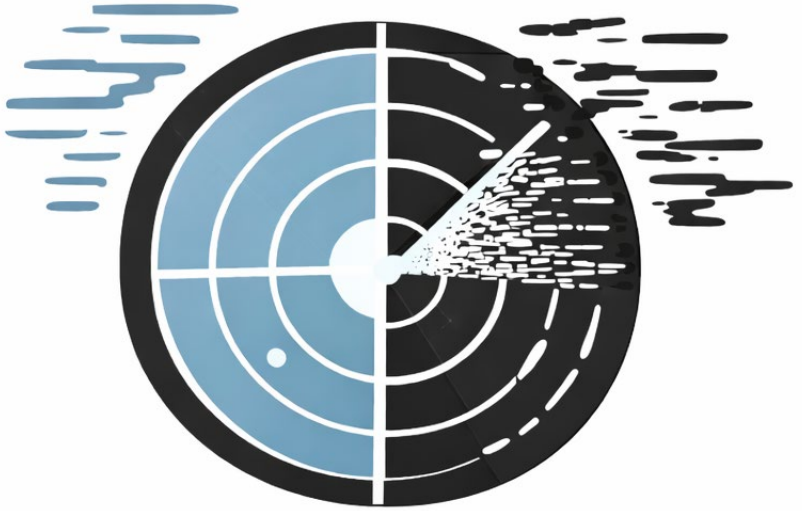
CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

Attention Economics



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.

Attention Economics

Purpose

→To understand the difference between important security signals and everyday noise.
→To become aware that attention is a limited resource.
→To prioritize what requires action and what does not.
→To reduce the risk of overlooking critical warnings in a busy workday.

Mental model

→*Attackers compete for your attention.*

Participants

→All employees

Input

→Overview of incidents.

Incidents (examples)

1. Email about a changed supplier bank account number.
2. Pop-up about a software update.
3. A colleague asking for quick help.
4. An email marked “urgent” from an unknown sender.
5. Error message from the production system.
6. Notification about a new Teams meeting.
7. IT email about possible phishing.
8. SMS from a “shipping company.”
9. System warning that appears frequently.
10. Internal message from a manager without details.

Procedure: Step 1 – Sort Signals and Noise

→The participants must place each incident into one of three categories:
  →**Signal** - requires attention or action.
  →**Noise** - can be ignored or postponed.
  →**Uncertain** - requires clarification.
→The participants discuss:
  →What makes this incident important or unimportant?
  →What makes us likely to overlook signals?

Procedure: Step 2 – Attention Economics (10 min.)

→The participants answer the following reflection questions:

→What competes most for your attention in everyday work?

→When are you most vulnerable to overlooking signals?

→Which types of messages easily get lost in the noise?

👉 **The key point:** Attackers exploit the fact that people cannot pay attention to everything all the time.

Procedure: Step 3 – Design Better Signals (10–15 min.)

→The participants work with the following questions:
- →How can important security signals be made clearer?
- →What could the organization do to reduce noise?
- →What can employees themselves do to protect their attention?

Possible answers: Step 1 – Sort Signals and Noise

→Signal (requires action/attention):

- →Email about a changed supplier bank account number → High risk of financial fraud.
- →Email marked “urgent” from an unknown sender → Classic social engineering pattern.
- →IT email about possible phishing → Intentional security signal.
- →SMS from a “shipping company” with a link → Known attack method.

→Noise (can wait/be ignored):

- →Teams notification about a new meeting.
- →Standard pop-up about a software update.
- →A colleague asking for help with a routine task.
- →System warning that frequently appears without consequences.

→Uncertain (requires clarification):

- →Error message from the production system.
- →Internal message from a manager without details.

👉 **Key point:** It is not always the content itself, but the context (sender, timing, pressure) that determines whether something is a signal or noise.

Possible answers: Step 2 – Attention Economics

1. What competes most for employees' attention?

→ Operations and production ("things need to keep running").
→ Time pressure and deadlines.
→ Large volumes of emails, messages, and notifications.
→ Interruptions from colleagues and phone calls.

2. When are employees most vulnerable?

→ During time pressure or production issues.
→ At the end of the day/end of the week.
→ When the message appears "routine."
→ When the sender pretends to be an authority figure.

3. Which messages easily get lost in the noise?

→ Generelle sikkerhedsmails.
→ General security emails.
→ Repeated warnings without clear consequences.
→ Technical messages without clear action steps.
→ Long emails without prioritization.

👉 **Key point:** Attackers exploit the fact that human attention is limited and hide attacks within the large volume of legitimate communication.

Possible answers: Step 3 – Design Better Signals

1. How can important security signals be made clearer?

→ Clear headings: “REQUIRES ACTION.
→ ”Short and concrete language.
→ One clear action (e.g., “Do not click - forward instead”).
→ Recognizable and consistent sender.

2. How can the organization reduce noise?

→ Fewer, but more targeted emails.
→ Guidelines for the use of “urgent.”
→ Consolidation of information into fixed channels.
→ Remove unnecessary system notifications.

3. What can employees themselves do?

→ Pause when facing time pressure or authority.
→ Delay taking action if something feels wrong.
→ Use known contact channels for verification.
→ Accept that it is okay to ask “one time too many.