.the tech collective

powered by Implement

Culture & Method

Who am I

Anders Balslev

Partner, Cyber Tech Services / .the tech collective @ Implement
SME, Cyber and Cultural Awareness

Implement since June 2025

PwC, 6 years as Director & business advisor
Deloitte, 5 years as Director & business advisor
Outpost 24, 4 years as Country Director Nordics & Baltics

Defense, 10 years

“Culture is what people do when no one is watching. Awareness training helps turn values into everyday actions.”

.the tech collective
powered by Implement

Who we are

A unified and strong **collaborative offering between The Tech Collective and Implement Consulting Group**

We are a collective of technologists, developers, testers and engineers with a passion for using technology and digital solutions to drive meaningful outcomes for people.

We are techies.

We have organized ourselves in companies of specific subject matter expertise. The Company serving Freightliner is the “Cyber Tech Service A/S”, a part of The Tech Collective. The company have become a market and community leader in its specialized domain focusing on implementation and operating services.

.the tech collective
powered by Implement

IMPLEMENT
CONSULTING GROUP_

Together, we are a **one-stop shop** that offers expertise spanning all the needs of the suite of work packages – from technical implementation to legal advisory and management consulting.

We are a collective of subject matter experts with strong analytical competencies. And we care just as much about the soft skills as we do about the hard skills.

We are nerds.

We have a deep commitment to bringing our expertise into play in a way that engages other people through best-practice but also creative ways. We call it change with impact. Every project introduces a change into an organisation, therefore everything we do is grounded in change management practices. And we tailor the team size and engagement methods to your exact needs for maximum flexibility.

Our stats

- 0 clients has left us
- Cost effective
- No salespeople
- Known to be unknown
- High quality deliverables

50+

Cyber technicians with deep, operational Microsoft capabilities across Entra, Sentinel, M365 and Defender

65+

Cyber advisors with demonstrated domain knowledge within compliance, privacy and information security

10+

Security leaders with CISO and top-leadership experience from large cooperations

15+

ICS/OT security professionals across both technical and advisory domains

15+

Offensive technicians, incident responders and forensic experts

Our SOC and IR credentials by sector

- Pharmaceuticals
- Mining & minerals
- Utility & water
- Financial Services
- Logistics

Creating a shared language for Culture

Elaboration: What is Culture?

Culture in an organization is not just values printed on a poster; it is the sum of:

- **Actions**
- **Habits**
- **Norms**
- **Decisions**

That people make in their everyday work. It doesn't matter what they do, desk job, construction site, operating heavy machinery

It's what we **do**, **say**, **reward**, and **avoid**.

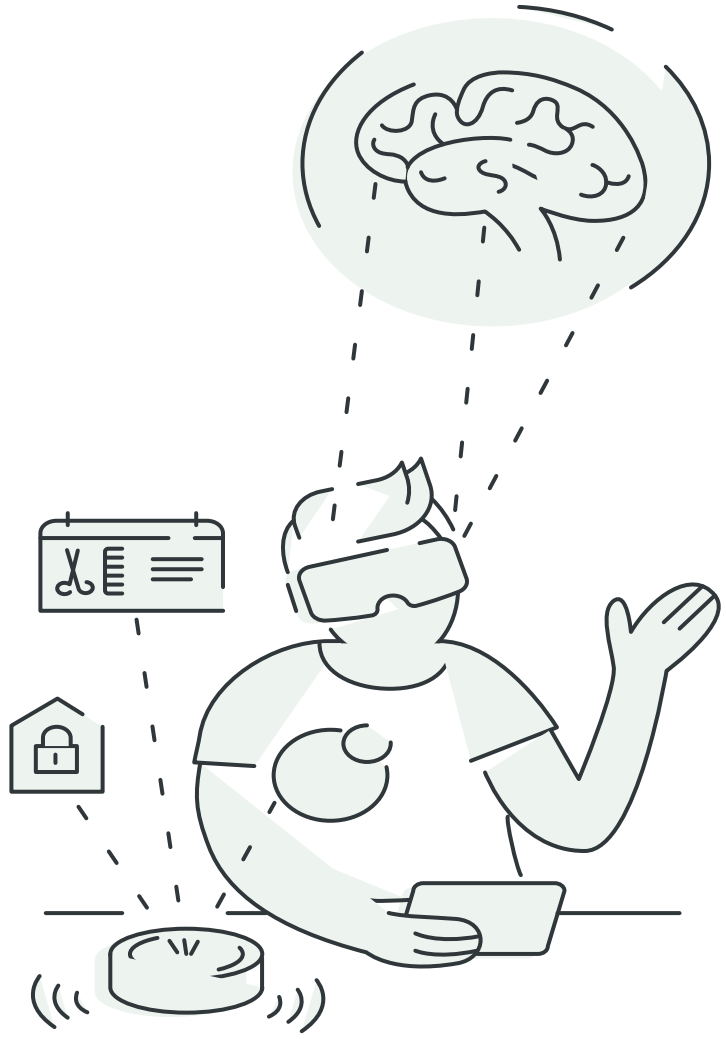
Culture is both **invisible and tangible**:

Invisible: It lives in assumptions, expectations, and atmospheres for example, how safe we ***feel*** about speaking up.

Tangible: It shows up in meetings, emails, onboarding processes, how we handle mistakes, and how we celebrate success.

Culture is not something we *have* – it's something we *do*.

Example: Cyber Culture in Practice



Imagine two organizations with the same security policy, but with very different cultures:

Organization A – “Compliance Culture”

Employees complete awareness training because they ***have to***.

Mistakes are rarely reported, people fear consequences.

Security is seen as IT’s responsibility.

