frontiers | Frontiers in Education

TYPE Original Research
PUBLISHED 04 November 2022
DOI 10.3389/feduc.2022.998335

Check for updates

OPEN ACCESS

EDITED BY
Tom Crick,
Swansea University, United Kingdom

REVIEWED BY
Tom Prickett,
Northumbria University,
United Kingdom
James Harold Davenport,
University of Bath, United Kingdom

*CORRESPONDENCE
Ginta Majore
ginta.majore@va.lv
Ricardo Gregorio Lugo
ricardo.g.lugo@hiof.no

SPECIALTY SECTION
This article was submitted to Higher Education, a section of the journal Frontiers in Education

RECEIVED 19 July 2022
ACCEPTED 03 October 2022
PUBLISHED 04 November 2022

CITATION
Pirta-Dreimane R, Brilingaitė A, Majore G, Knox BJ, Lapin K, Parish K, Sütterlin S and Lugo RG (2022) Application of intervention mapping in cybersecurity education design. *Front. Educ.* 7:998335. doi: 10.3389/feduc.2022.998335

COPYRIGHT
© 2022 Pirta-Dreimane, Brilingaitė, Majore, Knox, Lapin, Parish, Sütterlin and Lugo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Application of intervention mapping in cybersecurity education design

Rūta Pirta-Dreimane[1], Agnė Brilingaitė[2], Ginta Majore[3]*, Benjamin James Knox[4,5], Kristina Lapin[2], Karen Parish[4], Stefan Sütterlin[5,6] and Ricardo Gregorio Lugo[4,5]*

[1]Information Technology Institute, Riga Technical University, Riga, Latvia, [2]Cybersecurity Laboratory, Institute of Computer Science, Vilnius University, Vilnius, Lithuania, [3]Sociotechnical Systems Engineering Institute, Vidzeme University of Applied Sciences, Valmiera, Latvia, [4]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjovik, Norway, [5]Faculty of Health, Welfare and Organisation, Østfold University College, Halden, Norway, [6]Faculty of Computer Science, Albstadt-Sigmaringen University, Sigmaringen, Germany

Education in Cybersecurity is considered one of the key challenges facing the modern digitized world. Several frameworks, e.g., developed by NIST or ENISA, have defined requirements for cybersecurity education but do not give recommendations for their development. Developing appropriate education offerings need to incorporate theory-based approaches that are evidence supported. Adopting the Intervention Mapping paradigm, we propose an educational framework incorporating validated theoretical and evidence-based approaches to cybersecurity education encompassing stakeholders' input, identified competency needs, and how to implement and evaluate learning outcomes. This paper presents a case study of how Intervention Mapping can be used to help design cybersecurity education, discuss challenges in educational and professional aspects of cybersecurity, and present an applied educational approach based on Intervention Mapping and its evaluation.

KEYWORDS

cybersecurity roles, cybersecurity education, competence modeling, scenario-based learning, personality traits, Intervention Mapping

1. Introduction

Advancing cybersecurity competence to match digital proliferation is essential for both professionals and everyday users. Developing a comprehensive education pathway can contribute to providing a secure cyber environment at multiple levels, ranging from individual to medium sized enterprises. This entails designing a cybersecurity education program where individual roles, responsibilities, and required domain skill-sets are incorporated to ensure competencies align with internationally recognized standards in the field.

Attending to vital education requirements of among others, Cyber and Information Security Managers, Data Protection Officers, Network Administrators, Security Architects, Security Implementers (e.g., developers, programmers), Executive Officers, and everyday users is what defines a cybersecurity posture within an organization. A continuous educational process should consider actors within and around these functional areas to ensure the integrity of the cybersecurity system through role hierarchies and across competence spectrums. According to Bratianu et al. (2020) *"a competence is a dynamic integration of knowledge, skills, and attitude capable of performing a generic task, in a given context, at a certain quality level."* Competence can, therefore, be understood as both internal prerequisites, such as knowledge, skills, traits, cognitive factors (i.e., beliefs, attitudes, self-efficacy, working memory, decision-making), and cognitive-affective factors (self-regulation, meta-cognition) and external prerequisites—Social context e.g., educational programs, specific scenarios, role being fulfilled, relationship dynamics. In developing a cybersecurity education ecosystem these component parts of competence development must be taken into consideration.

Cyber hygiene, system and information protection, and the human factor form the main concepts for future educational development. Today though, there exists a gap between what learners know about the 'cyber-world' and applying appropriate behaviors to maximize performance and avoid slips (habits and behaviors) and mistakes (mental model knowledge Thomson, 2019). More specifically, task requirements in cyber entail users have competencies that encapsulate domain specific knowledge and abilities, and human behavior understanding (self and others, Jøsok, 2020). This includes critical understanding of pre-dispositions and situational factors.

This paper proposes an education framework that incorporates roles, tasks, competencies, and desired behaviors within the domain of cyber. This is informed by the NIST NICE Framework (Newhouse et al., 2017; Wetzel, 2021) and Tuning project (García Olalla et al., 2008) recommendations for cybersecurity educational outcome requirements. This integrated competence approach provides the foundation to an approach for an education framework for cybersecurity capabilities development, in a more holistic way that integrates human and Information Technology (IT) skills. This approach emphasizes the boundaries of responsibility among the cybersecurity workforce, as each role raises different requirements for learning objectives. The proposed framework consists of processes and components that build a competence model, pre-requisites, dependencies among different model elements, and implementation. It also considers technological challenges ensuring in-person and online learning scenarios. To develop such an education ecosystem, based on the above conceptualization of competence development, we propose and present a six-step Intervention Mapping (IM) approach. A case study is then used to provide an example for assessment indicators, exemplify tasks/structures for learning scenarios, and illustrate the flexibility of the proposed methodology. This methodology could inform higher and continuous adult education to fill known gaps in existing cybersecurity education systems.

The rest of the paper is structured as follows. Section 2 covers the research methodology, including the background, design of the cybersecurity education ecosystem, and case study description. Section 3 presents the case study results, and Section 4 discusses the design and application challenges of the proposed framework. Section 5 concludes the paper and offers direction for future study.

2. Methods

First, this section introduces the Intervention Mapping approach. Afterward, it provides the background of educational frameworks and skill assessment. Then, the design of the educational ecosystem is presented, and a case study of its application is described.

