Cybersecurity and Safety: A Clash or a Union of Cultures?

Dr. Claire Blackett

Senior Human Factors Consultant

RISK PILOT

About me

Dr. Claire Blackett
Senior Human Factors Consultant
Risk Pilot, Gothenburg, Sweden

claire.blackett@riskpilot.se
linkedin.com/in/claireblackett/
researchgate.net/profile/Claire-Blackett

Background

- PhD in Accident Investigation Methods & Organisational Learning, University College Dublin, Ireland.
- Almost 20 years' working with human factors & human reliability in the nuclear, petroleum, rail, maritime, healthcare, process industries – UK, Norway, Sweden.
- Joined Risk Pilot as a consultant in December 2023 – working with HF engineering & human reliability analysis.

Example research interests

- Cybersecurity culture
  - Reegard, K., Blackett, C., & Katta V. (2019) The Concept of Cybersecurity Culture. In Proceedings of 29th ESREL Conference, 22-26 September, Hannover, Germany.
- The ethical use of AI in industry & society
  - Blackett, C. (2022) The Ethics of AI in Autonomous Transport. In Proceedings of the 32nd ESREL Conference, 28 August – 1 September, Dublin, Ireland.
- Human factors & human reliability for advanced reactors
  - Blackett, C., Skraaning, G., Kaarstad, M., & Eitrheim, M.R.H. (2023) Human Factors Considerations for Remote Operation of Small Modular Reactors. In Proceedings of 13th NPIC/HMIT Conference, 15-20 July, Knoxville, TN.

Mentimeter Questions 1 & 2

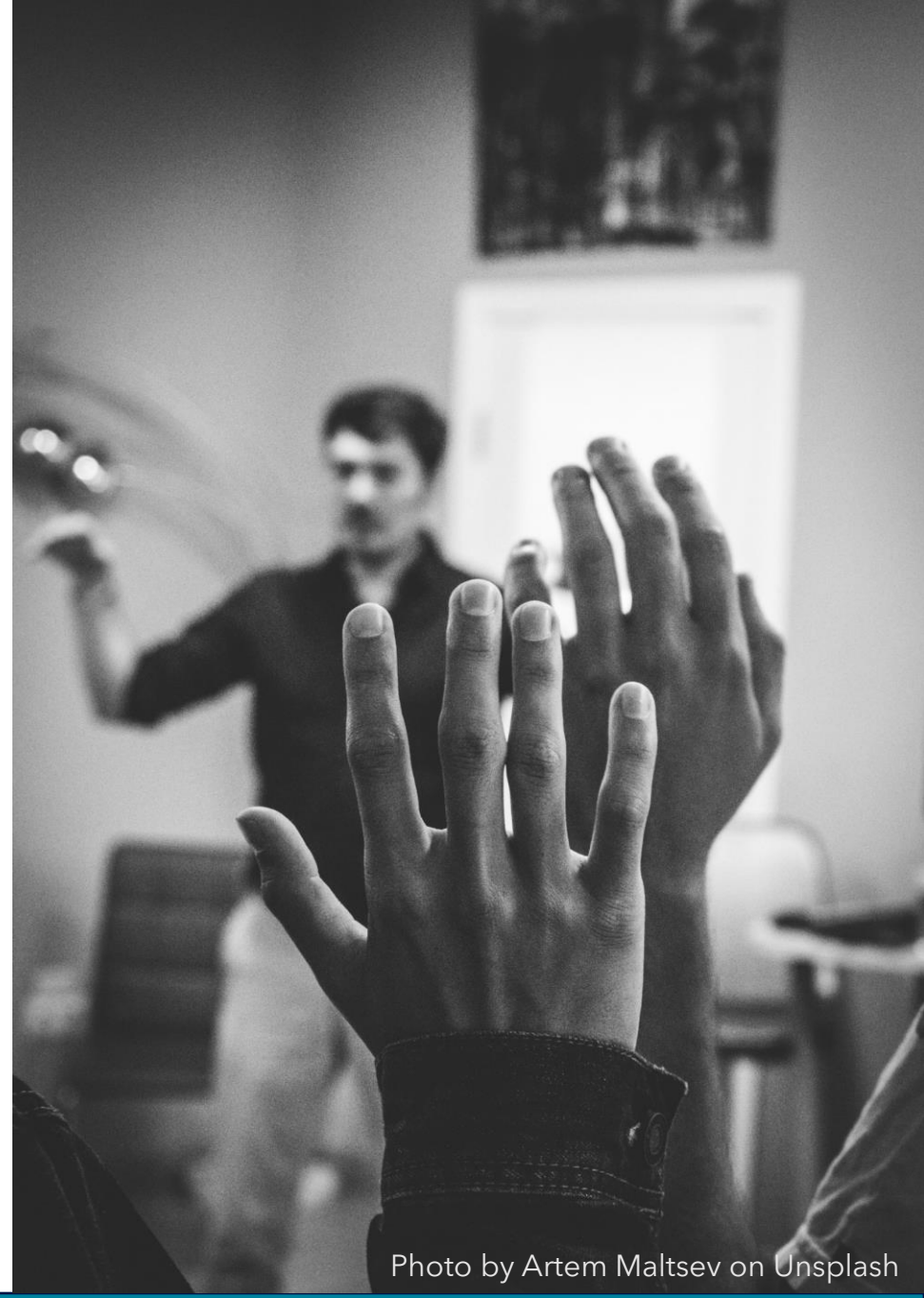


Photo by Artem Maltsev on Unsplash

Cybersecurity is evolving

- No longer the sole responsibility of the IT department
- Facing new and rapidly changing challenges from a modern workplace that is radically different from before

Photo by Anastasia Nelen on Unsplash

The changing threat landscape

- Technological developments have enabled increased digitalisation of the workplace and more mobile working
- The COVID-19 pandemic has had a huge impact on remote working, and the integration of work across multiple platforms & devices
- There has been increased decentralisation of the workplace

Photo by Surface on Unsplash

The changing threat landscape

- There has been a huge upsurge in the availability and sophistication of AI tools that can be used to create convincing text and images

Photo by Surface on Unsplash

The changing threat landscape

In the voice of David Attenborough, what is ChatGPT?

Ah, yes, the ChatGPT. A remarkable creation of human ingenuity and technological advancement. Developed by OpenAI, the ChatGPT is a language model trained on an unprecedented amount of data, allowing it to generate human-like responses to a wide variety of prompts.

