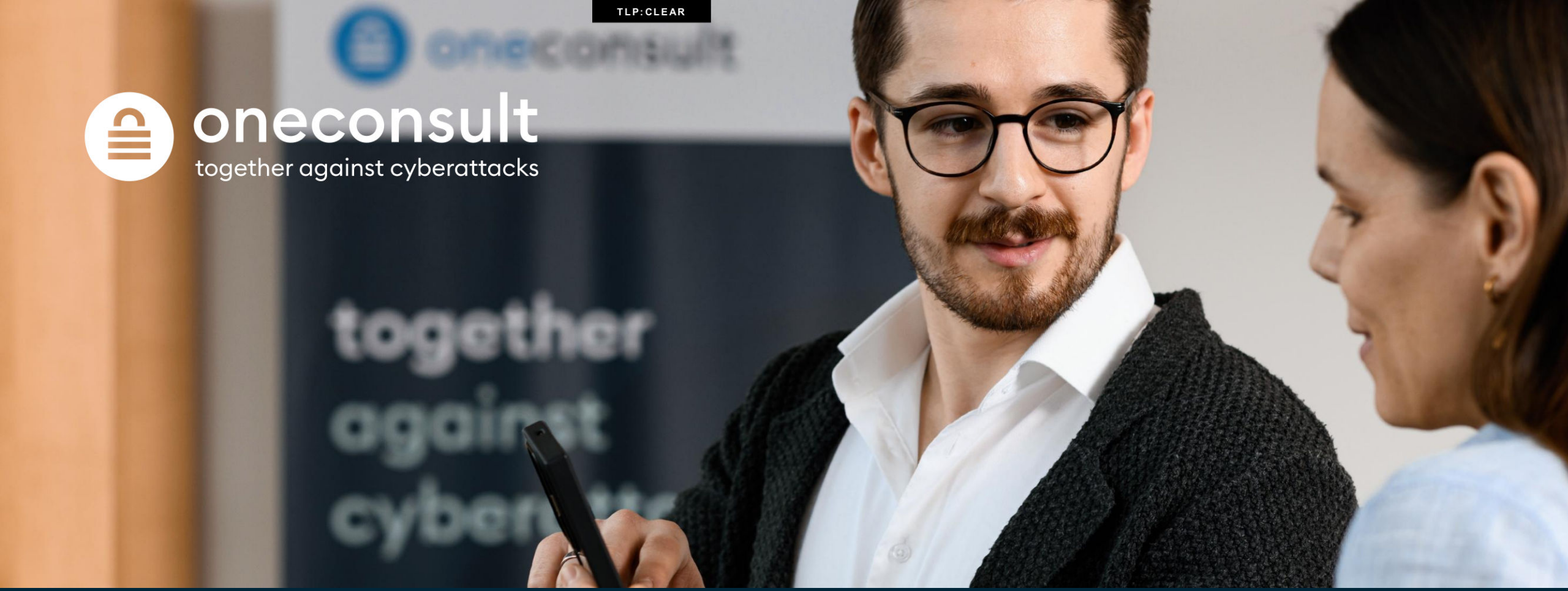
TLP:CLEAR

oneconsult
together against cyberattacks



Motivate and Prepare for Cyber Crises

Swiss Cyber Storm 2025 – Resilience in a Mad, Mad World

OCINT-CSIRT

oneconsult
together against cyberattacks

60+
Significant incidents per year

~80%
“It’s a crisis!”

160+
SME cases per year

~60%
“It’s a crisis!”

