To appear in the 7th IEEE Cyber Science and Technology Congress (CyberSciTech 2022), September 12-15, 2022, Calabria, Italy.

Multi-dimensional Cybersecurity Education Design: A Case Study

Rūta Pirta-Dreimane
Information Technology Institute
Riga Technical University
Riga, Latvia
0000-0001-8568-0276

Agnė Brilingaitė
Institute of Computer Science
Vilnius University
Vilnius, Lithuania
0000-0001-9768-4258

Evita Roponena
Information Technology Institute
Riga Technical University
Riga, Latvia
Evita.Roponena@rtu.lv

Karen Parish
Department of Information Security and Communication Technology
Norwegian University of Science and Technology
Gjøvik, Norway
karen.parish@ntnu.no

***Abstract*—Global economies depend on business continuity within the digital space, and cybersecurity is becoming a strategic capability among nations and continents. Accordingly, the need for the cyber workforce is increasing within all public and private sectors. International communities report that skilled specialists are lacking, and the building of cyber-resilience should consider individuals as humans are at the center of most attacks. Existing and emerging cybersecurity competence frameworks focus on the development of subject-specific skills. However, cybersecurity is an interdisciplinary subject requiring understanding human behavior and behaving in the digital space in security-conscious manner in daily routines. Therefore, several dimensions should be integrated into educational programs to support the development of critical competencies, including subject-specific skills and knowledge areas, general skills, and behavioral changes. The paper presents the intervention-mapping-based methodology supporting a multi-dimensional cybersecurity educational design. The methodology applies to different education paths (academic and professional). The pilot study supports the application of the methodology and provides a preliminary evaluation of the chosen approach. The pilot case incorporated continuing education (professional) and master-level (academic) student groups. The study considered critical thinking competence development linked to risk assessment based on cyber threats identifiable within the provided scenario. The results demonstrated the potential value of integrating non-technical topics into the development of role-specific competences.**

***Index Terms*—cybersecurity education, behavior change, IT risk assessment, critical thinking, intervention mapping**

I. Introduction

Today's hyperconnected digital world drives global economies, meanwhile, emerging technologies create new threats to organizations and individuals [1]. Across continents, cybersecurity leaders and joint initiatives emphasize the shortage in the cyber-skilled workforce and suggest the directions to fill the gap. For example, the European Union (EU) revised the education action plan to raise cybersecurity awareness among individuals and encourage upskilling and reskilling [2].

The existing cybersecurity competence frameworks, e.g., the National Initiative for Cybersecurity Education (NICE) Workforce Framework (NIST NICE framework) [3] and the European Union Agency for Cybersecurity (ENISA) skill framework (ENISA framework) [4], distinguish professional roles and associated tasks focusing on technical competencies. Nevertheless, cybersecurity is an interdisciplinary, diverse field [5], [6]. Therefore, several dimensions must be integrated into education programs, including subject-specific and general knowledge areas, general skills, and behavior changes. ENISA emphasizes a need to reflect the skill range in terms of contents and levels because general skills are crucial in the industry [7].

This paper aims to propose a high-level multi-dimensional educational methodology supporting the integration of general skills and behavioral changes into the development of role-specific skills. The three-layered methodology contains a competence model as a top block linking educational practices with stakeholder requirements and specialist roles. The middle block describes the process based on the intervention mapping [8] to integrate general skill development into the study courses. The education design process can be based also on similar systematic methods, as ADDIE model [9]. Finally, the tools and training environments make the base for the methodology as they can provide and limit the range of learning activities required to develop and assess skills. The paper also presents the pilot case study to support and illustrate the application of the methodology. The methodology was applied in continuing and master-level education, combining critical thinking competence with other general skills to develop IT security risk assessment professional skills for defined roles. The pilot case showed how general topics back up the development of role-specific competencies using predefined close-to-reality

The "Advancing Human Performance in Cybersecurity", ADVANCES, benefits from nearly €1 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).

978-1-6654-6297-6/22/$31.00 ©2022 IEEE

scenarios. The results showed that the proposed methodology suggests that the chosen approach increases student acceptance and awareness of behavior changes.

The paper is structured as follows. Section II reviews related work. Section III introduces the methodology to develop role specific technical and general skills and consider the behavior changes of learners. The case study is presented in Section IV, and Section V discusses its results. Section VI concludes the paper and points out future work directions.

II. Related Work

This section reviews existing practices and recommendations used for cybersecurity training and education to identify whether cybersecurity training methods are integrated with psychological aspects, such as developing critical thinking.

Launched by major international computing societies (ACM, IEEE CS, AIS SIGSEC, and IFIP WG 11.8), the CSEC2017 Joint Task Force on Cybersecurity Education (JTF) proposed the first curricular recommendations in cybersecurity education [6]. The working group emphasizes that cybersecurity is an interdisciplinary course, including law, policy, risk management, computing, and human factors, for example, critical thinking, working under uncertainty, and ethics.