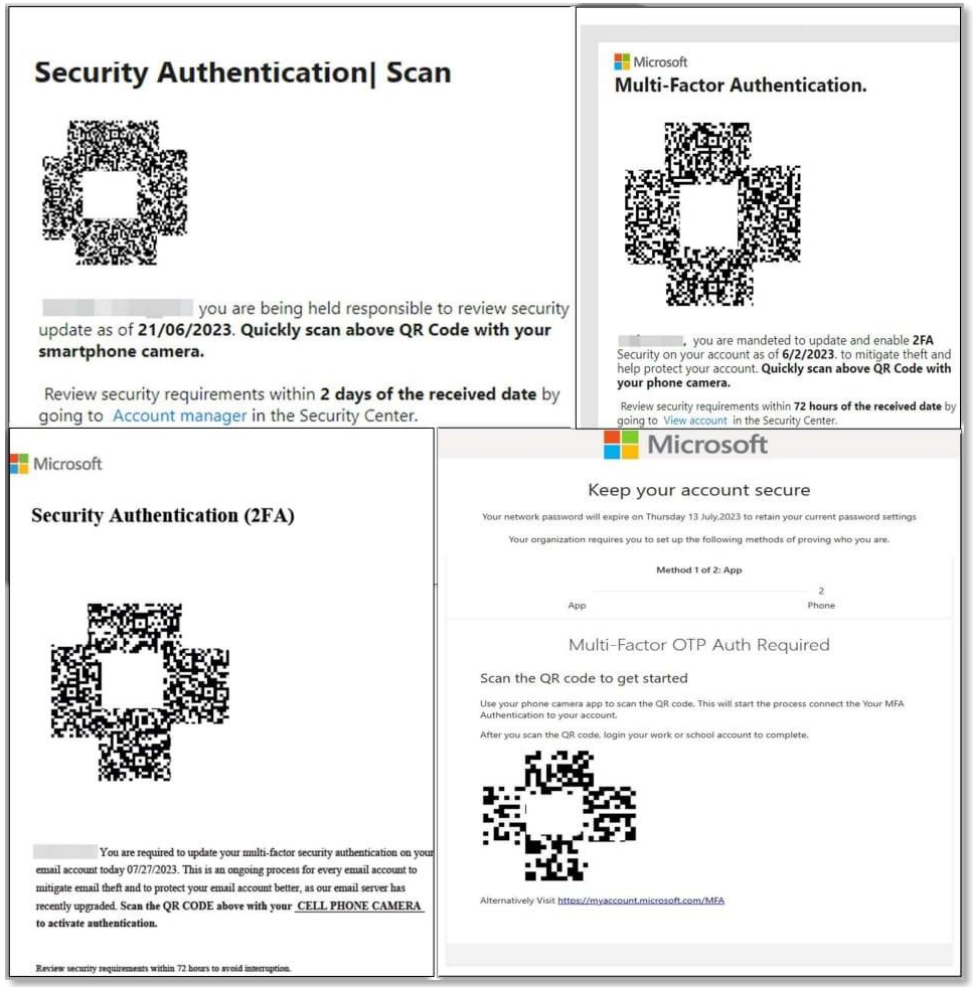
Its abilities are truly astounding. It can converse on nearly any topic, answer questions, offer insights, and even create original content. It's a tool that has the potential to revolutionize the way we interact with technology, and perhaps even with each other.

But with great power comes great responsibility. As the ChatGPT continues to evolve and improve, we must consider the ethical implications of its use. We must ensure that it is used for the betterment of humanity, and not for nefarious purposes.

In short, the ChatGPT is a remarkable achievement in the field of artificial intelligence, but its true value will depend on how we choose to use it.

Photo by Surface on Unsplash

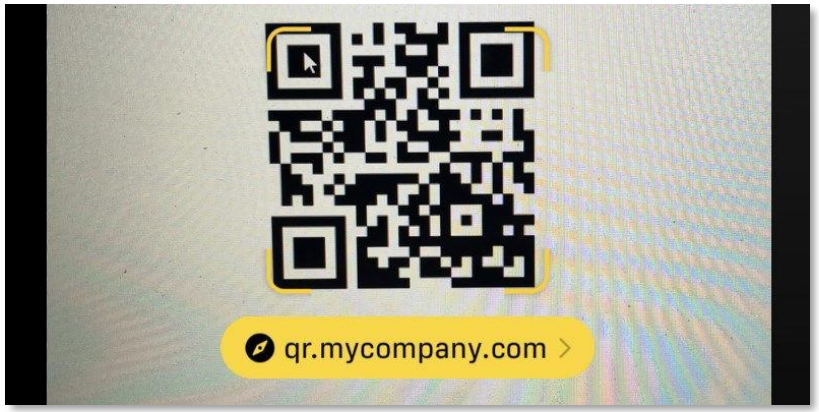
Attack on US organisations using QR codes and phishing emails



- QR codes increasingly used in everyday life since COVID-19 pandemic
- In 2023, cybersecurity researchers uncovered a phishing campaign that used QR codes to try to acquire Microsoft credentials
- Approx. 1000 emails were identified targeting
  - A large US energy company (29% of emails)
  - Manufacturing firms (15%)
  - Insurance companies (9%)
  - Technology companies (7%)
  - Financial services (6%)

Sources: therecord.com and bleepingcomputer.com

Example: Attack on US organisations using QR codes and phishing emails



Example redirect code.
Image from qrplanet.com

- QR codes have not typically been used in the past by cyber criminals at this scale
- This may indicate that cyber criminals are testing this out as a potential new way to gain access to sensitive information
- This attack was first detected in May 2023, and according to Cofense cybersecurity firm:

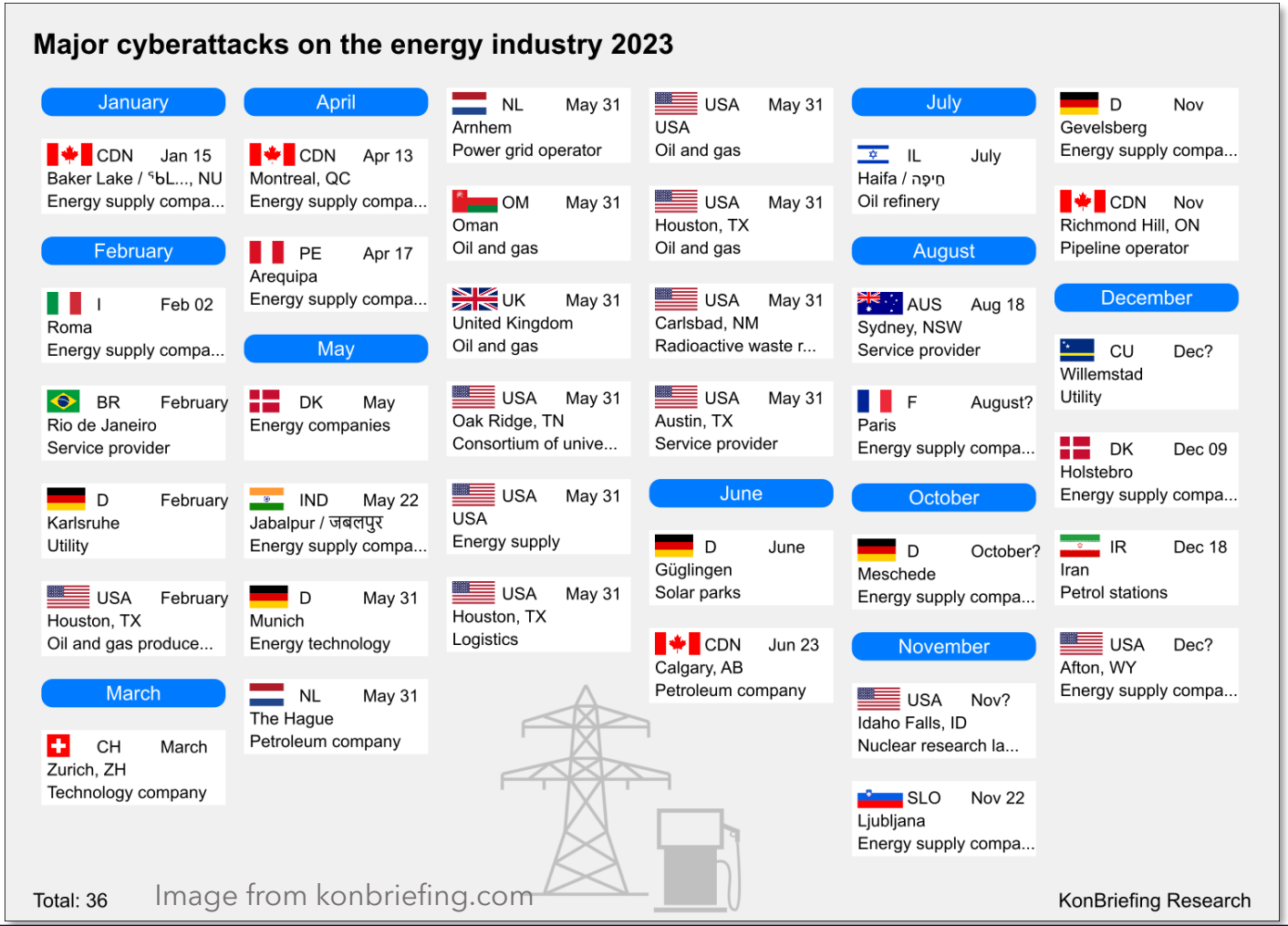
> *"The average month-to-month growth percentage of the campaign is more than 270%. The overall campaign has increased by more than 2,400% since May 2023."*

Sources: https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/

Increase in attacks on energy companies and critical infrastructure

Cyberattacks on the energy sector have been steadily increasing since 2018, reaching "alarmingly high levels" after the Russian invasion of Ukraine in 2022.

