

Cyber Physical Risk in Chemical Manufacturing: When Cyber Attacks Become Safety Hazards

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

Can an attacker access a system which is:

- Air gapped
- Manually Operated
- Analogue or Mechanical

If an operator does their Bidding?

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

HOLD UP YOUR MOBILE PHONE

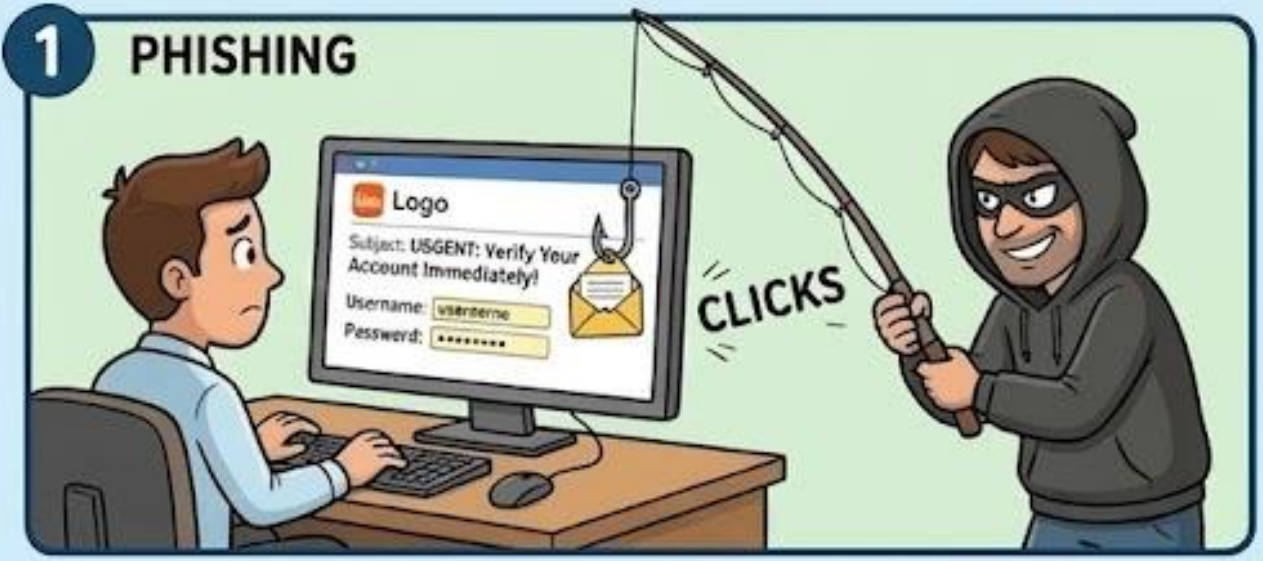


© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

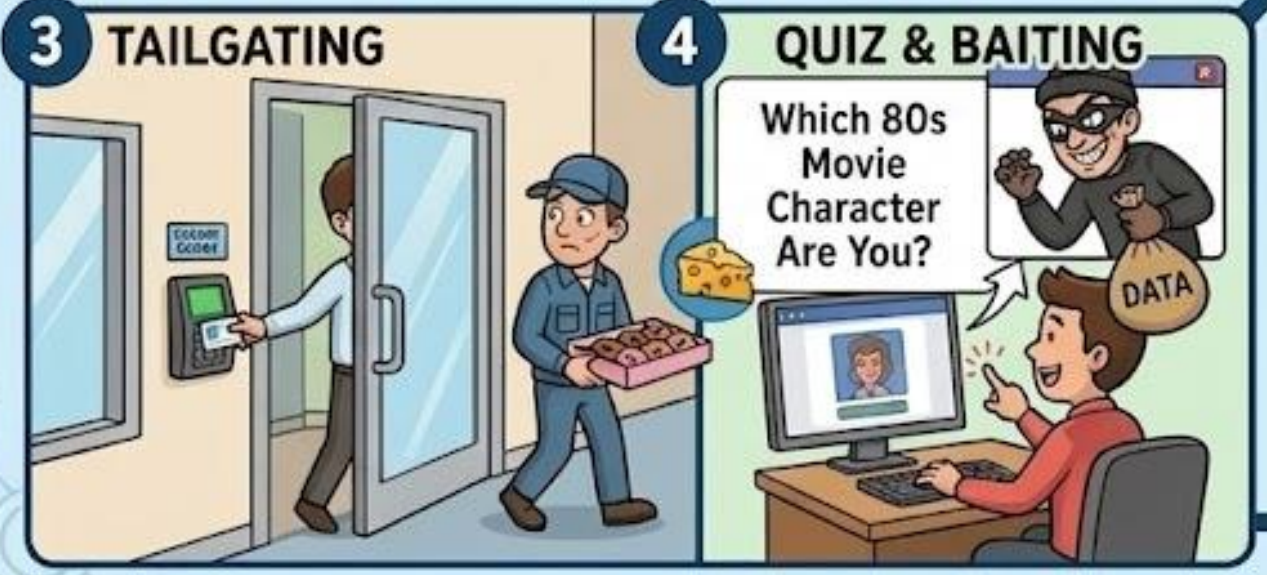
TURN ON THE TORCH

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