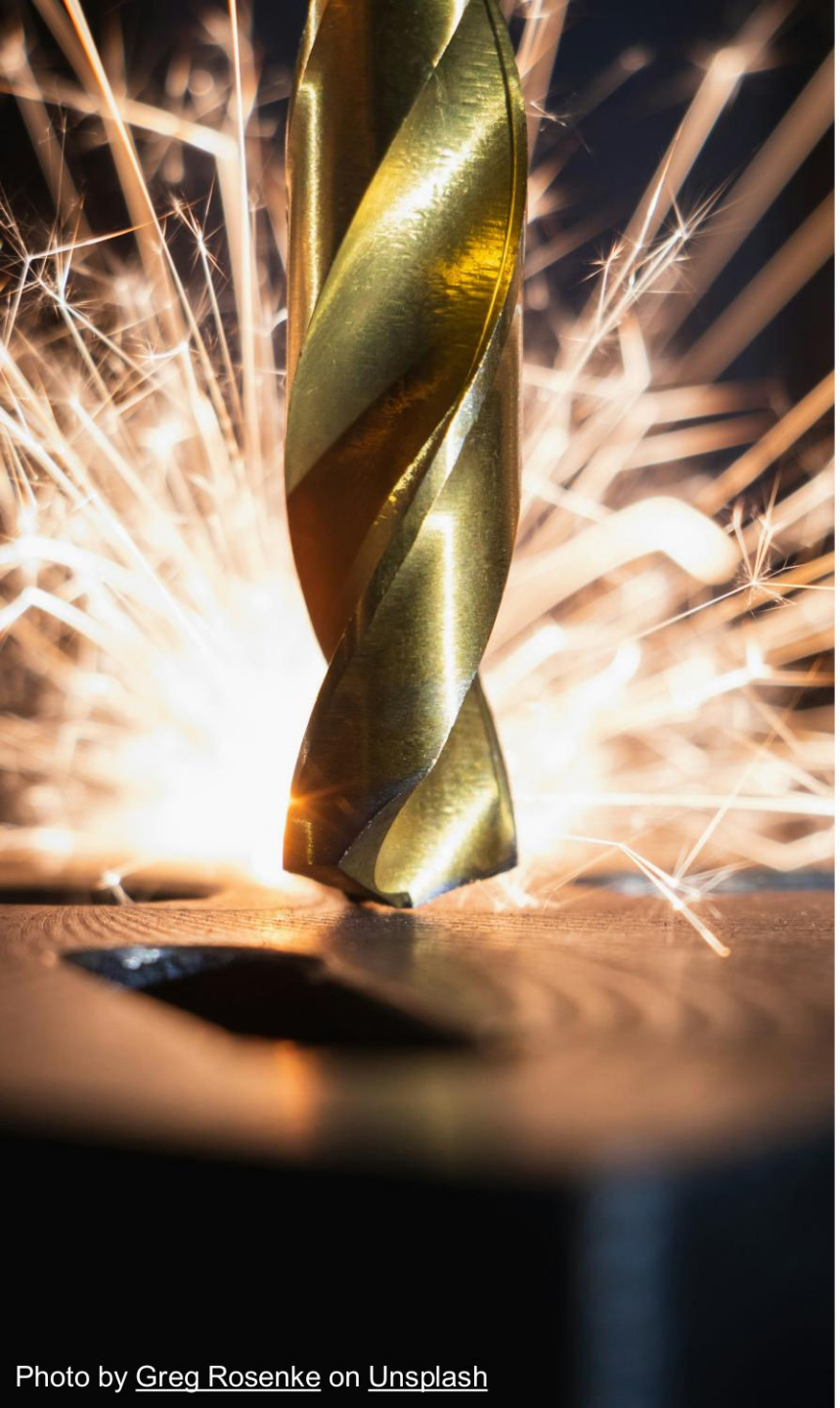


Photo by Greg Rosenke on Unsplash

oneconsult
together against cyberattacks

Our Case

- Global **manufacturer** with market leadership in Europe
- Operating in **over 50 countries**
- More than **25 production facilities worldwide**
- **Publicly traded**

oneconsult
together against cyber attacks

Budget approved.

Leadership and commitment still pending.

Photo by Benjamin Child on Unsplash

oneconsult
together against cyberattacks

Gaps, Gaps and More Gaps!

Like many others, the **information security team hired consultants** to conduct assessments and gap analyses.

Surprise: **Gaps were found**!

However, this **did not help**:

- The executive board thanked them for bringing the gaps to their attention
- They **delegated the task of closing the gaps to the information security team**
- Tasked the internal auditing team with keeping an eye on it

Photo by raquel raq on Unsplash

oneconsult
together against cyberattacks

Definition of Success

In case of a cyber incident / crisis

- ✓ Crisis team members **understand their individual roles and responsibilities**.
- ✓ The **Executive Board** recognizes its **central role** in the crisis team.
- ✓ The crisis team **takes leadership** during (cyber) crises.
- ✓ **Regular training and exercises** are conducted to prepare for cyber crises.
- ✓ The Executive Board **acknowledges gaps** outside IT & information security.
  - ✓ **Business continuity** management is currently lacking.
  - ✓ **Public Relations** is not actively preparing for crisis communication scenarios.
  - ✓ The **Legal** team is not fully aware of relevant legal frameworks and obligations.
- ✓ The crisis team recognizes that a **cyber crisis is not solely a technical issue**, but a multidisciplinary challenge.

oneconsult
together against cyberattacks

Cyber crises don’t stop at the server room

You most likely work here

Technology

- Take immediate actions
- Understand the situation
  - Scope of attack
  - Objective of attack
  - Root cause
- Everyone wants and needs more and more information
- Rebuild with more security controls

Incident Operations / Crisis Team

- Establish crisis team
- Set up emergency operation
- Define the way back to normal
  - Take the business perspective
  - Stay focused
  - Think ahead

Legal

- Reporting obligations
  - Stock exchange law
  - Data protection laws
  - Contractual obligations
- Support Negotiations
  - Sanctions
- Support activities
  - Public statements
  - Engage law enforcement

Communication

- Map the stakeholders
  - Shareholders
  - Public
  - Employees
- Prepare and publish statements
- Interact with the media
- Monitor the conversation
- Rebuild trust

Careful, this requires the involvement of **the whole organization**!

