



an NTT DATA Company

Liberbank



TRILATERAL
RESEARCH



Aerospace
and Defense



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre



Human Factors Based Non-Tech Risk Mitigation in Finance

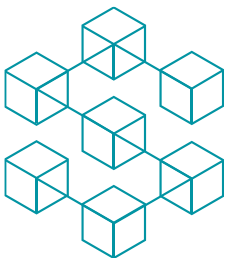
Online Training Workshop on Finance Sector Security

Eva-Maria Griesbacher (Uni Graz) / Martin Griesbacher (RISE)

January 14th 2021



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923

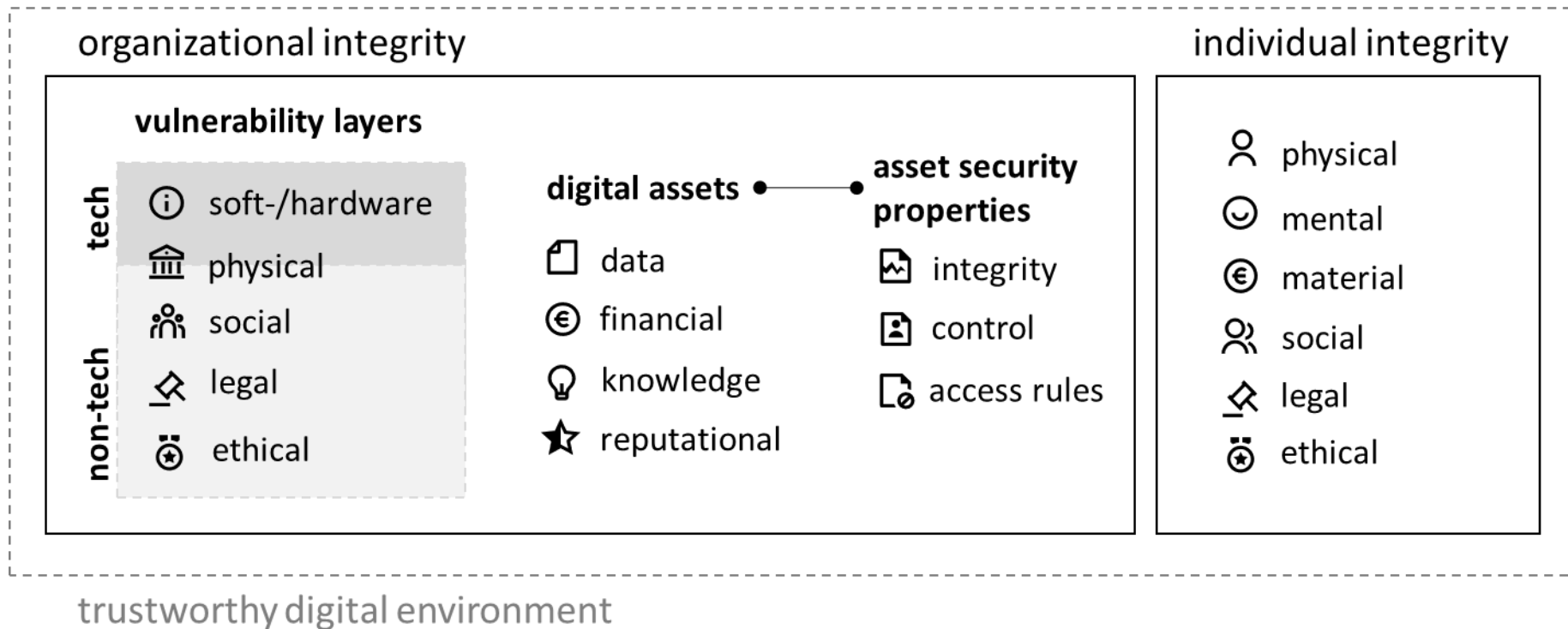


- Horizon 2020 project SOTER (IA)
„Cybersecurity Optimisation and Training for Enhanced Resilience in Finance“
- Two key objectives
 - Technological: digital onboarding process
 - „Non-technological“: Cybersecurity Competence Training
PIs: **Eva-Maria Griesbacher**, **Paul Rabel** (Uni Graz); **Robin Renwick** (Trilateral Research Ireland); **Martin Griesbacher** (RISE)

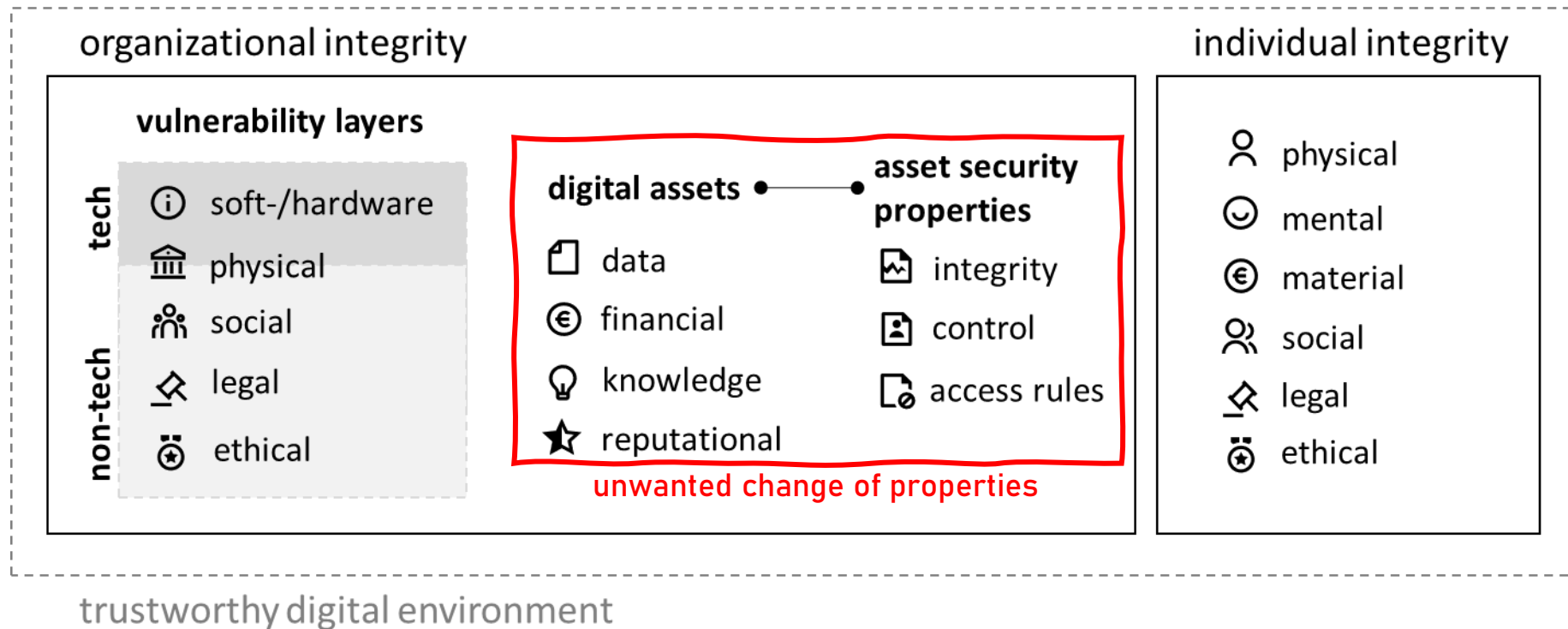
- Partners:



