Technology, Knowledge and Learning
https://doi.org/10.1007/s10758-024-09769-8

ORIGINAL RESEARCH

Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach

Rūta Pirta-Dreimane[1] · Agnė Brilingaitė[2] · Evita Roponena[1] · Karen Parish[3] · Jānis Grabis[1] · Ricardo Gregorio Lugo[4] · Mārtiņš Bonders[1]

Accepted: 10 July 2024

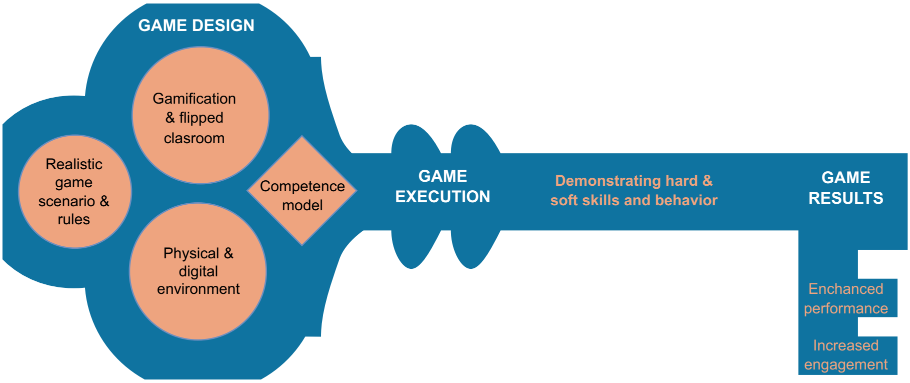
Abstract

Incorporating gamification elements and innovative approaches in training programs are promising for addressing cybersecurity knowledge gaps. Cybersecurity education should combine hard and soft skill development when building the capacity to manage cyber incidents requiring timely communication, team collaboration, and self-efficacy in risk assessment and incident mitigation. The paper presents a design and evaluation of the technology-enhanced cybersecurity education approach CAPE which works as a hybrid escape room. It combines a virtualized infrastructure simulating the business environment and the physical environment where game participants play the role of the incident response team at the organization's premises. The CAPE could be applied as a student-centered approach in the educational environment. The work employed a multiple-methods research approach to design a gamified approach and investigate crisis communication, collaboration, self-regulation, and technical competences in incident management scenarios. The design science methodology empowered the game's construction with an attack surface covering physical and digital security. The undergraduate students participated in the pilot execution and completed the psychological questionnaires. The results were analyzed using statistical methods. Results of the CAPE execution showed a positive impact on student performance and increased interest in cybersecurity. The designed approach promoted field-specific competence development. The results demonstrated the significance of psychological aspects related to incident management.

Extended author information available on the last page of the article

Published online: 30 July 2024

Graphical abstract


GAME DESIGN
Gamification & flipped clasroom
Realistic game scenario & rules
Competence model
Physical & digital environment
GAME EXECUTION
Demonstrating hard & soft skills and behavior
GAME RESULTS
Enchanced performance
Increased engagement

Keywords Cybersecurity education · Escape room design · Incident response · Incident management training · Crisis communication · Team collaboration · Serious game

1 Introduction

Cyber crises require deep technical knowledge to minimize response time and ensure business continuity with efficient mitigation. As defined by the IEEE Computer Society (IEEE, 2017), enterprises require building a security architecture and ensuring a proper disaster preparedness level to recover from adversities, including security breaches. However, general skills and behavioral traits are also essential to ensure good communication, responsibility distribution, and efficient work in problem-solving during incident management processes. After all, these processes involve incident escalation and sharing with stakeholders (Onwubiko & Ouazzane, 2022).