2.1. Intervention mapping

Intervention Mapping (IM; Bartholomew Eldridge et al., 2016) is a protocol for building theory-based and evidence-based promotion initiatives and is characterized by three distinct aspects: 1) an ecological approach, 2) the participation of stakeholders, and 3) the application of theories and evidence. While IM has been developed for health promotion domains, it has also been adapted to other domains due to its applicability and efficiency for development and evaluation (Kok et al., 2011). IM uses a six-step process for planning program development (Bartholomew Eldridge et al., 2016):

1. Needs assessment based on the PRECEDE-PROCEED model (refer to Bartholomew Eldridge et al., 2016).
2. The identification and definition of performance and change objectives based on scientific analyses of problems and their causes.
3. The use of theory-based intervention methods and practical applications to change (determinants of) behavior.
4. The production of program components, design, and production.
5. The anticipation of program adoption, implementation, and sustainability.
6. The anticipation of process and effect evaluation.

Intervention Mapping is an iterative rather than linear process where the IM steps are revisited during the intervention development even though it is presented as a sequence of phases. The process is also cumulative where each phase builds on the

previous ones, and failure to pay attention to one step can lead to errors and poor decisions in program development. This ensures that IM planners are guided by theoretical models and empirical evidence in two areas: 1) identifying behavioral and environmental determinants related to a target problem, and 2) selecting the most appropriate theoretical methods and practical applications to address the identified determinants.

For cybersecurity educational development, the IM process described above can also be applied. Stage 1 of the IM requires to identify stakeholders, which for cybersecurity are the educational institutions and their staff and students, as well as public and private institutions that will employ future cybersecurity operators. Performance and change objectives in cybersecurity have been identified as common cybersecurity breaches that arise from human errors in both technical and non-technical personnel, and these breaches are well documented and can be used as training scenarios (stage 2). Positive cybersecurity behaviors have been identified but these need to be trained and incorporate evidence based approaches from other socio-technical domains (i.e., aviation, medicine; stage 3). This paper, with the description of the educational framework, also presents possible program components (refer to case study) that can be implemented and evaluated (stages 4–6).

While IM has been adopted in many other domains such as the health sector (Kok et al., 2016), energy consumption (Kok et al., 2011), and mental skills training in the armed forces (Mattie et al., 2020), IM has only been proposed as an approach to train and increase security awareness for small-medium enterprises (Renaud and Warkentin, 2017).

The following sections will describe the current educational approaches, cybersecurity roles, and job demand, and then propose an educational framework developed with the IM approach supported by a case study and its evaluation.

2.2. Cybersecurity education frameworks

Cybersecurity is a highly interdisciplinary field of study. Exploration of the educational methods applied across different fields associated with cybersecurity indicated the need to design a unified educational framework for cybersecurity.

While foundational learning is well understood (Bloom, 1985) socio-technical domains are more complex and thus require higher cognitive processes i.e., meta-cognition and self-regulation to learn more efficiently and be able to apply knowledge appropriately. Cybersecurity and other socio-technical domains have been shown to impose higher cognitive workload due to human-to-human and human-to-machine interaction (Ask et al., 2021). These cognitive load types, such as stress, working memory, and perceptual overload, impact students' learning abilities. Therefore, unnecessary distractions that hamper learning and knowledge transfer should be eliminated (Sweller et al., 2019). In science education, it is argued that the instructional model of argument-driven inquiry is integrated into the learning practice (Sengul et al., 2021).

A notable attempt at bridging the gap between cybersecurity education and industry expectations is the NICE Cybersecurity Workforce Framework (Newhouse et al., 2017). This framework identifies the Knowledge, Skills, and Abilities (KSAs) needed to perform cybersecurity work. Moreover, the framework formulates tasks that compose the work in a specific specialty area or role. The NICE framework Revision 1 links Tasks with specific Knowledge and Skills (TKS; Petersen et al., 2020). The revised framework provides a common lexicon and enables education and training programs to prepare professionals for TKSs and the competence required for specific cybersecurity roles. Tasks describe the work to be done, whereas Knowledge and Skill relate to the learner's abilities. By using their Knowledge and Skills during education or training, learners can complete tasks to achieve organizational objectives. Other competence definition in Tuning states that it combines cognitive and metacognitive skills (i.e., situational awareness), knowledge and understanding, interpersonal communication skills, intellectual and practical skills, and ethical values and they are developed in all course units and assessed at different stages of a programme (García Olalla et al., 2008).

Further efforts resulted in the development of the Cybersecurity Competency Model (Keeton et al., 2019). This model complements the NICE framework by including the competencies needed by the cybersecurity workforce and professionals (OPM, 2018). It defines competencies as the "capability of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position" (Keeton et al., 2019, p.2). The Cybersecurity Competency Model by the U.S. Department of Labor, Employment and Training Administration divides roles with responsibilities into general and technical competencies and defines different sets a grading criterion to cybersecurity positions (adapted from Keeton et al., 2019).

The model identifies two levels of positions: Senior level positions are graded above General Schedule 15th grade level (US payscale to determine the salaries of civilian government employees; GS-15 pay grade is generally reserved for top-level positions). The larger organizations with three level structures need further specification of the roles and responsibilities. Tiers 1–3 define foundational soft skill competencies needed for workplace functionality, while Tiers 4–5 define the required technical competencies. Tiers 4 and 5 are not individually oriented but represent the broader needs of cybersecurity where individuals can gain expertise based on their interests. The top tier is specific to specified occupations with the defined KSA's that are relevant for that position.

A UK case study on cybersecurity education demonstrates the positive effect of national accreditation and reveals specific

recommendation for curriculum developments (Crick et al., 2019).

Computing curricula 2020 highlights the importance of pragmatic student accomplishments and performance (Impagliazzo and Pears, 2018, p.45). Competencies therefore encapsulate both subject-specific (hard) and human-specific (soft) skills (Wetzel, 2021). Raj et al. (2022) specify soft skills in computing as professional dispositions that comprise abilities to demonstrate perspective, to show empathy, and to have self-awareness. Since computing competencies include not only cognitive aspects, Bloom's taxonomy is not sufficient to assess them. For assessing computing students' performance the hierarchy of competencies suggests including recognition, understanding, capability, conscious competence and proficiency (Bowers et al., 2019).

These frameworks describe the performance and change objectives, alongside the theoretical foundation and inform the development of scenarios that can assist behavior change identified in the IM stages 2 and 3. For an educational program to meet the learning outcomes defined by these frameworks, cybersecurity roles, behaviors, and evaluations of these roles and behaviors need to be implemented into current educational offerings.

The European Union Agency for Network and Information Security (ENISA) has also developed guidelines for cybersecurity education and training (European Union Agency for Cybersecurity, ENISA, 2022) but this framework is still under construction and validation (to be finished in Q4 2022). But ENISA has identified that social sciences need to be incorporated into cybersecurity education, where roles at all levels (i.e., CISO, cybersecurity managers, policy makers) and pertinent behaviors (i.e., attitudes, motivation, communications) are defined (ENISA, 2018). This is due to the accumulated research that shows that human aspects of behavior, such as attitudes, motivation, and communication, need to be addressed in training and education so that pro cybersecurity behaviors, such as compliance, in the general public can be adopted (ENISA, 2018). ENISA also points out that slips and errors need to be reduced among security professionals, and that the inclusion of social science approaches can help mitigate risky cybersecurity behaviors.