The National Initiative for Cybersecurity Education (NICE) presented the Cybersecurity Workforce Framework (NIST NICE framework) [3], describing the task statement and the knowledge and skills statements required to perform the task. According to the NIST NICE framework, these statements are the foundation for cybersecurity education. Although the framework provides the method to group the tasks, skills, knowledge, competencies, work roles and teams, it mainly focuses on education for the organization's employees and does not provide the methodology for educating students.

Developed by various community college educators, the Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020) [10] is based on CSEC2017 and inspired by CAE-CD 2Y knowledge units [11] and NIST NICE [3]. The guidance focuses on competencies and learning outcomes. The Cyber2yr2020 competencies include the ability to describe various human factors that could affect privacy and security and the ability to compare different mental models and their impact on the user's response to cybersecurity risks.

Strategic Programs for Advanced Research and Technology in Europe (SPARTA) Cybersecurity Skills Framework [5] links cybersecurity work roles and required expertise and demonstrates how to develop a curriculum reflecting job market requirements. To support educators in the design of the study programs, the authors propose to use the Curricula Designer tool. The authors highlight the importance of cybersecurity interdisciplinary and general skills. However, methodology mainly focuses on technical and operational competences in role-based competence mapping.

The Cyber Security Body of Knowledge (CyBOK) guide [12] maps established cybersecurity knowledge to cyber education programs and professions. The guide is divided into 21 Knowledge Areas categorised as human, organizational and regulatory aspects, cyber-attacks and defences, system security, software and platform security, and infrastructure security. The guide highlights the importance of training and confidence creation in risk communication to ensure a sense of responsibility as a human factor.

Various studies suggest that it is possible to improve cybersecurity education by integrating psychological principles. Taylor et al. [13] highlight that understanding social psychology and cognitive psychology can help improve understanding of human behavior, decision-making process, risk analysis, and fraud identification. Thackray et al. [14] suggest that psychological training helps cybersecurity specialists gain these aspects and develops an understanding of hacker motivation.

Existing competence frameworks and curricula mainly focus on subject-specific competences definitions. Gradually models incorporate general skills. Meanwhile, personality traits and the integration of cybersecurity behavior changes is still not widely used in education and remain a challenge [15].

III. Methodology

The proposed methodology consists of three key building blocks—competence model, course design process, and learning & training environment (see Fig. 1).

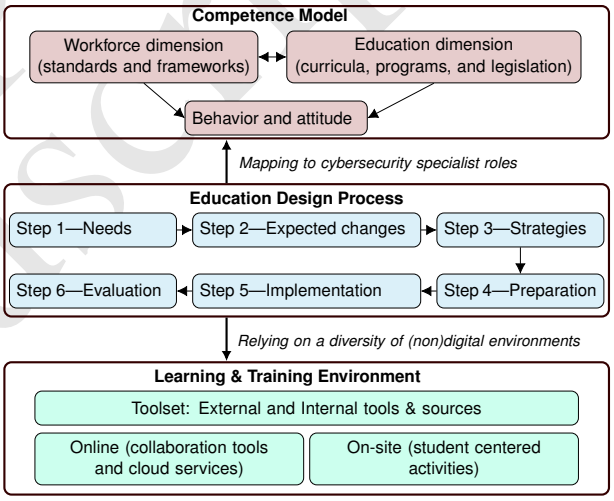

Fig. 1. Methodology overview

The competence model interconnects workforce and education dimensions defined by the stakeholder positions, standards, and formal regulations. Thus, the model block links defined specialist roles and associated tasks with specific competences and related learning objectives. The model combines such central components:

1) *Work roles* are the most detailed groupings of cybersecurity-related work, including a list of attributes, i.e. knowledge, skills, and abilities required to perform tasks associated with the role [3].
2) *Tasks* represent specific defined pieces of work that, combined with other identified tasks, compose the work scope in a speciality area or work role [3].

3) *Competencies* describe capabilities 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 [3].
4) *Behavior and characteristics* define individual actions and attitudes towards others on particular occasions. Behavior is how the person responds to a particular situation or stimulus. Personalities are characterized by traits, which are relatively enduring characteristics that influence our behavior across many situations [16].

The methodology emphasizes the importance of a solid combination of subject-specific and general skills to enable roles specific task execution. Therefore, the process block of the methodology (see Fig. 1) suggests the main steps based on intervention mapping approach [8] to integrate human factors into the educational environment. The process starts with exploring the audience's needs (Step 1) providing grounds to identify target roles, tasks, and competencies (Step 2). After selecting learning strategies and defining learning outcomes (Step 3), course preparation follows (Step 4). Finally, the course is executed (Step 5) and evaluated accordingly (Step 6).