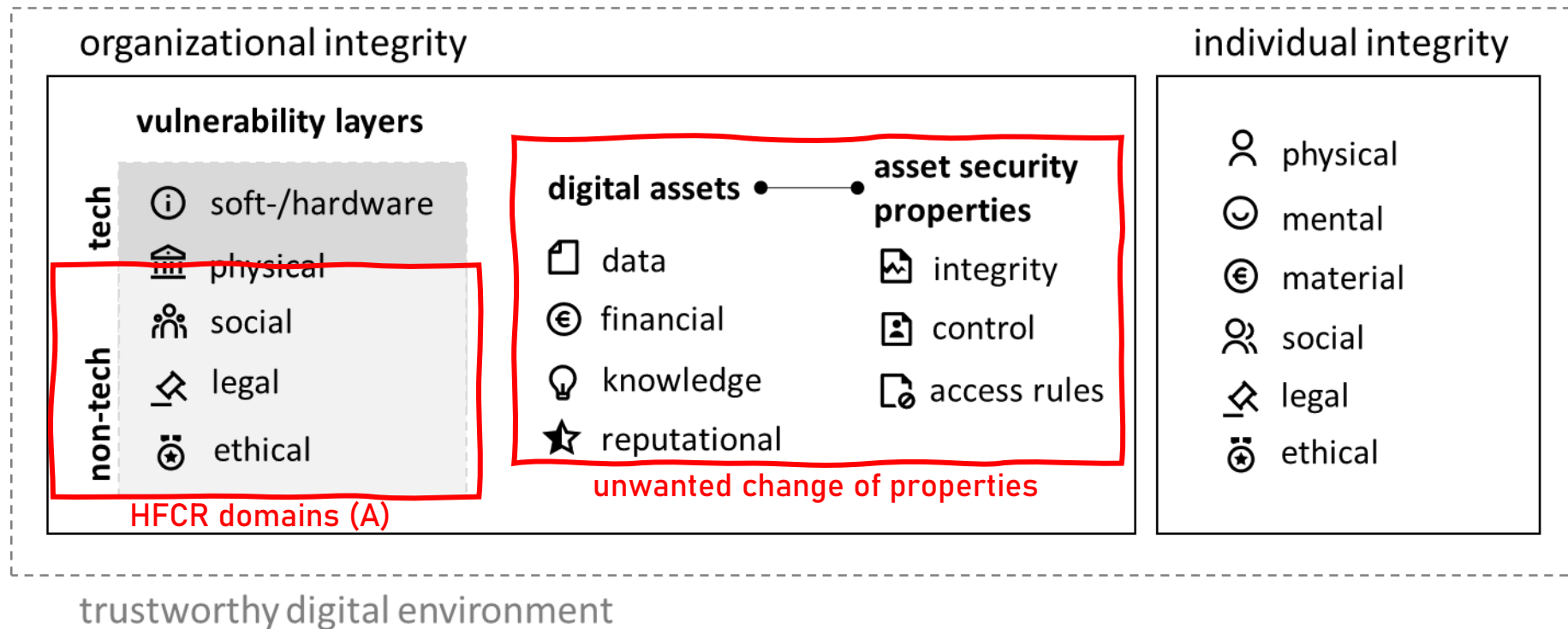
Localisation of human factor based Cybersecurity Risks (HFCCR)



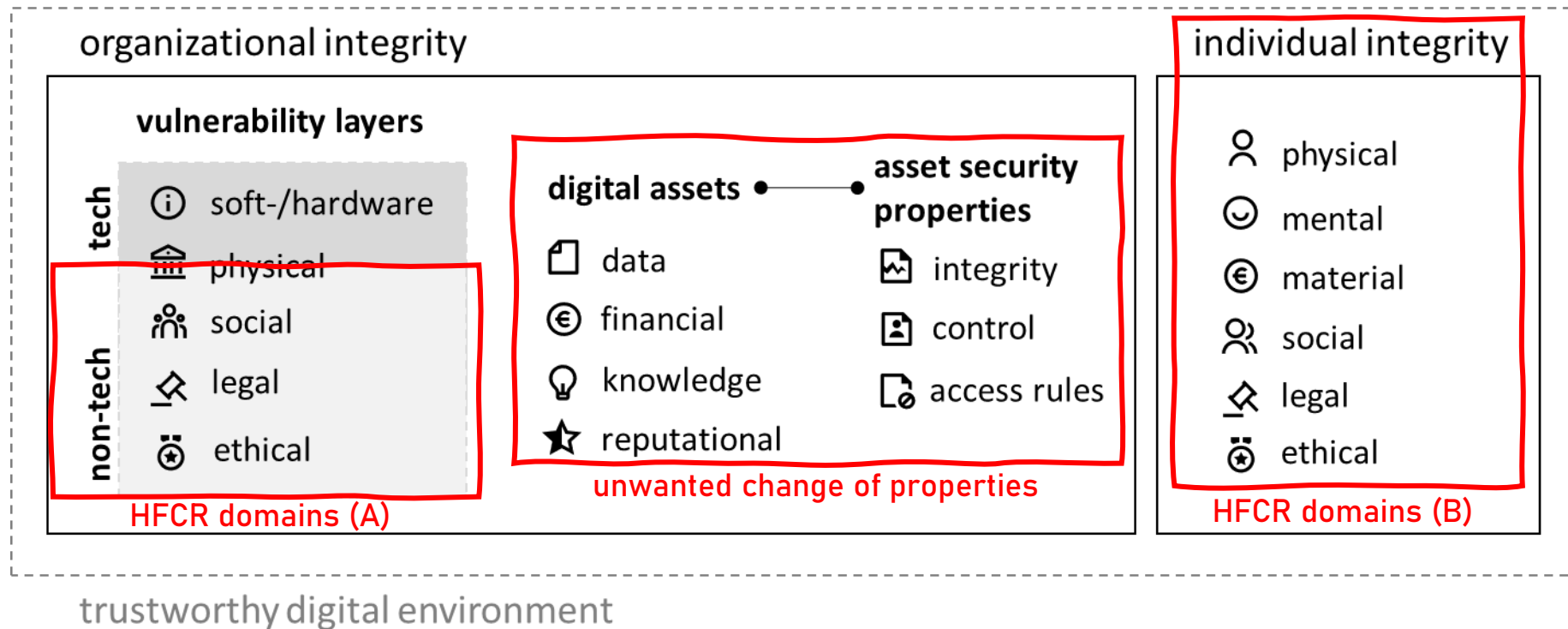
Localisation of human factor based Cybersecurity Risks (HFCCR)



