# SOTER

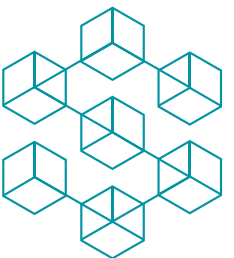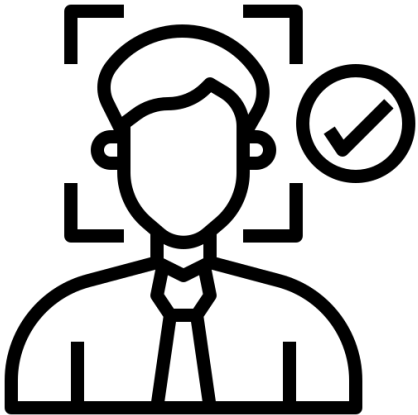# cyberSecurity Optimization and Training for Enhanced Resilience in the finance sector

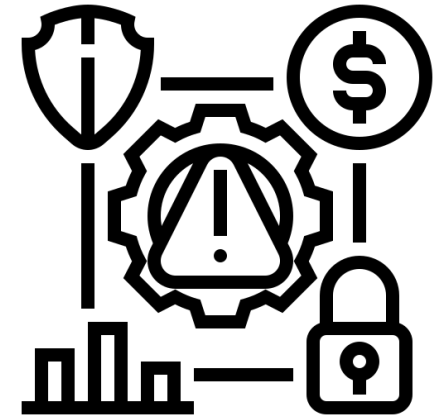## CPS4CIP 2021: Robin Renwick, Trilateral Research

**SOTER**

Digital onboarding/KYC Platform

Training and awareness platform

Human factor risk assessment framework

icon attribution: www.flaticon.com – surang | freepik | eucalyp

SOTER

Understand human-factor based cybersecurity practices in a financial organisation by gathering different perspectives.

Holistic understanding can lead more effective cybersecurity.

Social research methods contribute to a more human-orientated risk assessment framework

# Hypotheses

Management, the cybersecurity department, and general employees have conflicting priorities regarding cybersecurity.

Certain pressures exist that act as disablers of effective cybersecurity in the organisation.

Viewing employees as threat vectors impacts trust levels within the organisation.

# Methodology

SOTER
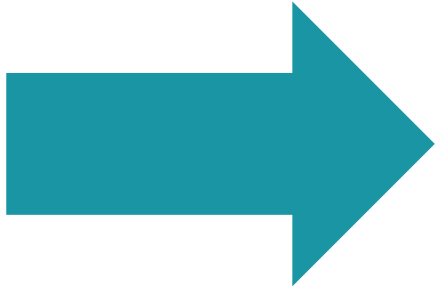
17 interviewees

- 3 Senior Managers
- 5 Middle Managers

- 3 Back Office Staff

- 3 IS/Cybersecurity Managers
- 3 IS/Cybersecurity Staff

# Methodology

**SOTER**

Interview questions – desk research and discussion between partners
- Warm-up questions
- 6 open-ended questions
- 3 hypothetical scenarios

Interviews via Teams
30-60 minutes

Transcription
Thematic analysis – coding, translation codes and group themes
Group discussion themes

# Findings

SOTER

General themes:

1. perspectives (security || business || usability)

2. resource allocation (time || money || staff)

3. collective responsibility || professional responsibility

4. importance of training, knowledge and awareness

5. trust and reputation

# Questions?

Robin Renwick: robin.renwick@trilateralresearch.com

Eliza Jordan: eliza.jordan@trilateralresearch.com