The implementation of skill development depends on the available toolset and learning environments. Various collaboration tools and virtual learning environments support online activities, events, and information sharing, including tests, challenges, learning material, and external sources (documentations). An on-site learning environment enables face-to-face activities involving online tools. Modern education relies on the student-centered approach, but tool specifics can limit or open possibilities related to educational paths.

IV. Course Design

The proposed methodology was applied in a pilot case that incorporated two different groups of learners—continuing education students and IT master students. Both groups represented different learner profiles with specific needs and objectives.

Continuing education students are professionals in non-IT fields who want to re-skill and start a career in IT. Master students are local and international students with practical work experience and an undergraduate degree in IT who aim to become cybersecurity professionals. The numbers of continuing education and IT master students were 13 and 17, respectively.

The continuing education students design and execution timeline is presented in Fig. 2. Fig. 2 presents the design and execution timeline for the continuing education program. Individual knowledge assessment test was executed before the training. The test contained a brief sample organization description with a risk assessment task, structured in the online tool. Afterward, two training sessions were conducted, integrating lectures and group-oriented practical assignments. The tasks relied on the learning scenario (IT risk assessment, third-party risk assessment, data protection impact assessment for the sample organization). Firstly, the course addressed subject-specific and context-related topics; afterward, general and expected behavior-related topics were introduced. Between sessions, students watched prepared videos. After training sessions, a knowledge assessment test was conducted (similar to the one before training).

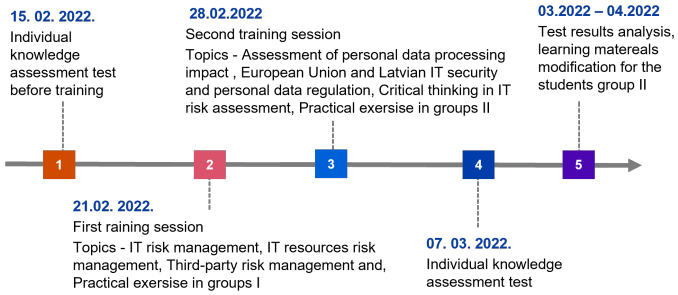

Fig. 2. Continuing education course timeline

The second student group training schedule was analogous, and the training started after first group results analysis and learning materials update. The course content was designed using the methodology described in Section III, and Fig. 3 illustrates the pilot course design.

A. Step 1—Assess the Needs

Training needs and requirements were assessed by analyzing different sources – existing cybersecurity competency models and curricula, industry requirements, legalisation, experts recommendations and learners' profiles, including their expectations and needs. Learners' profiles were defined using design thinking methods [17], [18]. Requirements and needs were collected by literature analysis, interviews, focus group sessions, and feedback analysis from previous training sessions (three years perspective). The main topics of interest highlighted by the learners were subject-specific and related to technical competencies. Learners identified the following *subject-specific* topics of interest: IT aspects in personal data protection, IT risk management, best practices in information security governance, and information security tools. The identified requirements and needs were mapped with relevant target roles and tasks from the NIST NICE framework [19] to enable role and task-specific training scenario design and execution. A variety of learners' profiles (existing roles, expected career paths, personal portfolios and backgrounds) led to selection of several target roles. Four *target roles* were selected—Cybersecurity and Strategy Planner, Security Control Assessor, Privacy Officer, and Information Security Manager. The tasks associated with the roles were identified based on NIST recommendations [19]. Role-based essential interrelated tasks were selected for the study course content design. Following roles, similar or interrelated *target tasks* were selected for the training (see Fig. 3): (1) Establish a risk management strategy for the organization that includes a determination of risk tolerance, (2) Perform security reviews, identify gaps,