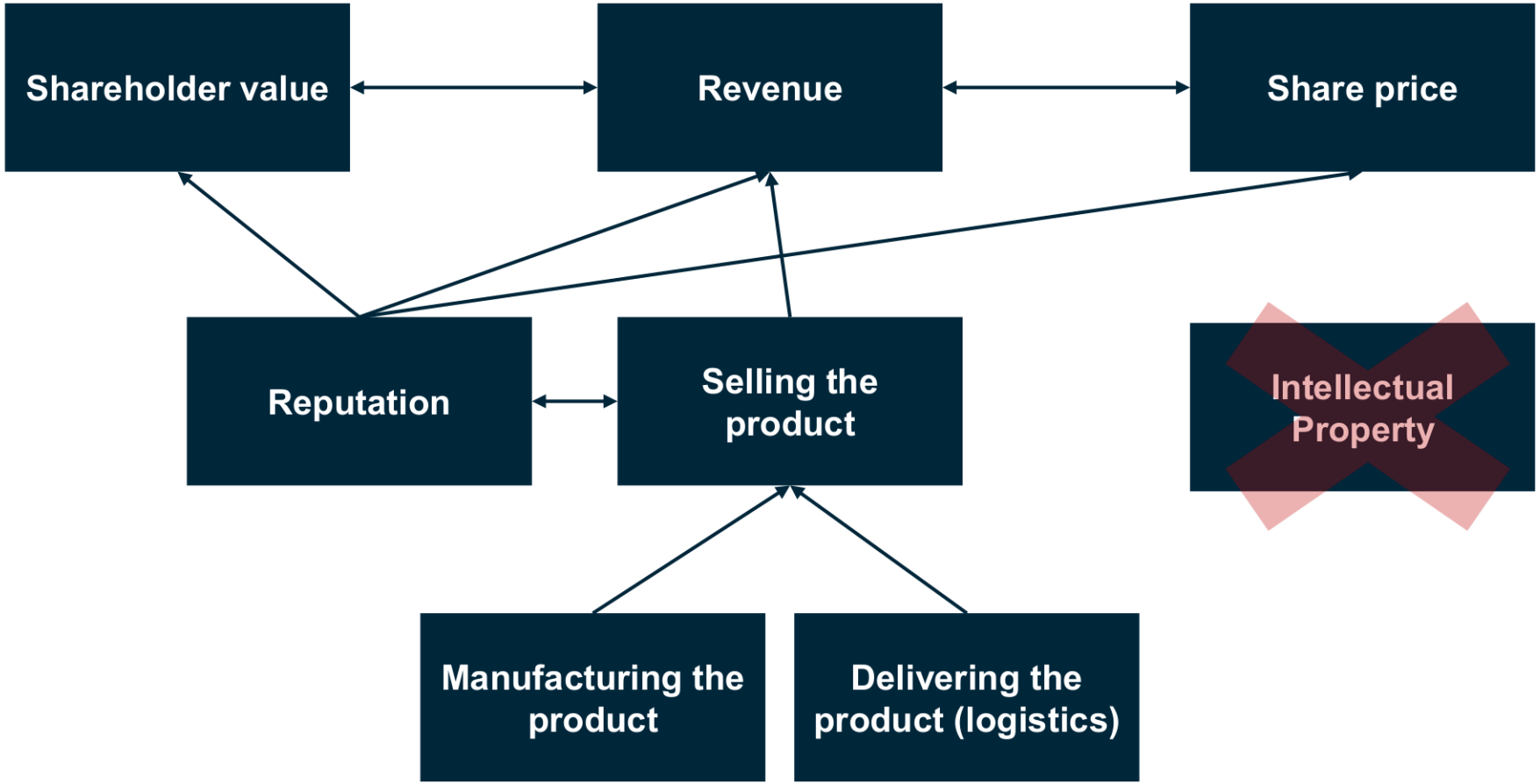
oneconsult
together against cyberattacks

01. Get them hooked

oneconsult
together against cyberattacks

Why should they care?

