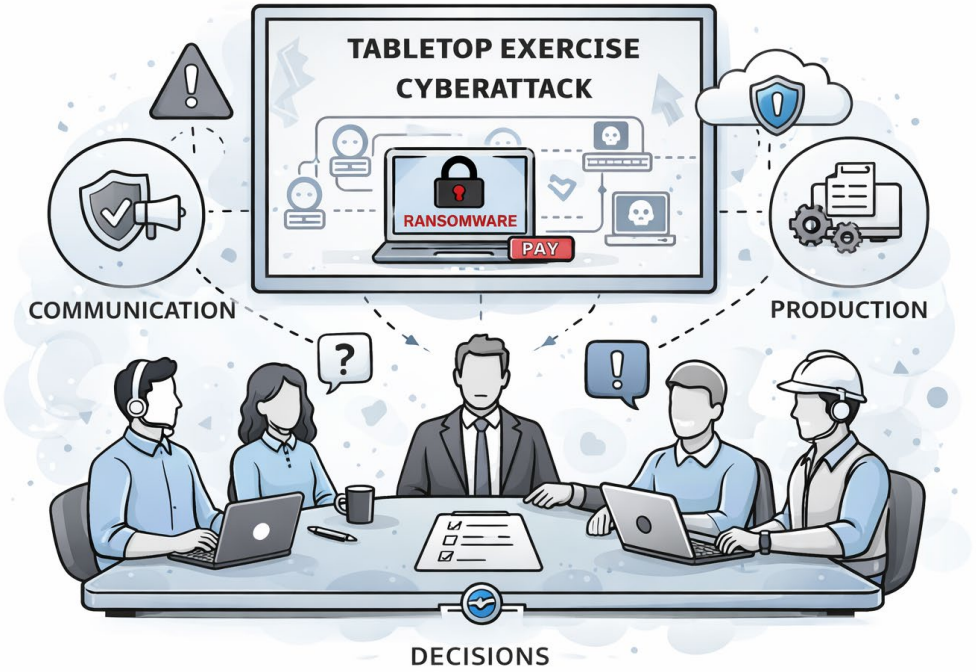
Tabletop Exercise



The tool have been provided in connection with the project **Cybersecurity and Business Continuity** (www.cyber-smv.dk), funded by the Danish Industry Foundation. Publication date: 29.12.2025

Tabletop Exercise*

→A tabletop exercise is a structured walkthrough of a realistic cyberattack, where relevant roles (management, information technology (IT), operational technology (OT), operations, communications, etc.) discuss:

- → What is happening?
- → Who is responsible for what?
- → Which decisions need to be made – and when?
- → How should communication be handled internally and externally?

→The purpose of the exercise is to test:

- → The organization's preparedness for a cyber incident.
- → The interaction between IT and OT.
- → Decision-making processes under pressure.
- → Internal and external communication.

→The exercise typically takes place as a facilitated meeting - no systems are shut down or attacked in practice.

*It is called a **tabletop exercise** because the exercise originally took place around a table ("tabletop"), where participants worked together with maps, plans, scenarios, and decisions without carrying out the actions in real life.

Scenario phases

→Phase 1: Detection.
→Phase 2: Escalation and decision-making.
→Phase 3: IT/OT impact.
→Phase 4: Communication.
→Phase 5: Recovery.

Outcome

→Roles and responsibilities (completed during the exercise):
- → Role, name, and responsibilities for, for example, the incident response lead, IT manager, production manager, communications officer, and external participants (customers or suppliers).

→Document identified strengths.

→Document identified weaknesses.

→Improvement areas:
- → List actions, responsible owner, and deadline.

→Follow-up:
- → When will the exercise be repeated?
- → Does the cyber incident response plan need to be updated?
- → Should technical tests be carried out (e.g., backup recovery or PLC failover)?

Examples of tabletop exercises

	Ransomware hits the ERP system – production is indirectly affected	The attack spreads from office IT to the production network	Supplier access is misused (remote support)	Data breach involving employee or customer data
Type	IT → OT	IT ↔ OT	Supply chain / OT	IT / compliance
Scenario	An employee clicks on a phishing link The ERP system is encrypted Production planning and order management are unavailable	IT detects malware on multiple PCs The OT responsible notices instability in the SCADA system There is a risk of production shutdown	An external supplier has remote access to PLC/SCADA The account is compromised Unauthorized changes are detected	HR or customer data is leaked The press or customers make inquiries A deadline applies for reporting to the Data Protection Authority
Tabletop focus	When do we recognize that it is ransomware? Who decides to shut down systems? Can production continue manually? When and how are customers informed?	Are IT and OT sufficiently segregated? Who is authorized to decide to stop production? When is safety prioritized over output?	How is the misuse detected? Who contacts the supplier? Is all external access shut down – and when? Documentation and accountability	When does it constitute a data breach? Who reports it to the Data Protection Authority? What do we say publicly – and when?
Primarily tests	Management decisions Backup and recovery Communication	Interaction between IT and production Decision authority Escalation	Supplier management Access control Incident preparedness outside normal working hours	Legal understanding Communication preparedness The role of management