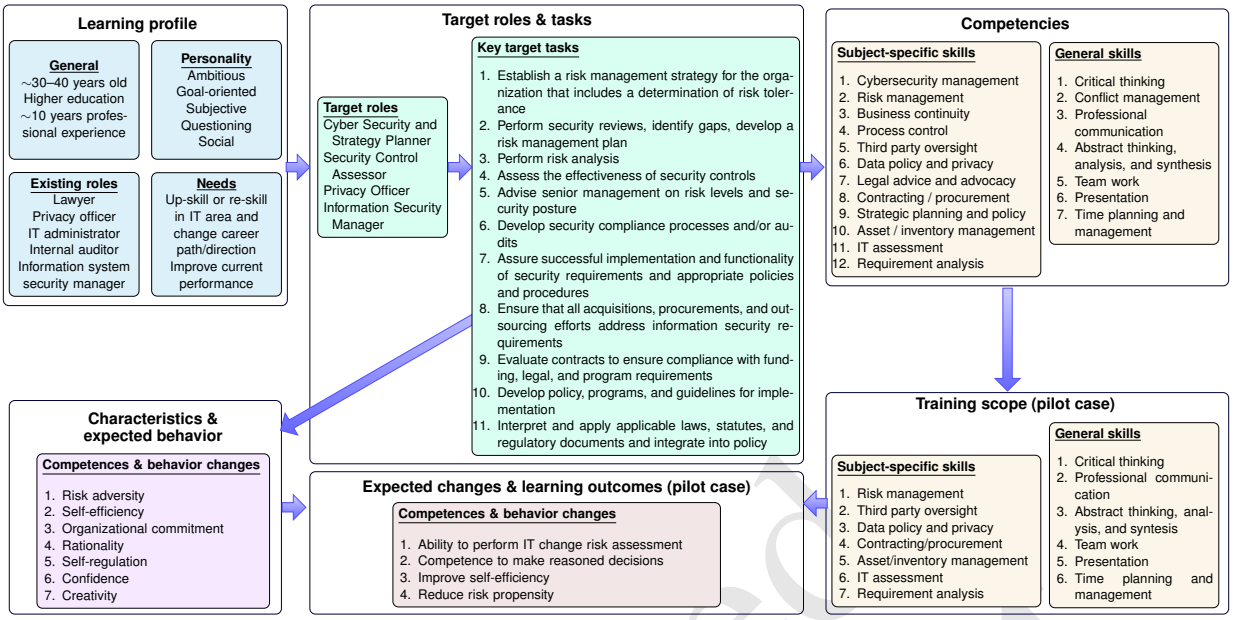

Fig. 3. Pilot course design

develop a risk management plan, (3) Perform risk analysis, and (4) Assess the effectiveness of security controls and others.

B. Step 2—Define Expected Changes

Target roles and required subject-specific competences to execute defined tasks were selected from NIST framework [3]. The following *subject-specific competencies* were selected: Risk management, Cybersecurity management, Business continuity, Process control, Third-party oversight, Data policy and privacy, Legal advice and advocacy, Contracting/procurement, Strategic planning and policy, Asset / inventory management, IT assessment, and Requirement analysis.

Required general competencies were selected from the Tuning competence model [20] based on IT industry and education experts [21]–[23] and related research [5] recommendations about key general competencies for cybersecurity professionals. The following *general competences* were selected: Critical thinking, Conflict management, Professional communication, Abstract thinking, Analysis and synthesis, Team work, Presentation, Time planning and management.

Expected behavior and target personality traits were defined based on research team experts (psychologists) assessment, related research [24], [25] and industry experts recommendations [26]. The following *characteristics and expected behavior* items were selected: Risk adversity, Self-efficiency, Organizational commitment, Rationality, Self-regulation, Confidence, Creativity.

Competences and expected behavior were mapped to learning topics. For the pilot case IT security risk governance related knowledge were selected, as it was relevant for both selected training groups students profiles and needs, as well as different sources highlighted its importance to build cybersecurity capabilities foundation [5], [6], [19]. Expected changes in trainee performance and learning objectives were defined to ensure required competences and expected behavior changes. The following *learning outcomes* were defined: Ability to perform IT change risk assessment, Competence to make reasoned decisions, Improve self-efficiency, Reduce risk propensity.

Continuing education learners group profiles, target roles, tasks, competences and learning outcome mapping are presented in Fig. 3. Other group target roles, tasks, competences and learning outcomes also fit to the model (more technical competences were incorporated on other sessions).

C. Step 3—Define Strategies

A scenario-based learning method was chosen as a primary method to enable learning outcomes. It aims to connect the student learning process with the real-world challenges [27]. The selected learning scenario was “a significant IT change” within the enterprise IT landscape. The IT change meant implementing a new information system hosted on the public cloud and provided as service (SaaS). The overview of the prepared training scenario is shown in Table I.

The scenario-based method was complemented by traditional lecture-based learning (audiovisual materials) and short learning videos to develop an awareness of attitude impact on business continuity.

D. Step 4—Make Course Preparation

The course content was adjusted to trigger general competences development and behavioral changes. A specific session was designed to execute a new learning scenario that included *subject-specific topics*—IT risk management, IT resources risk management, and Assessment of personal data processing impact. Additionally, the following *general*

TABLE I
CHARACTERISTICS CARD FOR LEARNING SCENARIO

Name:	Significant IT Change—implementation of the new information system
Scenario overview:	Latvian private sector organization has an outdated IT landscape. The organization lacks IT competencies and capabilities. It is willing to replace one of the outdated information systems (ERP system) and procure a SaaS ERP solution hosted on the cloud environment. The organization has selected the offshore service, and the SaaS solution will be hosted outside the EU. The case description incorporated several risk factors related to the sample enterprise vulnerabilities, such as human factors (missing competences, sub-optimal decision-taking structure, low employees awareness level, etc.), technical and technological factors (insecure integration patterns and network protocols, non-existing network protection and data quality controls, etc.) as well as legal (non-compliance to GDPR) and third-party management related aspects. The case is presented to students in a separate description (app. 2 pages).
Context:	Industry—Manufacturing, Region / Country—EU / Latvia, Information system type—SaaS, Sourcing—Procurement
Exercise:	Perform IT resources risk assessment; Perform third party risk assessment (work in groups); Discussion of results
Learning environment	Online tools: ZOOM break-out rooms, Miro collaboration tool, Google sheets, MS Forms
Time:	10 hours total (2 hours practical task in groups, 2 hours individual assignment)

topic was incorporated in the scenario: Critical thinking in IT risk assessment. Finally, *context-specific topics* were added for learning scenario support: Third-party risk management, European Union and Latvian IT security and personal data regulation.