Localisation of human factor based Cybersecurity Risks (HFCCR)

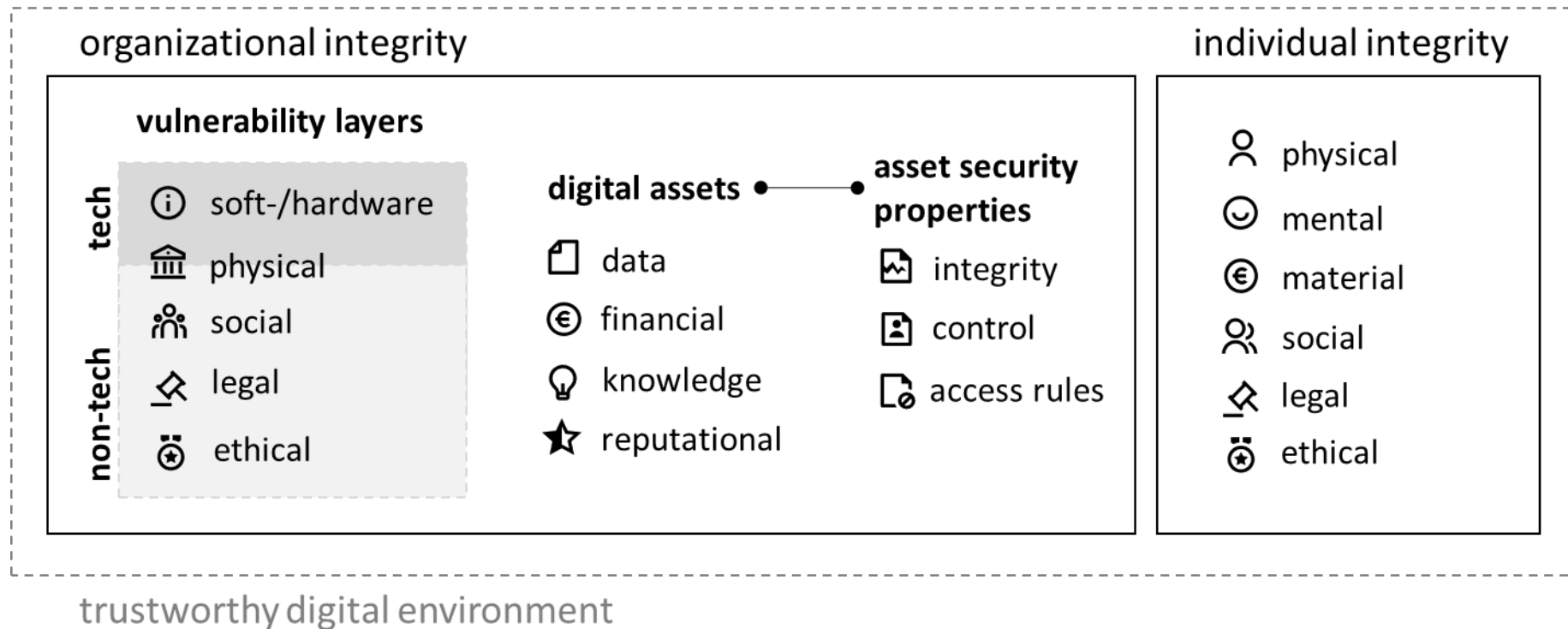


Localisation of human factor based Cybersecurity Risks (HFCCR)



HFCR mitigation strategies

naive optimism “strategy” vs. control regime strategy?



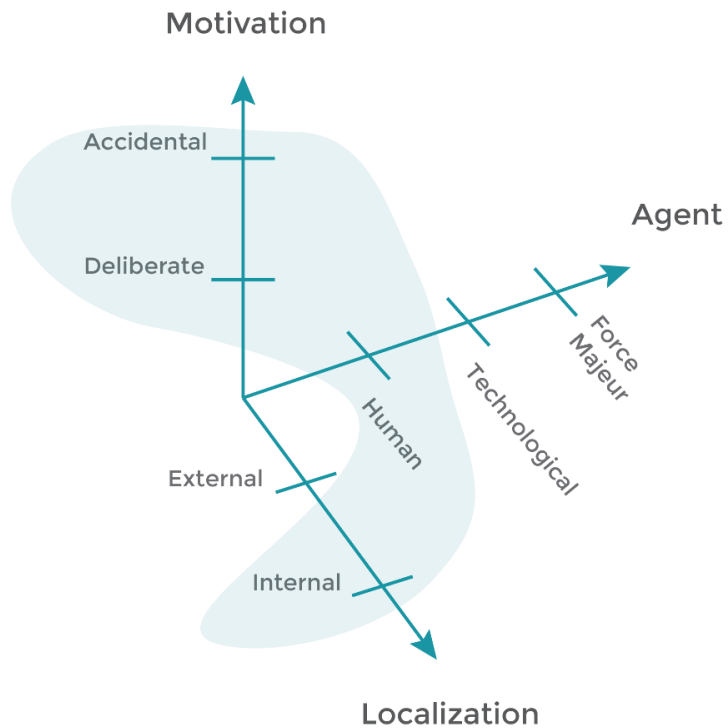
HFCR mitigation strategies

naive optimism “strategy” vs. control regime strategy?