(source: International Energy Agency, 2023)



Mentimeter
Questions 3 & 4

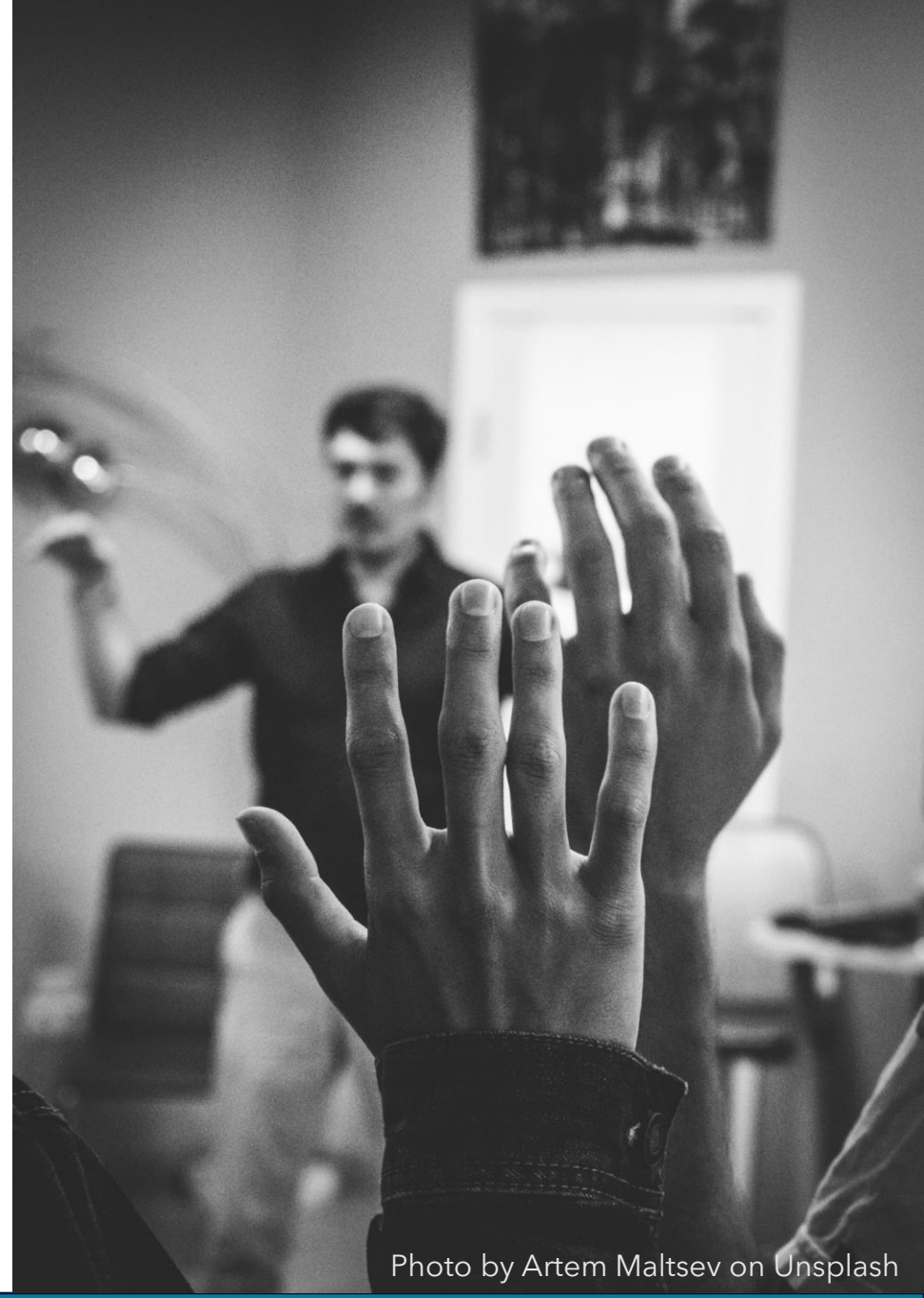


Photo by Artem Maltsev on Unsplash

Acknowledging the human factor

- Humans have traditionally been seen as the weakest link in the cybersecurity defence chain
- The majority of attacks are still attributed to “human error”
- The concept of cybersecurity culture is gaining popularity, but is it effective?

Photo by Brooke Cagle on Unsplash

The human role in cybersecurity

In 2020, a study found "95% of cyber security breaches are due to human error" (source: www.thalesgroup.com)

A joint study from Stanford University Professor Jeff Hancock and security firm Tessian revealed that nine in 10 (88%) data breach incidents are caused by employees' mistakes. (source: cisomag.com)

Did you know that 74% of all breaches include a human element, be it stolen credentials or social engineering?
(source: www.nixu.com)