Incident management as a complex task demonstrates a vital organizational capability related to company readiness to respond to cyber threats and minimize their negative impact effectively. Incident management processes are associated with several roles, such as incident commander, incident responder, forensics investigator, communication lead, and legal counsel. Technical expertise, communication, analytical, problem-solving, and collaboration skills are essential in incident response. However, behavioral aspects also play a significant role in incident management, as the nature of incident response duties can be stressful and emotionally challenging (Budimir et al., 2020). Self-regulation and the ability to stay calm and focused can enhance the performance of cybersecurity specialists. Thus, specific approaches can be considered when building an effective collaborative team with respect to individual profiles (Shah et al., 2023). Therefore, cybersecurity education programs must consider the above dimensions to guarantee specialists are prepared to handle cyber-attack incidents and ensure the continued operation of services.

This paper introduces the educational approach CAPE to advancing hard and soft skills in cybersecurity. The design science research method (Hevner et al., 2004) was used to build the solution based on the escape room idea. Escape rooms provide an engaging way to develop students' competences (López-Belmonte et al., 2020), and they have been used to build critical thinking and problem-solving skills and to enhance communication and collaboration within a group (Duncan, 2020; Murphree and Vafa, 2020).

The key contributions of this paper are multi-fold. Firstly, we propose the design of the CAPE approach as a learning method integrating multiple dimensions of cybersecurity education. Secondly, computer-based and physical security aspects are merged in a single cybersecurity exercise. Additionally, the study provides insights into factors affecting cybersecurity trainees' performance. The objectives of the study are to investigate how the game-based learning approach influences the development of student competences in cybersecurity incident response (RO1), how communication, collaboration, team dynamics, and metacognition impact the student's performance (RO2), and whether the hybrid escape room promotes student engagement in cybersecurity activities (RO3). Even though the application of the cyber escape room approach in cybersecurity education is described in the literature, there is limited research on its effect on student competence development, behavior change, and engagement in the professional area. Therefore, we aim to fill this gap.

The CAPE approach combines student-centered education methods like gamification (Subhash & Cudney, 2018), problem-based learning (Hmelo-Silver, 2004), and flipped classroom principles (Gilboy et al., 2015). Therefore, we position the CAPE approach as a serious game design because its primary purpose is to develop skills. It creates a realistic cyber incident setup, but it also includes the *fun* part (Dörner et al., 2016). It addresses crisis communication, collaboration and self-regulation, and technical competences in incident management scenarios. To promote student engagement, the on-site environment is enriched with different physical game elements, such as Lego figures and posters. A wide range of digital tools supports the CAPE design. The virtual laboratory and collaboration tools mirror a work environment requiring collaboration and the application of technical skills. The pilot CAPE run was executed by involving undergraduate-level students in information technology (IT).

The paper is structured as follows. Section 2 provides the research background, and Sect. 3 presents the research approach of this work. Section 4 covers the CAPE competence model, including learning outcomes and expected behavior. Section 5 overviews the game scenario and its context. The digital and physical environment setup is presented in Sect. 6. Pilot study results are unveiled in Sect. 7. The results are discussed in Sect. 8. Section 9 provides conclusions and future research directions.

2 Background

This section groups related work based on areas of investigation for the escape room design, aiming to develop soft and hard skills.

2.1 Human Factors in Cybersecurity Education

Despite the rapid development of technical means and artificial intelligence (AI) and their use in cybersecurity, humans are still a central part of security because AI cannot adapt to unknown circumstances as well as a human can (Zhang et al., 2022). Therefore, understanding the current role of the actors in cybersecurity is vital.

The research emphasizes the importance of considering psychological aspects when creating a cybersecurity education program. McLeod and Dolezel (2022) concluded that information theft, security vulnerabilities, distrust of security, and security self-efficacy lead to the individual's feeling of capitulation or surrendering, impacting information security policy (ISP) non-compliance behavior. Aggarwal and Dhurkari (2023) found that stress and ISP non-compliance behavior have a weak positive correlation. The researchers also discovered that demographic factors are moderately related to this correlation. Kyytsöen et al. (2022) show that demographic characteristics impact information security skill self-assessment similarly.

