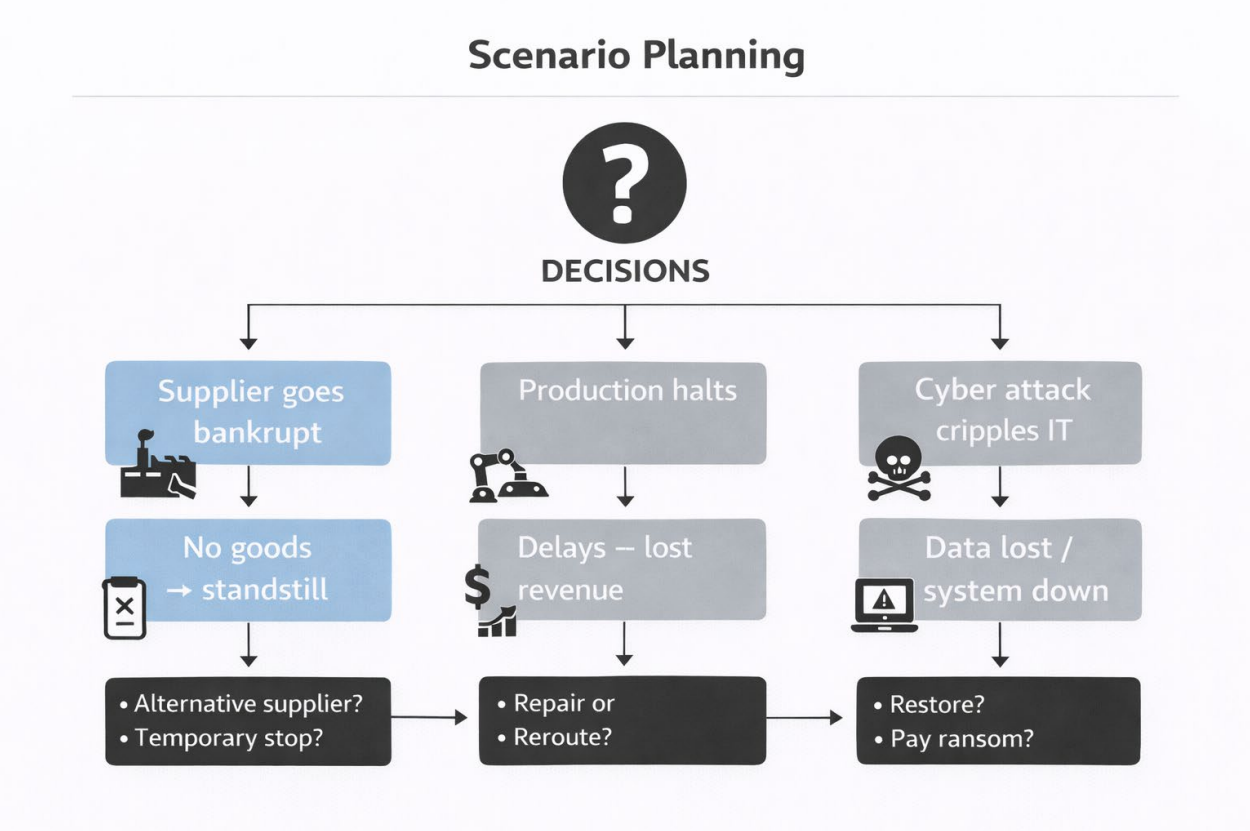
Scenario Planning



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

Cybersecurity scenario planning (IT and OT)

→Scenario planning for cybersecurity for information technology (IT) and operational technology (OT) is a method where a company systematically prepares for specific cyber attacks by reviewing realistic incident scenarios – both for general IT and OT.

→**Purpose and Scope:**

- →Purpose: For example, identifying critical cyber threats, assessing consequences and planning preparedness, and ensuring rapid and controlled handling of cyber incidents (e.g. ransomware, phishing and system crashes).
- →Scope: For example, IT systems (ERP, CRM, networks), OT systems (PLCs, SCADA, production equipment), data, employees and external parties.

