hyperproof

Tabletop Exercise Template

PURPOSE

Tests your organization's ability to respond effectively to supply chain disruptions while identifying gaps in communication and decision-making processes.

WHEN TO USE

Quarterly as part of business continuity planning, after major incidents, or when onboarding new team members to supply chain roles.

SCENARIO

Your primary software vendor experiences a ransomware attack that takes their systems offline indefinitely. This vendor provides your customer relationship management system used by 200+sales representatives.

Note: This is just a sample scenario, and you should tailor it for your organization's unique supply chain.

Exercise timeline (90 minutes):

Phase 1: Initial response (30 minutes)

- Minute 0: Facilitator announces the incident
- Minutes 1-15: Teams assess immediate impact and gather information
- Minutes 15-30: Teams develop initial response plan and communication strategy

Phase 2: Escalation and decision-making (30 minutes)

- Minutes 30-45: Teams brief executive leadership and request resources
- Minutes 45-60: Teams implement workaround solutions and vendor communication

Phase 3: Recovery planning (30 minutes)

- Minutes 60-75: Teams develop long-term recovery strategy
- Minutes 75-90: Debrief and identify improvement opportunities

Key discussion points

- How quickly did you identify the business impact?
- What information did you need but couldn't access?
- Who had the authority to make spending decisions for alternative solutions?
- How did you communicate with affected customers and internal teams?
- What would you do differently in a real incident?

Evaluation criteria

- ☐ Incident response team assembled within 15 minutes
- ☐ Business impact assessment completed within 30 minutes
- ☐ Executive notification occurred within 45 minutes
- ☐ Alternative solution identified within 60 minutes
- ☐ Customer communication plan developed within 75 minutes

Implementation tips

- Include representatives from all departments affected by supply chain disruptions
- Vary scenarios to test different types of supply chain risks (cyber, operational, financial)
- Document lessons learned and update incident response procedures accordingly