European Security and Defence College
Doc: ESDC/2023/059
Date: 16 February 2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2025**	Activity number **278**	**Implementing Behavioural Science Perspectives for Improved Cybersecurity Awareness Education in Organisations**	ECTS **1**

Target audience

The participants should be mid-ranking to senior military or civilian officials dealing with information security and cybersecurity from EU Institutions, Bodies and Agencies as well as EU Member States and third countries.

Open to:

- EU Member States / EU Institutions Bodies and Agencies and third countries

Aim

The aim of the course is to provide up-to-date knowledge about behavioural science founded predictors of success of cybersecurity training of staff. This includes measures to increase motivation and commitment, time-economic possibilities to assess individual cyber risks, perspectives on the individualization of cybersecurity training measures and conditions under which sustainable effects can be achieved.

Furthermore, this course will allow the participants to exchange views, share best practices on cybersecurity awareness interventions by improving their knowledge, skills and competencies in this domain.

By the end of this course, the participants will be familiar with the concept of improved cybersecurity awareness education in organisations.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised course, at tactical/operational level.* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning Outcomes

Knowledge	LO1- Learn about emerging trends and major features of social engineering LO2- Learn about the psychological mechanisms underlying social engineering LO3- Learn about typical obstacles, challenges and limiting factors of awareness trainings LO4- Learn about scientific models providing guidance towards effective and efficient awareness interventions LO5- Learn about indicators and assessment tools needed for effect evaluations

Skills	LO6- Being able to critically evaluate and judge the quality of external consultancy offers on awareness interventions LO7- Identify critical elements contributing to sustainable training effects LO8- Assess observable and latent characteristics associated with cyber resilience LO9- Apply intervention mapping as educational technique for efficient interventions
Responsibility and Autonomy	LO10- Apply of a structured approach in planning, executing and evaluating interventions LO11- Create of a formal report assessing critical indicators of outcome effects LO12- Select the most accurate and appropriate information LO13- Understand and apply empirically validated scientific concepts related to sustainable intervention success

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participants' satisfaction with the course*) and *level 3 evaluation* (*assessment of participants' long-term change in behaviour after the end of the course*). *Evaluation feed-back* is given in the level 1 evaluation on the residential modules.

In order to complete the course, the participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *Certificates* to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the *final evaluation report, which* is presented to the Executive Academic Board.

Course structure

The residential module is held over 3 days.

Main Topic	**Suggested Working Hours (required for individual learning)**	**Suggested Contents**
1. Psychological mechanisms of social engineering	6(3)	• Current and emerging social engineering threats and scams • Cognitive exploits and resulting attack vectors • Vulnerabilities of IT-professionals
2. Assessing individual vulnerabilities	9(3)	• Applying reliable metrics • Behavioural and non-behavioural indicators • Explaining non-compliance with existing policies • Understanding side effects of technological hardening • Differentiation and role of skills, knowledge, intentions
3. Designing successful behavioural change interventions	9(3)	• Predictors of sustainability • Fostering commitment • Common challenges faced in awareness trainings • Indicators of sub-optimal and low-quality consultancy • offers • Individualizing training
4. Evaluating conducted trainings and judging external services	5(2)	• Evaluating effects of interventions • Choice of metrics and their interpretation • Conditions for an organisational cyber security culture

TOTAL	29(11)	

Material

Required:

- **AKU 106a: Adversarial Behaviour**
- **AKU 106b: The Landscape of Hybrid Threats**

Recommended:

- *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (**NIS 2**)*
- *EU Policy on Cyber Defence, JOIN(22) 49 final, 10.11.2022*
- *The EU's Cybersecurity Strategy for the Digital Decade (December 2020)*
- *The EU Cybersecurity Act (June 2019)*
- *The EU Cyber Diplomacy Toolbox (June 2017)*
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*
- *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)*

Methodology

The course is based on the following methodology: Presentations, Panels talks, Q&A and/or workshops

Additional information

The Chatham House Rule is applied during all residential modules of the HLC: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".

The mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September).