2.3. Cybersecurity education development and assessment

While the NIST and NISA frameworks identify specialty areas and roles for a cybersecurity workforce, the importance of which knowledge, skills, and abilities are important is not specified (Armstrong et al., 2018). Recent research has begun to identify how KSAs can be integrated into cybersecurity training. Jones et al. (2018) identified that KSAs related to technical aspects (i.e., networks, vulnerabilities, and programming) and behavioral aspects (i.e., interpersonal communication) should be prioritized and integrated in cybersecurity curricula. This was done by asking cybersecurity experts in different fields. Armstrong et al. (2018) interviewed specific roles, penetration testers, and found that more technical aspects (i.e., penetration testing principles and tools, and system robustness, are more important, while understanding social engineering techniques were not that important. However, the Armstrong et al. (2018) study used NICE KSA for Vulnerability Assessment and Management Jobs which has no defined soft skill markers. Also performing a search for the soft skill terms such as social engineering, communication, and psychology in the NIST framework provided only one hit (social engineering), therefore, the NIST framework is missing human behavioral aspects that have been identified as important.

The IEEE Software Engineering Body of Knowledge (SWEBOK) (Borque and Fairley, 2014) codifies key foundational knowledge on which a range of educational programs may be built. Similarly, the essential knowledge on cybersecurity is covered in the Cyber Security Body of Knowledge, CyBOK (Rashid et al., 2018). CyBOK identifies 19 knowledge areas that are grouped into five areas: 1) human, organizational, and regulatory aspects; 2) attacks and defenses; 3) systems security; 4) software and platform security; 5) infrastructure security. CyBOK is aimed to support the development of a wide spectrum of educational programs, including secondary, undergraduate, postgraduate, and continuing professional development. The Joint Task Force on Cybersecurity Education has developed a comprehensive undergraduate curricular guidance in cybersecurity to support the development of educational programs (Bishop et al., 2017). The guidance identifies six knowledge areas that are spanned into cross-cutting concepts. The discipline determines the depth and approach of each knowledge area, which is then delivered to various curricula. Finally, application areas define the competency levels needed for each knowledge area.

Based on the aspects described above, cybersecurity education faces challenges when attempting to make realistic assessments of learners' competencies. One way to mitigate such challenges is using scenario-based learning, where learning takes place in a context in which it is applied. The simulated real-life situations provide a relevant learning experience and allow for making mistakes without dangerous consequences (Pandey, 2019). This allows for a platform to test one's mastery levels, while at the same time providing role-models and directed feedback to help build self-efficacy (Bandura, 1986; Kiffer and Tchibozo, 2013). Scenarios that provide real world simulations of Red Team attacks, has been shown to have better learning outcomes (Cheung et al., 2011).

Similarly, challenge-based learning encourages students to use their knowledge and technology to solve real-world problems (Cheung et al., 2011). Besides realistic scenarios,

this approach involves competitions between attackers and defenders that involve students and has been shown to give better learning results (Cheung et al., 2011). Such scenario-based approaches have also been shown to be effective also for assessing competency development (Maennel et al., 2017; Ghosh and Francia, 2021). Such active learning techniques have been incorporated into cybersecurity education (Knox et al., 2019). For example, collaborative and inquiry-based strategies incorporated into hands-on activities aim to maximize the impact of learning and engagement education (Konak, 2018). Transformational (aka serious) games encourage cybersecurity behavior change by translating self-efficacy theory into the game's design (Konak, 2018). Active team-based learning demonstrates higher self-efficacy in gaining cybersecurity knowledge, skills, and abilities (Chong, 2019). A professional cyber operator is required to possess role-specific competencies to perform specified tasks as described by the NICE Framework (Newhouse et al., 2017). Existing cybersecurity education frameworks mainly focus on subject-specific skills, for example, technical or administrative competencies. But the more general human-skills are also essential for effective task execution, as they characterize how relationships in the social environment affect outcomes since behaviors and personality characteristics are factors that can enhance or degrade performance (Ward et al., 2019).

Despite the various offerings of cybersecurity educational frameworks, the increasing number of successful cyber-attacks raises questions about their effectiveness (Chowdhury et al., 2022). Development of cybersecurity educational frameworks that incorporate behavior change paradigms, i.e., IM, should be based on theoretical foundations that also incorporate learning styles, cognitive abilities, and meta-cognitive development of individuals. This approach would allow for more tailored training orientated to the needs of various individuals and groups of employees.

2.4. Design of the cybersecurity educational ecosystem

Brilingaitė et al. (2020) propose a hybrid cyber defense exercise framework that aids the development and assessment of cybersecurity competences. This framework aims at optimizing exercises to the various skill levels of the trainees. In addition, it supports cyber defense exercises for groups with different roles that require various competences, including non-technical roles and/or functions. ACM Computer Science Curriculum (ACM/IEEE, 2020) among other programs also includes undergraduate programs in cybersecurity. This report states that cybersecurity involves a broad spectrum of jobs from technical, such as network defense, to managerial (e.g., policy compliance) positions. It stresses that every graduate of a cybersecurity program requires both technical skills and a managerial understanding of the organizational actions needed to ensure system-level security. Based on the recommended approaches, the model in Figure 1 presents an education ecosystem. The proposed ecosystem considers requirements for competencies and behaviors that an individual should have to fulfill a particular role and perform tasks in a specific way given a situation.

As presented in Figure 1, the trainee carries out tasks and demonstrates behavior during the task execution. Success of the task is measured by the result quality. But the trainee plays a particular role during the scenario while executing the task. Therefore, various indicators are required to assess the competence demonstrated and encapsulated by the role description. The predefined conditions and context impact and support the scenario to simulate certain circumstances for the trainee.

Therefore, holistic approaches must incorporate internal and external determinants for a trainee in the cybersecurity educational ecosystem. Internal determinants can be identified as knowledge, skills, and cognitive factors (i.e., self-efficacy, meta-cognition, and decision-making) while external determinants are comprised of specific scenarios, roles, and relationship dynamics. The cybersecurity education framework presented here is a holistic approach that can facilitate the planning and implementation of cybersecurity courses by using the six-step Intervention Mapping process (Fernandez et al., 2019). This will be presented through a case study presentation and analysis.