Image by @SecurityTrybe on Twitter

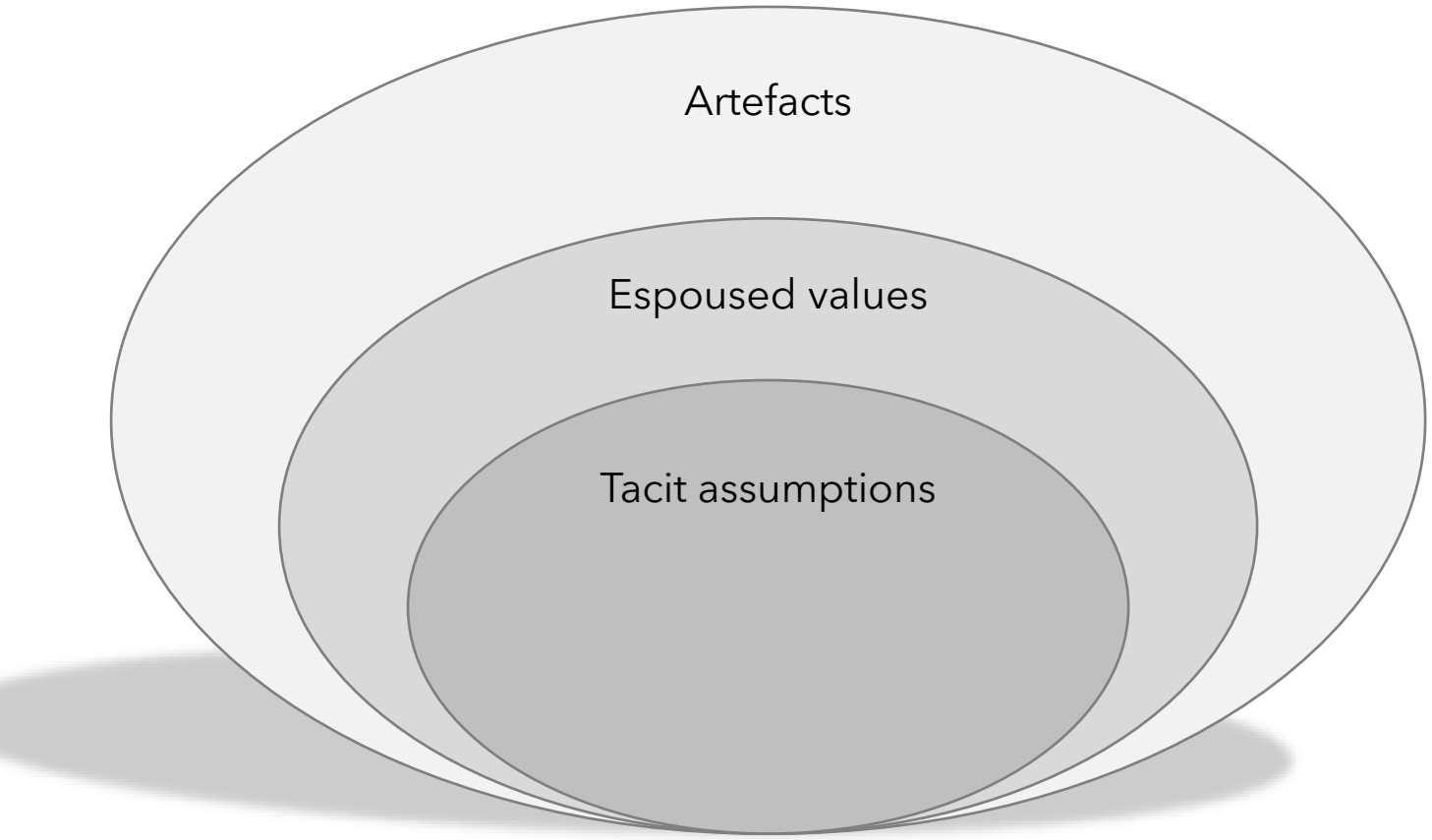
The concept of cybersecurity culture

- A relatively new phenomenon, only emerging within the last 10 years or so
- Acknowledgement that an organisation's culture can have a bearing on their ability to maintain an adequate level of cybersecurity
- Cybersecurity is a behavioural issue as well as a technological issue
- Understanding that management of cybersecurity is a "human challenge"

Source: Reegård et al. (2019) The concept of cybersecurity culture

Photo by charlesdeluvio on Unsplash

Adapting an organisational model



Source: Reegård et al. (2019) The concept of cybersecurity culture

Photo by charlesdeluvio on Unsplash

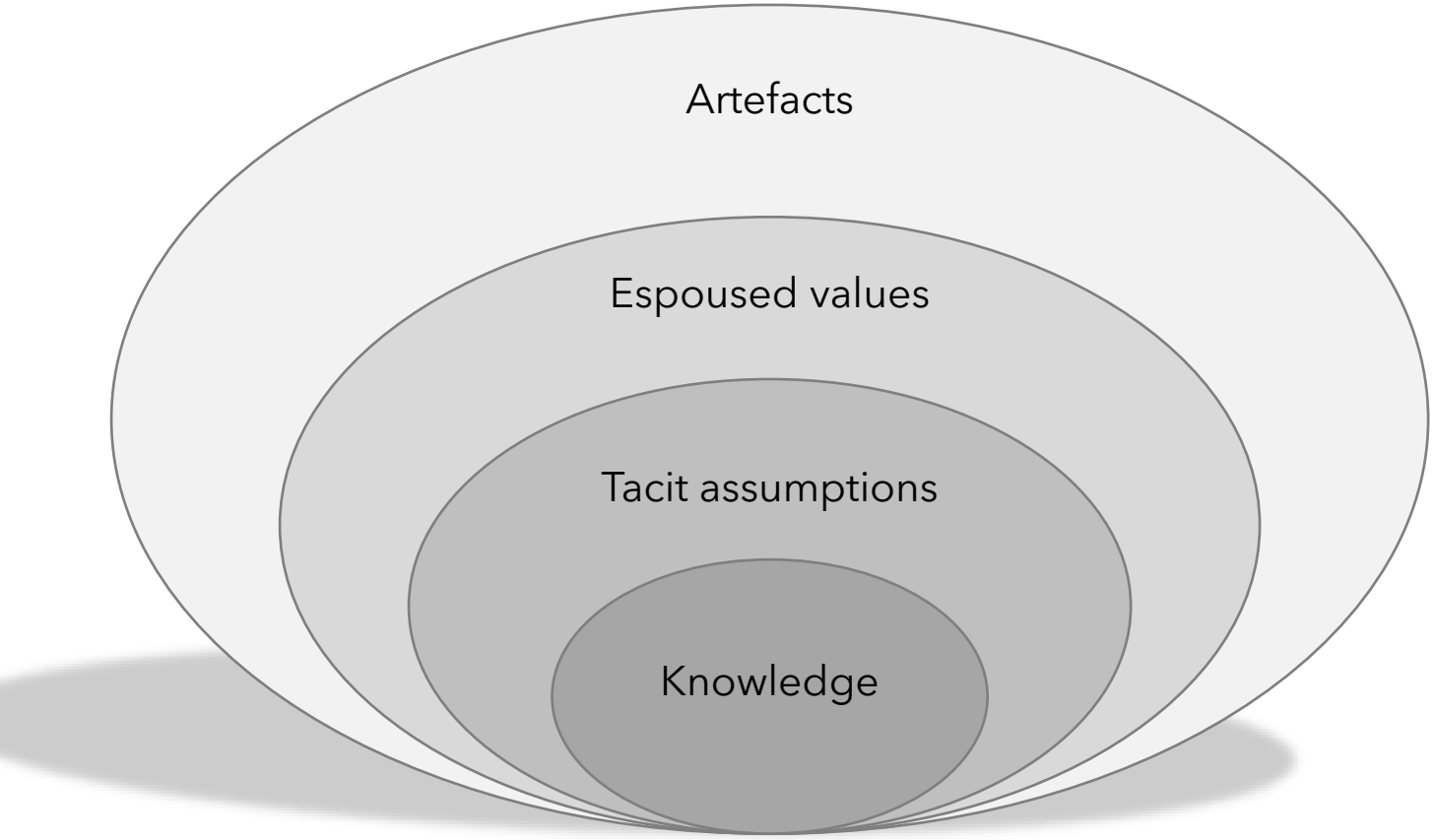
Common attributes with safety culture

- Refers to shared values among a group or organisation
- Is concerned with formal safety issues and closely related to management and supervisory systems
- Emphasizes the contribution of everyone in the organisation
- Impacts how individual members of the organisation behave at work
- Is reflected in contingency between reward systems and safety performance
- Is reflected in an organisations willingness to learn from errors, incidents and accidents
- Is relatively enduring, stable and resistant to change