Critical thinking is essential in emergency handling (as IT incident response), as well as in strategic and operational planning (as IT risk response planning) [28]. Industry professionals have highlighted five critical thinking skills [29]: Challenge assumptions, Consider alternatives, Evaluate data, Identify key drivers and Understand context. Relevant topics were included in the audiovisual materials and integrated into group exercises—IT resources risk assessment and Third-party risk assessment. Firstly, students were introduced to a subject-specific topic (IT risk management). Afterward, the exercise and learning scenario were presented. Students performed the IT risk assessment exercises for the given case in groups and prepared a report in a predefined form. In the second training part, a general topic was introduced (critical thinking). Afterward, the students were asked to apply explained skills and challenge the IT risk assessment prepared by other groups. Students' performance was examined with a similar individual task.

E. Step 5—Run Implementation

The course schedule was adjusted to incorporate new content, time divided to IT risk management topic increased by approximate 30 percents. The schedule is shown in the Fig. 2.

F. Step 6—Perform Evaluation

Evaluation incorporated three key aspects: Students' competence evaluation (before and after training), Students' behavior evaluation (before and after training), and Training approach and content evaluation. The evaluation methodology is presented in Table II. Each evaluation aspect included criteria, and the course entailed a measurement for each criterion.

To evaluate students' ability to identify "right" threats and vulnerabilities, the literature was reviewed to explore the most common context-specific information security risks for the learning scenario that involved cloud solutions, hosting outside EU, and web technologies. Table III contains the case-related cybersecurity risks and threats summarized from various literature sources such as reports, web articles, and scientific papers.

As shown in the figure, risks and threats were grouped into five categories: software as a service (SaaS), cloud solution, data migration from an old system to a new system, web application security, and data stored outside European Union. These categories were included in the use case scenario to review students' risk assessment abilities. For example, to reduce personal data leakage risk and ensure compliance with EU GDPR requirements requires organizations to implement additional measures, deviate resources and take relevant decisions when introducing solutions hosted outside the EU.

V. COURSE DELIVERY RESULTS

The pilot study included a qualitative assessment according to the evaluation methodology presented in Table II. The qualitative assessment enabled determining the significance of the introduced didactic approaches based on the expected impact on the achievement of learning outcomes. The case run and student feedback provided the initial evaluation of the methodology's applicability in the educational environment. The results showed that the applied methodology increased learners' performance in selected task execution, which might have been triggered by competence development and behavior change in task execution. The generalized evaluation outcomes are presented in the following sub-sections.

A. Students competences evaluation

Students demonstrated improved competences in the individual tests at the end of the course. Learners were able to perform IT change risk assessment and articulate professional terminology. Before the training, more than 50 percent of test tasks showed misinterpreted terminology (for example, confused terms "threat" and "vulnerability"). Overview of test results before and after training is presented in Fig. 4. The pilot study involved 30 students.

Students were able to justify their reasoning about the risk score. In justification, students mainly referred to sample organization threats and vulnerabilities. For example, students justified a high-risk score of the e-commerce service disruption

TABLE II
EVALUATION METHODOLOGY

Goal	Criteria	Measurement
Student competence evaluation	Ability to identify threats & vulnerabilities and assess risk level; Ability to justify the decision; Ability to identify the "right" threats & vulnerabilities	Test results review (understanding of concepts and definitions, logical risk justification & assessment; Comparison of test results to related research and expert evaluation results (most common context-specific information security risks)
Student behavior evaluation	Risk adversity; Self-confidence; Self-efficacy	Number of identified risks; Risk score (assumption: less risks with lower score = higher risk adversity); Students self-confidence score (1–10); Test completion time
Training approach and content evaluation	Student competence level; Course content usefulness	Comparison of competences after subject-specific skills training to achievements after training combining general & subject-specific skills ; Student feedback score (1–10)