2.5. Case study for methodology evaluation and triangulation

Using case studies to inform research can give insights that may be difficult to achieve with other approaches (i.e., quantitative measures) and can become the foundation of future experiments. Case studies can also establish the 'how' and the 'why' observed variables happen, especially when factors cannot be manipulated (Rowley, 2002). Case studies can be defined as a thorough analysis of a specific case (or cases) in a real-world setting. While there are difficulties in generalizing findings from case studies since they can be context specific, case studies can offer detailed descriptions and explanations of happening phenomena. This is due to case studies being empirical investigations into a current phenomenon in its real-life environment, especially when the distinction between phenomenon and context is blurred (Kohlbacher, 2006). It also deals with the technically unique problem of having far more variables of interest than data points, but also draws on a variety of sources of evidence, including data that must converge in a triangulating manner

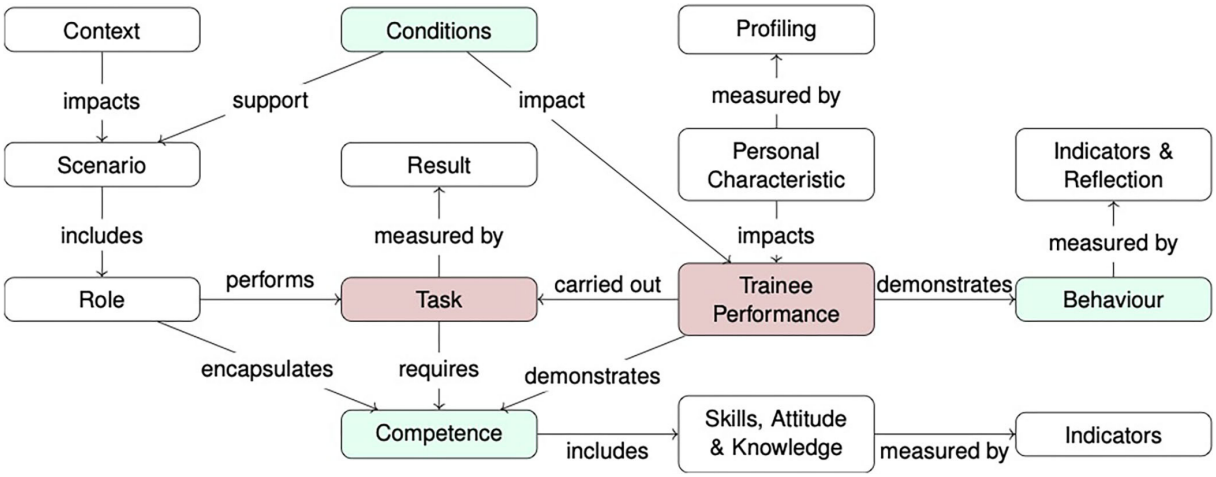

FIGURE 1
The trainee competence model within the cybersecurity education ecosystem reflects the close-to-real environment of the cybersecurity workforce.

leading to the creation of theoretical propositions to guide data collection and analysis (Rowley, 2002; Kohlbacher, 2006; Yin, 2013).

The proposed cybersecurity education development approach is presented as a case study. This case illustrates the implementation of the suggested approach to the Continuing Professional Development (CPD) course on information security hosted by the technical university in Latvia. Table 1 presents the key features of the course and it is delivered as part of the Latvian government's initiative to develop and improve citizens' digital skills. The course covers information security and cybersecurity aspects and aims to develop skills in analog and digital data risk mitigation and ITC assets protection. The course contains knowledge areas and knowledge units that are applicable to information security and cybersecurity. The course is designed based on the personnel needs and skill gaps identified by industry enterprises and associations and is digitally delivered with different interactive digital elements–information security tools, digital teams collaboration environment, and technical exercises. The course covers information security governance topics and includes the beginner-level technical exercises in the virtual environment.

The advantage of adopting this six-step IM protocol for course development is that it provides practical guidance on how to effectively plan and implement a course for cybersecurity competence development, identify needs and required behaviors, and helps in evaluating the efficiency of the course (Fernandez et al., 2019). The course includes several training scenarios and topics. The case study focused on competence "ability to perform IT change risk assessment" is presented in Figure 2.

The example scenario (refer to Figure 2 for dependencies among scenario prerequisites) is implementing a new information system in the enterprise. The scenario context includes technical requirements (software-as-a-service (SaaS), deployment in Cloud) and legal aspects (deployment outside of the EU). The scenario refers to a complex process, but the example considers the role of the cybersecurity risk manager. This role must perform an 'IT change risk assessment' as a task. The task result is a report that must be submitted in full or in parts, but on time. Consequently, time pressure is an additional condition that increases stress and could lead to intuitive behaviors. One of the competences required for the task is IT security risk assessment. Therefore, the 'trainee' would have to demonstrate abilities to make reasoned decisions and be critical and self-critical in the educational process. Of course, knowledge of IT risk assessment processes is mandatory for the task. The 'evaluator' would be able to observe the performance indicators *via* submitted parts of the report as a test with stated justifications, comparisons, and quality of risk assessment. The architect who designs the educational pathway could add specific pedagogical interventions that encourage meta-cognitive skill development (Knox et al., 2019). These can be embedded within the existing task to ensure task related efficacy improvement. Incorporating meta-cognitive aspects in learning can help students understand how one's behavior and predispositions can make them vulnerable or resilient in risk-taking decisions. This would then lead to better learning and increasing self-efficacy.

TABLE 1 CPD course characteristics card.

Course title	Information security and personal data protection
Course type	CPD course, 7th EQF level
Course amount	160 academic hours
Course goal and tasks	To provide knowledge and skills about information security and personal data protection to ensure the company's business continuity and achievement of business goals. The tasks of the course are: (1) To create an understanding of the main concepts of information security. (2) To develop information classification skills (in a IT security context). (3) To develop the skills of identifying information security threats and vulnerabilities. (4) To develop IT risk analysis skills. (5) To develop business continuity planning skills. (6) To create an understanding of information security management methodologies. (7) To develop skills in defining and implementing IT controls to ensure information security. (8) To create an understanding of the main concepts of personal data protection and regulations and guidelines. (9) To develop the skills of defining and implementing the necessary measures for personal data protection in the company's IT control environment.
Learning outcomes	(1) Understands the key concepts of information security and personal data protection. (2) Able to classify information. (3) Able to identify information security threats, vulnerabilities and develop proposals to mitigate them. (4) Able to analyse IT risks - be able to identify and assess the risks of IT resources and the risks of third parties. (5) Able to plan business continuity, perform business impact analysis and plan IT resources recovery. (6) Understands information security and personal data protection management methodologies, regulations and applicable standards (ISO 27000 group, etc.). (7) Able to define and implement the main necessary measures for the protection of personal data in the company's IT control environment.
Prerequisites	Older than 25 years; employed; at least Bachelor Degree
Students amount	20–25 per course
Student profile	Diverse students; different educational background and skill portfolio
Typical roles (focus)	Data protection officer; mid-level IT specialist and IT manager; IT auditor
Implementation and tools	Online; information security tools; online collaboration environment; technical exercises

3. Results

IM step 1: Needs assessment (Phase 1)

Step 1 of the IM (PRECEDE: Predisposing, Reinforcing and Enabling Constructs in Educational Diagnosis) includes stakeholder inclusion through social assessment. Before the course, each student requested to answer several questions including expectations, needs, and topics of interest. Also, 3 years of feedback on prior courses were analyzed to distinguish the principal aspects for improvement. The main subject-specific topics of interest highlighted by students were IT aspects in personal data protection, IT risk management, best practices in information security governance, and information security tools. Topics like IT security risk management and assessment of personal data processing were added as subject-specific topics.