Time pressure is one of the aspects that can impact human cyber behavior. Research shows that time pressure creates a stressful environment, and lengthy security procedures can enhance the stress that time pressure introduces (Chowdhury et al., 2020). Also, identity-based (how the individual identifies) motivation influences employee in-role and extra-role performance security behavior (Ogbanufe & Ge, 2023). Although the human habit theory could also be applicable to the cybersecurity behavior analysis of the individual, it has yet to be investigated in the cybersecurity research field (Weickert et al., 2023).

2.2 Game-Based Learning Methods

Game-based learning is an excellent way to educate learners and enhance their problem-solving abilities. Gamification is usually defined as the process of adding game-like elements, such as leaderboards and chats, to digital environments to increase the motivation of users to spend more time in the digital world (Wolfenden, 2019). In contrast to gamification, where only some game components are used for the learning process, a serious game is a full-fledged game that simulates the environment (Krath et al., 2021). A serious game is a digital game developed to entertain and achieve at least one additional goal, such as acquiring specific skills, raising awareness of certain topics, or changing behavior (Dörner et al., 2016). Both gamification and serious games are discussed in the scientific articles regarding cybersecurity education.

Cybersecurity-related tasks can be easily integrated into gamified engaging activities, increasing motivation to solve tasks and interest in cybersecurity (Nieto-Escamez & Roldán-Tapia, 2021). Gamified learning environments provide a safe space for the cybersecurity workforce to develop and demonstrate vital skills while being excited about challenges related to new cyber threats (Wolfenden, 2019). Cybersecurity training often includes capture the flag (CTF) exercises, mainly improving data and network security knowledge (Švábenský et al., 2021). However, it is challenging to map CTF activities to the competences defined by security experts (Švábenský et al., 2021).

The cybersecurity table-top exercises (TTX) mimic an actual cybersecurity incident without impacting business continuity. TTX could provide scenarios depending on the chosen role to evaluate competences as a multi-choice digital test (Kvietinskaitė et al., 2022), or it could be delivered through videos and printed materials to simulate specific cyber attacks (Bahuguna et al., 2019).

Yamin et al. (2021) proposed a serious game to develop cybersecurity exercise scenarios and emphasized that serious games could be a practical tool for modeling new realistic scenarios. Still, their impact on defense strategies requires further research. Moreover, Calvano et al. (2023) analyzed cybersecurity-related serious games. They concluded that some games focused on education, and poor gaming experience could have hindered knowledge acquisition. Therefore, we aim to design a serious game that integrates the interdisciplinary perspective and provides a balanced approach to skill development, behavior change, and gamification elements.

Serious games which include TTX, are designed for educational purposes, enhance metacognitive processes such as self-regulation, planning, monitoring, and evaluation, which are crucial for far transfer-the application of learned skills to new real-world contexts (see Sect. 4.2). The CAPE approach integrates several principles to support far transfer. By creating realistic scenarios that mimic real-world challenges, the approach allows players to practice and apply skills in contexts resembling their eventual use. Incorporating metacognitive prompts encourages reflective thinking, essential for understanding and applying cognitive processes in different situations (Zumbach et al., 2020; Pouralvar et al., 2019). Feedback mechanisms further aid learners in adjusting their strategies and improving their understanding of skill application (Braad et al., 2019). Additionally, TTX, provide structured scenarios that help participants practice and refine their skills in a controlled environment, further supporting the transfer of skills to real-world contexts. Thus, the CAPE approach effectively supports far transfer by embedding metacognitive strategies and realistic scenarios within its game design.

2.3 Training Platforms

Various gamified educational tools and serious games are available online; some of them are open-source for cybersecurity training. Players of the tabletop card game Cyber Threat Defender should build robust security and attack their opponents within the time limit (Center for Infrastructure Assurance & Security, 2023). The 3D office simulation CyberCIEGE (Thompson & Irvine, 2015) enables player interaction with virtual staff while implementing security policies and provides functionality to monitor the players' progress. Cyber Protect (Department of Defense, 2023) provides functionality to purchase and deploy tools for network protection against attackers. Scenarios of the NDTG (Ashley et al., 2022) training platform consider network defense challenges.