TABLE III
CYBERSECURITY RISKS AND THREATS IN LITERATURE

Context	Risk/Threat	Source
SaaS	Unused entities exposed	[30]
	Compromised APIs	[30]
	Misconfigured cloud users' privileges	[30]
	Critical data transferred to private cloud	[30]
	Unauthorized access to the hosting platform	[31]
	DDoS attack	[31]
	Data breach	[31]
	SaaS application data loss	[31]
	Service unavailability	[31]
	Malware distribution from SaaS website	[31]
Cloud solution	Abuse and Nefarious Use of Cloud Services	[32]
	Data breach	[32]
	Account hijacking	[32]
	Insider threats	[32]
	Compromised Cloud Server and Credentials	[32]
	Inadequate security solutions	[32]
	Regulation Compliance	[33]
	Business Continuity and resiliency	[33]
	User privacy and secondary usage of data	[33]
	Service and data integration	[33]
	Incidence analysis and forensics	[33]
	Non-production environment exposure	[33]
Data migration	Lack of data knowledge	[34]
	Incompatibilities of data migration between different vendors' applications	[34]
Web API security	Unencrypted Data	[35]
	Adware	[35], [36]
	Identity Theft	[35], [36]
	Data breaches	[36]
	Broken Access Control	[37]
	Cryptographic failures	[37]
	Injections	[37]
	Security misconfiguration	[37]
	Vulnerable and outdated components	[37]
	Identification and authentication failures	[37]
	Software and data integrity failures	[37]
	Security logging and monitoring failures	[37]
	Server-side request forgery	[37]
Data stored outside EU	Non-compliance with GDPR	[38]

caused by a DDoS attack with a weakly protected enterprise network and lack of monitoring capabilities. In most cases students related particular risks with sample enterprise vulnerabilities and industry research on the most common threats, as "OWASP TOP 10" [37]. The observation of the group exercise indicated that students could apply new knowledge

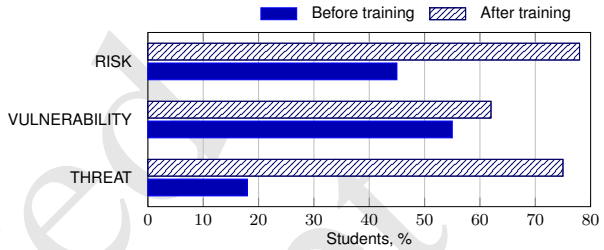

Fig. 4. Key terms knowledge evaluation

regarding critical thinking, for example, challenging their and colleagues' assumptions. During the past years, the training focused only on subject-specific skills, and students demonstrated lower analytical reasoning capabilities in the same task execution. Individual tests of both training groups highlighted the difference between the two training approaches. Students who learned critical thinking provided more than 80 % risk justification. Meantime, students who learned subject-specific topics only justified just 30 % of identified risks.

Testing results highlighted that only about 50 % of learners identified risks matched with typical risks associated with a particular scenario context (see Table III). In comparison to other areas, less of typical risks were identified in the SaaS security area. This result might be related to the limited knowledge about SaaS solutions and their specifics. In addition to IT change risk, several students also evaluated the sample organization's existing situation IT risks (before changes). About 30 % of identified risks were associated with physical security threats, as physical security issues were highlighted in the sample organization case description. More than 80% of the learners highlighted privacy and compliance (GDPR) related risks, as the training sessions included the particular related topic. Overview of test results before and after training is presented in Table IV. Overall, after training, students identified additional threats compared to results before training. It could be related to the critical thinking topics that covered recommendations about different data sources assessment.

B. Students behavior evaluation

The number of identified risks and risk scoring accuracy did not increase significantly. It can be related to the relatively

TABLE IV
REFERENCE RISKS IDENTIFICATION

Context	Risk/Threat	Before training	After training
SaaS security	Unused entities exposed		
	Compromised APIs		x
	Misconfigured cloud users' privileges		
	Critical data transferred to private cloud		
	Unauthorized access to the hosting platform		
	DDoS attack	x	x
	Data breach	x	x
	SaaS application data loss	x	x
	Service unavailability	x	x
	Malware distribution from SaaS website		
Cloud solution	Abuse and nefarious use of cloud services		
	Data breach	x	x
	Account hijacking		x
	Insider threats	x	x
	Compromised cloud server and credentials		
	Inadequate security solutions		x
	Regulation compliance	x	x
	Business continuity and resiliency	x	x
	User privacy and secondary usage of data	x	x
	Service and data integration	x	x
	Incidence analysis and forensics		
	Non-production environment exposure		
Data migration	Lack of data knowledge	x	x
	Incompatibilities of data migration	x	x
Web API security	Unencrypted data	x	
	Adware		
	Identity theft		x
	Data breaches	x	x
	Broken access control	x	x
	Cryptographic failures		
	Injections	x	x
	Security misconfiguration		x
	Vulnerable and outdated components	x	x
	Identification and authentication failures		
	Software and data integrity failures	x	x
	Security logging and monitoring failures		
	Server-side request forgery		x
Data stored outside EU	Non-compliance with GDPR	x	x

small training scope. It indicates that course plan of the following training sessions must be revisited to incorporate additional scenarios and topics. Empirical observations from the previous years' courses highlighted that learners' risk awareness might decrease after practical task execution (such as password hacking games) and after examining realistic incident cases.

Execution time of individual tasks decreased by more than 20 %, which can be related to competence increase and self-efficiency increase in the task execution.