UNDERSTANDING SOCIAL ENGINEERING:
Manipulating People for Information









THE CONSEQUENCE: DATA BREACH!

In 2024 there were
7.78 million attacks against
UK business

90% were Phishing



Source:
Cyber security breaches survey 2024
Gov.uk

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

The impact…



2024 - 2025



2025



2025



2024



2023



2017



2020 -



2022 -

Why these companies?

Why the effort?

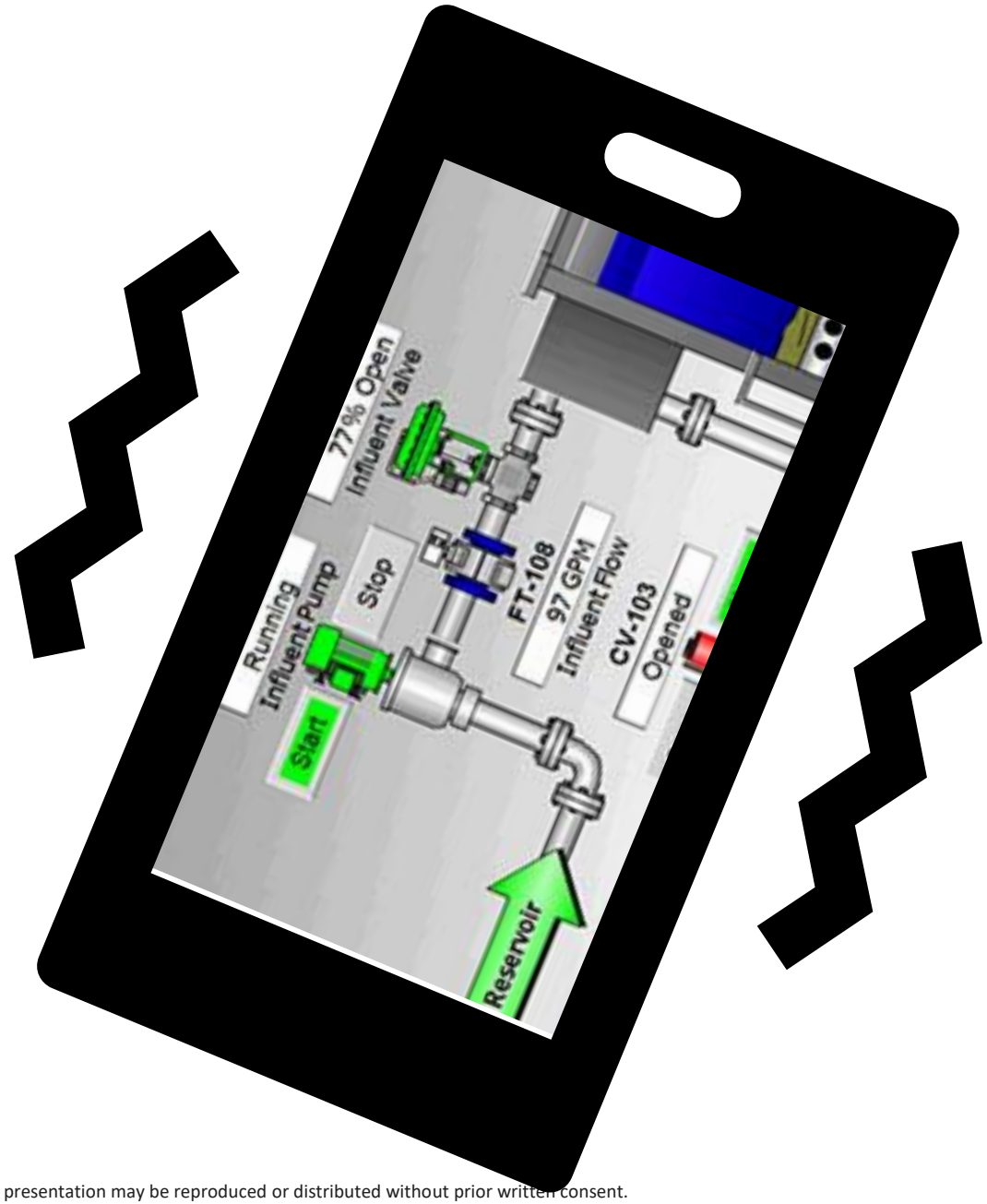
© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.