→ trustworthy digital environment strategy!

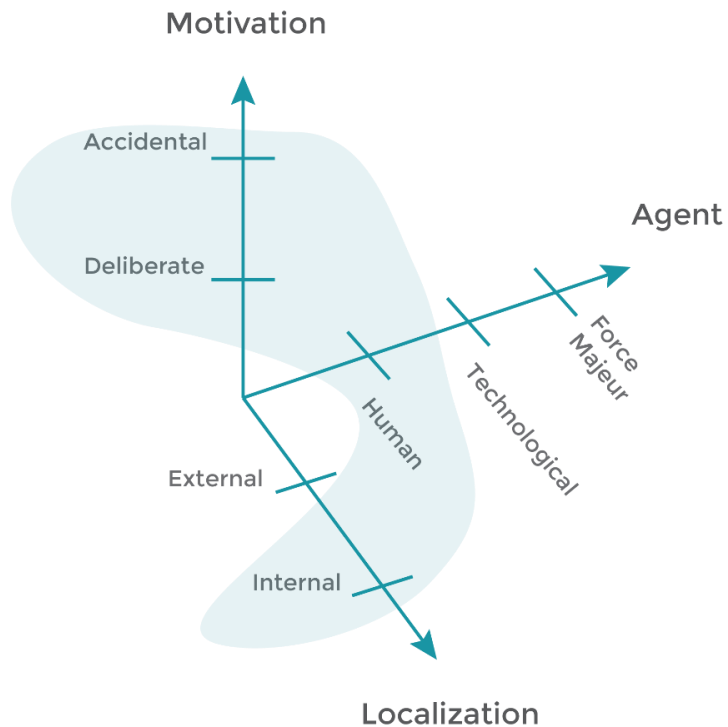
HFCR basics (organizational perspective)



Source: Mapping of human behaviour related threats and mitigation measures (I), SOTER D2.1

Figure 2. Threat Dimensions in the context of SOTER (adapted from Ruf et al. 2008, p.2) by Robin Renwick

HFCR basics (organizational perspective)



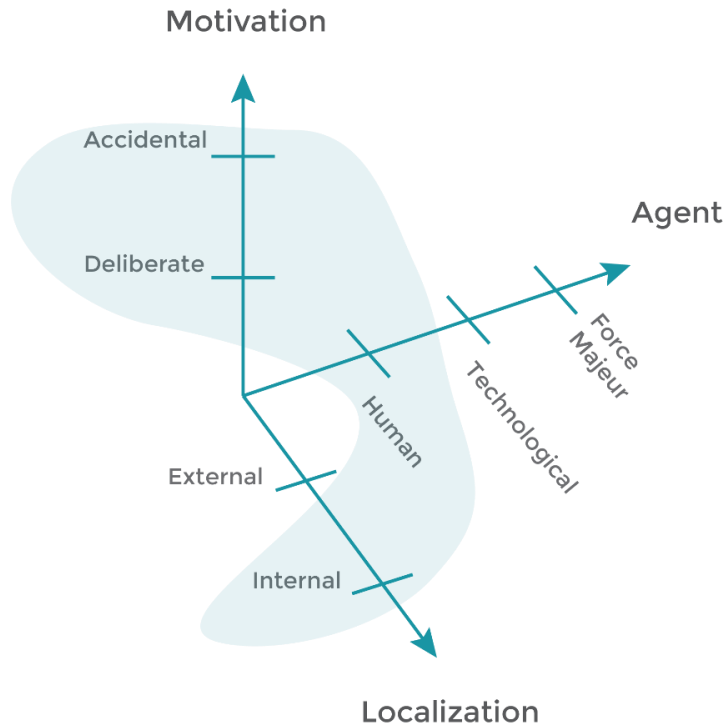
e.g.

- the incompetent employee
- the careless employee
- the stressed employee
- the disgruntled employee
- the greedy employee
- the compromised employee

Source: Mapping of human behaviour related threats and mitigation measures (I), SOTER D2.1

Figure 2. Threat Dimensions in the context of SOTER (adapted from Ruf et al. 2008, p.2) by Robin Renwick

HFCR basics (organizational perspective)



- e.g.
- the incompetent employee
 - the careless employee
 - the stressed employee
 - the disgruntled employee
 - the greedy employee
 - the compromised employee

SOTER HFCR Areas of Concern

1. Human error

- a. Lack of compliance
- b. Negligence
- c. Malpractice

2. Malicious insiders

Actions intended to harm the organisation

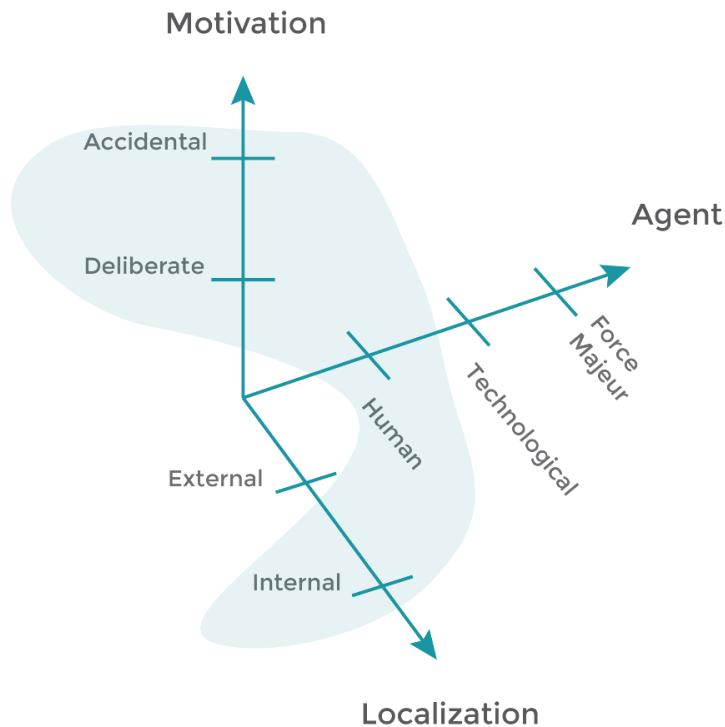
3. Legal & ethical threats

- a. Regulation (e.g. GDPR) related incidents
- b. Disinformation
- c. Public perception of organization