Organization B – “Security Culture”

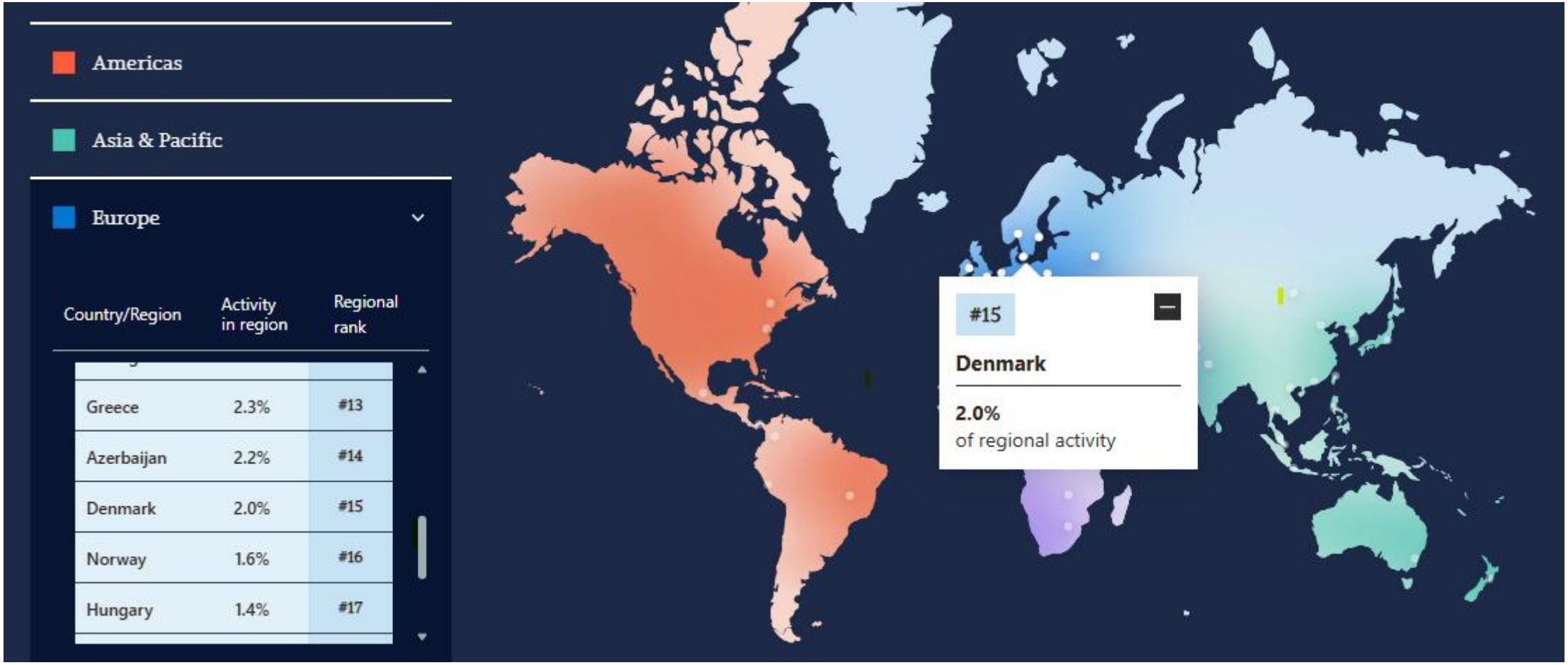
Awareness training is tailored and relevant, people share tips and experiences.

Mistakes are seen as learning opportunities, shared openly and used to improve.

Security is everyone’s responsibility, including marketing and sales.

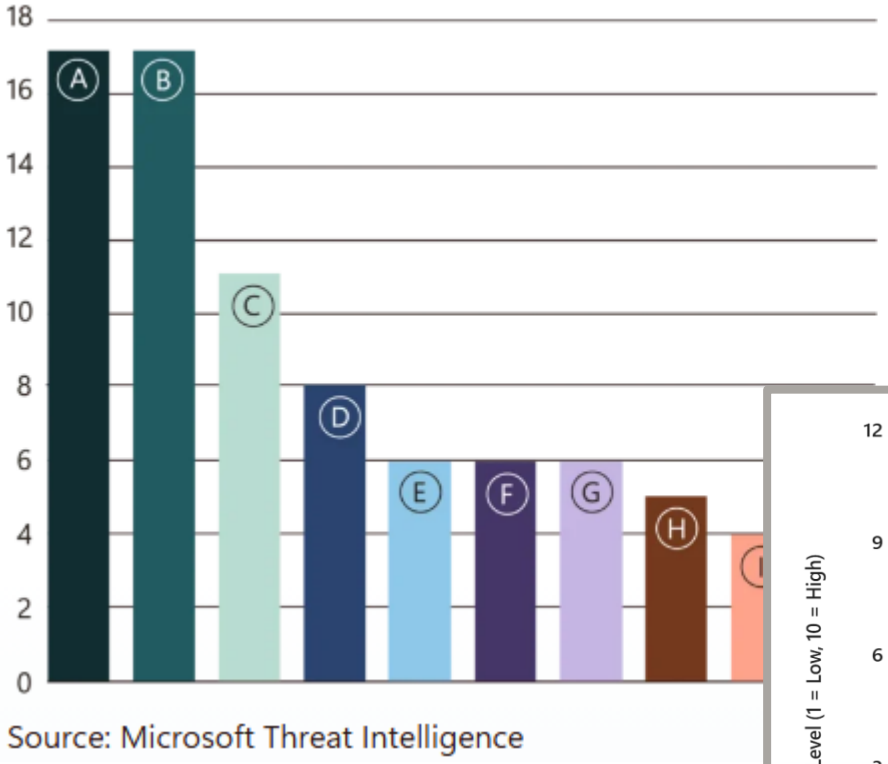
Both have the same policy,
but culture makes the difference.

Risk equals the need of training… Cyber as an example…



Kilde: Microsoft

Compared to others.

