ Contact law enforcement (per organizational policy)
- ☐ Engage legal counsel
- ☐ Execute the organization's ransom response policy (consultation required)
- ☐ Activate the organization's communication plan for stakeholders
- ☐ Document incident timeline
- ☐ Follow established notification procedures for regulatory requirements
- ☐ Mobilize the incident response team

Rapid Response Checklist

- ☐ Isolate affected systems
- ☐ Report the incident immediately (following organizational escalation policy)
- ☐ Assess data backup status
- ☐ Contact law enforcement (per organizational policy)
- ☐ Engage legal counsel
- ☐ Execute the organization's ransom response policy (consultation required)
- ☐ Activate the organization's communication plan for stakeholders
- ☐ Document incident timeline
- ☐ Follow established notification procedures for regulatory requirements
- ☐ Mobilize the incident response team

Rapid Response Checklist

- ☐ Isolate affected systems
- ☐ Report the incident immediately (following organizational escalation policy)
- ☐ Assess data backup status
- ☐ Contact law enforcement (per organizational policy)
- ☐ Engage legal counsel
- ☐ Execute the organization's ransom response policy (consultation required)
- ☐ Activate the organization's communication plan for stakeholders
- ☐ Document incident timeline
- ☐ Follow established notification procedures for regulatory requirements
- ☐ Mobilize the incident response team

Rapid Response Checklist

- ☐ Isolate affected systems
- ☐ Report the incident immediately (following organizational escalation policy)
- ☐ Assess data backup status
- ☐ Contact law enforcement (per organizational policy)
- ☐ Engage legal counsel
- ☐ Execute the organization's ransom response policy (consultation required)
- ☐ Activate the organization's communication plan for stakeholders
- ☐ Document incident timeline
- ☐ Follow established notification procedures for regulatory requirements
- ☐ Mobilize the incident response team

Rapid Response Checklist

- ☐ Isolate affected systems
- ☐ Report the incident immediately (following organizational escalation policy)
- ☐ Assess data backup status
- ☐ Contact law enforcement (per organizational policy)
- ☐ Engage legal counsel
- ☐ Execute the organization's ransom response policy (consultation required)
- ☐ Activate the organization's communication plan for stakeholders
- ☐ Document incident timeline
- ☐ Follow established notification procedures for regulatory requirements
- ☐ Mobilize the incident response team

Rapid Response Checklist

- ☐ Isolate affected systems
- ☐ Report the incident immediately (following organizational escalation policy)
- ☐ Assess data backup status
- ☐ Contact law enforcement (per organizational policy)
- ☐ Engage legal counsel
- ☐ Execute the organization's ransom response policy (consultation required)
- ☐ Activate the organization's communication plan for stakeholders
- ☐ Document incident timeline
- ☐ Follow established notification procedures for regulatory requirements
- ☐ Mobilize the incident response team

Activity 2 Attachment – Organizational Participant Reference Cards and Scenario Cards

Print this attachment and cut along the solid lines to separate the cards shown on this page.

For greater durability, print on card stock or heavyweight paper.



Participant Card IT Security Lead

- Responsible for technical incident containment and analysis
- Assesses the scope and nature of the security breach
- Implements immediate containment measures
- Directs forensic analysis activities
- Coordinates with external security vendors



Participant Card Incident Commander

- Overall incident response leader and decision-maker
- Coordinates all response team activities
- Makes critical strategic decisions
- Brief executive leadership
- Allocates resources and priorities



Participant Card Communications Lead

- Manages all internal and external messaging
- Executes existing communication plans
- Drafts stakeholder notifications
- Coordinates with the media and PR team
- Monitors social media and news coverage



Participant Card Legal Counsel

- Advises on legal implications and regulatory compliance
- Ensures compliance with breach notification laws
- Advises on evidence preservation
- Reviews all external communications
- Coordinates with law enforcement if needed



Participant Card HR Representative

- Handles employee-related aspects of incident response
- Manages internal employee communications
- Handles insider threat investigations
- Coordinates employee support services
- Addresses workforce continuity needs



Participant Card Department Manager

- Represents affected business unit operations
- Assesses business impact on your department
- Implements business continuity measures
- Coordinates with other department managers
- Reports operational status to Incident Commander



Scenario Ransomware Attack with Data Theft

“Your organization’s file servers are encrypted by ransomware. The attackers also stole customer financial data and are threatening to release it publicly if the ransom isn’t paid within 24 hours. Complication: The backup systems show signs of compromise from 2 weeks ago.”



Scenario Business Email Compromise

“The CFO’s email account was compromised and used to authorize a \$500,000 wire transfer to an unknown account. The transfer was completed this morning. Complication: Similar fraudulent emails have been sent to three major clients requesting ‘updated payment information.’”



Scenario Insider Data Theft

“A departing employee in IT was caught copying sensitive customer records to a personal USB drive. Security stopped them at the exit, but they claim the data is ‘just personal work files.’ Complication: The employee has already posted cryptic messages on LinkedIn about ‘taking valuable experience to my new role.’”

Activity 2 Attachment – Scenario Cards and Additional Complications Cards

Print this attachment and cut along the solid lines to separate the cards shown on this page.

For greater durability, print on card stock or heavyweight paper.



Scenario

Supply Chain Compromise

“ Your organization’s main software vendor reports that their update server was compromised, and malicious code may have been distributed to customers. Your systems received updates yesterday. Complication: The vendor is refusing to provide technical details, citing their own ongoing investigation. ”



Scenario

Physical Security Breach

“ An unauthorized person was found in the server room after hours with a laptop connected to the network. Security escorted them out, but they claimed to be ‘from IT support.’ Complication: Several employees report that their badge access logs show unusual after-hours activity they didn’t perform. ”



Scenario

Cloud Service Compromise

“ Your cloud storage service provider reports unauthorized access to your organization’s data repository containing customer information and trade secrets. The breach may have lasted several weeks. Complication: The cloud provider’s initial communication contains conflicting information about the timeline and scope. ”



Additional Complications

“ Media Alert: A technology blog has published an article about your organization’s security incident with specific details not yet publicly disclosed. ”



Additional Complications

“ Regulatory Notice: Your industry regulator has contacted you requesting immediate information about the incident and your response measures. ”



Additional Complications

“ Client Crisis: Your largest client has called an emergency meeting to discuss the security of their data and is threatening to terminate their contract. ”



Additional Complications

“ Internal Leak: Employees are discussing the incident details on internal messaging systems, and some information appears to be inaccurate. ”



Additional Complications

“ System Failure: During your response efforts, a critical business system has gone offline, potentially due to your containment measures. ”



Additional Complications

“ Legal Threat: You’ve received a letter from a law firm representing affected customers, demanding detailed information about the breach and your security measures. ”