COMPACT

CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

Grant Agreement: No 740712
Project Acronym: COMPACT
Project Title: COmpetitive Methods to protect local Public Administration from Cyber security Threats
Thematic Priority: Secure societies – Protecting freedom and security of Europe and its citizens
Start Date: May 1st, 2017
Duration: 30 months
Total cost: EUR 4 283 480
EU contribution: EUR 3 648 792,50

www.compact-project.eu

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 740712

Psychological factors in Cybersecurity

Daniela Wurhofer,
AIT Austrian Institute of Technology GmbH

Human Factor as a Risk in Cybersecurity

- According to the European Cybersecurity Report (Survey on Cyber security in the 28 European Union countries), **only 47% of EU citizens feel well informed about the risks of cybercrime**. About 29% do not feel very well informed and 21% say they do not feel informed at all about the risks of cybercrime (European Commission, Directorate-General for Home Affairs, & TNS Opinion & Social, 2015).
- The human factor has been argued to be the "**weakest link in the security chain**" (Schneier, 2000; Sasse & Flechais, 2005).

- Challenge to train workers to behave cyber-secure aware within their working context and to investigate **risks in terms of the human factor** in the specific working context.

Reserach Questions

1. What are individual/psychological predictors of security-related behavior of employees?

2. How and to which extent do these human factors influence security-related behavior?

3. Why do people in one situation behave in a security-conscious manner and in another they do not? What are contextual factors that influence security-related behavior?

Human Factor as a Risk in Cybersecurity

- Human Factor Profiling tool: Survey instrument to investigate risks related to the human factor
  - Aim to meet psychometric quality criteria (objectivity, reliability, validity)
  - It can be used
    - … as a screening tool to assess risks
    - … as basis for choosing suitable awareness methods
    - … for evaluating the effect of awareness trainings

Risk Assessment in Compact – imagine two teams..

Team A: High Risk

People within this team do not follow password guidelines, they do not lock their PC etc. Although they know the security policies and procedures, they don‘t care about security issues, they have the feeling that nothing can happen to them.

Team B: Low Risk

People within this team are not aware about the internal security guidelines. They had no training so far. However, they are motivated to behave security-aware. They have the impression that their organisation is “attractive” for a cyber-attack.

How to deal with different human “risks”..

1. What do we expect from workers? What do we want to achieve → cyber-secure behaviour?
2. What are individual/psychological predictors of cyber-secure behaviour? How and to which extent do these human factors influence cyber-secure behaviour?
3. Why do people in one situation behave in a security-conscious manner and in another they do not? What are contextual factors (working conditions, organisational variables) that influence cyber-secure behaviour?

Worker‘s cyber-secure behavior: A conceptualisation

Security compliance comprises the core activities that should be carried out by employees to maintain security; more specifically, adhering to security guidelines and procedures defined by the respective organization.

Individuals with high security compliance…

- ✓ *… hold in mind the cybersecurity guidelines when they do their job.*
- ✓ *... adhere to the correct cybersecurity procedures for carrying out their job.*
- ✓ *… ensure the highest levels of cybersecurity when they carry out their job.*