C. Training approach and content evaluation

The students rated course content usefulness for scenario execution as *Very good* (8.2 on a 10-point scale). Their confidence level about the ability to assess IT risks raised from *Good* (6.9) to *Very good* (8.5). The students reflected that the course content was interesting and admitted that scenario-based learning promoted general competences next to subject-specific ones.

A volume of trainee questions and comments showed that students without an IT background were more interested in general topics. Empirical observations pointed out that computer science students appreciate subject-specific (e.g., technical) topics more. Continuing education students assessed the risk more comprehensively than students with an IT background, mainly focusing on technological threats (such as malware and man-in-the middle attacks). Both groups identified insider and outsider threats and stressed the importance of human aspects in cybersecurity.

VI. CONCLUSION AND FUTURE WORK

Cybersecurity competences and education design recommendations are presented in several competence models, curricula, and frameworks [3], [6], [12]. However, they mainly focus on subject-specific competences, even though some directly accountable positions require a wide range of general skills and the ability to understand human behavior to make strategical decisions. Meanwhile, integrating personality traits and cybersecurity behavior changes in education is still a challenge.

The paper proposed the multi-dimensional cybersecurity education methodology and presented the case study of its application. The methodology enriches the *classical* education design process (as [8] or [9]) with a cybersecurity-specific competence model and diverse learning environment patterns to enable a complex process of role-based cybersecurity competence development. The approach requires adding study topics related to general skills, behavior, and characteristics and adjusting the learning strategy to the selected professional roles. The approach supports the design of different education paths, e.g., professional and academic. The pilot case incorporated two different groups of learners—continuing education students (professionals) and IT master students. Students were tested before and after training to evaluate their competence level.

The case study highlighted that general competences and behavioral changes related learning topics integration in cybersecurity education programs support learners to gain needed competences for effective target roles and tasks execution according to industry needs. In the pilot case, three of four expected learning outcomes were reached: 1) develop the ability to perform IT change risk assessment; 2) develop competence to make reasoned decisions; 3) increase self-efficiency. The fourth defined learning outcome of reducing risk propensity still requires course amount and content enrichment, as human behavior changes demands a complex activity.

Based on observations applying the proposed methodology in the course design raised students competences and led to improved performance compared to previously executed training that focused on subject-specific skills only.

The case study results can be interpreted as a preliminary evaluation of the proposed approach, as the student group was relatively small. The validity of the approach will be tested with larger groups. The case study included one real-life simulation scenario execution. For further methodology examination and specification, it is planned to prepare and integrate several multi-dimensional scenarios and test the methodology on 2–3 additional student groups, analyzing the performance of not less than 100 students.

Further evaluations could be used to validate the qualitative assessment concerning relationships between the study course design and the learning outcomes related to behavior and attitude changes in role-based scenarios.

REFERENCES

[1] World Economic Forum, "Global cybersecurity outlook 2022," January 2022, Insight report. [Online]. Available: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[2] The European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

[3] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte, "Workforce Framework for Cybersecurity (NICE Framework)," *NIST Special Publication 800–181*, 2020.

[4] European Union Agency for Cybersecurity, ENISA, "European cybersecurity skills framework," 2022. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf

[5] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, "Framework, tools and good practices for cybersecurity curricula," *IEEE Access*, vol. 9, pp. 94 723–94 747, 2021.

[6] Joint Task Force on Cybersecurity Education, *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. New York, NY, USA: ACM, 2018.

[7] J. R. Nurse, K. Adamos, A. Grammatopoulos, and F. D. Franco, "Addressing skills shortage and gap through higher education," European Union Agency for Cybersecurity (ENISA), Tech. Rep., November 2021.

[8] M. E. Fernandez, G. A. ten Hoor, S. van Lieshout, S. A. Rodriguez, R. S. Beidas, G. Parcel, R. A. C. Ruiter, C. M. Markham, and G. Kok, "Implementation mapping: Using intervention mapping to develop implementation strategies," *Frontiers in Public Health*, vol. 7, 2019.

[9] R. M. Branch, *Instructional design: The ADDIE approach*, 1st ed. Springer-Verlag, 2009.

[10] Cyber2yr2020 Task Group, *Cybersecurity Curricular Guidance for Associate-Degree Programs*. ACM, 2020, no. January.

[11] NSA and DHS, "2020 CAE Cyber Defense (CAE-CD) Knowledge Units," pp. 1–102, 2020. [Online]. Available: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

[12] P. Burnap, R. Carolina, M. A. S. A. Rashid, C. Troncoso, and W. Lee, *The Cyber Security Body of Knowledge*, 1st ed. CyBOK, 2021. [Online]. Available: https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

[13] J. Taylor, J. McAlaney, S. Hodge, H. Thackray, C. Richardson, S. James, and J. Dale, "Teaching psychological principles to cybersecurity students," in *IEEE Global Engineering Education Conference, EDUCON*. IEEE, 2017, pp. 1782–1789.