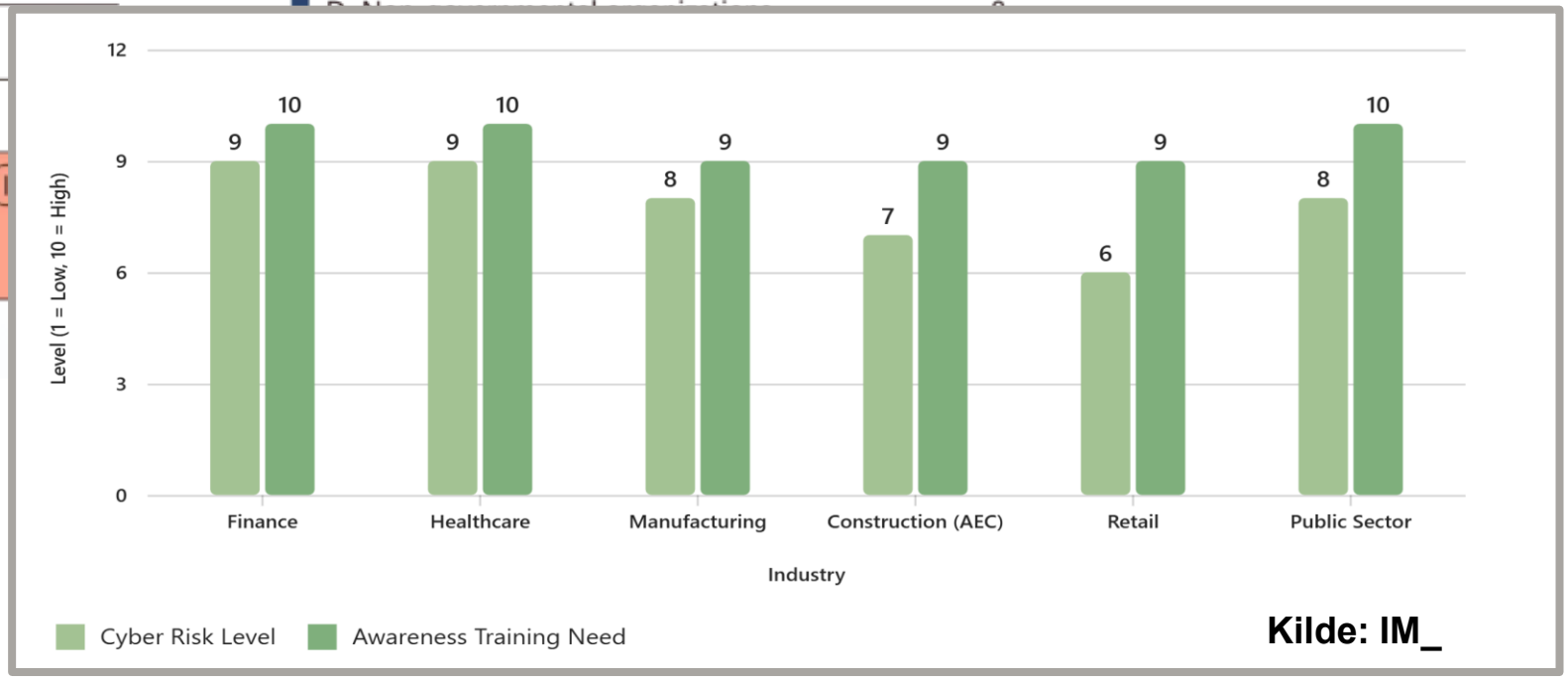


Source: Microsoft Threat Intelligence

Top ten global sectors most impacted by threat actors

January - June 2025

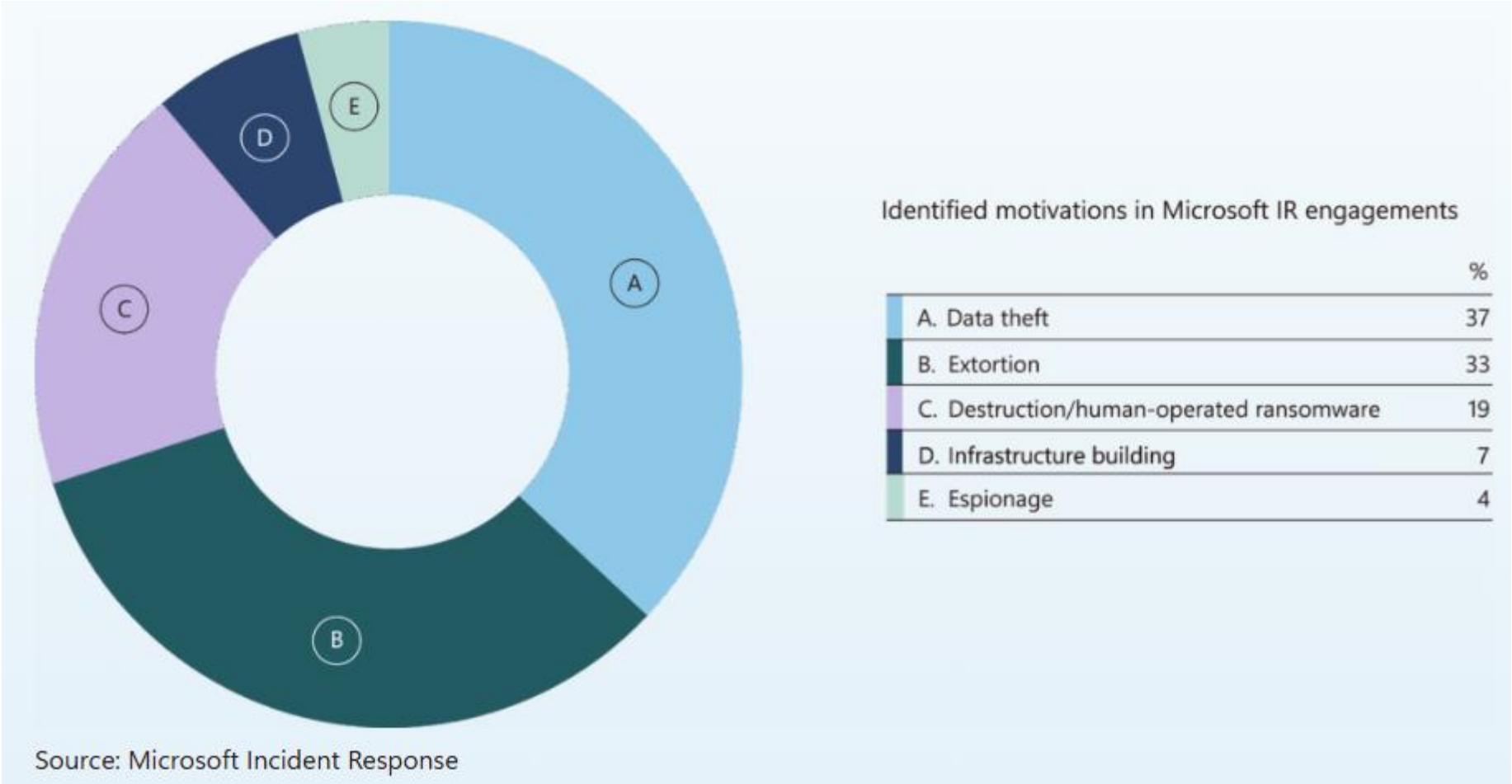
	%
A. Government agencies & services	17
B. Information technology	17
C. Research and academia	11



Kilde: IM_

Kilde: Microsoft

The why..



Identified motivations in Microsoft IR engagements

	%
A. Data theft	37
B. Extortion	33
C. Destruction/human-operated ransomware	19
D. Infrastructure building	7
E. Espionage	4

Kilde: Microsoft

Why do we need to do cultural training and development

Ransomware

Ransomware remains a critical cybersecurity concern. Microsoft observed a 2.75x year-over-year increase in human-operated ransomware-linked encounters, where at least one device in a network was targeted. Although these encounters have risen, the percentage of organizations that are ultimately ransomed (reaching the encryption stage) has decreased more than threefold over the past two years.

- **Foster a vigilant culture.** Employees are often the first to notice unusual behavior in a peer. Create a culture where reporting a concern is encouraged and rewarded.