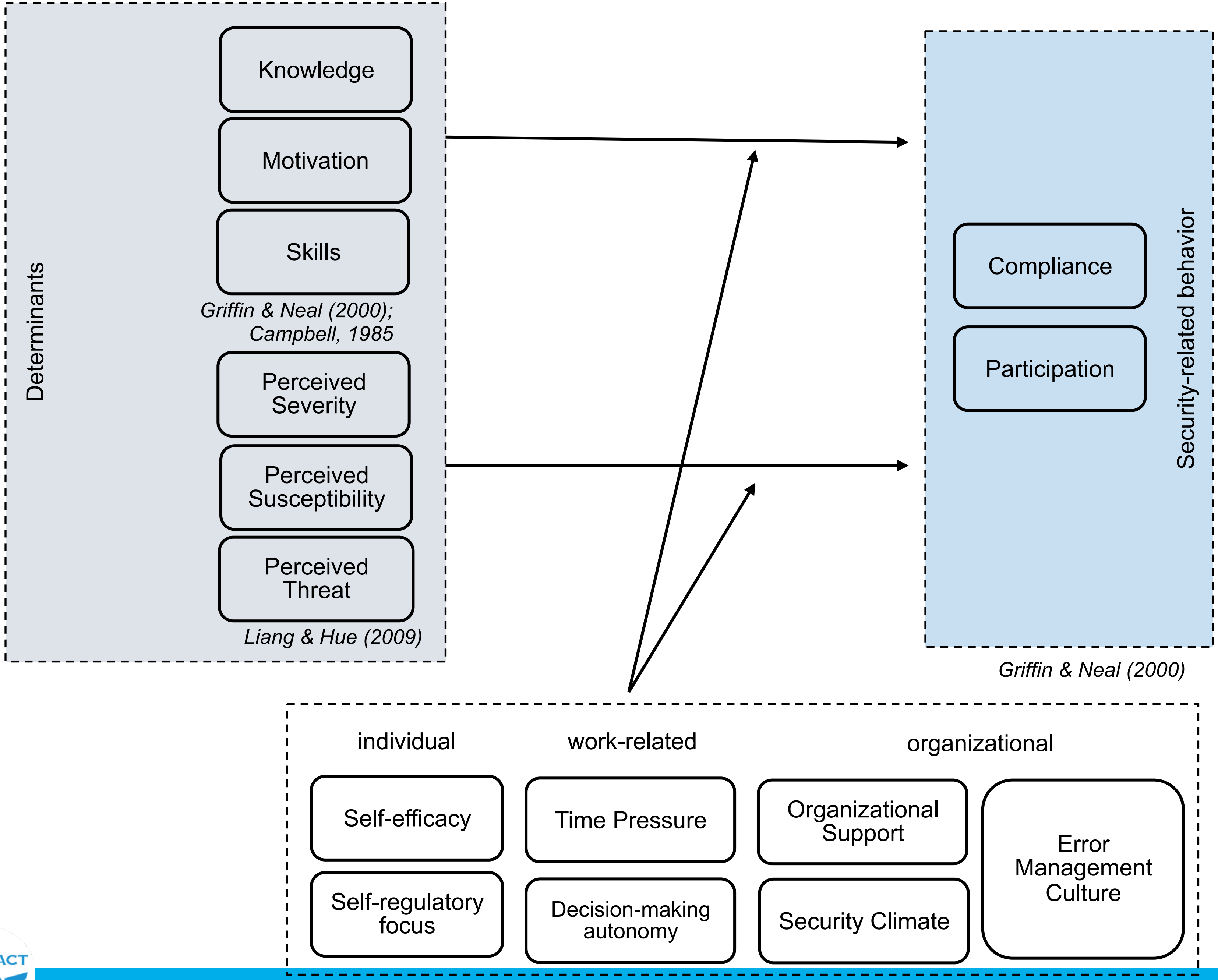
Security participation describes active participation of workers for voluntary security activities or also taking part at meetings with the topic cybersecurity. This behavior helps to develop organizational environment that supports security.

Individuals with high security participation…

- ✓ *… promote the cybersecurity guidelines within the organization.*
- ✓ *… put in extra effort to improve cybersecurity of the workplace.*
- ✓ *… voluntarily carry out tasks or activities that help to improve workplace cybersecurity.*

(adapted from Neal & Griffin, 2000)

Theoretical Research Framework as basis for Human-Factor Profiling



Individual Human Profiling Factors

Security Knowledge:

- Knowledge about security procedures and guidelines *(adapted from Griffin & Neal, 2000)*

Security Motivation:

- Idividual’s willingness to exert effort to enact security aware *(adapted from Griffin & Neal, 2000)*

Perceived Threat:

- Individual‘s perception that they are vulnerable and consequence of being attacked is serious *(Liang & Hue, 2009)*

Perceived Severity:

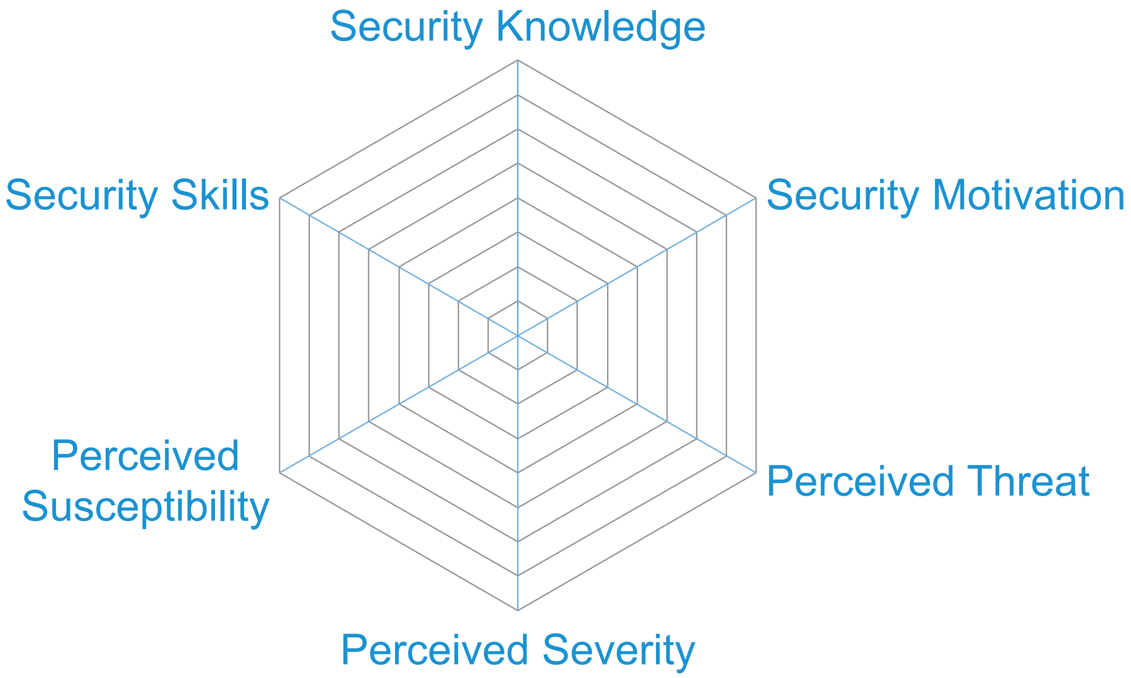
- Individual‘s perception that consequences of a cyber-attack are severe *(Liang & Hue, 2009)*

Perceived Susceptibility:

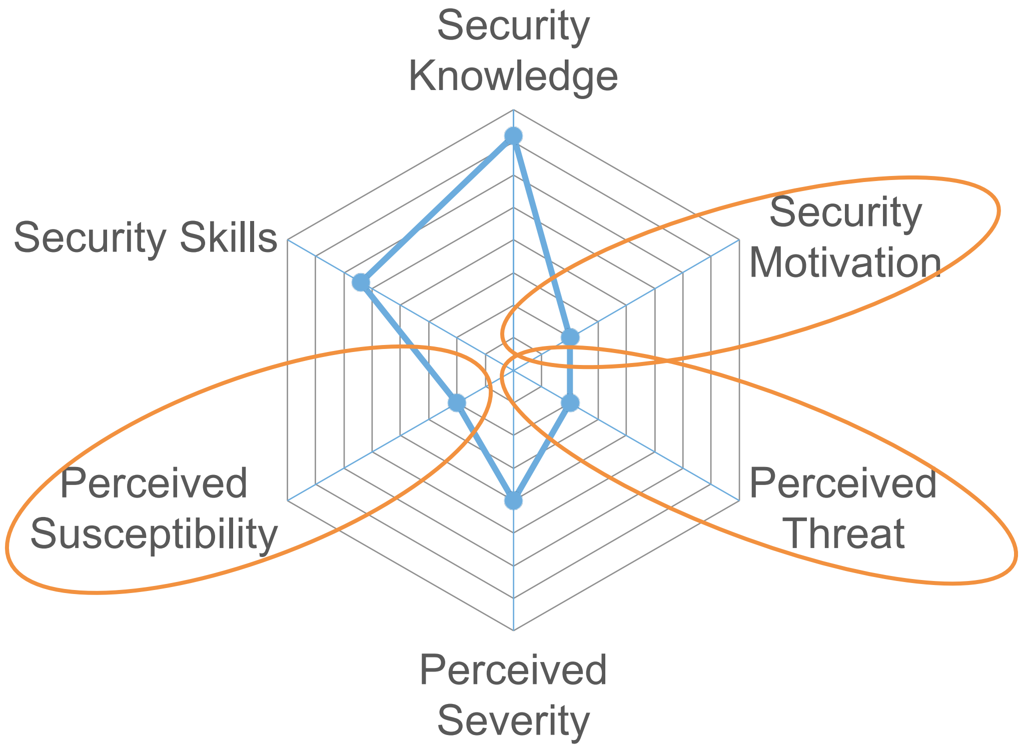
- Individual‘s perception that cyber-attacks will negatively affect him/her *(Liang & Hue, 2009)*