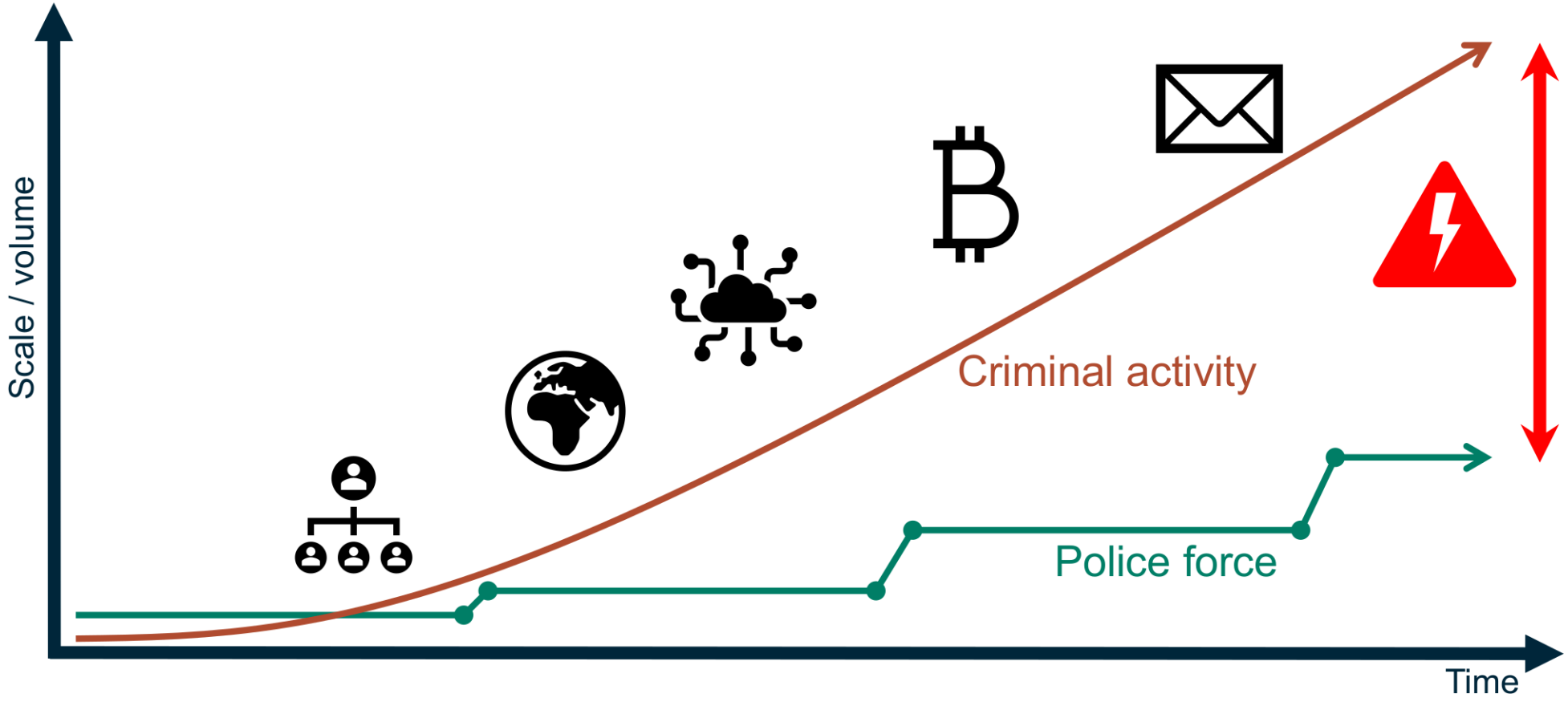
Understand your audience



oneconsult
together against cyberattacks

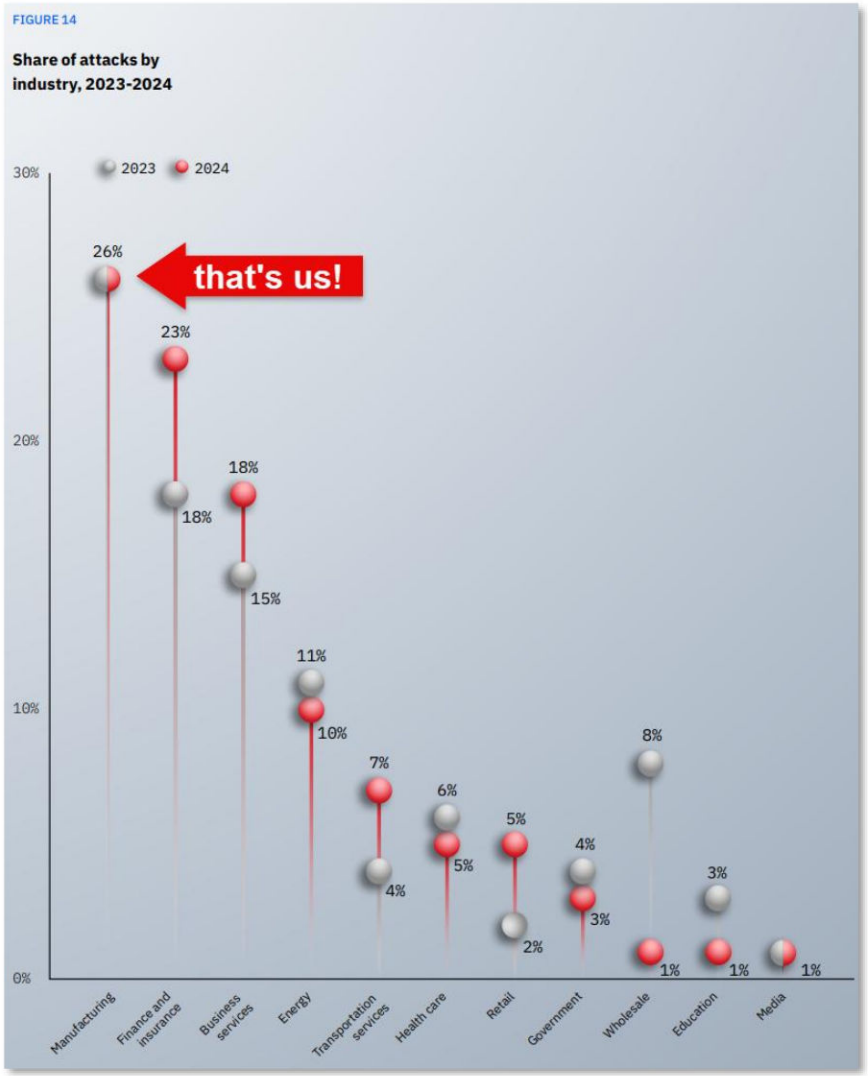