Taking into consideration targeted work roles from the NIST NICE framework (Newhouse et al., 2017)–Security Control Assessor, Privacy Officer, and Information Security Manager, student topics of interest were mapped to existing cybersecurity competency models and curricula (Newhouse et al., 2017; ACM/IEEE, 2020), industry enterprises' requirements, and expert recommendations (interviews). Required general competences were selected from the Tuning competence model (García Olalla et al., 2008) based on IT industry and education experts (Hibbs Pherson, 2017; Scholl, 2020; Fund, 2021) and related research (Huang and Pearlson, 2019; Hajny et al., 2021) recommendations about key general competences for cybersecurity professionals such as increasing self-efficacy, critical thinking, communication, and collaboration. Based on these analyses, outcome measures for the course were then identified as knowledge and skills relating to information

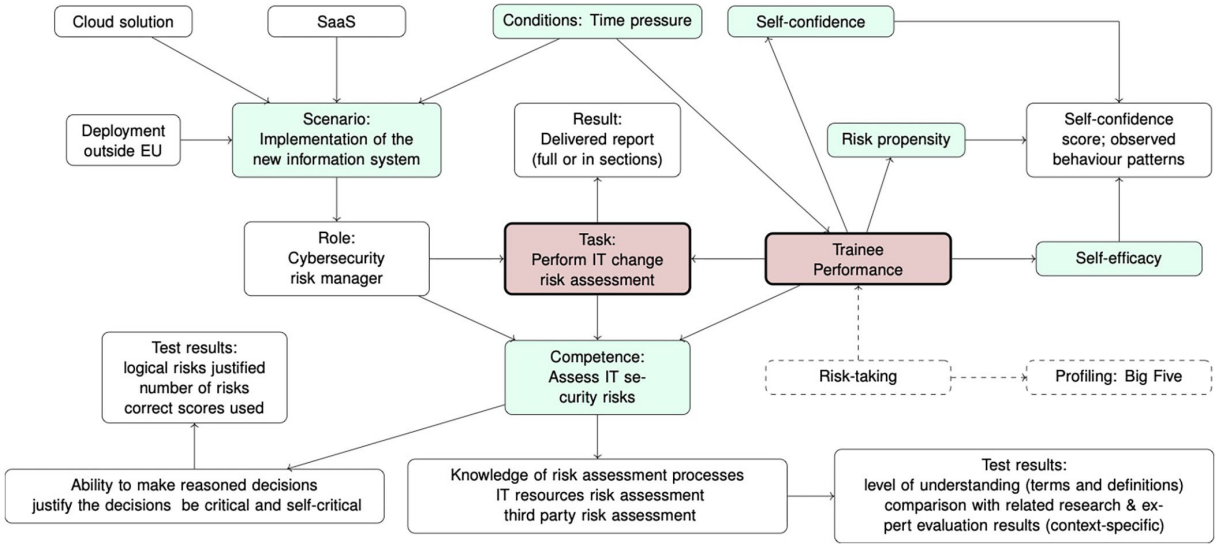

FIGURE 2
Illustration of how the model can be applied to develop the competence of risk assessment.

security and personal data protection. Besides subject-specific and general competences, key targeted behavior and characteristics were identified, based on related research (Kennison and Chan-Tin, 2020).

Expected changes for this course were to develop knowledge and skills for improved cybersecurity behaviors (self-efficacy, decision-making, and reduced risk propensity) through scenario-based learning on cybersecurity risk management in an organization regarding IT changes.

IM step 2: The identification and definition of performance and change objectives (Phase 2)

Maladaptive cybersecurity behaviors (i.e., impulsive clicking) have been identified as a major threat to both individual and organizational security (Canham et al., 2022). Therefore, the course focused on improving cognitive and behavioral factors such as self-efficacy, repeat clicking, and critical thinking in risk assessment to encourage learning. Maladaptive behaviors directly affect cybersecurity behaviors described in the tasks and learning outcomes presented in Table 1. But individual behaviors can only account for some of the explanation of cybersecurity breaches. Therefore, the course also informs about more systemic and organizational factors, i.e., third party risk assessment and European Union and Latvian security personal data regulations, and they were incorporated into the course to support the scenario (refer to WPENISA and NIST standards from Newhouse et al., 2017; Wetzel, 2021)—identify, protect, detect, respond, recover) to help identify problem behaviors around phishing susceptibility (i.e., predispositions, social engineering, and organizational commitment). Integration of the technical material supports development of cybersecurity skills and illustrates resilience strategies against social engineering attacks.

IM step 3: The use of theory-based intervention methods and practical applications to change (determinants of) behavior (Phase 3)

This step determines the components that must be in place to launch and sustain the change process after determining the suitable behavioral and environmental factors for the designed course. Elements here are classed as predisposing, reinforcing, and enabling, and they all influence the likelihood of desired behavioral and/or environmental changes.

Predisposing and reinforcement elements include the technical scenarios that were developed for the participants with accompanying teaching materials (lectures, audiovisual materials). This included learning the scenario which covered two lectures (10 h in total) and other presentations with audio-visual materials and short published videos. Then, group exercises and individual assignments supported the scenario. For example, impulsive clicking was identified as behavior to be changed (Phase 2: Cognitive and Behavioral Factors), participants were exposed to scenarios (predisposing) where they trained on reducing impulsive clicking behavior through

gamification approaches (reinforcing) while getting either automated or instructor feedback.

IM step 4: The production of program components, design, and production (Phase 4)

The fourth phase involves the definition of intervention strategies and final planning for their execution. This is based on policies, resources, and conditions in the strategy's organizational/community environment that could help or impede plan implementation. While the Cybersecurity Competency Model, NIST framework, and ENISA recommendations form the basis of the policies and regulations for the learning outcomes, the university where the course is developed has the necessary infrastructure to carry out the course. This involves having the developed online and physical resources and tools that were used during this exercise. One aspect to consider is the available toolsets and their efficiency in transferring knowledge, i.e., online vs. on-site, awareness training. Other regulatory aspects considered in the design of the course were based on educational parameters defined in the licensed continuing education study program (as course length). For specific program components please contact the first author of this manuscript for details.