Security Skills:

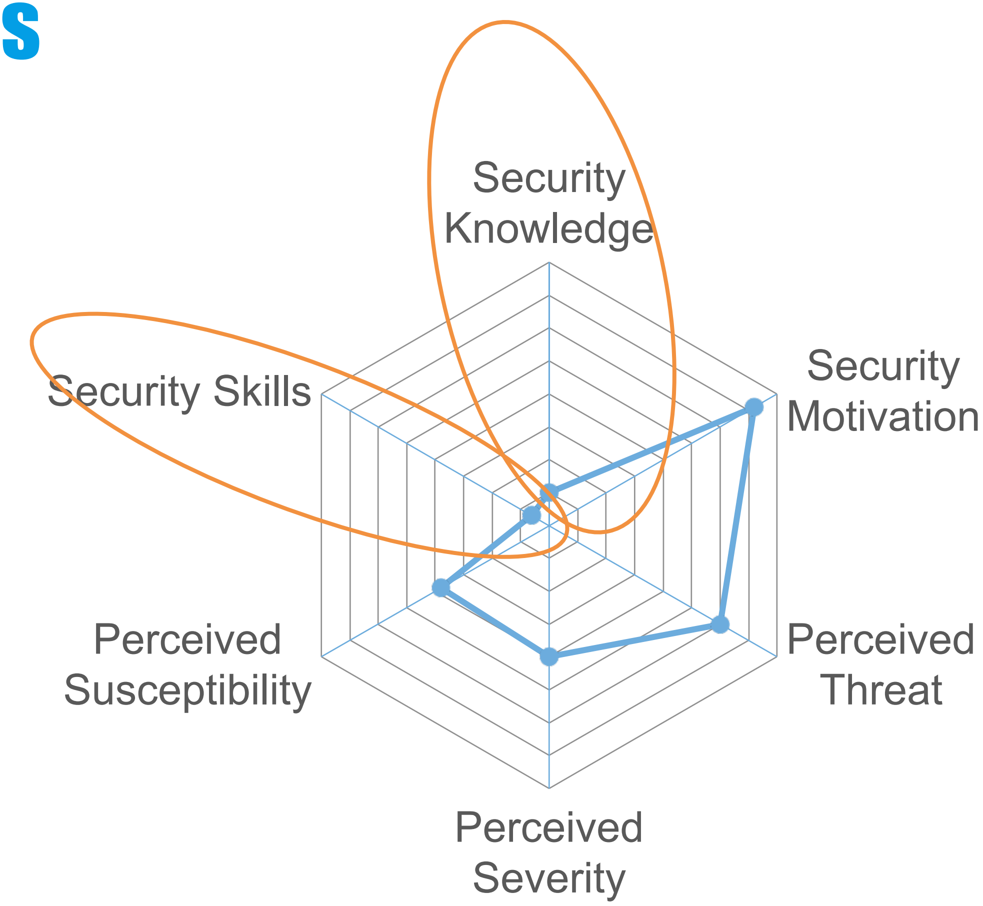
- Successful combination of declarative knowledge (knowing what to do) and procedural knowledge (knowing how to do it) *(adapted from Anderson, 1985; Kanfer & Ackerman, 1989)*