Cloud-based open-source platform KYPO (Vykopal et al., 2021) provides an interactive learning environment for cybersecurity on-site or remote training, including CTF-based sessions and various use cases. Open-source platform CyTrONE (Beuran et al., 2018) provides three categories of activities and allows the trainee to choose the difficulty level and visualize the cyber range. Riposte (Malone et al., 2021), a browser-based game applicable to cybersecurity education, enables the development of tasks with progressive difficulty and uses two styles of play: player versus player (PvP) and player versus environment (PvE). However, it does not support observing team dynamics or improving students' soft skills.

2.4 Escape Rooms

The escape room game format has been introduced previously for educational gamification (López-Belmonte et al., 2020). Gordillo et al. (2024) demonstrated that educational escape rooms were more effective than traditional classes in teaching a core topic of software engineering. The escapeED framework (Clarke et al., 2017) is a serious game highlighting six core elements of an educational escape room: participants, objectives, theme, puzzles, equipment, and evaluation. Objectives represent expected outcomes within some theme as a context. Participants complete puzzles in rooms having predefined equipment, and the evaluation explains the participants' performance. Traditional cybersecurity courses can be transformed into gamified exercises proposing them as Escape the Classroom tasks (Debello et al., 2022). The virtual escape room and a serious game

CySecEscape 2.0. (Löffler et al., 2021) includes puzzles addressing different topics. The ARI 3D (Decusatis et al., 2022) consists of different tasks designed as mini-games. The last two rooms focus on improving cybersecurity awareness rather than mimicking a real-life cybersecurity environment, and tracking the change in soft skill development is impossible. The escape rooms can also improve information privacy competences. For example, Papaioannou et al. (2022) developed an exciting scenario for a serious game where the guardian angel helps the player with tasks.

The students positively accepted two on-site escape rooms—for the defense and attack scenarios designed by Beguin et al. (2019). But there was no evidence of how useful the cyber escape approach is for cybersecurity education. Researchers of another study (Mello-Stark et al., 2020) could not conclude whether the on-site escape room engaged the participants' interests in cybersecurity.

3 CAPE Design and Implementation

The design science approach supported the development of the CAPE as a gamified method integrating multiple dimensions of cybersecurity education. This section presents the CAPE design and implementation.

3.1 Design Science Meta-study

The design science problem-solving method (Hevner et al., 2004) systematically connects practical problems with domain-specific solutions. Design science research enhances human knowledge by creating innovative artifacts: constructs, models, methods, and instantiations (Hevner et al., 2004). Models use constructs to represent a real-world problem and its solution in the chosen problem communication and definition language. Furthermore, methods define processes and guide how to solve problems. Instantiation demonstrates how other artifacts can be implemented in a working system. Three repeatable cycles make the design science research process (Hevner, 2007). The relevance cycle uses the environmental context and provides research requirements to improve the knowledge base and solve the research problem. The design cycle includes artifact development and evaluation. The rigor cycle supports the research with prior knowledge and ensures the solution is innovative.

This work aims to develop an interactive learning approach engaging students in cybersecurity activities, enabling the development of hard and soft skills, and supporting trainers with a toolset to observe a change in skill levels through game-based learning. The CAPE approach has to integrate several dimensions to improve human performance in cyberspace. Therefore, following the design science principles (Hevner et al., 2004), the meta-study was conducted in the CAPE development process. Figure 1 presents the investigated approach's environment, design, and knowledge base. Related literature on gamification applications in cybersecurity education (see Sect. 2), security guidelines, standards (Cichonski et al., 2012; European Union Agency for Cybersecurity, 2022), and the intervention mapping (IM) based methodology (Pirta-Dreimane et al., 2022) guidelines made the knowledge base. The *ADVANCES IM-based* methodology provided the foundation of the game design to integrate different dimensions of the competence model into the education programs, consider the needs of trainees, adapt realistic cybersecurity scenarios, and include the cybersecurity work roles and associated tasks.