Time for a killer chart!

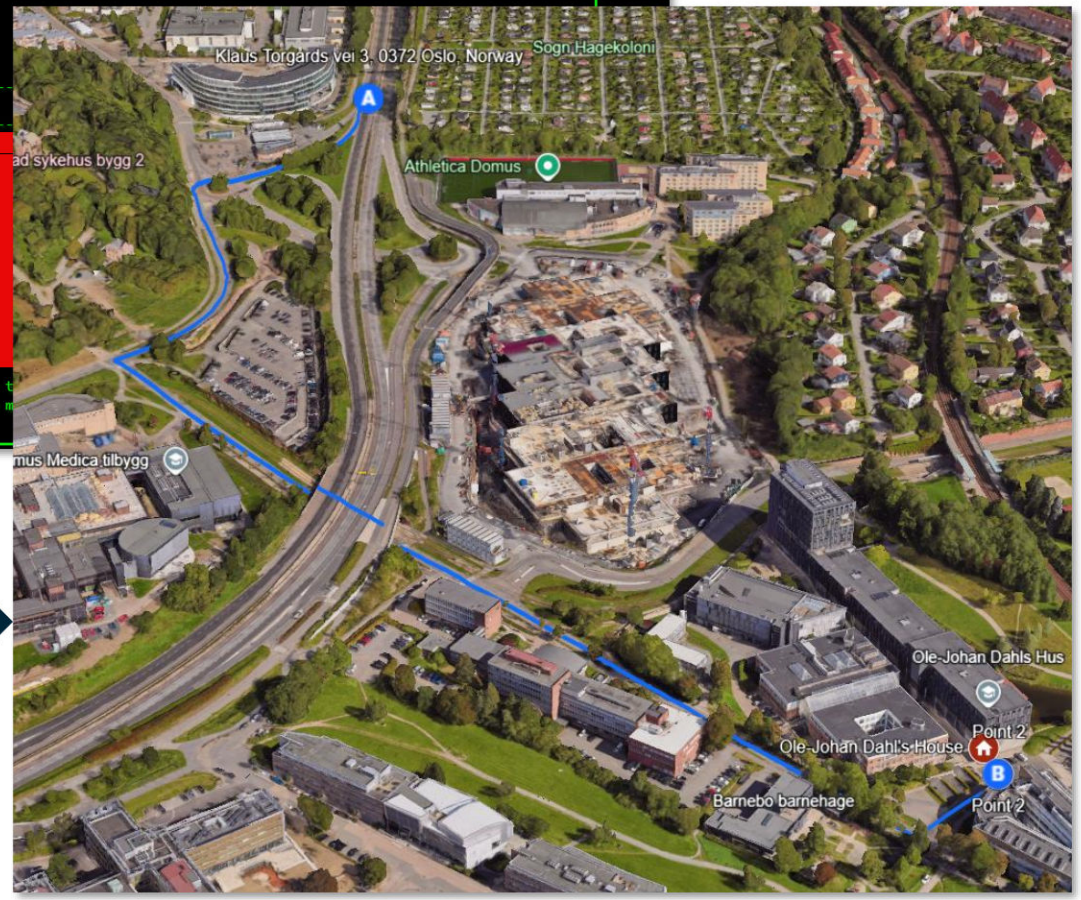
We must **change** **across the organization**.