How long does a Phishing mail take to create?

1. 2 hrs
2. 20 mins
3. 2 mins

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.



© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

This Photo by Unknown Author is licensed under CC BY-NC



Why are we hacked?

1. Money
2. Data
3. To Risk Lives

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

Hackers are after data and money…

but the consequential damage is not a concern…

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

How to protect

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

Risk Calibration

Risk appetite

- What Losses can I tolerate?
- What losses can I not tolerate?

Threat level

- Who is likely to attack me?
- What can I give them?

SAFETY is a key consideration

- Consider the potential for a dangerous state
- Consider the potential of ALL loss scenarios

EXAMPLE:

Loss of production setpoints - Furnace

Loss CAN be tolerated. I will cause minimal disruption and isn't particularly sensitive.

Corruption could potentially damage the furnace and **CANNOT** be tolerated.

Efforts are focussed on data **INTEGRITY**

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No s presentation may be reproduced or distributed without prior written consent.

Example – Furnace Losses

	Risk Of loss Describe the foreseen risk of loss (use prompts and guide words)					Tolerable Loss Describe the maximum tolerable risk (use the guide words to score)								
	Description	Affects Who	Scenario	Causes	Severity	Probability of Loss	Score	Compliance to law	Financially	Reputation	Customer Satisfaction	Operational Performance	Tolerable Probability	Score
L1	Loss of life or injury to people	Operators and Site personnel	Setpoint corrupts, furnace damages lining and loses integrity	Hot spots, over temperature	4		20	1	3	2	4	1		4
L2	Loss of or damage to property	Site operations	Furnace damaged, needs significant repairs	Hot spots, over temperature	3	5	15	5	2	3	2	1	3	6
L3	Loss of or damage to objects outside the property	Nearby buisnesses	Fire spreading off site	Furnace failure	4	4	16	5	2	2	4	1	2	4
L4	Loss of mission	Excessive downtime or loss of customer data	Operational setpoints and procedures lost	Data theft / loss	2		10	5	2	2	2	2		8
L5	Loss of customer satisfaction	Customers receive defective components	Chemistry and treatments not correct	Setpoints corrupted or lost	2	5	10	5	2	2	2	2	4	8
L6	Loss of sensitive information	Customer data lost	Data lost or stolen	Data theft or IT failure	3	5	15	5	3	3	2	5	2	6

LARGE GAP – MAXIMUM FOCUS

SMALLER GAP – LESS MEASURE NEEDED

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.

Three Stage Approach

ASSESS

Assess The threats
Understand The consequences
Is this a risk level you can live with?



PROTECT

Zero Trust	Authenticate everything and everyone
Encrypt	Stored or moving, if they can't read it…
Minimise	Access points, physical and cyber
Update	Evolve the protections, manage patches
Resilience	Defence in depth and detection

COMMUNICATE

Risk	Why are we doing this
Educate	Training and awareness
Aware	Near misses, weakness reporting
Respond	Incident reporting and response

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.



Cyber criminals don’t conduct risk assessments…

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this pres ay be reproduced or distributed without prior written consent.



Jon Wiggins

Technical Manager – Functional Safety and Cyber Security

Connect with me on LinkedIn

© 2026 DEKRA SE or its subsidiaries. All rights reserved. No part of this presentation may be reproduced or distributed without prior written consent.