IM step 5: The anticipation of program adoption, implementation, and sustainability (Phase 5)

From an educator's perspective, course preparation was more complex compared to the preparation of courses covering only subject-specific competences. Key challenges were limited knowledge of the instructor in other disciplines (i.e., psychology). Other factors to consider were that existing courses have a defined amount of (academic hours, contact hours, ECTS) and mandatory topics, while newly developed courses that focus on novel aspects (i.e., soft skill development in technical scenarios) have no validated or recommended format to achieve competency outcomes. For example, the flipped classroom could enable course enrichment with interdisciplinary topics. Therefore, this multi-dimensional course was developed in collaboration with representatives of different disciplines at the university and their research and educational collaborators from computer science, psychology, and social sciences. Based on the developments described in Steps 1–4 this program was implemented in the spring of 2022.

IM step 6: The anticipation of process and effect evaluation (Phase 6–8)

This step focuses on evaluating the program's process (Phase 6), impact (Phase 7), and outcome (Phase 8) through program assessment of key performance indicators, such as objective performance examinations, follow-up interviews, or evaluation reports (Renaud and Warkentin, 2017; Fernandez et al., 2019). Changes in predisposing, reinforcing, and enabling factors, as well as behavioral and environmental elements (e.g., changes in knowledge, beliefs, attitudes, intentions, and social and environmental barriers/supports) are assessed in impact evaluations. Finally, outcome evaluation assesses the program's impact on cybersecurity behaviors. This section summarizes results from the case study and presents changes in student performance and attitude toward courses and cybersecurity topics when the changes were applied. In general, the changes were accepted positively by students as they enabled new insights into cybersecurity and ensured competence development in a student preferred way.

Process evaluation (Phase 6)

Process evaluation determines the extent to which the program was implemented according to protocol. The updates within the courses allowed educators to investigate cybersecurity topics from different perspectives. By applying the methodology, the instructors provided close to reality cases (roles, scenarios, and contexts) that stimulated student engagement in activities.

Impact evaluation (Phase 7): Student satisfaction and engagement

Impact evaluation assesses change in predisposing, reinforcing, and enabling factors as well as behavioral and environmental factors (e.g., changes in knowledge, beliefs, and self-efficacy) Students rated course content usefulness for scenario execution as "Very good" (8.2). Their confidence level in the ability to assess IT risks raised from "Good" (6.9) to "Very good" (8.5). After study sessions, students reflected that they did not realize that cybersecurity competences are so broad. Previously they concentrated mainly on technical skills.

Outcome evaluation (Phase 8): Impact on the competence development

Applying the proposed methodology can be seen to have an overall positive impact on learners' perceived performance. In the selected scenario related tasks execution, what might be

related to student competence development and slight behavior change. Students were able to perform the IT change risk assessment and understand professional terminology. In the test before training in more than 70% of cases, the scenario related terminology was misinterpreted (for example, mixed terms "threat" and "vulnerability"). After training in more than 70% of cases, correct terminology was used. Students also were able to identify different categories of risks. For example, before the course, more than 90% of cases, only few risks were associated with external threats, such as Distributed Denial of Service (DDoS) attacks. After completing the course, students were able to justify their reasoning about organizational risks. For example, they showed better understanding by giving higher risk scores to enterprise e-commerce services distribution caused by DDoS attacks by identifying risk factors such as weakly protected enterprise networks and lack of monitoring capabilities. Also, task execution time was reduced by more than 20%. This can be interpreted as relational to competence increase, as well as increasing self-efficiency in task execution.

During the group exercise, it was observed that students applied new knowledge regarding critical thinking that was delivered through the course. For example, they challenged their team members' assumptions and explored alternatives. Course instructor led situation analysis and group discussions (enabling) led to higher risk awareness scores compared to preliminary risk assessment (before the critical thinking related session). This could indicate a slight movement toward risk-averse behavior change.

4. Discussion

The focus of this paper was to apply the IM approach to cybersecurity education by presenting the IM steps in the development of an educational course in cybersecurity. Maladaptive cybersecurity behaviors that can impact both personal and organizational security have been well documented recently (Hadlington, 2017). Education, both academic and through continued professional development, for technical and non-technical personnel have been identified as necessary to increase pro-cybersecurity behaviors but how to approach this is still not investigated thoroughly (Manson and Pike, 2014). While the existing literature has given guidelines and learning outcomes (Newhouse et al., 2017; Wetzel, 2021), human behavioral aspects still need to be integrated into studies. Assessing the outcomes of newly developed educational offerings needs to be confirmed with validated approaches. IM has been shown to be effective in planning, developing, implementing, and evaluating program outcomes (Kok et al., 2016) and this approach can also be an effective tool for the evaluation of cybersecurity education. The IM steps allow for the inclusion of relevant stakeholders, in this case, students and educators, to be part in developing educational approaches that are evidence-based.

The use of a case study helps in this specific cybersecurity course on information security and risk mitigation, allows for the development of the course to be influenced by the stakeholders, both students and the academic institution, while considering policy and resources (i.e., NIST, ENISA) to help structure the course in ways it can then be evaluated. The evaluation of the course (process, impact, outcome) allows for the case study analysis to deal with the many variables that could influence outcome results, which then helps triangulate the findings. For example, human-technology interaction can be difficult to measure directly since observing learning during specific contexts, such as this cybersecurity exercise, can be influenced by many factors such as instructor feedback or individual affective states, and it can be difficult to distinguish which factors are more influential during the exercise. But, together with the literature synthesis on cybersecurity education, involvement of the stakeholders for educational design, and the outcome measures, this case study uses this triangulation approach to verify its efficiency (Rowley, 2002; Kohlbacher, 2006; Yin, 2013). This course integrated reality-based scenarios with both technical challenges with soft skill testing (self-efficacy, risky decision-making), a demand that has been proposed by ENISA. The outcome evaluations showed that students improved their terminology, their confidence in their skills increased, and could identify security threats with more precision, all while their time on task was reduced. Also, course instructors, during feedback sessions, observed increased critical thinking toward assumptions and more risk-aversive behaviors.

While the course is context specific to information security and risk management, and the findings cannot be generalized to broader populations, it is the IM process that can be adopted. While IM has shown efficacy in other domains (Kok et al., 2011), this is an initial application of IM in cybersecurity education. The IM steps applied to cybersecurity education presented here show that it can be a useful tool to develop and evaluate the educational design. The first 5 IM steps describe how the program was developed and implemented, and step 6 then helped evaluate the findings. The three evaluation aspects (process, impact, and outcome) help verify the first 5 IM steps and also helps in calibrating future changes to the developed program until it reaches the planned goals.