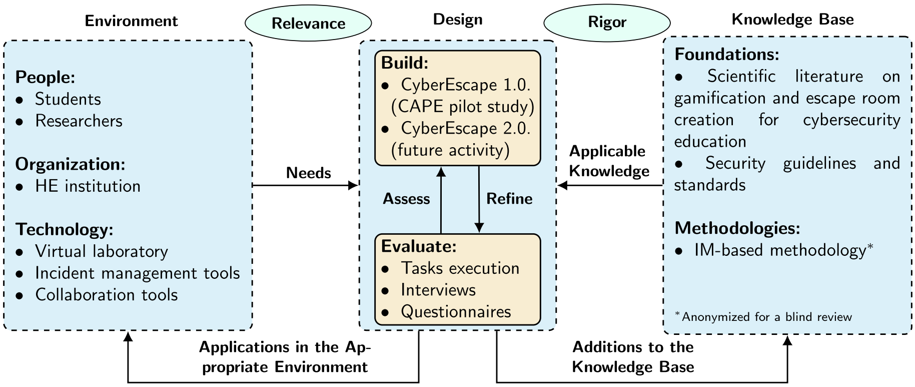

Environment
Relevance
Design
Rigor
Knowledge Base
People:
• Students
• Researchers
Organization:
• HE institution
Technology:
• Virtual laboratory
• Incident management tools
• Collaboration tools
Needs
Build:
• CyberEscape 1.0. (CAPE pilot study)
• CyberEscape 2.0. (future activity)
Assess
Refine
Evaluate:
• Tasks execution
• Interviews
• Questionnaires
Applicable Knowledge
Foundations:
• Scientific literature on gamification and escape room creation for cybersecurity education
• Security guidelines and standards
Methodologies:
• IM-based methodology*
*Anonymized for a blind review
Applications in the Appropriate Environment
Additions to the Knowledge Base

Fig. 1 Design science approach for CAPE development (adapted from Hevner et al. (2004))

Additionally, this study employed a social science research methodology with a multiple-methods approach to include both post-positivistic and social constructionist constructs in the research design (Kuckartz, 2014). This approach expands the study's scope as both quantitative and qualitative methods are used to explore the research objectives (Greene, 2012). The objectives were addressed using a quantitative approach to measuring the students' performance, communication, collaboration, group dynamics, self-efficacy, self-regulation, and motivation during the pilot CAPE execution, CyberEscape 1.0. During the pre- and post-training phases, the students filled out questionnaires. Moreover, the research team adopted a qualitative approach using semi-structured group interviews to focus on the student engagement experiences during the execution of CyberEscape and the student's perceptions of how the pre-exercise training (flipped classroom approach) enhanced their performance.

The flipped classroom approach promotes active learning by requiring learners to complete pre-class activities by themselves before in-class activities (Hew et al., 2021). The flipped learning approach directly benefits from the use of technologies. According to Baig and Yadegaridehkordi (2023), the most popular technologies used in a flipped classroom are video creation tools, learning management systems, content repositories, podcasts, collaboration tools, and online assessment tools. In our case, video creation tools and content repositories were used to provide students with learning materials prior to the main event, almost like Cho et al. (2021), excluding quizzes. The students were given a week to familiarize themselves with five 10–15 min long videos that included topics such as introduction to information security and definitions, incident management steps, typical information security incidents, crisis communication, and collaboration and self-regulation in crisis. Additionally, students were provided with related online materials for additional reading.

Piloting CAPE is the first cycle of planned research to evaluate the CAPE approach and find the improvements for the next design cycle—the next game version. The intention is to determine if there is a need to repeat the relevance cycle.