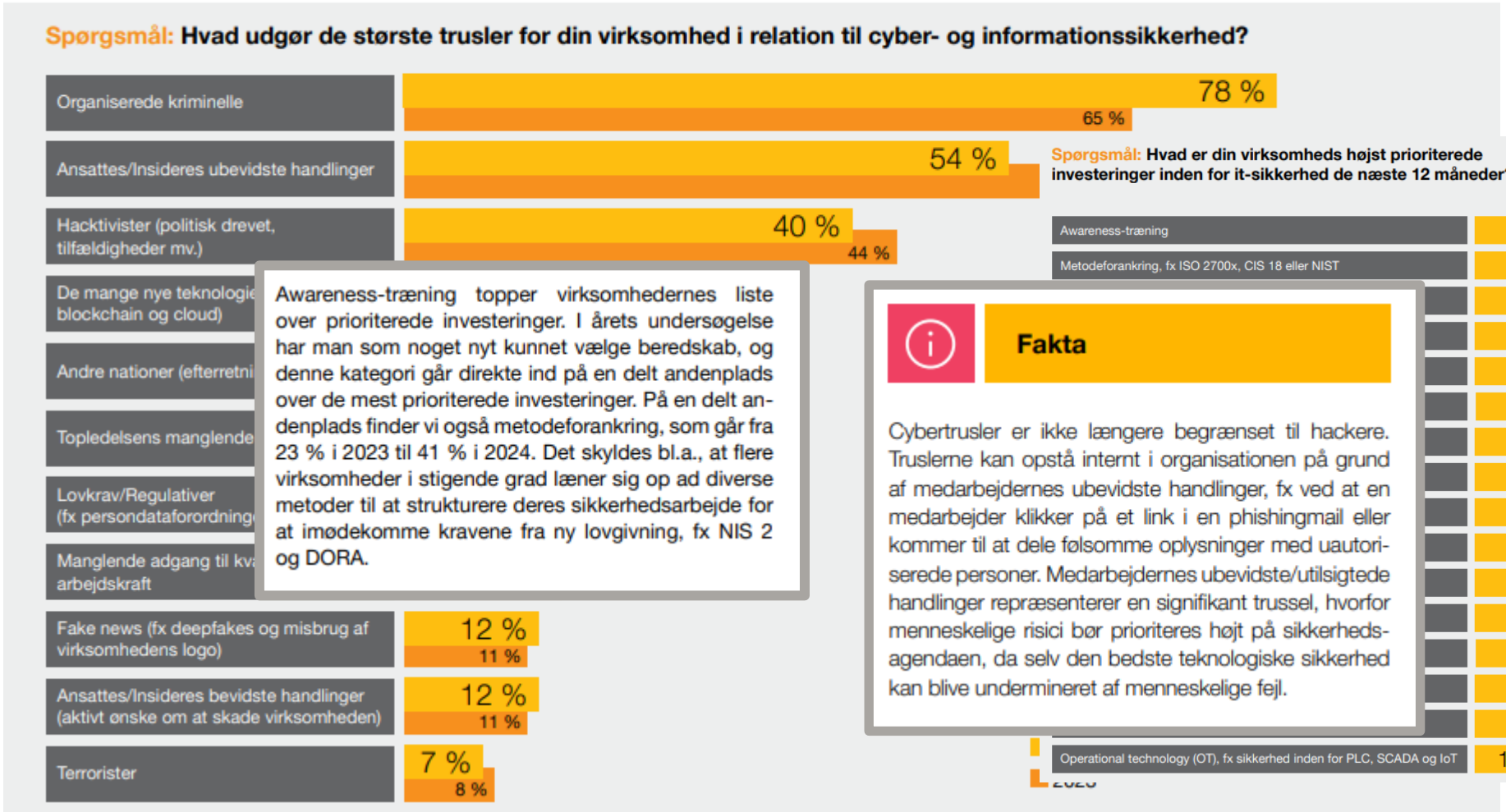
Cyberattack augmentation refers to the use of AI to enhance traditional cyberattacks. The chart on the right highlights the primary areas of augmentation, most of which are based in the automation of previously time-intensive activities.

Defenders must counter AI augmentation by fostering a strong cybersecurity culture, training users to recognize manipulation tactics, and implementing authenticated communication channels. AI-driven detection systems that flag

Kilde: Microsoft

Why do we need to do cultural training and development - Continued

Virksomhederne anser i år organiserede kriminelle for en større trussel end tidligere, når det kommer til cyber- og informationssikkerhed. Således svarer hele 78 % af respondenterne, at organiserede kriminelle er blandt de største trusler mod deres virksomhed. Samtidig er truslen fra ansattes/insideres ubevidste handlinger aftaget i forhold til de seneste år.



Fakta

Cybertrusler er ikke længere begrænset til hackere. Truslerne kan opstå internt i organisationen på grund af medarbejdernes ubevidste handlinger, fx ved at en medarbejder klikker på et link i en phishingmail eller kommer til at dele følsomme oplysninger med uautoriserede personer. Medarbejdernes ubevidste/utilsigtede handlinger repræsenterer en signifikant trussel, hvorfor menneskelige risici bør prioriteres højt på sikkerhedsagendaen, da selv den bedste teknologiske sikkerhed kan blive undermineret af menneskelige fejl.