Source: Mapping of human behaviour related threats and mitigation measures (I), SOTER D2.1

Figure 2. Threat Dimensions in the context of SOTER (adapted from Ruf et al. 2008, p.2) by Robin Renwick

HFCR basics (organizational perspective)



| | |
|--|---|
| General | EBA guidelines |
| GDPR, NIS, eIDAS, NIST CS framework, ENISA | ICT and security risk management, on PSD 2, contingency preparedness (COVID-19), outsourcing arrangements |
| ISO/IEC 27000-family | |
| PSD 2 | Incident Reporting |
| MLD 5 | Regulation and Standards (e.g. from ECB, EBF ...) |
| (national regulation) | |
| e.g. in Spain, Austria, ... | organisational |

SOTER HFCR Areas of Concern

1. Human error

- a. Lack of compliance
- b. Negligence
- c. Malpractice

2. Malicious insiders

Actions intended to harm the organisation

3. Legal & ethical threats

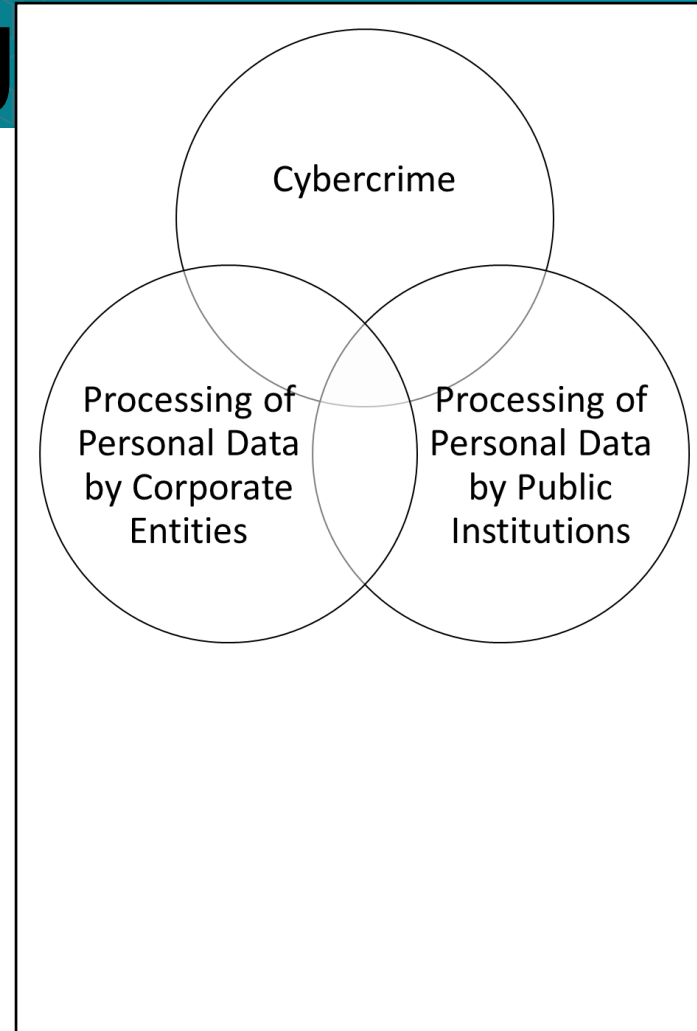
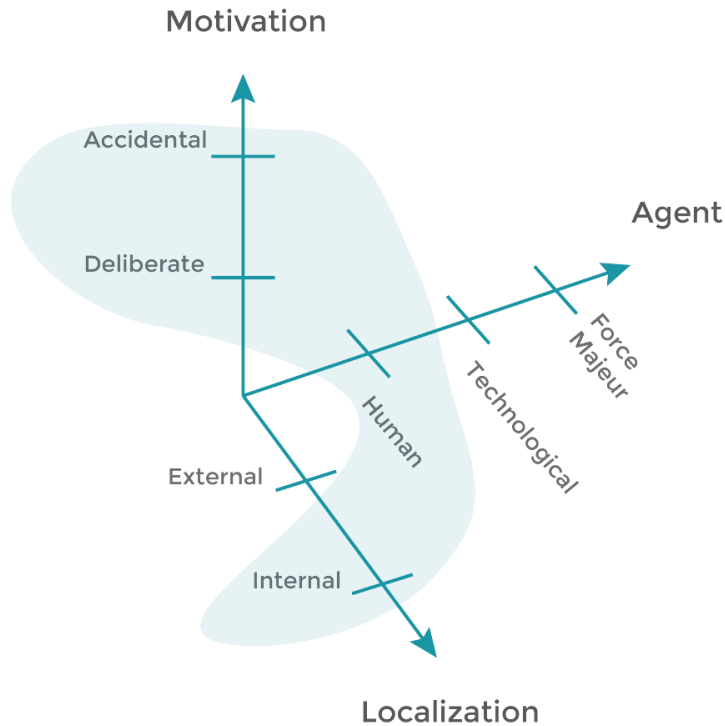
- a. Regulation (e.g. GDPR) related incidents
- b. Disinformation
- c. Public perception of organization

Source: Mapping of human behaviour related threats and mitigation measures (I), SOTER D2.1
Figure 2. Threat Dimensions in the context of SOTER (adapted from Ruf et al. 2008, p.2) by Robin Renwick

HFCCR basics

(org

erspective)



SOTER HFCCR Areas of Concern

1. Human error

- a. Lack of compliance
- b. Negligence
- c. Malpractice

2. Malicious insiders

Actions intended to harm the organisation

3. Legal & ethical threats

- a. Regulation (e.g. GDPR) related incidents
- b. Disinformation
- c. Public perception of organization

Source: Mapping of human behaviour related threats and mitigation measures (I), SOTER D2.1