[14] H. Thackray, J. McAlaney, H. Dogan, J. Taylor, and C. Richardson, "Social psychology: An under-used tool in cybersecurity," in *the 30th International BCS Human Computer Interaction Conference, HCI 2016*, 2016, pp. 1–3.

[15] J. Taylor-Jackson, J. McAlaney, J. L. Foster, A. Bello, A. Maurushat, and J. Dale, "Incorporating psychology into cyber security education: A pedagogical approach," in *Financial Cryptography and Data Security*. Cham: Springer International Publishing, 2020, pp. 207–217.

[16] C. Stangor and J. Walinga, *Introduction to psychology*. Canada: BC Open Textbook Project and BCcampus, 2014.

[17] I. Wrogemann, L. Sarp, N. Süsser, and J. Falk, *Design Thinking Manual for Adult Learning Providers*, 2020, d-Learning – Design Thinking as a means to innovative product development in adult learning. [Online]. Available: https://cesie.org/media/d-learning-manual-en.pdf

[18] S. Panke, "Design thinking in education: Perspectives, opportunities and challenges," *Open Education Studies*, vol. 1, no. 1, pp. 281–306, 2019.

[19] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National initiative for cybersecurity education (nice) cybersecurity workforce framework," *NIST Special Publication 800*, p. 181, 2017.

[20] Tuning Educational Structures in Europe. Generic competences. [Online]. Available: https://www.unideusto.org/tuningeu/competences/generic.html

[21] F. Scholl, "Developing your portfolio of soft skills for cybersecurity," 2020. [Online]. Available: https://quonline.quinnipiac.edu/blog/developing-your-portfolio-of-soft-skills-for-cybersecurity.php/

[22] B. Fund. (2021) 16 soft skills you need to succeed in cyber security. [Online]. Available: https://flatironschool.com/blog/soft-skills-cyber-security

[23] K. H. Pherson. Key critical thinking skills for security professionals. [Online]. Available: https://www.sourcesecurity.com/insights/key-critical-thinking-skills-security-professionals-co-14642-ga.22310.html?utm_source=SIc&utm_medium=Redirect&utm_campaign=Int%20Redirect%20Popup

[24] S. M. Kennison and E. Chan-Tin, "Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors," *Frontiers in Psychology*, vol. 11, 2020.

[25] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Computers & Security*, vol. 73, no. 4, pp. 345–358, 2018.

[26] J. Barker, *Confident Cyber Security: How to Get Started in Cyber Security and Futureproof Your Career*. United Kingdom: Kogan Page Ltd, 2020.

[27] T. Ghosh and G. Francia, "Assessing competencies using scenario-based learning in cybersecurity," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 539–552, 2021.

[28] S. Nowduri, "Critical thinking skills and best practices for cyber security," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 4, pp. 391–409, 2018.

[29] K. H. Pherson and R. H. Pherson, *Critical thinking for strategic intelligence*. CQ Press, 2020.

[30] VARONIS Cloud Research Team, "2021 SAAS RISK REPORT," VARONIS, Tech. Rep., 2021. [Online]. Available: https://info.varonis.com/hubfs/Research-2021SaaSRiskReport.pdf?hsCtaTracking=cd869a49-bf8e-4b5e-b5ce-21bdbdfccb62%7Cec2e4d5f-cef1-4838-88ca-123d91758707

[31] O. Akinrolabu, S. New, and A. Martin, "Assessing the Security Risks of Multicloud SaaS Applications: A Real-World Case Study," in *6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 / 5th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2019*. IEEE, 2019, pp. 81–88.

[32] Cloud Security Alliance, "Top Threats to Cloud Computing: Deep Dive," Cloud Security Alliance, Tech. Rep., 2018. [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloud-computing-deep-dive.pdf

[33] S. Babu, C. Ph, V. Bansal, and P. Telang, "Cisco: Top 10 Cloud Risks That Will Keep You Awake at Night," Cisco, Tech. Rep., 2010. [Online]. Available: https://owasp.org/www-pdf-archive/Cloud-Top10-Security-Risks.pdf

[34] A. Jaju and A. Lamba. (2022) How to Mitigate the Risks and Challenges in Data Migration. [Online]. Available: https://angle.ankura.com/post/102hjcr/how-to-mitigate-the-risks-and-challenges-in-data-migration

[35] C. Odogwu. (2021) 6 Online Shopping Security Threats and How to Avoid Them. [Online]. Available: https://www.makeuseof.com/online-shopping-security-threats/

[36] D. A. M. Aseri, "Security Issues For Online Shoppers," *International Journal of Scientific and Technology Research*, vol. 10, no. 3, pp. 112–116, 2021.

[37] OWASP. (2021) OWASP Top Ten. [Online]. Available: https://owasp.org/www-project-top-ten/

[38] European Commission. (2017) Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_15