5. Conclusion

Holistic cybersecurity education development and evaluation was the main objective of this paper. The proposed methodology includes multiple dimensions for advancing cybersecurity competencies among professionals, and soon to be professionals. The central dimension is

identified competence scope which includes work roles for the future professional. As a second dimension is the implementation path for competence development. The third dimension is the proposed learning environment which includes tools and methodologies for competence development. These three dimensions can be integrated into existing and new programs through Intervention Mapping. Developing this multi-dimensional approach to cybersecurity can contribute to how we meet the challenges of a digitized world.

Our future study will explore the capabilities of the proposed model and cover quantitative research to identify limitations and possibilities for automated scenario setups.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding authors.

Author contributions

RP-D, AB, GM, RL, KP, and SS contributed to the key conception and design of the study. AB, GM, BK, RL, and SS wrote the introduction draft. BK, RL, and KP elaborated on the intervention mapping. KL contributed to the analysis of related work. RP-D performed and described the case study. AB supported writing the description. RP-D, AB, GM, and RL completed the analysis and discussed the results. RP-D and AB prepared the figures. All authors contributed to the manuscript revision, read, and approved the submitted version.

Funding

The Advancing Human Performance in Cybersecurity, ADVANCES, benefits from nearly million grant from Iceland, Liechtenstein, and Norway through the EEA Grants. The aim of the project is to advance the performance of cybersecurity specialists by personalizing the competence development path and risk assessment. Project contract with the Research Council of Lithuania (LMTLT) No is S-BMT-21-6 (LT08-2-LMT-K-01-051).

Acknowledgments

We thank all other ADVANCES team members that provided constructive feedback during the preparation of this study.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

ACM/IEEE (2020). *Computing Curricula 2020 (CC2020): Paradigms for Global Computing Education*. New York, NY: Association for Computing Machinery.

Armstrong, M. E., Jones, K. S., Namin, A. S., and Newton, D. C. (2018). The knowledge, skills, and abilities used by penetration testers: results of interviews with cybersecurity professionals in vulnerability assessment and management. *Proc. Hum. Factors Ergon. Soc. Ann. Meet.* 62, 709–713. doi: 10.1177/1541931218621161

Ask, T. F., Sütterlin, S., Knox, B. J., and Lugo, R. G. (2021). "Situational states influence on team workload demands in cyber defense exercise," in *HCI International 2021-Late Breaking Papers: Cognition, Inclusion, Learning, and Culture*, eds C. Stephanidis, D. Harris, W.-C. Li, D. D. Schmorrow, C. M. Fidopiastis, M. Antona, Q. Gao, J. Zhou, P. Zaphiris, A. Ioannou, R. A. Sottilare, J. Schwarz, and M. Rauterberg (Cham: Springer International Publishing), 3–20.

Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive Theory*. Prentice Hall, NJ: Englewood Cliffs.

Bartholomew Eldridge, L. K., Markham, C. M., Ruiter, R. A. C., Fernàndez, M. E., Kok, G., and Parcel, G. S. (2016). *Planning Health Promotion Programs; An Intervention Mapping Approach*. San Francisco, CA: Jossey-Bass.

Bishop, M., Burley, D., Buck, S., Ekstrom, J. J., Futcher, L., Gibson, D., et al. (2017). "Cybersecurity curricular guidelines," in *Information Security Education for a Global Digital Society*, eds M. Bishop, L. Futcher, N. Miloslavskaya, and M. Theocharidou (Cham: Springer International Publishing), 3–13.

Bloom, B. (1985). *Developing Talent in Young People*. New York, NY: BoD-Books on Demand.

Bourque, P., and Fairley, R. E. (2014). *Guide to the Software Engineering Body of Knowledge, Version 3.0*. IEEE Computer Society. Available online at: www.swebok.org

Bowers, D., Petre, M., and Howson, O. (2019). "Aligning competence hierarchies with bloom's taxonomies: changing the focus for computing education," in *Proceedings of the 19th Koli Calling International Conference on Computing Education Research* (New York, NY: Association for Computing Machinery), 1–2.

Bratianu, C., Hadad, S., and Bejinaru, R. (2020). Paradigm shift in business education: a competence-based approach. *Sustainability* 12, 1348. doi: 10.3390/su12041348

Brilingaitė, A., Bukauskas, L., and Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Comput. Security* 88, 101607. doi: 10.1016/j.cose.2019.101607

Canham, M., Posey, C., and Constantino, M. (2022). Phish derby: Shoring the human shield through gamified phishing attacks. *Front. Educ.* 6, 807277. doi: 10.3389/feduc.2021.807277

Cheung, R. S., Cohen, J. P., Lo, H. Z., and Elia, F. (2011). "Challenge based learning in cybersecurity education," in *Proceedings of the International Conference on Security and Management (SAM)* (Las Vegas), 524–529.

Chong, R. C. (2019). "Examining the relationship of active team-based learning and technology and engineering students' research self-efficacy in a cybersecurity traineeship class," in *2019 ASEE Annual Conference Exposition* (Tampa, FL), 1–16.

Chowdhury, N., Katsikas, S., and Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: a delphi method-based study. *Comput. Security* 113, 102551. doi: 10.1016/j.cose.2021.102551

Crick, T., Davenport, J. H., Irons, A., and Prickett, T. (2019). "A uk case study on cybersecurity education and accreditation," in *IEEE Frontiers in Education Conference (FIE)* (Covington, KY: IEEE), 1–9.

ENISA (2018). "Cybersecurity culture guidelines: behavioural aspects of cybersecurity," in *European Union Agency for Network and Information Security* (Attiki).

European Union Agency for Cybersecurity, ENISA (2022). *European Cybersecurity Skills Framework*. Available online at: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf (accessed April 15, 2022).

Fernandez, M. E., ten Hoor, G. A., van Lieshout, S., Rodriguez, S. A., Beidas, R. S., Parcel, G., et al. (2019). Implementation mapping: using intervention mapping to develop implementation strategies. *Front. Public Health* 7, 158. doi: 10.3389/fpubh.2019.00158

Fund, B. (2021). *16 soft skills you need to succeed in cyber security*. Technical report, Flatiron School.

García Olalla, A., Malla Mora, G., Marín Paredes, J. A., Moya Otero, J., Muñoz San Ildefonso, I., Poblete Ruiz, M., et al. (2008). *Competence-Based Learning: A Proposal for the Assessment of Generic Competences*. University of Deusto, TUNING. Available online at: https://www.unideusto.org/tuningeu/images/stories/Publications/Book_Competence_Based_Learning.pdf.