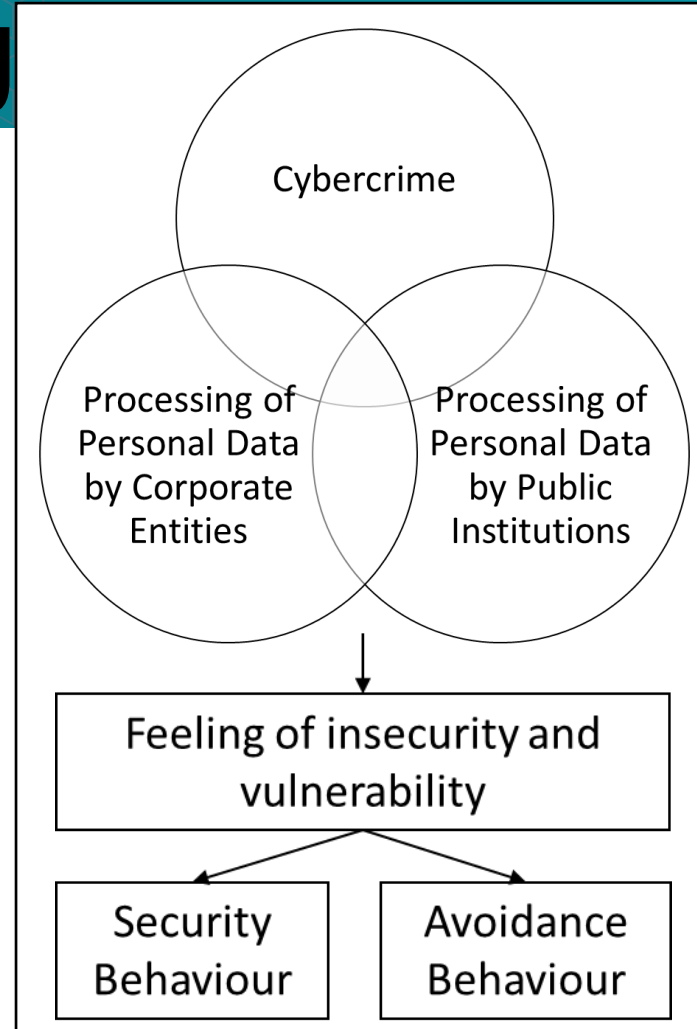
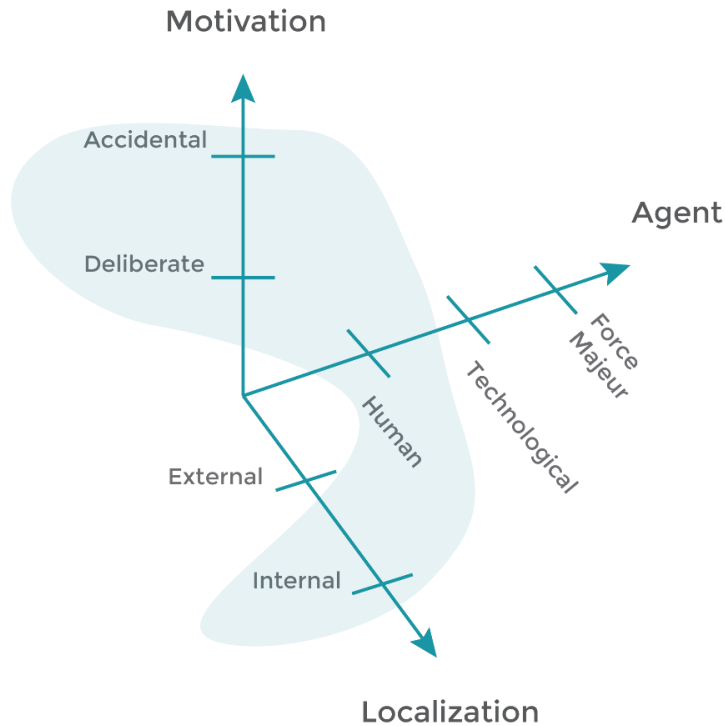
Figure 2. Threat Dimensions in the context of SOTER (adapted from Ruf et al. 2008, p.2) by Robin Renwick

Source: TRUESSEC.eu, D3.1 (EC H2020 CONTRACT: 731711)

HFCR basics

(org

erspective)



SOTER HFCR Areas of Concern

1. Human error

- a. Lack of compliance
- b. Negligence
- c. Malpractice

2. Malicious insiders

Actions intended to harm the organisation

3. Legal & ethical threats

- a. Regulation (e.g. GDPR) related incidents
- b. Disinformation
- c. Public perception of organization

Source: Mapping of human behaviour related threats and mitigation measures (I), SOTER D2.1

Figure 2. Threat Dimensions in the context of SOTER (adapted from Ruf et al. 2008, p.2) by Robin Renwick

Source: TRUESSEC.eu, D3.1 (EC H2020 CONTRACT: 731711)

ENISA Top Threats 2020-01 to 2020-06

1. Malware
2. Web-based attacks
- 3. Phishing**
4. Web application attacks
5. Spam
6. DDoS
7. Identity theft
8. Data breach
- 9. Insider threat**
10. Botnets
11. Physical manipulation, damage, theft and loss
- 12. Information leakage**
13. Ransomware
14. Cyberespionage
15. Cryptojacking

ENISA Attack vectors

- **Attack the human element**
- Web and browser based attack vectors
- Internet exposed assets
- Exploitation of vulnerabilities/misconfigurations and cryptographic/network/security protocol flaws
- Supply-chain attacks
- Network propagation/lateral movement
- Active network attacks
- Privilege or user credentials misuse/escalation
- Fileless or memory-based attacks
- **Misinformation/disinformation**

Common Attack Pattern Enumeration and Classification (CAPEC, selected)

- Parameter injection
- Pharming
- Phishing
- Fake the source of data
- Principal Spoof
- Establish rogue location
- Clickjacking
- Malicious software download/update
- Pretexting
- Influence Perception
- Target Influence via Framing
- Influence via Incentives
- Obstruction (Physical Security)