Individual Human Profiling Factors

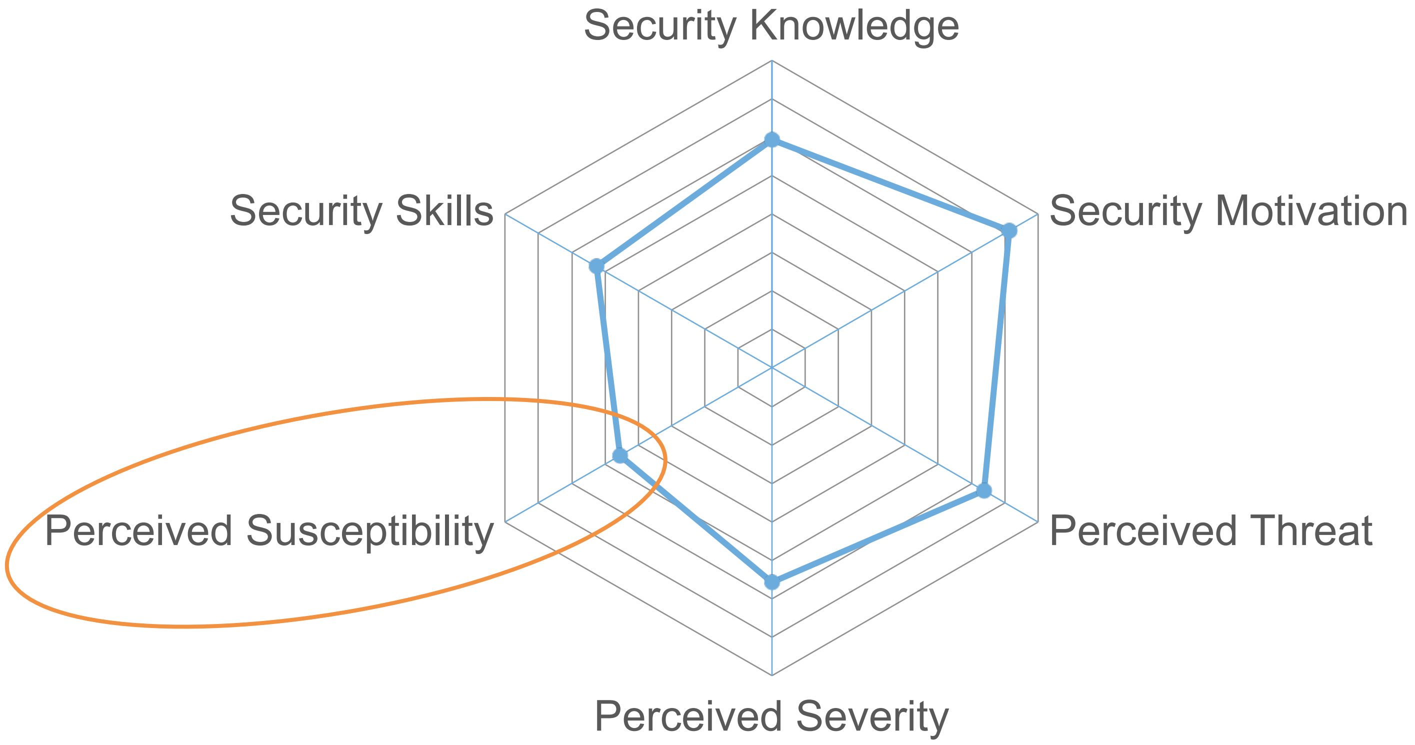


Team A



Team B

Individual Human Profiling Factor – Example from COMPACT