Source: Reegård et al. (2019) The concept of cybersecurity culture

Photo by charlesdeluvio on Unsplash

The concept of cybersecurity culture



Source: Reegård et al. (2019) The concept of cybersecurity culture

Photo by charlesdeluvio on Unsplash

Mentimeter Questions 5 & 6

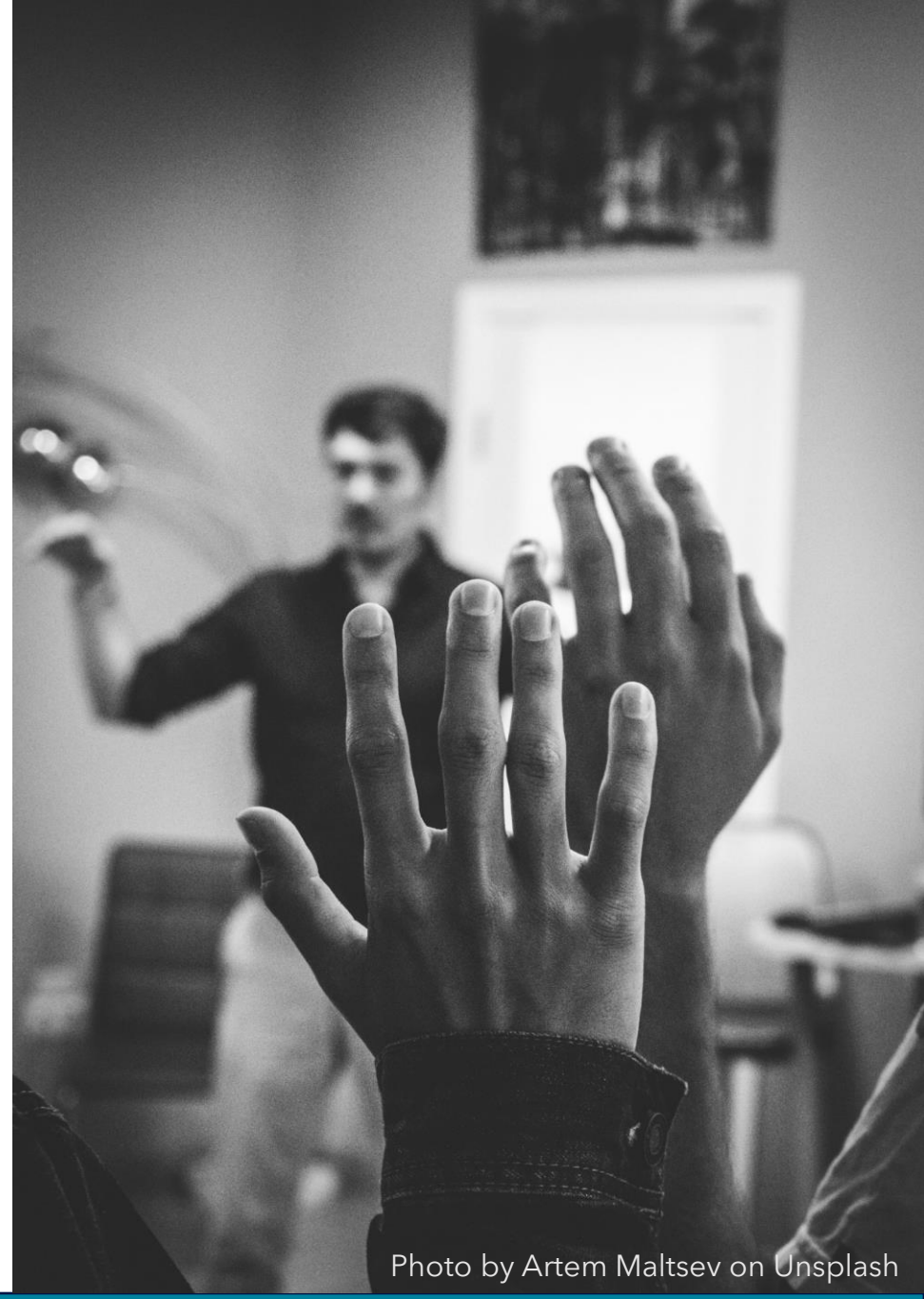
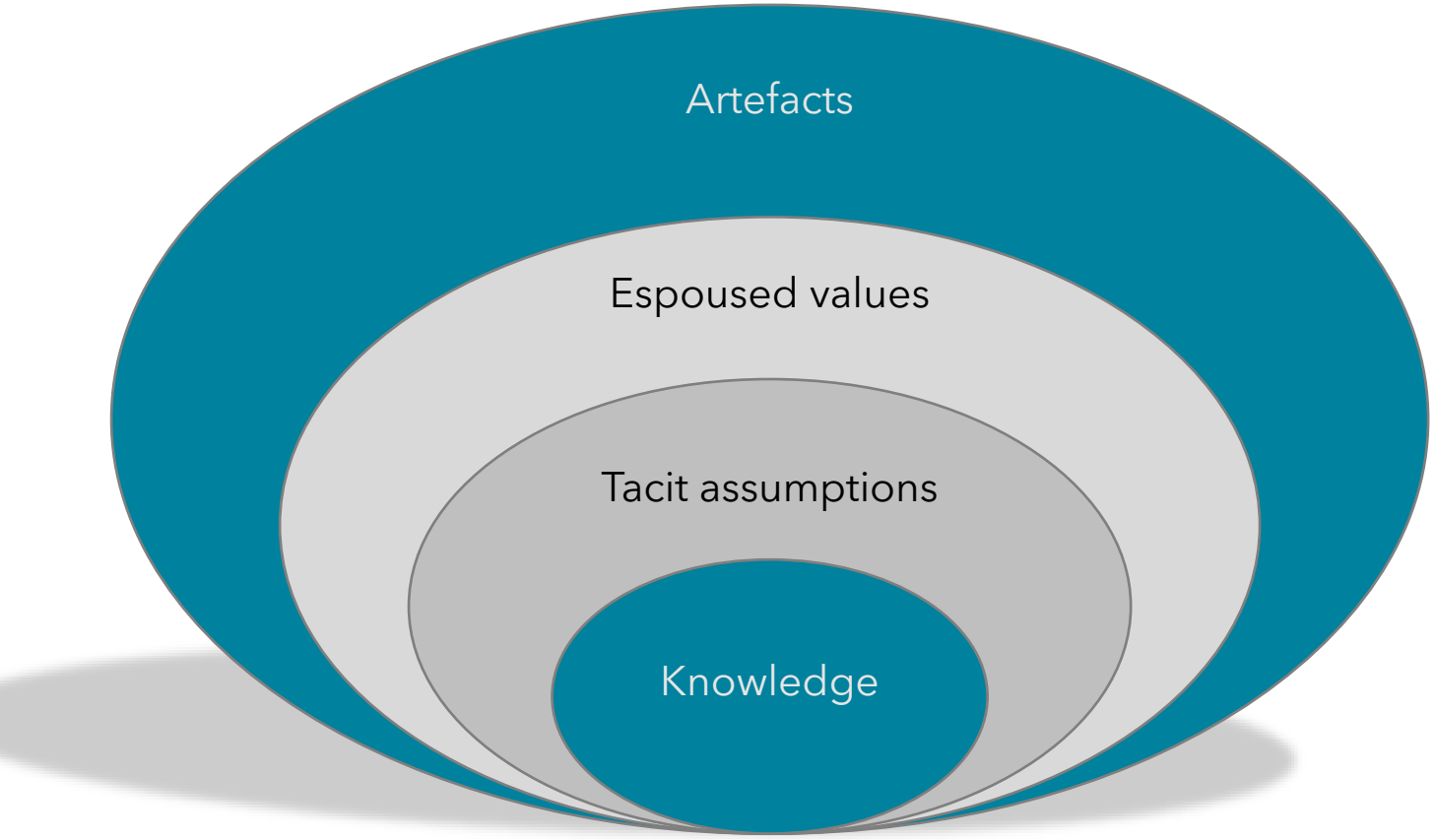


Photo by Artem Maltsev on Unsplash

The concept of cybersecurity culture



Source: Reegård et al. (2019) The concept of cybersecurity culture

Photo by charlesdeluvio on Unsplash

Can we learn from safety culture?

- What can safety culture professionals and researchers teach us about how to implement behavioural change in an organisation?
- How/has safety culture evolved to meet the challenges of the changing workplace?
- What are the potential pitfalls that we need to avoid when considering cybersecurity culture?

Photo by sol on Unsplash

Example: cybersecurity fatigue

- A growing phenomenon whereby people are overwhelmed, stressed and demotivated by security measures across numerous applications, for both work and in their personal life
  - Multiple, unique passwords that are required to be changed frequently
  - Overuse of multi-factor authentication
  - Repeated security warnings and IT alerts that are often meaningless
  - Mandatory and repetitive security awareness training videos
  - Etc.

