NET-TECH CONSULTING

Real People, Real Protection, Right Now

Tabletop Exercises
Cyber Incident Response

No-fault simulation to validate roles, decisions, communications, and evidence — before the real incident.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Why tabletop exercises exist

Plans don’t fail on paper — they fail under pressure.

Incidents create decision fog

- Roles blur
- Communication gets noisy
- Evidence goes missing
- Recovery assumptions break

Tabletops turn intent into muscle memory

- Practice the IRP flow
- Clarify escalation paths
- Pressure-test tooling and vendors
- Surface gaps while it’s safe

Outcome

- Clear “who does what”
- A prioritized improvement list
- Evidence you can reuse for audits and insurance

What a tabletop is

A 90–120 minute, discussion-based simulation — scoped and facilitated.

Core characteristics

- No-blame / no-fault
- Realistic scenario with injects
- Focus on decisions + comms
- Captures timing and evidence needs

Common scenarios

- Ransomware / malware
- Microsoft 365 compromise
- Vendor access incident
- Operational disruption with cyber root cause

Designed to improve the program

- Feeds updates into the IRP and DRP
- Creates remediation items with owners
- Builds repeatable cadence (quarterly/annual)

NET-TECH CONSULTING
Real People, Real Protection, Right Now

What you walk away with

A complete tabletop “evidence pack” — not just a meeting.

Exercise kit

- Annotated agenda
- Facilitator guide + narrative
- Participant materials + sign-in
- Inject scenarios

After-action outputs

- After-Action Report (AAR)
- Strengths observed
- Gaps + recommendations
- Action items with owners

Documentation & evidence

- Meeting notes + incident timeline (if produced)
- Links to supporting logs/tickets
- Artifacts stored where your team tracks compliance

NET-TECH CONSULTING
Real People, Real Protection, Right Now

How it works

Prep → simulate → capture findings → update plans.

Prep (48 hrs prior)

- Confirm participants
- Share IRP/DRP/WISP
- Gather rosters + logs

Session (90–120 min)

- Walk scenario phases
- Introduce injects
- Capture decisions + gaps

After-action (1–3 days)

- Draft AAR
- Prioritize actions
- Assign owners

Update + evidence

- Revise IRP/DRP
- Store artifacts
- Schedule follow-up

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Scenario flow (example)

Ransomware simulation — from detection to recovery.

1

Detect + confirm

User reports, alerts, service disruption

2

Triage + categorize

Open incident ticket, classify severity

3

Notify stakeholders

Activate IRT roles and escalation

4

Contain

Isolate devices, revoke access, disable accounts

5

Recover + restore

Validate backups, restore systems, confirm endpoints

6

Document + improve

Timeline, exceptions, AAR, update IRP/DRP

Communications, insurance & escalation

Clear channels, fast decisions, defensible documentation.

Internal channels

- IRT coordination: Teams channel or emergency bridge
- Documentation: incident ticket with updates + links
- Exception register: log key deviations and decisions

Insurance & legal touchpoints

- Notify carrier within 24–48 hrs of confirmed incident
- Document: timeline, affected systems, containment actions
- Legal review before public / regulatory comms
- Escalate if regulated data may be impacted

Tabletop forces the hard questions

- Who approves external statements?
- What if ticketing/email is down?
- What if the most recent backup is corrupted?

Roles + decision points

We confirm ownership, escalation, and what “done” means.

Typical participants

- IT Director / IT lead
- vCISO / security lead
- Compliance / risk lead
- CFO (impact + insurance)
- HR (employee comms/access)

Optional injects (pressure tests)

- Endpoint control dashboard unreachable
- Backup appears corrupted
- External partner requests a formal statement
- Payroll / critical app access disrupted

Wrap-up prompts

- What went well?
- Where was there confusion or ambiguity?
- What should we revise in the IRP/DRP?
- What can we improve in the next 30 days?

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Where tabletop exercises fit

They validate the program — and create a backlog you can execute.

vGRC + vCISO service

- Quarterly/annual tabletop cadence
- Evidence capture and reporting
- Follow-through on corrective actions

Fast-Track Remediation

- Close the top gaps the tabletop exposes
- Update plans and proof
- Reduce repeat findings next cycle

Tooling alignment (optional)

- Validate alerting and escalation paths
- Confirm backup and recovery assumptions
- Reduce “unknowns” across vendors and platforms

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Next steps

Pick the scenario, confirm the room, and run the simulation.

To schedule a tabletop

- Choose scenario type (ransomware, M365 compromise, vendor incident)
- Confirm participants (IT + compliance + finance + HR as needed)
- Share current IRP/DRP/WISP 48 hours prior
- We deliver the AAR + evidence pack after the session

Contact

Scott Munden | Chief Compliance Officer
scott.Munden@net-tech.us | 877-449-8324