SOTER HFCR Areas of Concern

1. Human error

- a. Lack of compliance
- b. Negligence
- c. Malpractice

2. Malicious insiders

Actions intended to harm the organisation

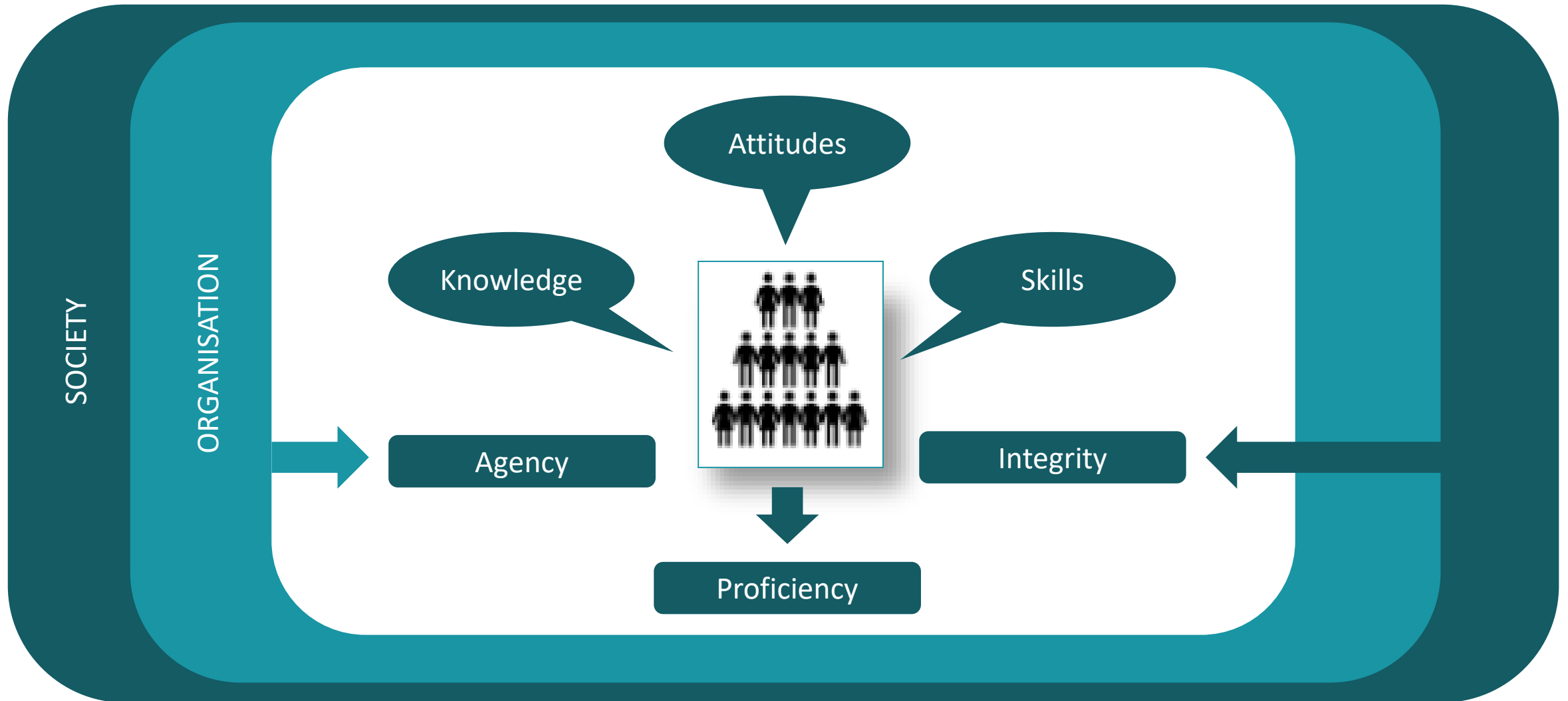
3. Legal & ethical threats

- a. Regulation (e.g. GDPR) related incidents
- b. Disinformation
- c. Public perception of organization

Sources:

ENISA threat taxonomy 2016, ENISA attack vector taxonomy 2016, ENISA List of top 15 threats 2020-01 to 2020-04; CAPEC (<https://capec.mitre.org>) , soterproject.eu

Mitigation through Competence Training



Mitigation through Competence Training

*Cybersecurity competence comprises the **capability, willingness, motivation and agency** of people to **solve cybersecurity problems individually or in cooperation with others** based on their **knowledge, skills and proficiency** in a form and way that organisational integrity as well as **physical, mental, material, social, ethical and legal integrity** of the individuals involved is **measurably** safeguarded.*

SOTER Cybersecurity Competence Catalogue

| | Cybersecurity Competences | | |
|--|---|---|---|
| Training Module A: Digital Information Competence | Confidential personal data/information handling | Responsible sharing of private information | Assessment of accuracy and integrity of information |
| | Confidential business data/information handling | Privacy settings for private digital devices and services | |
| Training Module B: Digital Safety Competence | Physical Safety | Network handling | Assurance of device safety |
| | Safe browsing | Safe digital communication | Creation of safe credentials |
| Training Module C: Threat/Anomaly Recognition | Social Engineering Recognition | Physical Environment Sensibility | Insider Threat Recognition |
| | Malware (Infection) Recognition | Identity Fraud recognition | |
| Training Module D: Incident Handling | Incident documentation | Incident communication | |
| | Incident reporting | Collaborative incident management | |
| | Identification of Cybersecurity Competence Gaps | | Problem-Solving Competence |

Mitigate Human Error Risk

Identify:

- What to train
- Who to train
- How to train

1.Human error

- a. Lack of compliance
- b. Negligence
- c. Malpractice



Training of employees

2.Malicious insiders

Actions intended to harm the organisation



Training on management level

3.Legal & ethical threats

- a. Regulation (e.g. GDPR) related incidents
- b. Disinformation
- c. Public perception of organization