oneconsult
together against cyberattacks

The story we told them to get attention





oneconsult
together against cyberattacks

The story we told them to get attention

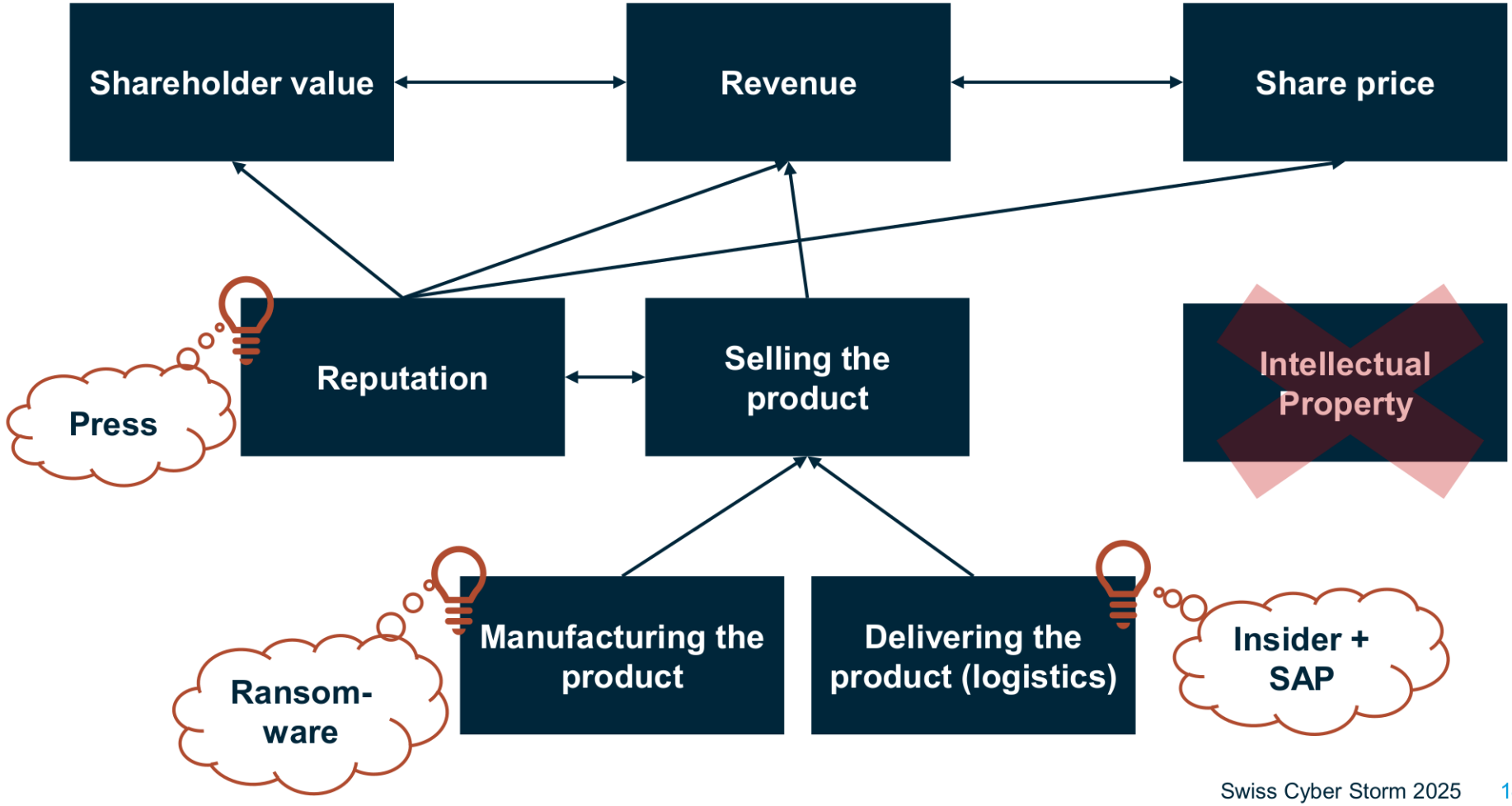
oneconsult
together against cyberattacks

02. Let them experience it

oneconsult
together against cyberattacks

Why should they care?