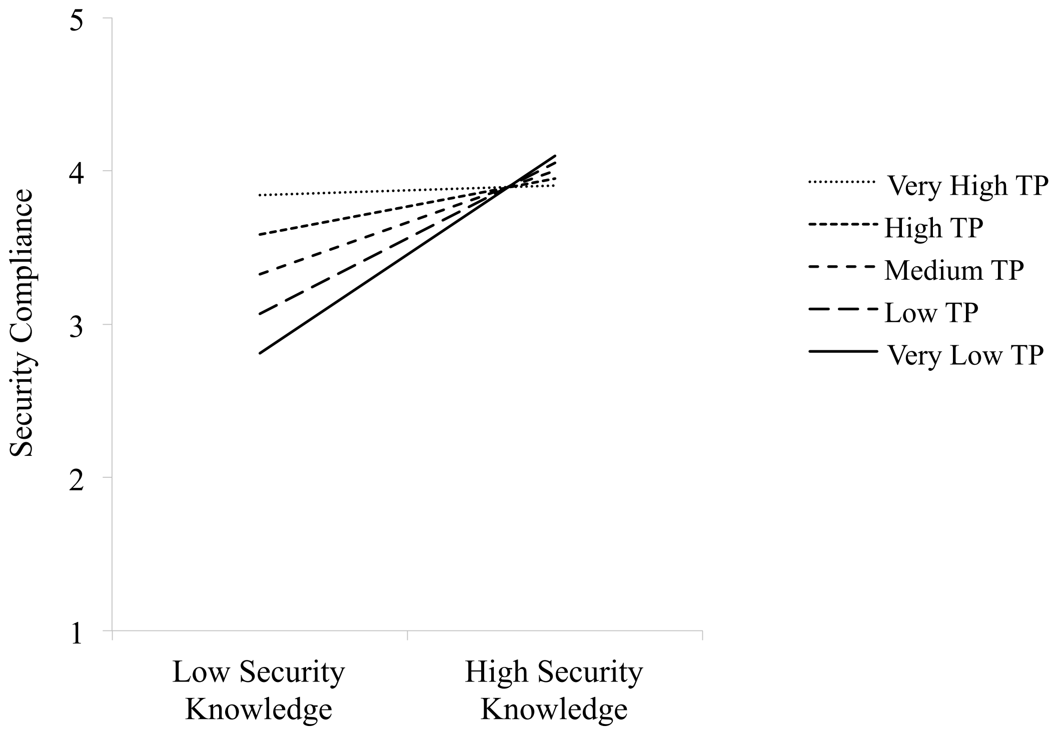
192 employees from one LPAs

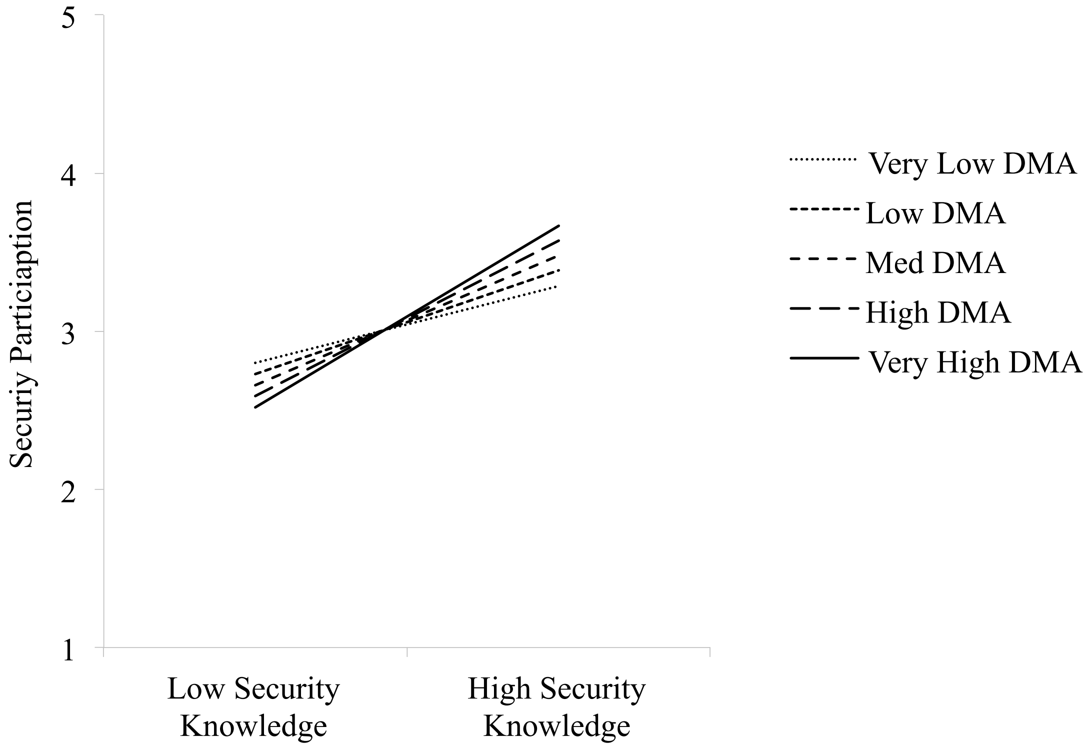
We go beyond individual human factors...