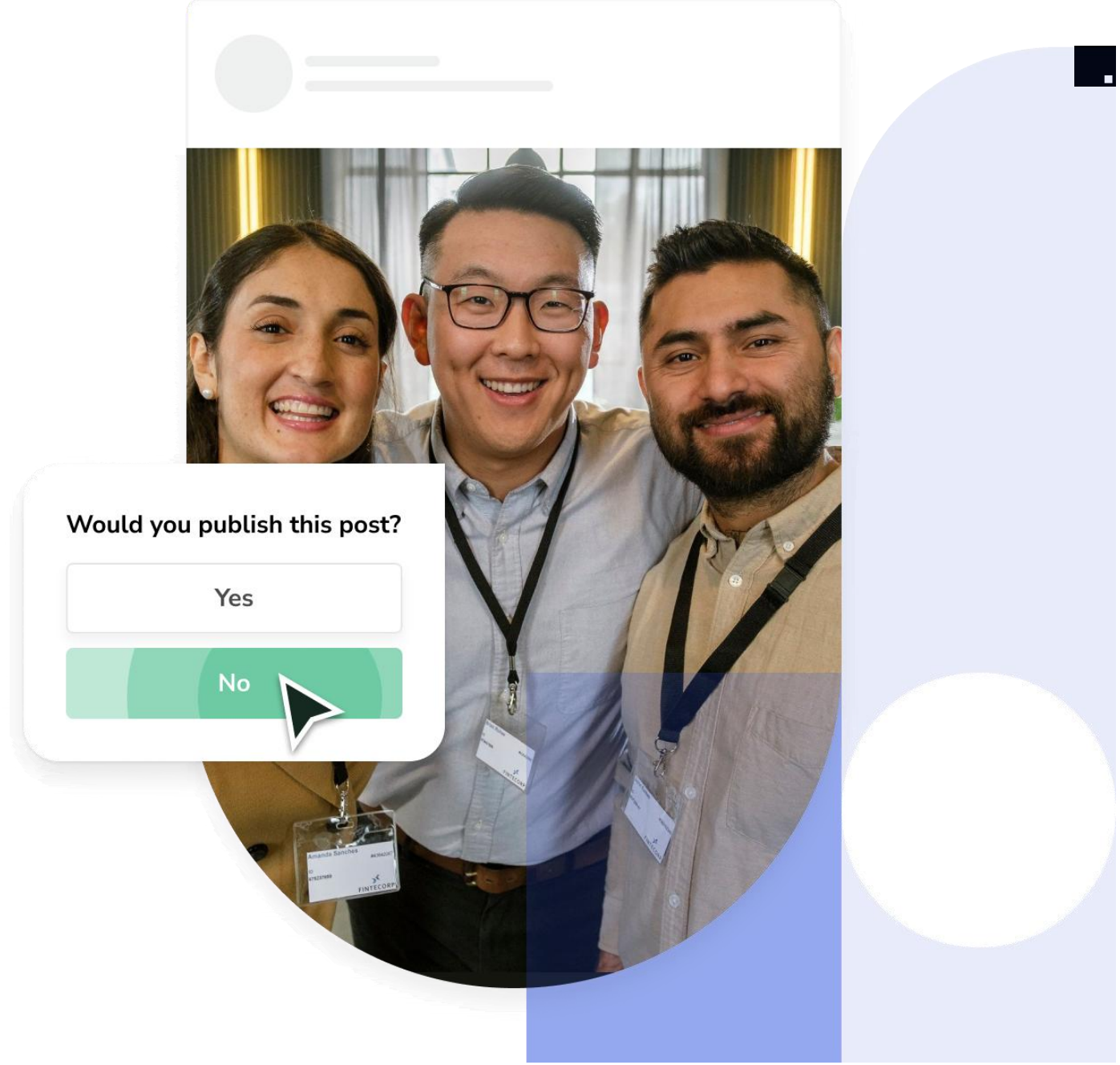
Kilde: PwC

The Challenge of Human Risk Management

Human risk is often overlooked as a part of an organization's cybersecurity.

That means the focus is all on the technical solutions but not on the employees. Often the IT department are left with the task of HRM and will increase the workload of an IT department, without increasing the actual awareness.

The *fix* needs to be located where the *risk* are located.



Nano Learning concept

Short and precise
A learning will typically be 2-4 minutes

Focused content
One idea, One subject, One skill per session

On Demand
Digital and available when the users needs it

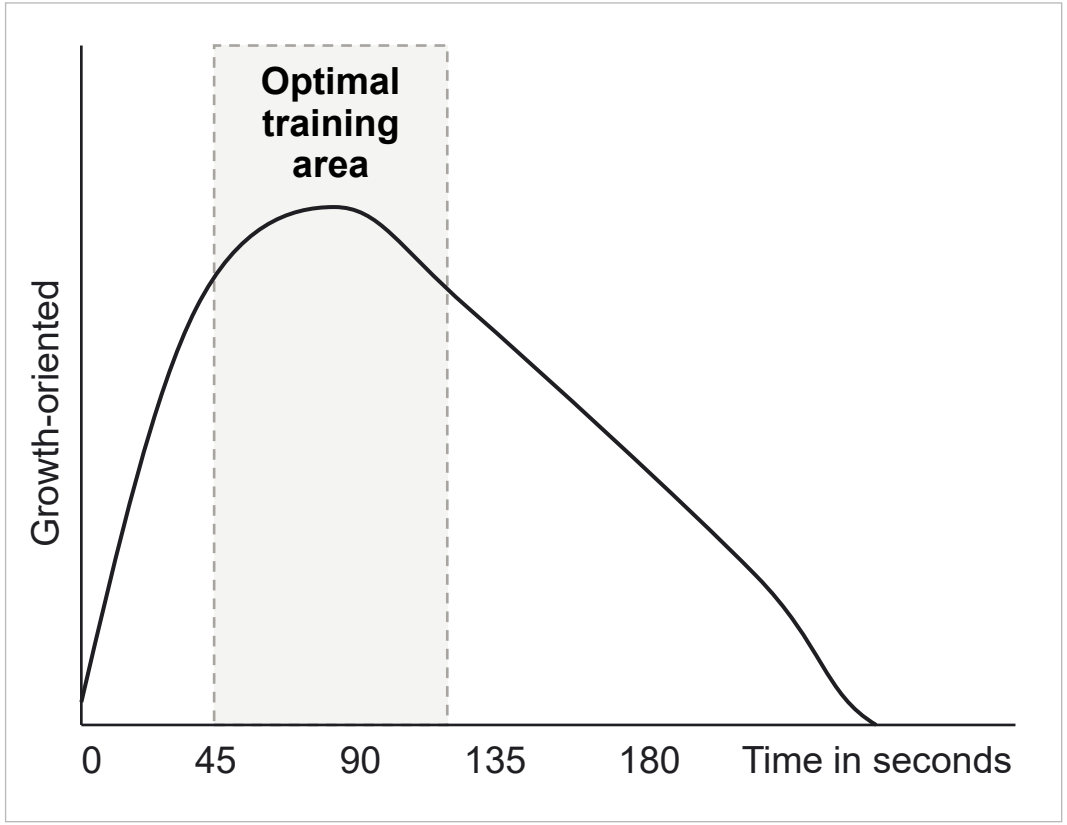
Interactive or passive
Video, Quiz, infographics, micro learnings or interactive / passive visuals in your everyday environment