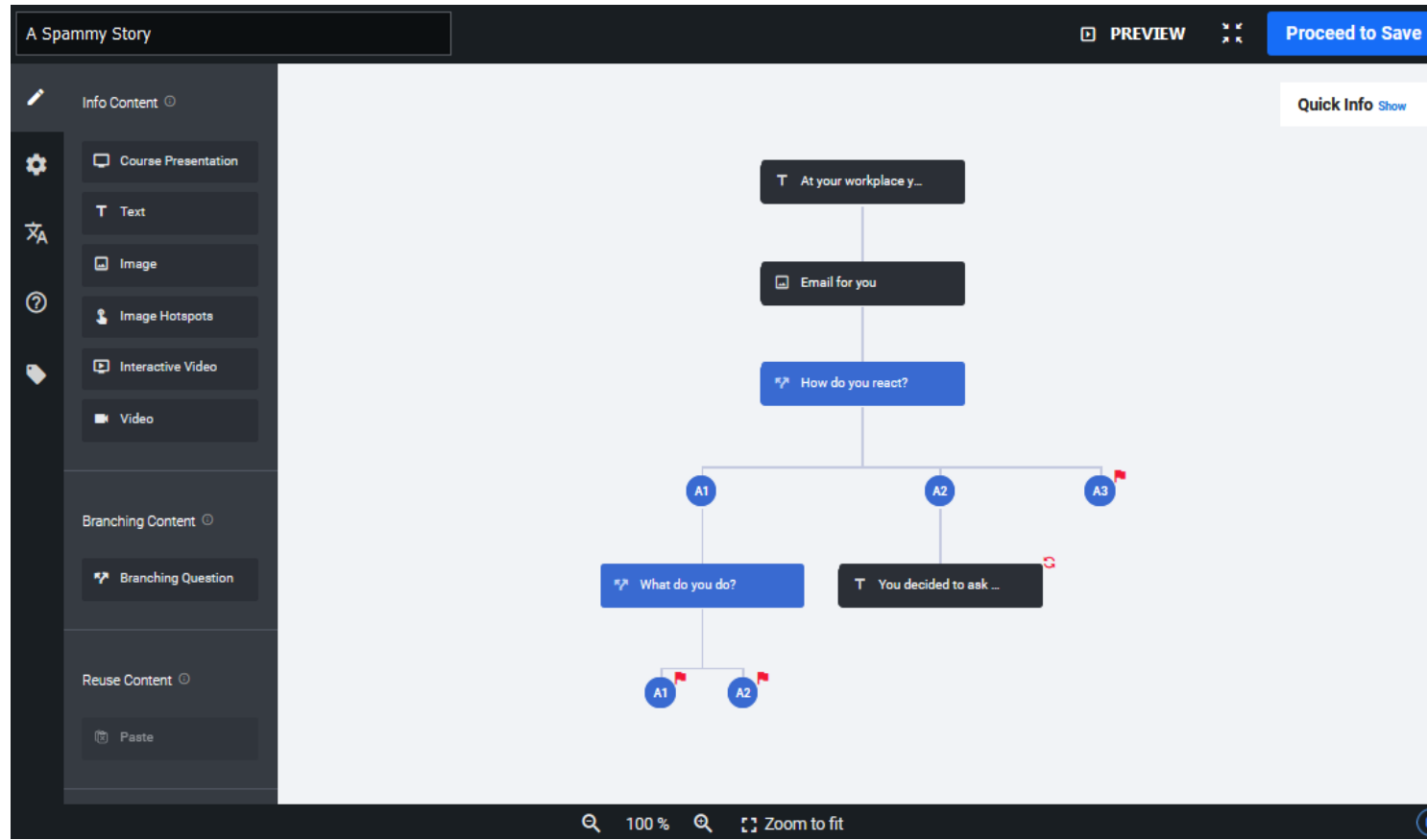
Training on management level

SOTER

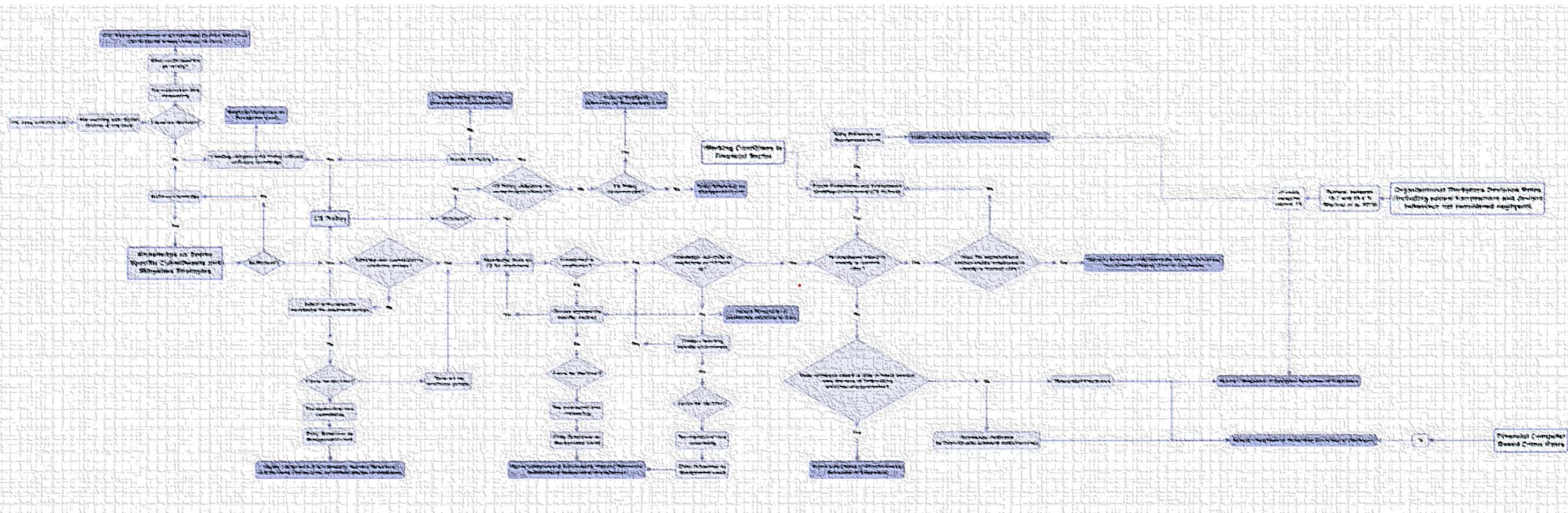
Cybersecurity Training Platform



H5P Branching Scenario Editor for CSCT Storyline Elements



The HFCR Mitigation Flowchart





an NTT DATA Company

Liberbank



TRILATERAL
RESEARCH



Aerospace
and Defense



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre



Questions?

eva.griesbacher@uni-graz.at
martin.griesbacher@rise-world.com



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923