Derive a tabletop exercise scenario



oneconsult
together against cyberattacks

Do a tabletop exercise.

Make it realistic!

Get them into the right headspace and mood.

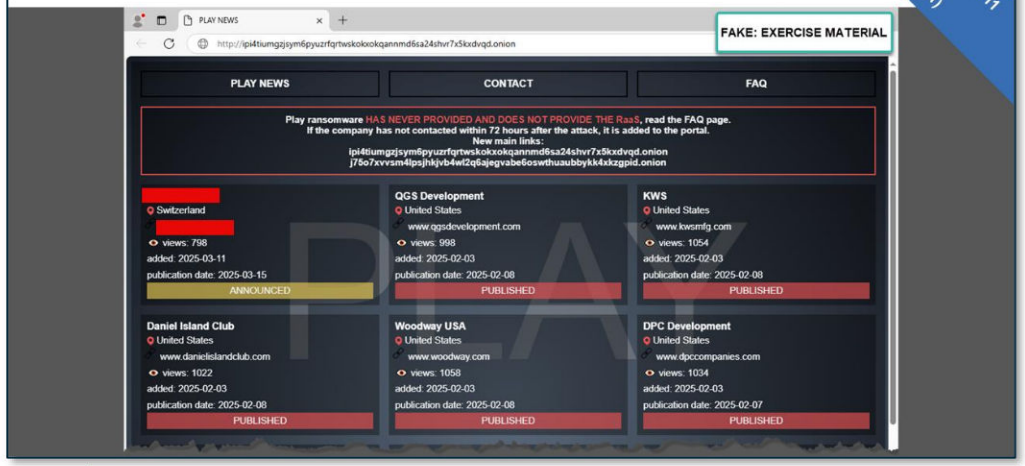
Photo by Oleg Laptev on Unsplash

oneconsult
together against cyberattacks

Use visuals that evoke emotions

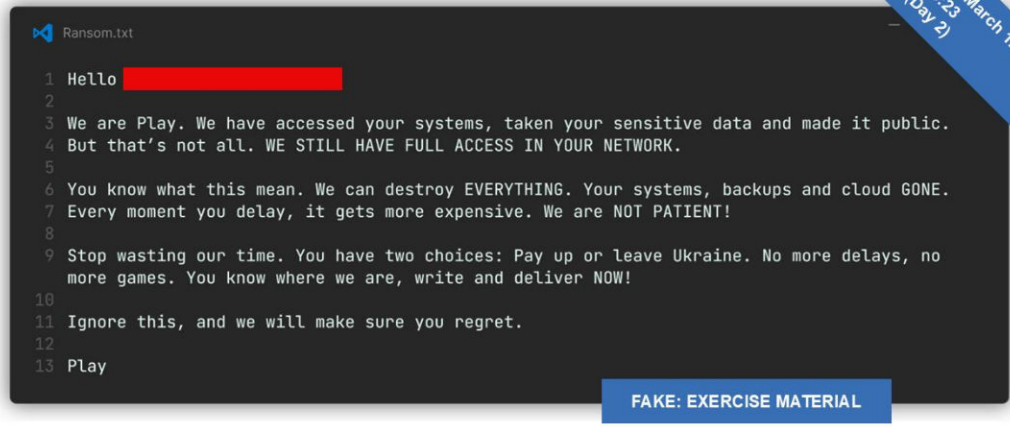
Claim published by the Play ransomware group
Overview Page

Tuesday, March 11
15:54
(Day 1)



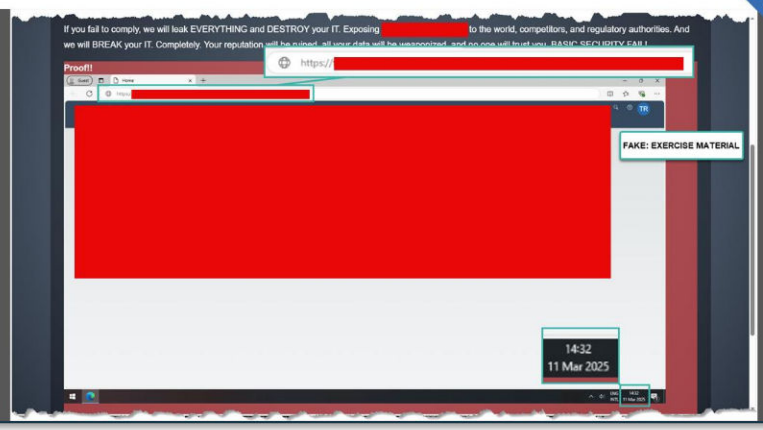
Ransom Emails

Wednesday, March 12
18:23
(Day 2)