Human learning optimization

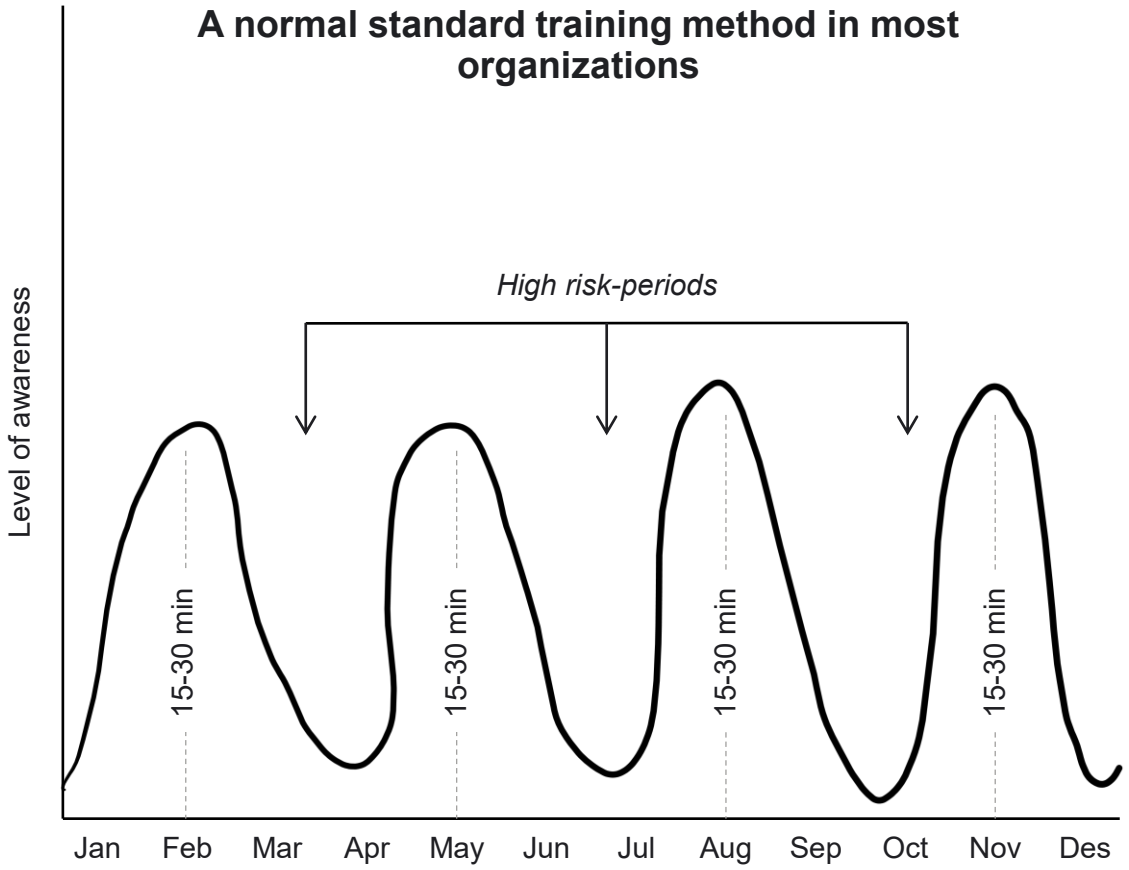
Time
Short trainings are ensuring high motivation, and a high learning ability as a human. Often content outside the area of interest, will equals a fast drop in motivation already after 90 seconds.

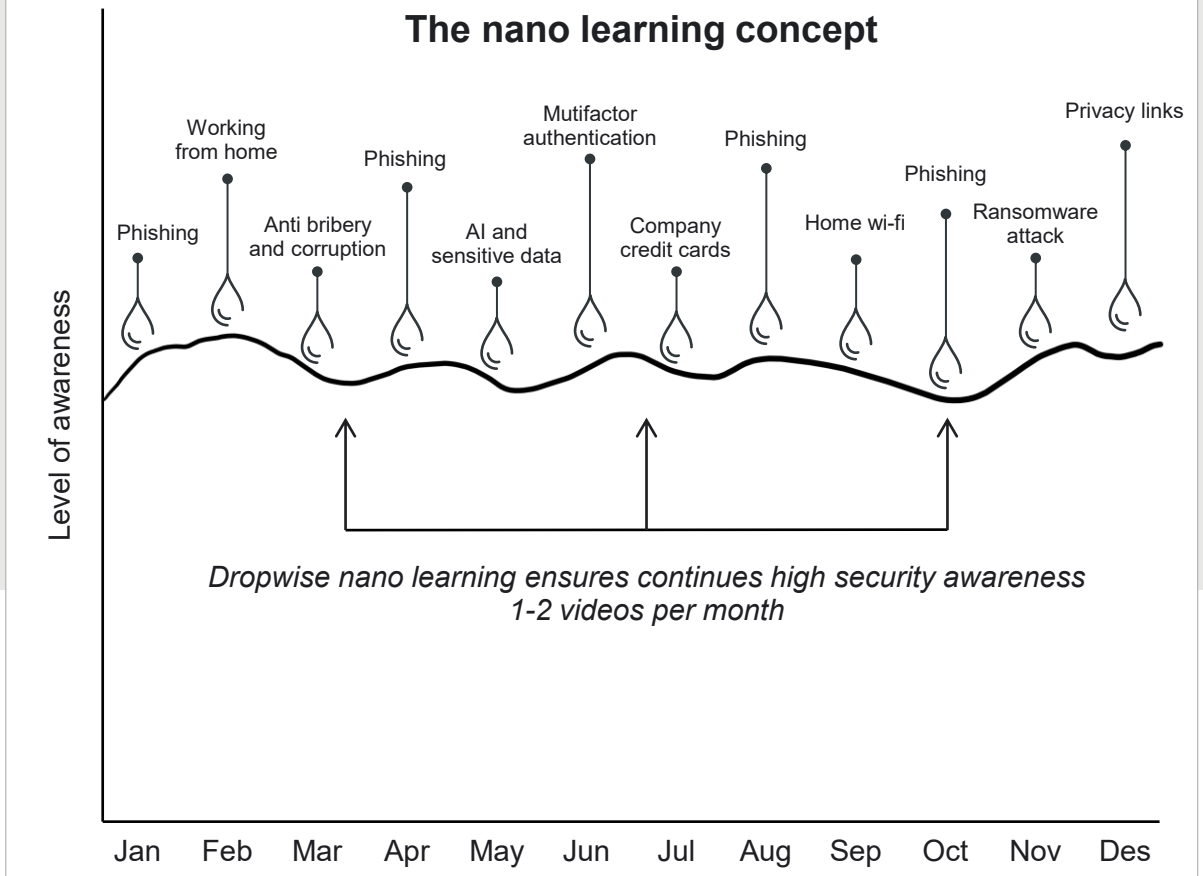
Visuals
As a human, seeing visuals, not only allows our brain, to remember in a more optimized way, it actually makes situations more recognizable when incidents accrue in real life scenarios.