Why do people in one situation behave in a cyber-secure manner and not in another?

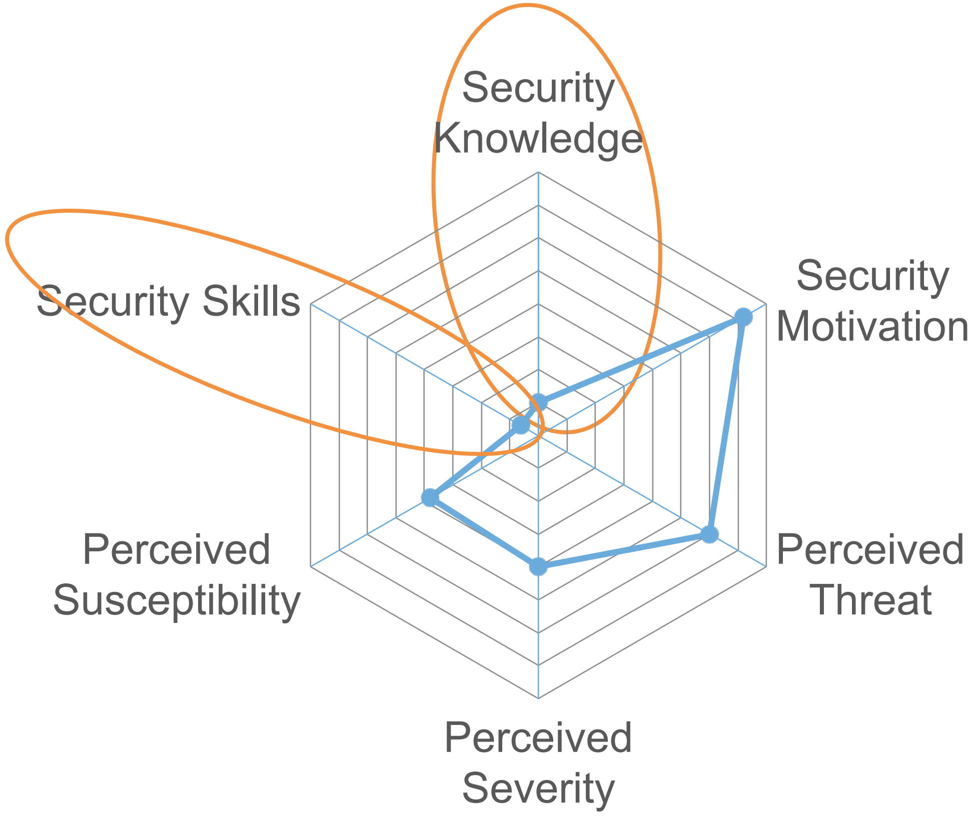
What are contextual factors (i.e., work-related, organizational) that support cyber-security behaviour?