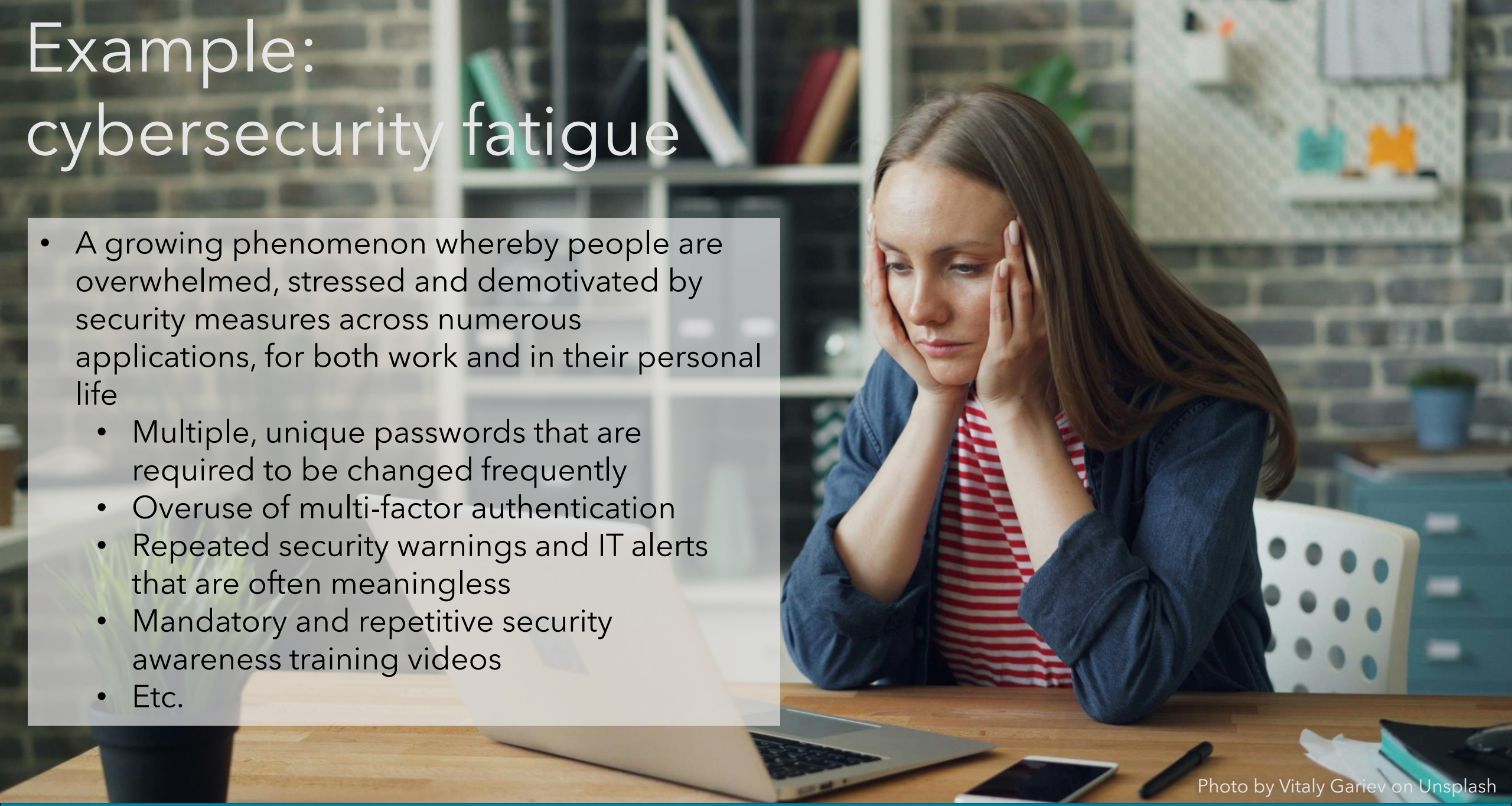


Photo by Vitaly Gariev on Unsplash

Perhaps the problem is that, because *everything* is connected to the internet, and we are online all the time, cybersecurity is everywhere, and it is overwhelming.

It's not just a work issue, it's a life issue.

Photo by NordWood Themes on Unsplash

Mentimeter
Questions 7 & 8

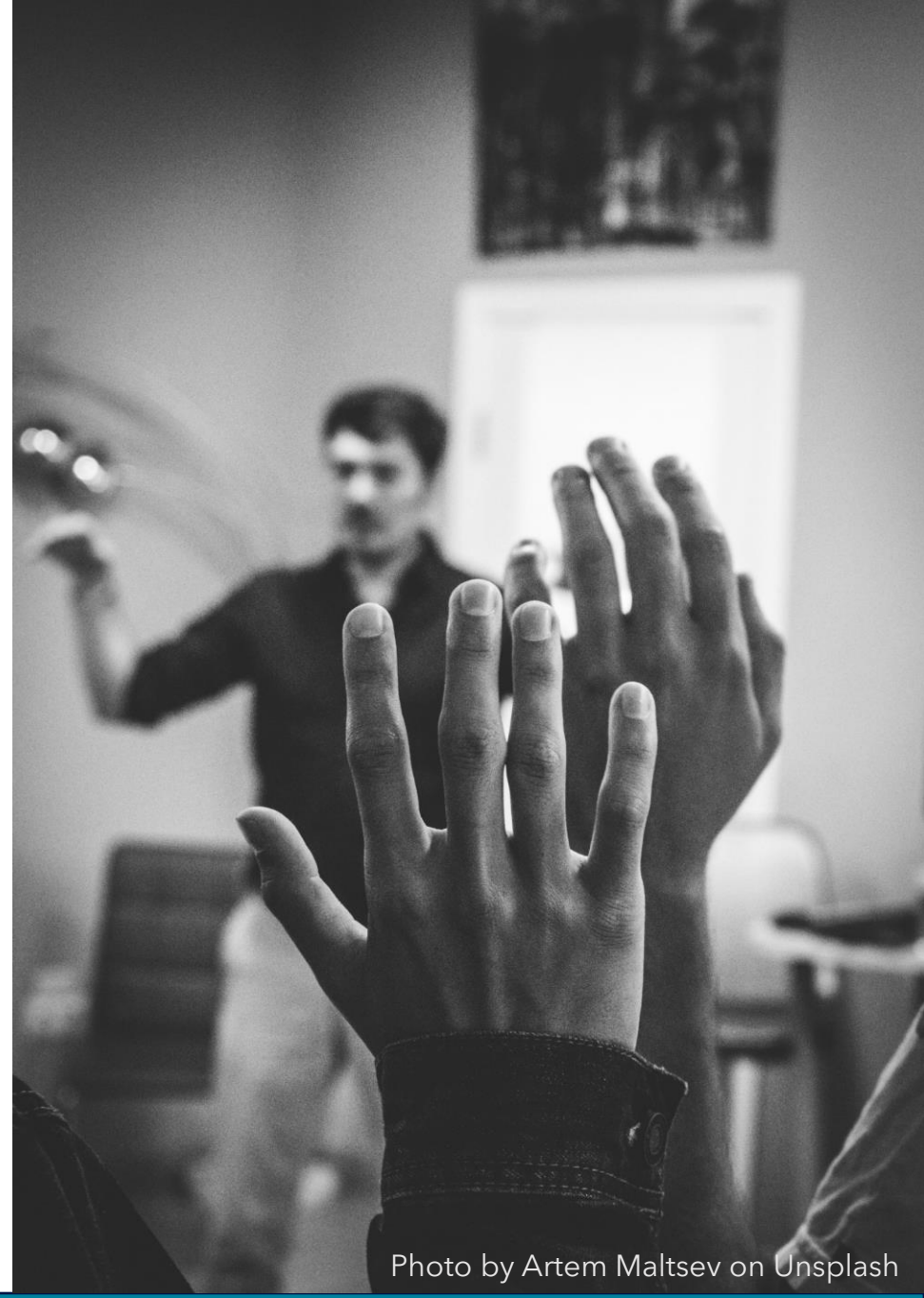
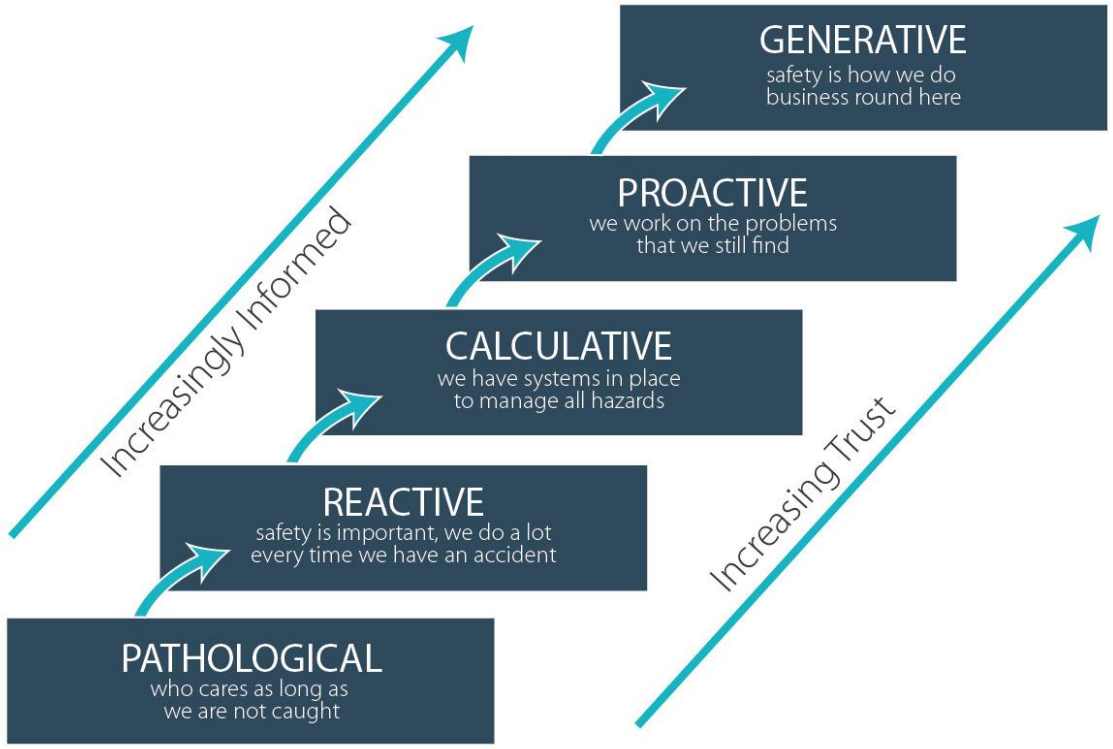