Proof published by the Play ransomware group

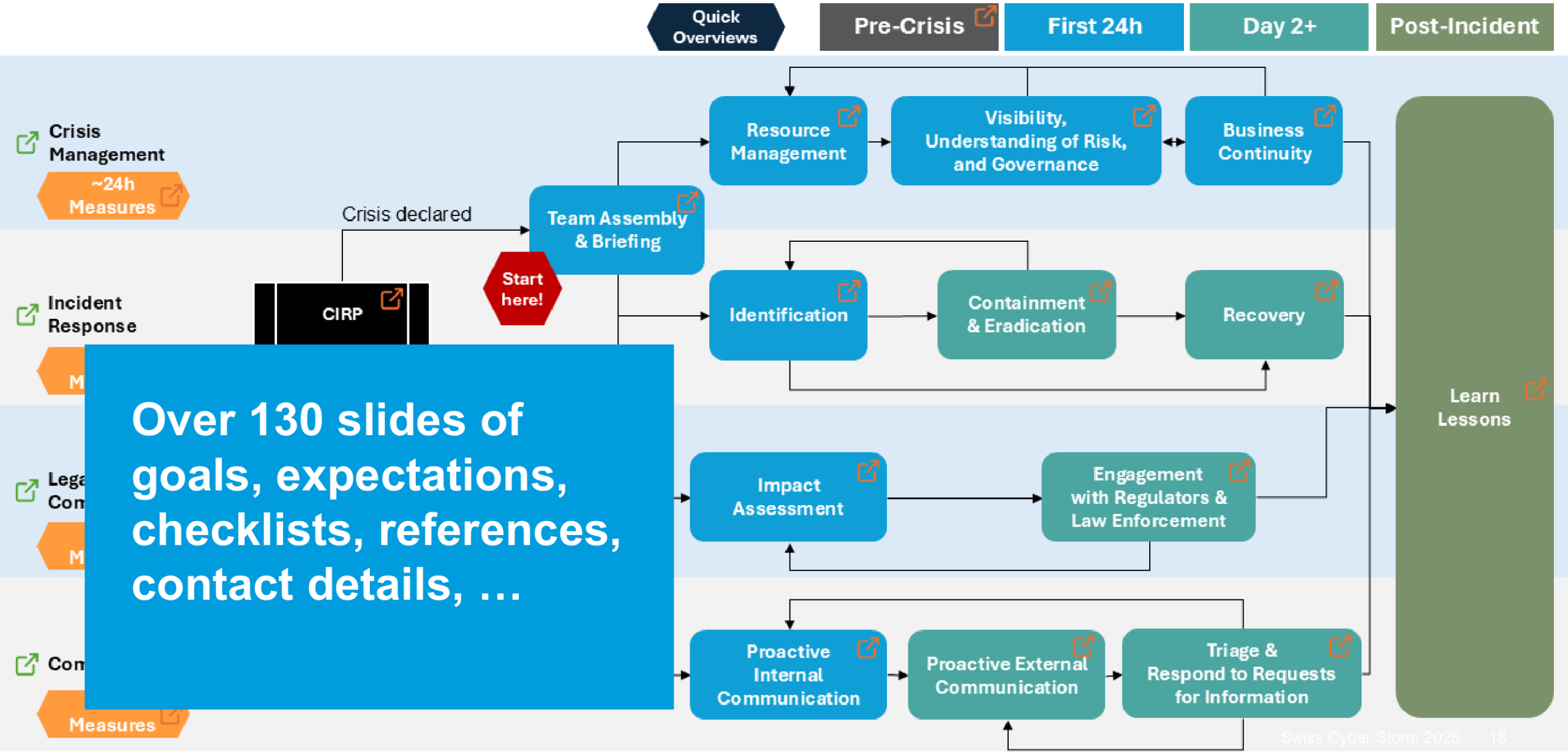
Wednesday, March 12
10:30
(Day 2)



oneconsult
together against cyberattacks

03. Love the outcome

Crisis Management Process



Questions?

oneconsult

together against cyberattacks

Contact

Gregor Wegberg

Head of Digital Forensics & Incident Response

Member of the Management Board

E-Mail: gregor.Wegberg@oneconsult.com

Let's connect

oneconsult
together against cyberattacks

Thank you

oneconsult

together against cyberattacks