Procedure

1. Define the Team: Assemble a cross-functional team with IT, OT, production, and management.
2. Map Assets: Identify critical IT and OT systems.
3. Identify Threats and Scenarios: Brainstorm possible cyber threats and failure scenarios for both IT and OT.
4. Make a Consequence Analysis.
5. Prioritize Scenarios: Assess which threats require the most focus.
6. Strategies and Preparedness: Describe preventive and reactive measures.
7. Plan Training and Testing: Simulate scenarios and evaluate.
8. Maintain: Update the plan annually, after changes in technology or organization, and after exercises.

Map assets: Identify critical IT and OT systems

System	Type (IT/OT)	Description	Criticality (H, M, L)	Owner

Note: H = High, M = Medium, L = Low

Map assets: Identify critical IT and OT systems (examples)

System	Type (IT/OT)	Description	Criticality (H, M, L)	Owner
ERP-system	IT	Manages finances, inventory, purchasing, planning; without it, order processing and purchasing can stop.	High	IT-Manager
MES-system	OT	Control of machines. Monitors production schedules, resource allocation, and workflow; critical for efficient production.	High	Production Manager
SCADA-system	OT	Remote monitoring of process plants; stops production if unavailable.	High	Production Manager
Backup-system	IT	Ensures data redundancy; critical for rapid recovery from IT incidents.	High	IT-Manager
E-mail and communication system	IT	Internal and external communication; essential for coordination and crisis management.	High	IT-Manager
Sensors/IoT-entities	OT	Physical devices that collect data from the environment (e.g., temperature, pressure, vibration, humidity or position) and send the data digitally to other systems via networks (internet, local area network, mobile network, etc.).	Medium	Responsible for OT

Note: H = High, M = Medium, L = Low

Identify Threats and Scenarios (examples)

Threat/Scenarios	Attack type	Probability	Consequence	Priority	Indicators
Ransomware on ERP	IT	Medium	High	High	Unusual file encryption, login error
Phishing attacks against employees	IT	High	Medium	High	Suspicious emails, unauthorized login attempts
Malware on production control (PLC/SCADA)	OT	Low	High	High	Abnormal machine commands, production stops
DDoS attacks against networks	IT	Medium	Medium	Medium	Network outage, slow internet access
Sabotage via external suppliers	OT	Low	High	High	Unusual activity in OT systems

Note: DDoS = Distributed Denied-of-Service (is a cyber attack where many computers simultaneously overload a server or network, making a website or digital service slow or completely inaccessible to normal users).

Consequence Analysis

For each threat/scenario, the following is described:

1. Production downtime (hours/days).
2. Financial loss.
3. Employee safety risk.
4. Extent of data loss or leak.
5. Reputational risk.

Strategies and Preparedness (examples)

Scenario	Preventive strategies	Reactive strategies	Responsible
Ransomware on ERP	Antivirus, firewall, training, backup	Restore from backup, isolate systems, inform emergency staff	IT-Manager
Phishing attacks against employees	Security awareness training, email filtering	Lock compromised accounts, change passwords	IT-Manager
Malware on production control (PLC/SCADA)	OT network segmentation, software update	Isolate affected PLC, manual operation, safety team activated	Responsible for OT
DDoS attacks against networks	Redundant network, cloud protection	Traffic filtering, contact Internet Service Provider	IT-Manager
Sabotage via external suppliers	Access control, contract requirements, monitoring	Audit of logs, crisis team activated	Responsible for OT

Training and Test (examples)

IT

→Phishing simulations.
→Backup recovery.
→Network attack testing.

OT

→SCADA / PLC failover test (a planned test to check whether a redundant PLC setup can automatically and correctly take over control if the primary PLC fails or is taken out of service).
→Manual operation under attack.
→Scenario exercises with crisis management staff.

Maintenance

→Update scenarios at least annually or after major changes in IT/OT.
→Revise contact information, roles, and responsibilities.
→Evaluate training and testing results and adjust strategies.