Photo by Artem Maltsev on Unsplash

What can we learn from safety culture?

- Behavioural change takes time
- “There is no silver bullet”
- It is normal to have plateaus, or to even go backwards sometimes

What can we learn from safety culture?



Source: Fosdick et al. (2024). Creating a Cultural Maturity Model to Assess Safe System Readiness Within Road Safety Organisations. Journal of Road Safety, 35(1), 52–64.
Source: Tappura et al. (2022). Creation of satisfactory safety culture by developing its key dimensions. Safety Science Volume 154, October 2022, 105849.

Photo by Matthew Henry on Unsplash

The potential for goal conflict

- IAEA 10 traits of a healthy safety culture

1. Individual responsibility
2. Questioning attitude
3. Effective safety communication
4. Leadership responsibility
5. Decision-making
6. Respectful work environment
7. Continuous learning
8. Problem identification and resolution
9. Environment for raising concerns
10. Work processes

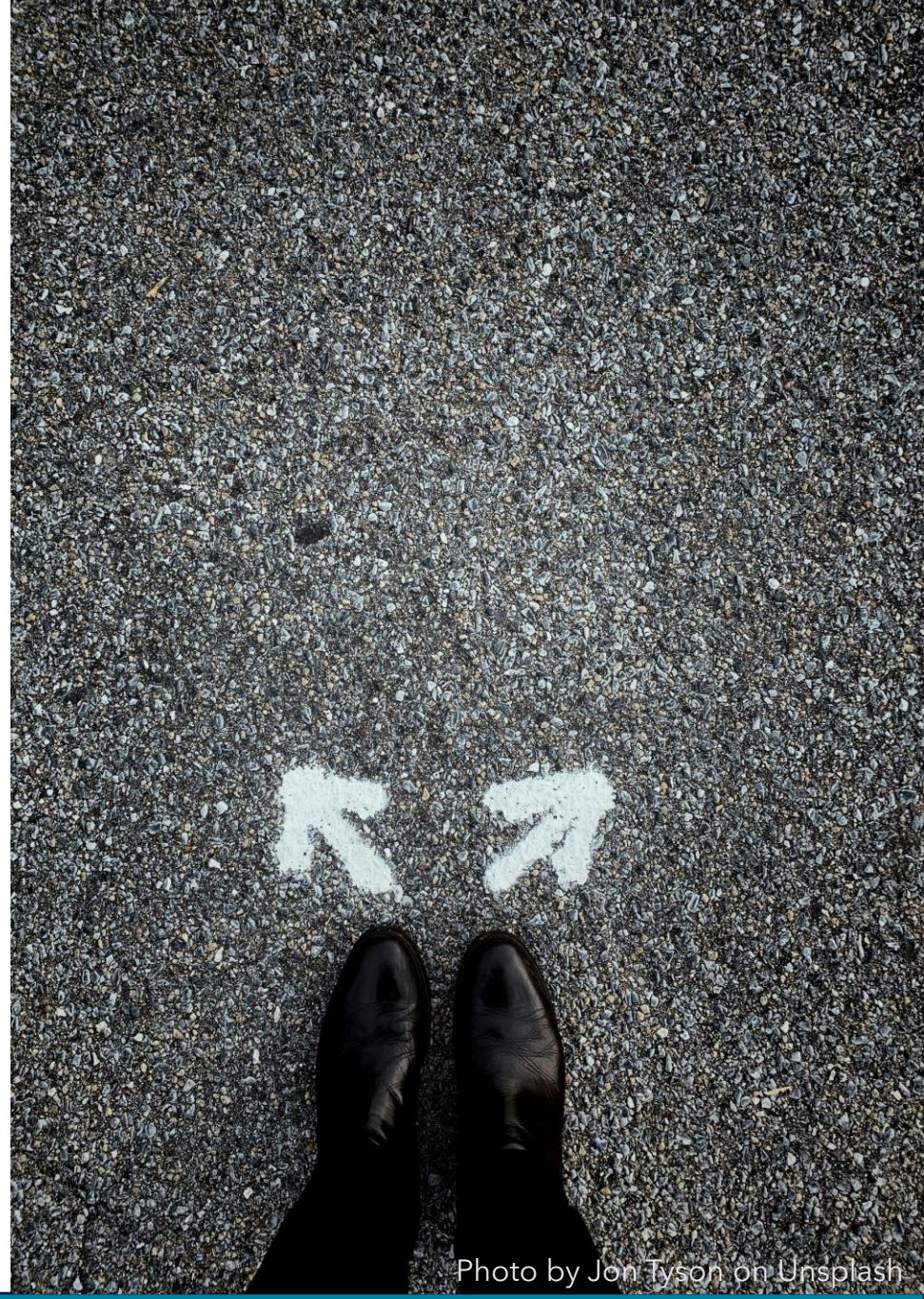


Photo by Jon Tyson on Unsplash