Work-related variables:
Time Pressure and Decision-Making Autonomy





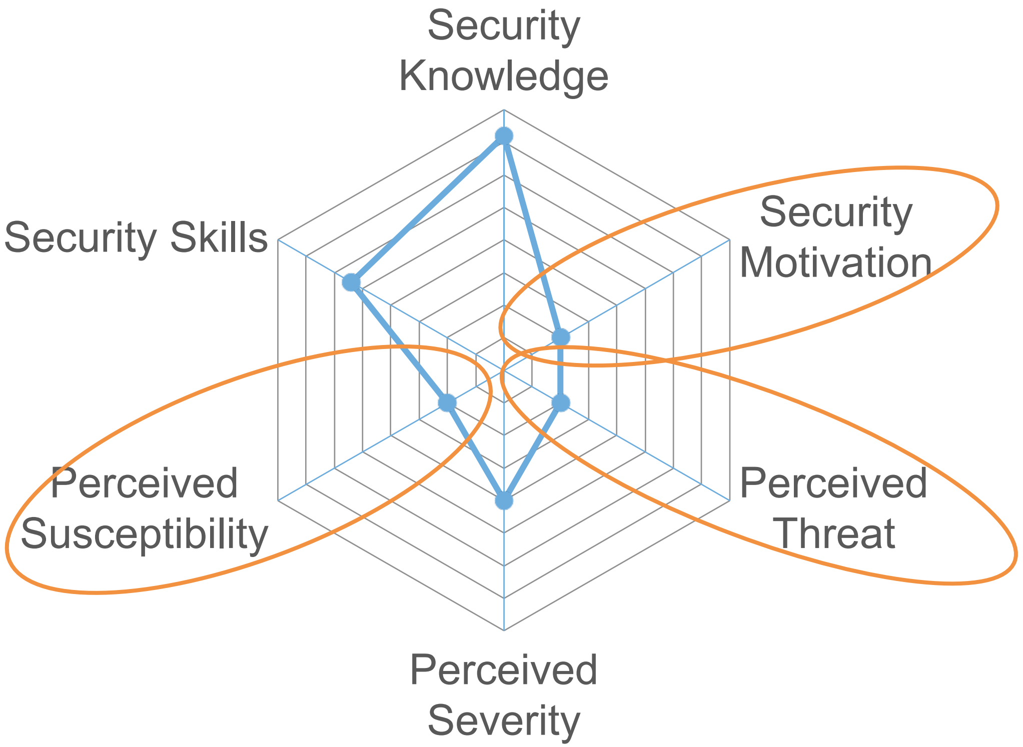
Individual Human Profiling Factors



Team B

- **Traditional training methods** that focus on training security knowledge (i.e., knowing the security policies and security procedures) and security skills
- Compact examples..
  - KIPS (detailled information in a next presentation)
  - *Investigators Diary* - Team Investigation for deepening knowledge (focus is transferring knowledge in the working context) –

Individual Human Profiling Factors



Team A

- Awareness Method that focus on understanding **consequences** of a cyber-attack, and convey the **importance** of security behavior
- Compact examples..
  - KIPS (detailed information in a next presentation)
  - CSMG (detailed information in a next presentation)
  - *Sectopia Browser-game* – allows employees to change perspectives as they get into the role of a supervisor who has to justify security policies

Human Factor Profiling – use it as …

- … as a **screening tool** to assess cybersecurity risks
- … as basis for **choosing suitable awareness methods**
- … for **evaluating the effect of awareness trainings**

COMPACT consortium partners 14 organisations from seven EU countries.

Austria | Germany | Italy | Portugal | Spain | United Kingdom

ENGINEERING

cini consorzio interuniversitario nazionale per l'informatica

inov inesc • inovação

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

KU LEUVEN

Wirtschaftsbetrieb der Stadt Bremerhaven BIT

S21 SEC Your Cybersecurity Company

silensec

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

KASPERSKY lab

Comune di Bologna

AMADORA Câmara Municipal

Donostiako Udala Ayuntamiento de San Sebastián

Comune di Afragola

Project Coordination:

Paolo Roccetti

Engineering Ingegneria Informatica spa

Via Riccardo Morandi, 32 - 00148 Roma

E-mail: paolo.roccetti@eng.it

Technical Coordination

Luigi Coppolino

Università degli Studi di Napoli «Parthenope»

Centro Direzionale di Napoli, Isola C4- 80121 Napoli

E-mail: luigi.coppolino@uniparthenope.it

Grant Agreement: No. 740712
Project Acronym: COMPACT
Project Title: COmpetitive Methods to protect local Public Administration from Cyber security Threats
Thematic Priority: Secure societies – Protecting freedom and security of Europe and its citizens
Start Date: May 1st, 2017
Duration: 30 months
Total cost: EUR 4 283 480
EU contribution: EUR 3 648 792,50

www.compact-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740712