Audio
Audios supports emotions in humans, contributing to a higher learning ability gives a higher angering of the training.

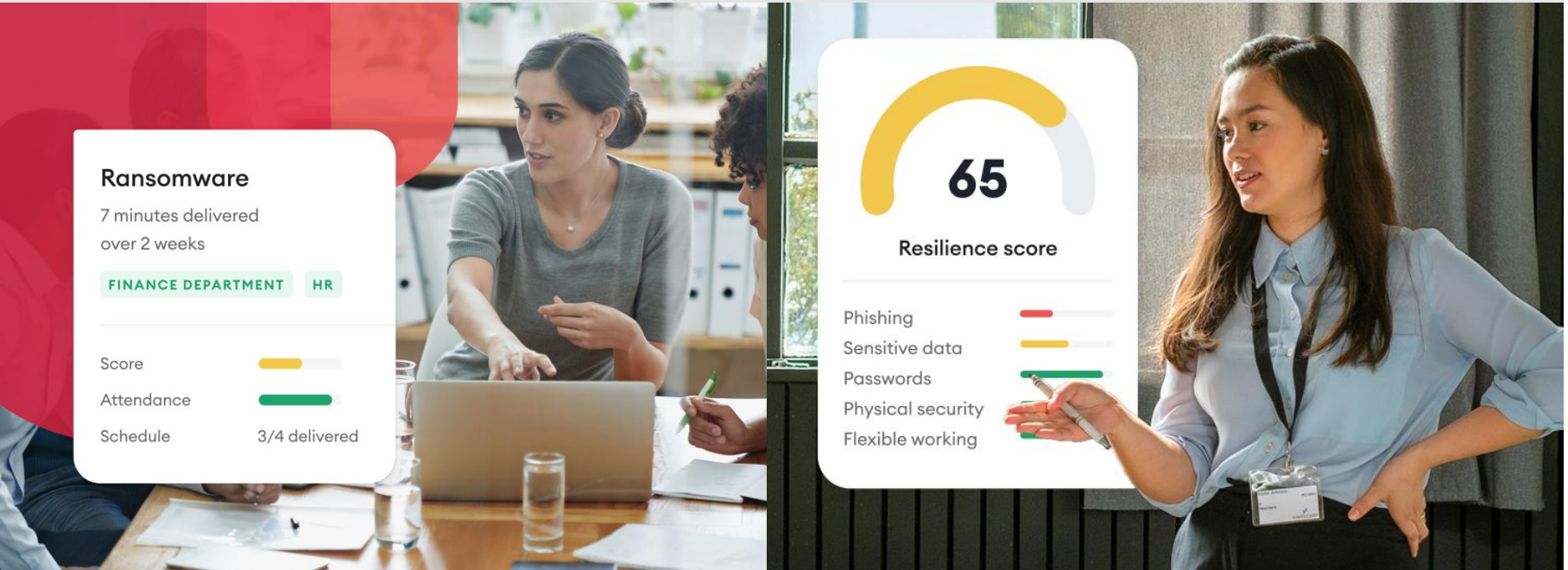


Maximize the outcome of the training

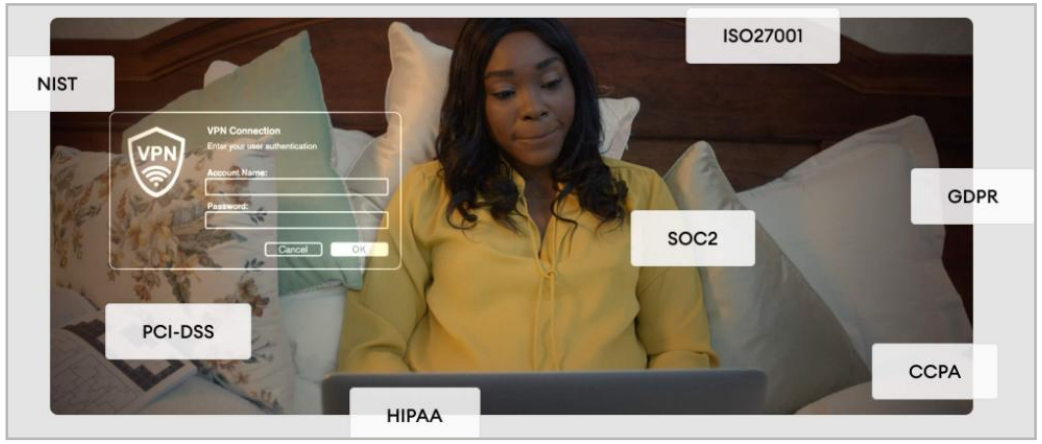


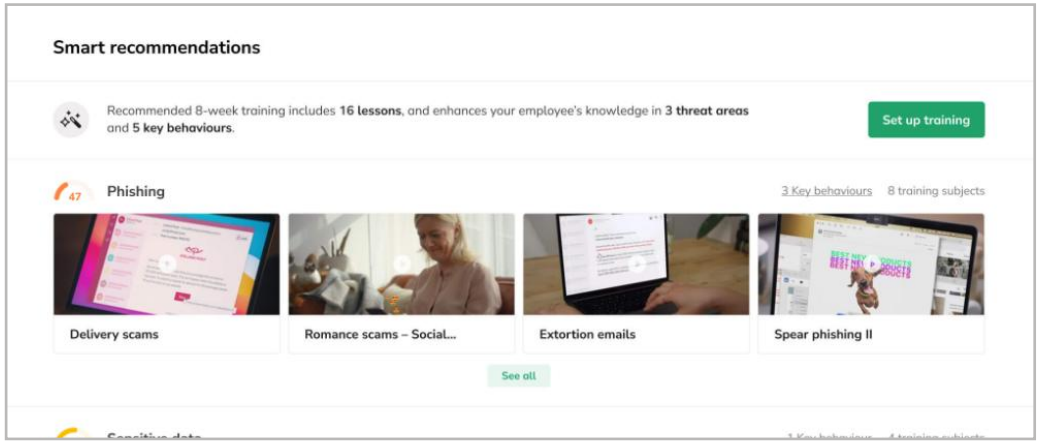


Human risk assessment

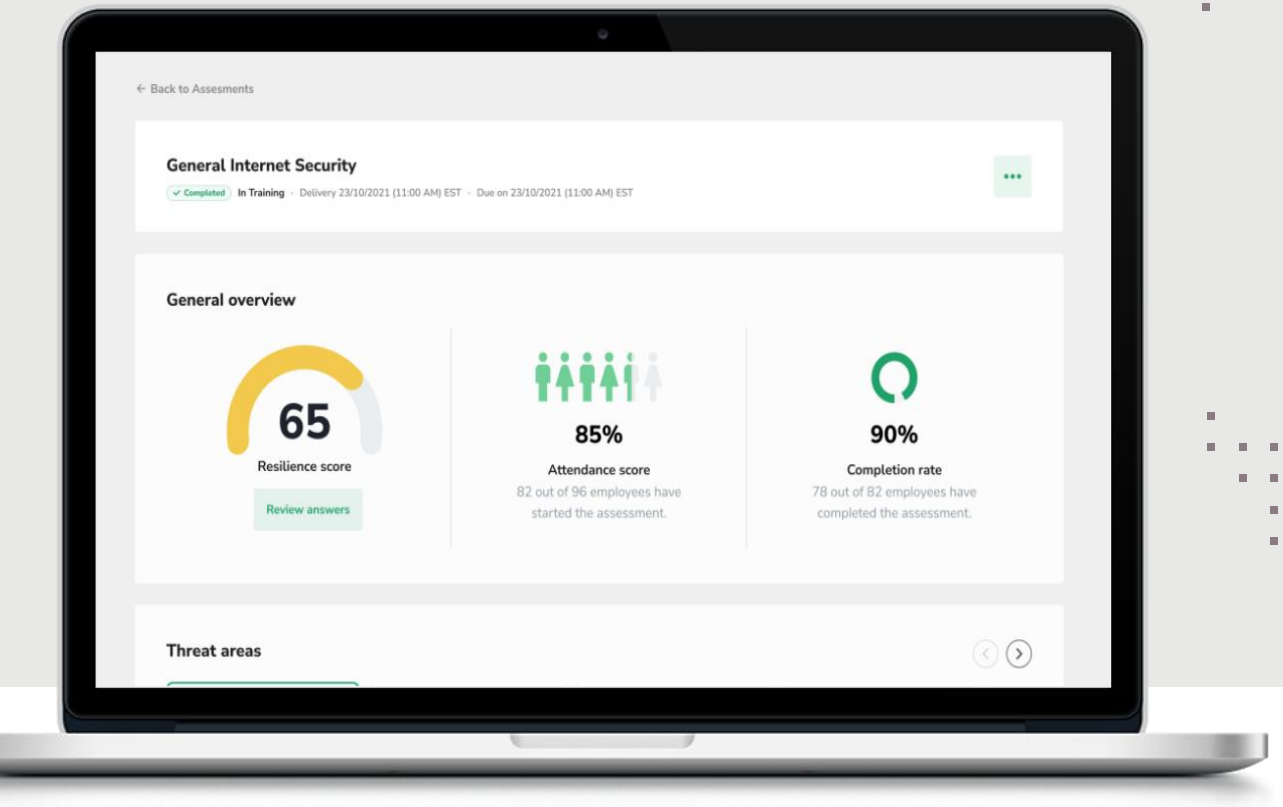


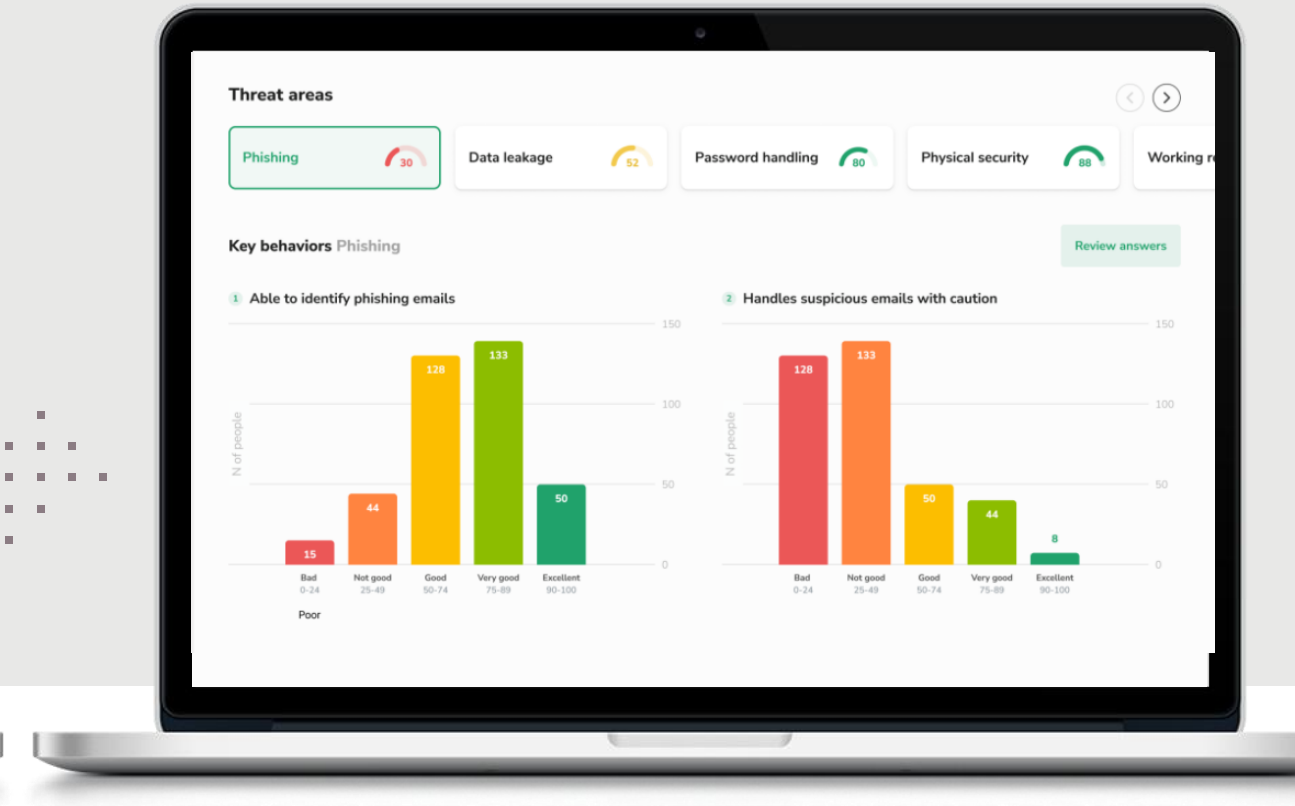
Training method





General Reporting





Dashboards allows easy visibility and actions to ensure overview and outlines the progress an organization reaches. All results can be extracted via PDF, open API, integrations and CSV. files to support data workflows for optimal output. Certificate for employees are issued upon completion.

Interactive and real-life situations based on a No blame – No shame methodology

.the tech collective

powered by Implement