INDUSTRIAL CYBERSECURITY TABLETOP EXERCISE PLANNING CHEAT SHEET

"1 in 5 industrial sites — power substations, manufacturing plants, and water operations — experience cyber incidents that disrupt safety and engineering production. 20% of facilities take more than a month to recover."

Practical preparation for engineering-aligned ICS/OT incident response exercises protects our critical infrastructure.

THE ICS DEFENSE FORCE ICS/OT TABLETOP EXERCISE PLANNING CHEAT SHEET

Security and engineering teams that practice regularly with realistic, threat-informed tabletop scenarios consistently demonstrate stronger coordination across engineering, operations, and cybersecurity They identify gaps earlier, reduce hesitation during incidents, and improve detection and industrial incident containment across the full ICS cyber kill chain. This cheat sheet helps your team capture the essential information needed to begin planning a realistic, high-value, engineering-aligned ICS/OT incident response exercise.

1. CORE INFORMATION

Facility / Site Name: _____
Sector / Operations Type: _____
Primary Processes / Critical Functions: _____
Required Participants (OT, IT, Engineering, Cyber, Ops): _____

2. READINESS CHECK (SELECT ALL THAT APPLY)

☐ Documented ICS/OT incident response (IR) plan exists
☐ Roles defined across OT, IT, Engineering, and Security
☐ Engineering asset backups exist (PLC / HMI / SCADA servers) and have been tested
☐ Recent OT/ICS network visibility review completed

☐ Previous tabletop exercise completed within the last 12 months
☐ Leadership is aware of ICS/OT incident priorities

3. EXERCISE PRIORITIES (SELECT ALL THAT APPLY)

☐ Improve OT/IT/Engineering coordination
☐ Validate ICS/OT IR Plan, roles & responsibilities
☐ Test engineering escalation & decision flow
☐ Analyze safety impacts and manual-mode processes
☐ Identify visibility, logging, and boundary gaps for threat hunting
☐ Satisfy compliance or audit requirements
☐ Other: _____

4. CRITICAL SYSTEMS (HIGH-LEVEL ONLY)

PLCs / RTUs / HMIs: _____
SCADA / Historian: _____
Safety Systems: _____
Remote Access Paths: _____
Engineering Workstations: _____
Manufacturing Execution Systems (MES): _____
Quality Control Systems: _____
Enterprise Resource Planning Systems (ERP): _____

5. SCENARIO CONSTRAINTS

☐ Must not impact production or live engineering process
☐ Must consider manual mode / fail-safe states
☐ Include relevant vendors or contractors
☐ Respect safety, regulatory, and operational constraints

6. SUCCESS INDICATORS

☐ Clearer ICS/OT incident response roles and responsibilities
☐ Improved decision flow across stakeholder teams
☐ Identified engineering and operational constraints
☐ Identified critical engineering assets
☐ Identified dependencies on external resources, networks, assets, and connections
☐ Documented action items to improve readiness

7. OPTIONAL (IF ENGAGING WITH ICS DEFENSE FORCE)

Industry data shows that 1 in 5 industrial sites—including power substations, manufacturing plants, and water operations—experience cyber incidents that disrupt safety and production, with 20% taking more than a month to recover.

Organizations can use this *Industrial Cybersecurity Tabletop Exercise Planning Cheat Sheet* to self-facilitate discussions and begin exercising their ICS/OT incident response plans—an important first step!

To maximize value and impact, organizations can opt for a fully facilitated, engineering-aligned tabletop. ICS Defense Force delivers realistic, sector-specific ICS/OT exercises that strengthen coordination across engineering, operations, and cybersecurity through structured injects, guided decision points, and independent challenge—supported by custom, facility-specific participant workbooks that surface gaps teams often can't identify on their own.

To learn more and discuss your ICS/OT incident response tabletop exercise, connect with Dean on LinkedIn or contact ICS Defense Force directly.

https://www.icsdefenseforce.com/