Mentimeter Question 9

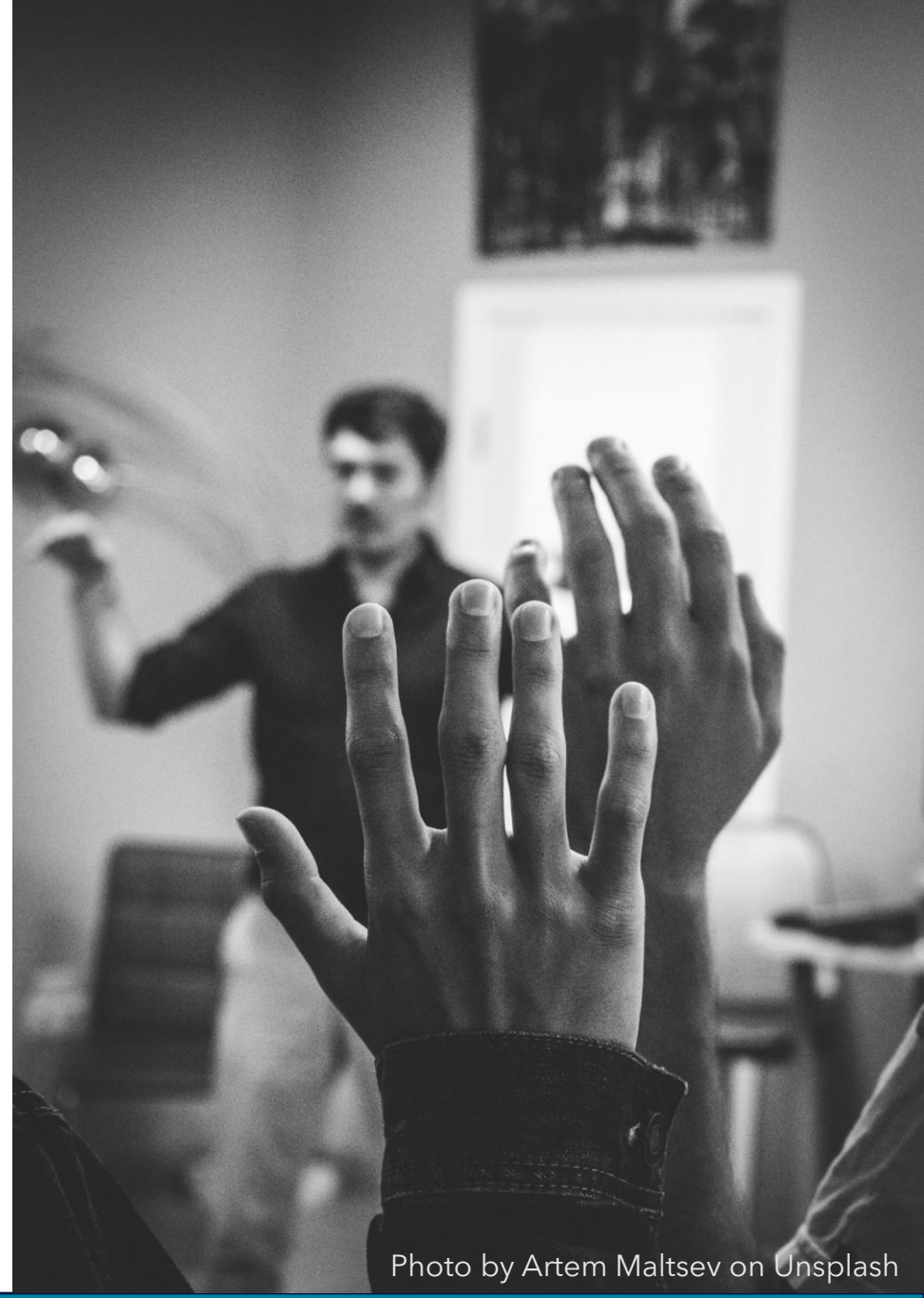


Photo by Artem Maltsev on Unsplash

Final thoughts

- Cybercrime is a real and persistent threat
- It is only a matter of time before Swedish energy companies and critical infrastructure are targeted
- A human-centered approach is necessary to develop a strong cybersecurity culture
- There may be a lot to learn from safety culture, and there may also exist some goal conflicts that must be investigated and resolved

Photo by Annie Spratt on Unsplash

Research at Risk Pilot

- Co-authoring a paper with RISE on the topic of cybersecurity culture & safety culture
- Looking for funding & collaboration partners to investigate this topic further
- Goal is to develop practical guidance for organisations to implement a human-centered cybersecurity culture approach that works in harmony with safety culture initiatives.

https://riskpilot.se/

Mentimeter Question 10

Thank you!

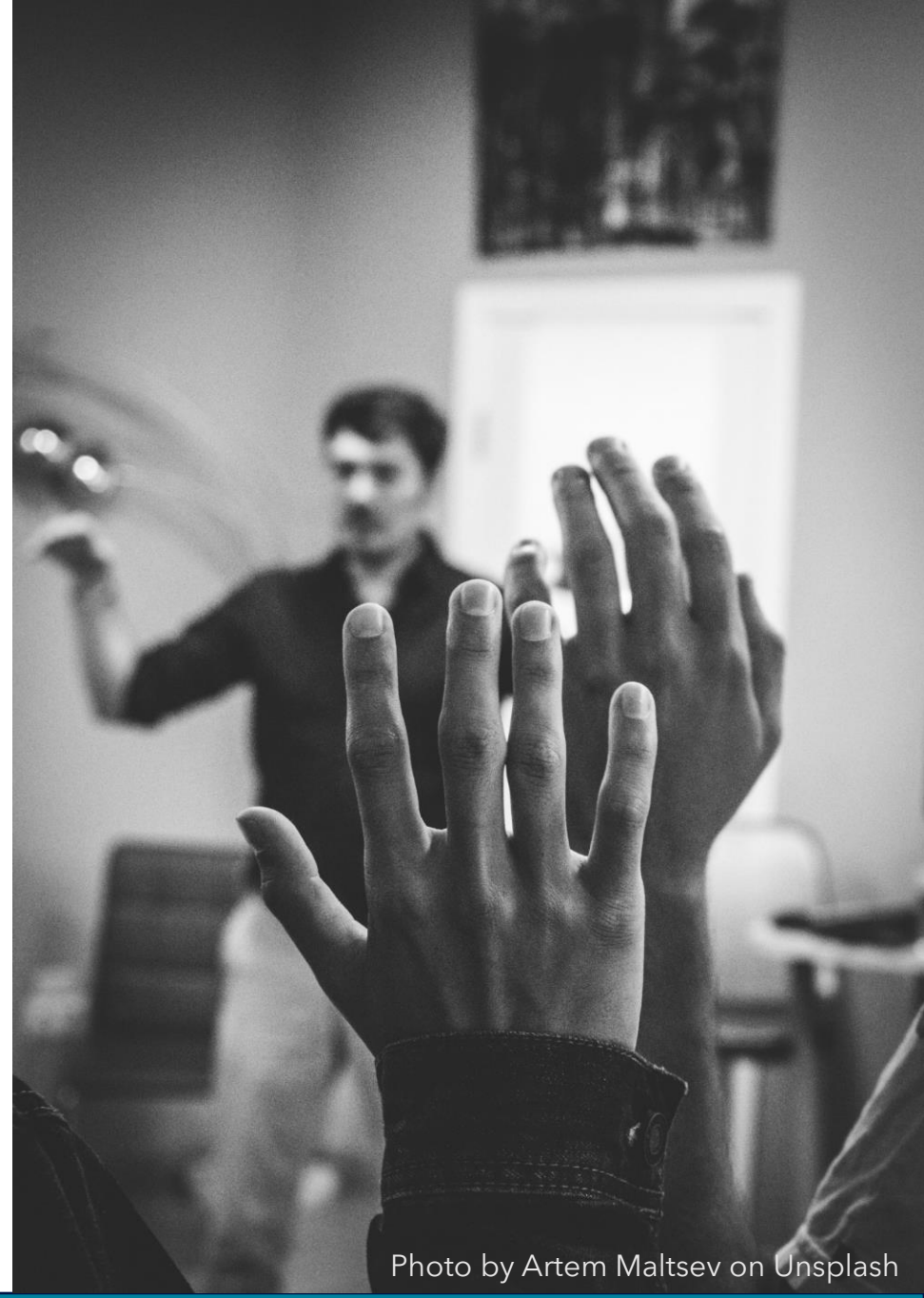


Photo by Artem Maltsev on Unsplash