CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

Defense in Depth

www.cyber-smv.dk

The tool has been developed as part of the project **Cybersecurity and Business Continuity** (www.cyber-smv.dk), supported by the Danish Industry Foundation. Published on May 12, 2026.

Defense in Depth

Purpose

→To understand why security is an interaction between people, processes, and technology.

→To eliminate the idea of ‘the one right tool’.

Mental model

→*No security measure is perfect — but several working together are effective.*

Participants

→Employees from administration and production.

→Particularly relevant for management and process owners.

Input

→Visualization of multiple security layers.

→Examples of controls (multi-factor authentication, procedures, awareness).

Short scenario

A. Short company scenario

→ A Danish manufacturing company with approximately 90 employees:
- → ERP system.
- → Operational Technology (OT).
- → Suppliers and remote access.
- → Email, access cards, and shared networks.

→ The company wants to protect:
- → Production.
- → Customer data.
- → Deliveries.
- → Reputation.

B. Incident:

→ An attacker attempts to:
- → Trick employees into revealing login credentials through phishing.
- → Gain access to systems.
- → Move toward the production environment.

Process: Step 1 – Map the layers

Task: What layers of protection exist, or should exist, in the company?

→Layers should be identified within areas such as:
- →People (behavior, awareness, training).
- →Processes (procedures, approvals, escalation).
- →Technology (systems, access control, segmentation).
- →Physical security (access, locks, visitors).

→Examples:
- →Access cards.
- →Multi-factor authentication.
- →Segmentation.
- →Awareness training.
- →Backup.
- →Management approval.

Process: Step 2 – Remove a layer

Task: Choose one layer that fails or is missing.
→What happens if this layer does not work?
→Which other layers can still limit the damage?
→Where does the company become vulnerable?

👉 **Key point:** The layers should overlap, not stand alone.

Process: Step 3 – The employee's role in the layers (10–15 min.)

Questions:

→Which layers depend directly on employee behavior?
→Where can a single action strengthen or weaken multiple layers?
→What can employees specifically do to be an active layer of defense?

→Examples:
- → Pause before clicking.
- → Follow procedures, even under pressure.
- → React to irregularities.
- → Report errors and suspicious activity.

Possible solutions: Step 1 – Map the layers

Example of identified layers in a Danish manufacturing SME

- → People:
  - → Employees' awareness of emails and phone calls.
  - → Awareness training in phishing and social engineering.
  - → A culture where it is acceptable to pause and ask questions.
- → Processes:
  - → Approval procedures for changes to supplier data.
  - → A clear escalation path in case of suspected security incidents.
  - → Access management based on roles and job responsibilities.
- → Technology:
  - → Multi-factor authentication.
  - → Antivirus and email filtering.
  - → Network segmentation between office IT and production.
  - → Logging and monitoring.
- → Physical security:
  - → Access cards for buildings.
  - → Visitor registration.
  - → Separation between office and production areas.

👉 **Key point:** Security consists of several overlapping layers, and many of them are not technical, but organizational and human.

Possible solutions: Step 2 – Remove a layer

Example: Multi-factor authentication does not work/is not enabled

What happens if this layer fails?
→ The attacker can log in using a stolen username and password.
→ The risk of unauthorized access increases significantly.

Which other layers can still limit the damage?
→ Role-based permissions limit what the attacker can view and change.
→ Network segmentation protects the production systems.
→ Monitoring can detect unusual behavior.
→ Employees can react to suspicious activity.

Where does the company become vulnerable?
→ If several layers are missing at the same time (e.g., monitoring is also missing).
→ If access rights are too broad.

👉 **Key point:** One layer is never enough. The layers must compensate for each other when something fails.

Possible solutions: Step 3 – The employee's role in the layers

Which layers depend directly on employee behavior?

- → Phishing protection (whether the first click happens or not).
- → Compliance with procedures and approvals.
- → Reporting suspicious incidents.
- → Physical access (closing doors, following visitor rules).

Where can one action strengthen or weaken multiple layers?

Example:

- → If an employee clicks on a phishing link → It weakens both the human layer and the technical layer.
- → If an employee pauses and reports a suspicious email → It strengthens both the human layer, monitoring, and processes.

What can employees specifically do?

- → Take time to assess emails and phone calls, especially under pressure.
- → Follow procedures, even when they seem inconvenient.
- → React to irregularities and speak up.
- → Accept security measures such as multi-factor authentication and controls.

👉 **Key point:** Employees are not the weakest link, but an active security layer when the framework supports them.