European Security and Defence College
Doc: ESDC/2023/162
Date: 23 May 2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Implementing Behavioural Science Perspectives for Improved Cybersecurity Awareness Education in Organisations**	ECTS
Feb. 2025	**278**		**2**

Target audience	Aim
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	The aim of the course is to provide up-to-date knowledge about behavioural science founded predictors of success of cybersecurity training of staff. It is designed to equip individuals with the necessary knowledge, skills, and competencies to effectively educate and raise awareness about cybersecurity within various educational settings. This comprehensive course combines theoretical concepts with practical exercises, enabling participants to become proficient cyber educators capable of delivering impactful cybersecurity training. Participants will understand the systematic approach, evidence-based design, audience focus, behaviour change principles, collaboration with stakeholders, evaluation and iteration, and sustainability aspects of intervention mapping for developing effective cybersecurity training programs. Educators may build engaging and personalised training experiences that effectively address the unique difficulties of cybersecurity education by employing these ideas.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber and on EU's Policy on Cyber Defence	• *Aligned with ECSF Role 7. Cybersecurity Educator* • *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- Attain knowledge of existing cybersecurity-related training resources LO2-Describe cybersecurity education and training standards, methodologies and frameworks LO3- Learn about the psychological mechanisms underlying social engineering LO4- Identify needs in cybersecurity awareness, training and education

Skills	LO5- Design, develop and deliver learning programmes to cover cybersecurity needs using intervention mapping approaches LO6- Identify critical elements contributing to sustainable training effects LO7- Develop cybersecurity exercises LO8- Develop evaluation programs for the awareness, training and education activities LO9- Develop strategies for monitoring, evaluating and reporting training effectiveness LO10- Create of a formal report assessing critical indicators of outcome effects LO11- Communicate, present and report to relevant stakeholders
Responsibility and Autonomy	LO12- Develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need LO13- Organise, design and deliver cybersecurity and data protection awareness-raising activities, seminars, courses, practical training LO14- 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 5 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
European Cybersecurity Frameworks	6(3)	Overview of Cybersecurity education frameworks and resources Understanding the principles of learning and behaviour change Overview of the role and responsibilities of a cyber educator Understanding the importance of cybersecurity awareness and education
Logic Model of the Problem	3	Perform an assessment of the cybersecurity problem, relevant behaviours, and the environmental variables surrounding the at-risk populations. This assessment has two major components: a scientific examination of the cybersecurity risks, behavioural patterns, and sociological aspects inside the at-risk group or community, and an attempt to become acquainted with the community, its people, and its strengths. This first stage yields a complete explanation of the cybersecurity

		problem, its consequences for quality of life, the behavioural and environmental variables that contribute to the problem, and the determinants that drive these behaviours and environmental causes. • Conduct a needs assessment to create a logic model of the problem • Describe the context for the intervention, including the population, setting, and community • State program goals
Program Outcomes and Objectives	8(3)	Create a foundation for the intervention by identifying the people and factors that will change as a result of the intervention. This process creates a series of matrices that encompass several ecological levels (ranging from individual to social) and integrate performance objectives for each level with selected personal and environmental elements. These matrices produce change objectives, which are the intervention's immediate targets. To broaden the scope of performance objectives beyond the individual, specific roles within each ecological level are identified. When compared to standard program goals and objectives, describing what needs to be changed at each ecological level and identifying the individuals accountable for effecting those changes provides more specific focal points for the intervention. • State expected outcomes for behavior and environment • Specify performance objectives for behavioral and environmental outcomes • Select determinants for behavioral and environmental outcomes • Construct matrices of change objectives • Create a logic model of change
Program Design	9(4)	Utilise theory-informed approaches and convert them into practical applications that bring about changes in the behaviour of individuals and small groups, as well as influence organisational and social factors to impact the overall environment. An intervention method refers to a well-defined process that combines theoretical postulates and empirical research to outline how changes can be achieved in the behaviour of individuals, groups, or social structures. While a method is a theory-based technique designed to influence behaviour or environmental conditions, an application refers to the organisation and implementation of these change methods into practical and actionable strategies. • Generate program themes, components, scope, and sequence • Choose theory- and evidence-based change methods • Select or design practical applications to deliver change methods
Program Production	4	Develop a description of the scope and sequencing of the intervention's components, finalised program materials, and program protocols. This step necessitates a thorough assessment of the intended program participants as well as the program context. This stage provides detailed instructions for communicating program intent to producers. • Refine program structure and organisation • Prepare plans for program materials • Draft messages, materials, and protocols • Pretest, refine, and produce materials
Program Implementation Plan	4	Adoption and implementation performance objectives are compared to internal and external determinants in matrices that are developed. A change objective is created to encourage

		program adoption and use by connecting each performance objective with a determinant. Then, in order to create theory-informed adoption and implementation plans, these objectives are operationalized using techniques and tactics. The end result of this step is a comprehensive plan for achieving program adoption and implementation by influencing the behaviour of people or groups who will decide whether to adopt and use the program. • Identify potential program users (adopters, implementers, and maintainers) • State outcomes and performance objectives for program use • Construct matrices of change objectives for program use • Design implementation interventions
Developing Evaluation	6 (3)	This step completes an evaluation plan started during requirements assessment and developed during Intervention Mapping. Intervention Mapping planners decide change goals, tactics, strategies, and execution. Theoretical and research-based decisions may not be ideal or correct. Effect and process evaluation lets planners evaluate their mapping decisions at each phase. Researchers examine changes in learning, behaviour, the environment, and performance targets to assess an intervention's impact. During the previous steps, these factors were specified and measured, making evaluation easier. • Develop indicators and measures for assessment • Specify the evaluation design
Designing Tabletops for Learning	8 (3)	The objectives of the table-top are to demonstrate general concepts in cybersecurity such as: • The process of discovering and managing security incidents • Common failure points in the security incident management process • The value of cooperation and sharing of information • The limitations of people, processes and technology • The importance of teamwork and clear role assignment • The intersection of information technology, media and law in cybersecurity
Future Trends, Collaboration, Networks	4	• Exploring advancements in technology and their implications for cybersecurity • Discussing the impact of artificial intelligence, Internet of Things (IoT), and cloud computing • Staying updated with current cybersecurity trends and emerging threats • Engaging with other cyber educators and professionals • Sharing best practices and resources
Judging external services	4	Applying the previously gained knowledge to judge the quality and potential deficits of commercially offered external consultancy: • Data-driven quality monitoring and improvement • Indicators of success and of sustainability • Concept and indicators of organizational security culture
TOTAL	**56 (16)**	

Material	Methodology
Required: ● *Renaud, K., & Warkentin, M. (2017, June). Using intervention mapping to breach the cyber-defense deficit. In 12th Annual Symposium on Information Security.* ● *Pirta-Dreimane, R., et al. (2022). Application of intervention mapping in cybersecurity education design. Frontiers in Education, 7, 1-12.* ● *European Cybersecurity Skills Framework Role Profiles* ● *European Cybersecurity Skills Framework (ECSF).* ● *European Cybersecurity Month (ECSM) Campaign Report, (2023). European Union Agency for Cybersecurity (ENISA), DOI 10.2824/36758* ● *Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.* ● *Ottis, R. (2014). Light weight table-top exercise for cybersecurity education. Journal of Homeland Security and Emergency Management, 11(4), 579-592.* **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 course is based on the following methodology: Presentations, group work, group presentations, 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).