IR Tabletop Best Practices

June 2026

TBDCyber

INCIDENT RESPONSE SIMULATION GUIDE

Before designing a tabletop exercise (TTX), align on the target audience, decision type, and outcome the session is meant to drive

3 options for TTX target audience

C-Suite / Board

Business / Corporate Functions

Technical

Technical

- **Primary focus:** Detection, triage, containment, eradication, recovery
- **Best fit when:** The goal is to test operational response, tool dependencies, escalation paths, and technical handoffs
- **Typical participants:** Security, IT, infrastructure, application owners, platform teams, key technical vendors
- **Design considerations:** Use realistic alerts, system impacts, and response decisions tied to the environment

Business / corporate functions

- **Primary focus:** Business disruption, client impact, legal review, communications, finance, HR, and service continuity
- **Best fit when:** The goal is to test cross-functional coordination and business leaders response for incident beyond IT
- **Typical participants:** Business leaders, service line owners, Legal, Communications, HR, Finance, Risk, Operations
- **Design considerations:** Include customer impacts, regulatory deadlines, escalations, and external party engagement points

C-suite / board

- **Primary focus:** Crisis leadership, materiality, disclosure, enterprise prioritization, and oversight decisions
- **Best fit when:** The goal is to test executive judgment, strategic tradeoffs, and board visibility during a high-impact event
- **Typical participants:** C-suite leaders, Board representatives, CISO, CIO, CLO, and select senior functional leads
- **Design considerations:** Align early with the CIO and CLO on scope, sensitivity, approval approach, and Board timing

TBDCyber

INCIDENT RESPONSE SIMULATION GUIDE

For exercise designers and facilitators

DO: Design with purpose

- Define clear objectives tied to real organizational risks (ransomware, data exfiltration)
- Build multi-phase scenarios that escalate (detection > analysis > containment > recovery > post-incident)
- Include cross-functional participants(e.g. InfoSec, Legal, Finance, Communications)
- Tailor scenarios to business-specific systems and vendor dependencies
- Set an annual tabletop strategy to align leadership on target audiences, priority scenarios, and exercise cadence

DON'T: Common pitfalls

- Limit exercises to technical security teams only; include business and executive stakeholders
- Assume SOC or tooling will always be available
- Skip the communications cascade test, including external notifications
- Design exercises based solely on IT scenarios, without revenue-critical systems
- Share the scenario details to stakeholders prior to TTX
- Focus on trying to find the right answer, discussion is paramount

What should you do during the TTX?

Execution best practices

- Test leadership succession: what happens if the CISO or incident commander is unavailable?
- Inject real-world pressure: media inquiries, regulatory deadlines, ransom demands
- Probe for documented processes vs. tribal knowledge; if it's not written down, it's a gap
- Evaluate both technical response and communications readiness in the same exercise
- Validate fallback communications by testing primary, alternate, contingency, and emergency channels if core tools are unavailable
- Test engagement handoffs, and decision points for external parties such as counsel and outside IR

What should you do after the TTX?

Post-exercise: close the loop

- Deliver after-action findings with priority levels (Primary, Secondary, Tertiary) and timelines
- Categorize Areas for Improvement: short-term (1-3 mo), mid-term (3-6 mo), long-term (6-12 mo)
- Track remediation progress with assigned owners and due dates
- Use findings to update the IRP, BCP, playbooks, and communication protocols
- Schedule follow-up exercises within 6-12 months to validate improvements

TBDCyber

INCIDENT RESPONSE SIMULATION GUIDE

For exercise participants

What should participants do to prepare for a tabletop exercise?

Before a tabletop exercise

1

- Review the incident response plan and know your role
- Confirm your escalation path and backup decision-makers
- Know where critical documents are stored (e.g., contracts, playbooks)
- Review lessons learned and Areas for Improvement from prior exercises
- Understand manual workarounds if key systems go down

During a tabletop exercise

2

- Respond as you would in a real incident, not with what "sounds good"
- Surface gaps openly and focus on future improvement and not performance
- Think about communications early
- Consider downstream impacts: clients, regulators, tenants
- Own the tasks, and try to explain what happens next
- Challenge assumptions about availability and backups

After a tabletop exercise

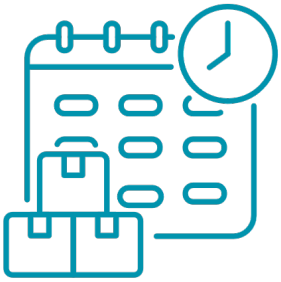
3

- Own your assigned Areas for Improvement and commit to implementation timelines
- Participate in updates as needed and familiarize yourself with revised playbooks, runbooks, and contact lists
- Share lessons learned with your broader team
- Advocate for follow-up exercises to validate improvements

TBDCyber

4 AREAS FOR A COMPLETE TTX PREP KIT

Scheduling, objectives, roles, and inject planning

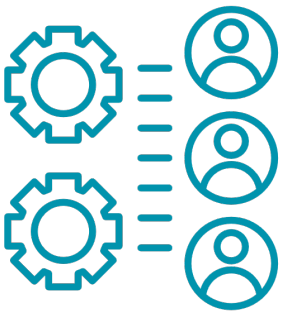


01. Scheduling and logistics

- ❑ Confirm date, duration, and attendee list with alternates
- ❑ Send pre-reads: IRP, comms plan, contact lists, vendor support paths
- ❑ Validate access to exercise artifacts: email, EDR, SIEM, ticketing
- ❑ Confirm bridge details and backup channels for PACE

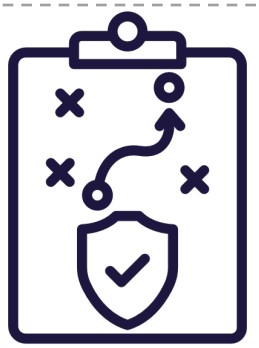
02. Objectives

- ❑ Test detection to containment decisions using real alerts and evidence
- ❑ Confirm escalation paths and leadership handoffs
- ❑ Exercise communications cascade and executive approvals
- ❑ Capture Areas for Improvement with owners and target timelines



03. Roles

1. Facilitator and inject controller
2. Incident commander and technical leads (SOC, IAM, infra, apps)
3. Legal, privacy, corporate communications, service line leaders
4. External parties on call: breach counsel, outside IR, cyber insurer
5. Scribe and timekeeper



04. Inject planning

- ❑ Define inject phases: detection, analysis, containment, recovery
- ❑ Create injects with artifacts and decision prompts
- ❑ Include comms, legal, vendor, and executive pressure injects
- ❑ Avoid sharing scenario details prior to the TTX

TBDCyber