Ghosh, T., and Francia, G. (2021). Assessing competencies using scenario-based learning in cybersecurity. *J. Cybersecurity Privacy* 1, 539–552. doi: 10.3390/jcp1040027

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* 3, e00346. doi: 10.1016/j.heliyon.2017.e00346

Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., and De Nicola, R. (2021). Framework, tools and good practices for cybersecurity curricula. *IEEE Access* 9, 94723–94747. doi: 10.1109/ACCESS.2021.3093952

Hibbs Pherson, K. (2017). *Key Critical Thinking Skills For Security Professionals*. Available online at: https://www.sourcesecurity.com/insights/key-critical-thinking-skills-security-professionals-co-14642-ga.22310.html (accessed April 11, 2022).

Huang, K., and Pearlson, K. (2019). "For what technology can't fix: Building a model of organizational cybersecurity culture," in *Proceedings of the 52nd Hawaii International Conference on System Sciences* (Maui, HI), 6398–6407.

Impagliazzo, J., and Pears, A. N. (2018). "The cc2020 project – computing curricula guidelines for the 2020s," in *2018 IEEE Global Engineering Education Conference (EDUCON)* (Santa Cruz de Tenerife: IEEE), 2021–2024.

Jones, K. S., Namin, A. S., and Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Trans. Comput. Educ.* 18, 1–12. doi: 10.1145/3152893

Jøsok, Ø. (2020). *Cyber Operator Competencies: The Role of Cognitive Competencies in Cyber Operator Practice and Education* (Ph.D. Thesis). Høgskolen i Innlandet.

Keeton, J., Brown, H. N., Miller, C., and Campbell, S. (2019). *Mississippi cybersecurity labor market analysis*. Technical report, The University of Southern Mississippi.

Kennison, S. M., and Chan-Tin, E. (2020). Taking risks with cybersecurity: using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Front. Psychol.* 11, 546546. doi: 10.3389/fpsyg.2020.546546

Kiffer, S., and Tchibozo, G. (2013). Developing the teaching competences of novice faculty members: a review of international literature. *Policy Fut. Educ.* 11, 277–289. doi: 10.2304/pfie.2013.11.3.277

Knox, B. J., Lugo, R. G., Helkala, K., and Sütterlin, S. (2019). Slow education and cognitive agility: Improving military cyber cadet cognitive performance for better governance of cyberpower. *Int. J. Cyber Warfare Terrorism* 9, 48–66. doi: 10.4018/IJCWT.2019010104

Kohlbacher, F. (2006). "The use of qualitative content analysis in case study research," in *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, Vol. 7* (Berlin).

Kok, G., Gottlieb, N. H., Peters, G.-J. Y., Mullen, P. D., Parcel, G. S., Ruiter, R. A. C., et al. (2016). A taxonomy of behaviour change methods: an intervention mapping approach. *Health Psychol. Rev.* 10, 297–312. doi: 10.1080/17437199.2015.1077155

Kok, G., Lo, S. H., Peters, G.-J. Y., and Ruiter, R. A. (2011). Changing energy-related behavior: an Intervention Mapping approach. *Energy Policy* 39, 5280–5286. doi: 10.1016/j.enpol.2011.05.036

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in k-12 students. *J. Cybersecurity Educ. Res. Pract.* 2018, 6.

Maennel, K., Ottis, R., and Maennel, O. (2017). "Improving and measuring learning effectiveness at cyber defense exercises," in *Nordic Conference on Secure IT Systems* (Tartu: Springer), 123–138.

Manson, D., and Pike, R. (2014). The case for depth in cybersecurity education. *ACM Inroads* 5, 47–52. doi: 10.1145/2568195.2568212

Mattie, C., Guest, K., Bailey, S. M., Collins, J. D., and Gucciardi, D. F. (2020). Development of a mental skills training intervention for the canadian special operations forces command: an intervention mapping approach. *Psychol. Sport Exerc.* 50, 101720. doi: 10.1016/j.psychsport.2020.101720

Newhouse, W., Keith, S., Scribner, B., and Witte, G. (2017). National initiative for cybersecurity education (nice) cybersecurity workforce framework. *NIST Special Publ.* 800, 181. doi: 10.6028/NIST.SP.800-181

OPM (2018). *Interpretive guidance for cybersecurity positions attracting, hiring and retaining a federal cybersecurity workforce*. Technical report, United States Office of Personnel Management. Available online at: https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf.

Pandey, A. (2019). *A 5-Step Plan to Create a Captivating Scenario-Based Corporate Training*. ELearning Industry. Available online at: https://elearningindustry.com/scenario-based-learningcorporate-training-how-create (accessed April 15, 2021).

Petersen, R., Santos, D., Smith, M., and Witte, G. (2020). *Workforce framework for cybersecurity (nice framework)*. Technical report, National Institute of Standards and Technology.

Raj, R., Sabin, M., Impagliazzo, J., Bowers, D., Daniels, M., Hermans, F., et al. (2022). "Professional competencies in computing education: Pedagogies and assessment," in *Proceedings of the 2021 Working Group Reports on Innovation and Technology in Computer Science Education, ITiCSE-WGR '21* (New York, NY: Association for Computing Machinery), 133–161.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., et al. (2018). Scoping the cyber security body of knowledge. *IEEE Security Privacy* 16, 96–102. doi: 10.1109/MSP.2018.2701150

Renaud, K., and Warkentin, M. (2017). "Using intervention mapping to breach the cyber-defense deficit," in *Proceedings of the 12th Annual Symposium on Information Assurance (ASIA'17)* (Albany; New York, NY), 14–22.

Rowley, J. (2002). Using case studies in research. *Manag. Res. News* 25, 16–27. doi: 10.1108/01409170210782990

Scholl, F. (2020). *Developing your portfolio of soft skills for cybersecurity*. Technical report, Quinnipiac University.

Sengul, O., Enderle, P. J., and Schwartz, R. S. (2021). Examining science teachers' enactment of argument-driven inquiry (adi) instructional model. *Int. J. Sci. Educ.* 43, 1273–1291. doi: 10.1080/09500693.2021.1908641

Sweller, J., van Merriënboer, J. J., and Paas, F. (2019). Cognitive architecture and instructional design: 20 years later. *Educ. Psychol. Rev.* 31, 261–292. doi: 10.1007/s10648-019-09465-5

Thomson, R. (2019). "The cyber domains: understanding expertise for network security," in *The Oxford Handbook of Expertise* (Oxford: Oxford University Press), 21.

Ward, P., Schraagen, J. M., Gore, J., Roth, E., Hoffman, R. R., and Klein, G. (2019). "Reflections on the study of expertise and its implications for tomorrow's world," in *The Oxford handbook of expertise, The Oxford Library of Psychology* (Oxford: Oxford University Press, United Kingdom).

Wetzel, K. A. (2021). *NICE Framework Competencies: Assessing Learners for Cybersecurity Work*. NIST Internal Report, 18.

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation* 19, 321–332. doi: 10.1177/1356389013497081