3.2 Preparation and Execution Steps

An engineering cycle in design science research includes implementation and evaluation (Wieringa, 2014). The CAPE pilot was executed at the institution of higher education with students as participants and young researchers as observers. Preparation incorporated tasks in several steps:

1. Public Relations. Design marketing materials and publish the announcement to the event with a registration link.
2. Scenario. Clarify the competence model, design the attack vector (physical and digital), and determine the timeline of events.
3. E-learning Course. Develop the course, record videos, prepare additional learning materials, and arrange collaboration tools.
4. Virtual Laboratory. Set up the infrastructure, implement the cyber range, and script (semi)automated tools to simulate attacks.
5. Physical Environment. Design tasks with physical artifacts (Legos), print paper-based artifacts, and arrange observers team collaboration space (chat).
6. Playbook. Prepare instructions for students and observers and train the observers.
7. Evaluation Tools. Design the evaluation criteria and develop online & offline questionnaires.

The above-listed tasks and game execution make the Preparation and Implementation steps according to the ADVANCES IM-based methodology (Pirta-Dreimane et al., 2022). The CAPE approach as a learning method and dominant features of the competence model are selected within the previous steps (Needs, Expected Changes, and Strategies). Validation and evaluation of the approach's impact on the performance complete the methodology based on the guidelines. According to the designed scenario, considering the developed competence model and playbook, the research team used artifacts of the digital and physical infrastructure to execute the game. Participants filled out questionnaires and were interviewed to research behavioral aspects. Figure 2 provides an overview of data collection stages and methods.

Before the game, students completed an online self-assessment questionnaire on their competencies in cybersecurity incident management. During the game student, task execution results were rated according to the defined evaluation metric and scores per task

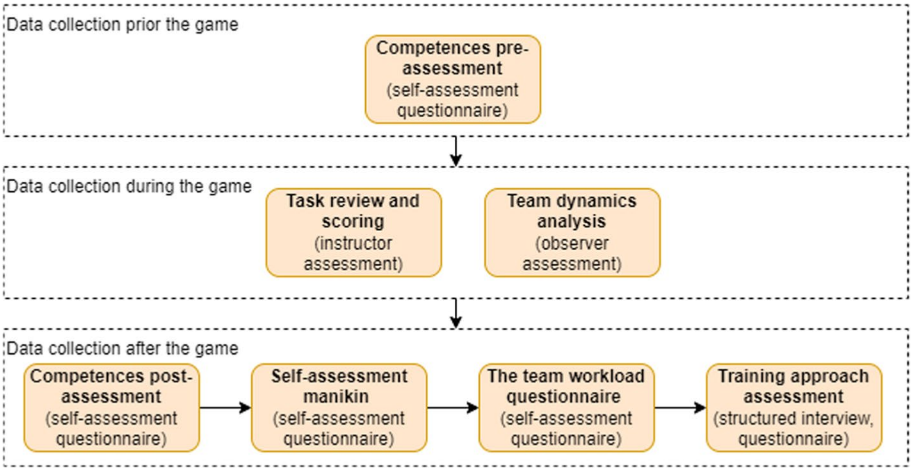

Data collection prior the game
Competences pre-assessment (self-assessment questionnaire)
Data collection during the game
Task review and scoring (instructor assessment)
Team dynamics analysis (observer assessment)
Data collection after the game
Competences post-assessment (self-assessment questionnaire)
Self-assessment manikin (self-assessment questionnaire)
The team workload questionnaire (self-assessment questionnaire)
Training approach assessment (structured interview, questionnaire)

Fig. 2 Data collection phases

(see Table 1). The assessment strategy was presented to the students before the game. Table 1 provides point values assigned for each task. For example, team building based on the CSIRT role framework was worth 4 points, and crisis communications had a value of 8.

Instructors rated task execution results during the execution (see Fig. 2). In each room, an observer assessed the students' behavioral aspects. Observers filled out a checklist to count interactions among team members with a committed leader and interactions among team members without a leader involved. Observers also identified several aspects of team communication, such as leadership style, communication style, and team support and motivation. However, since these observations were subjective, they were not used as formal evaluation criteria.

After the game, several measurements were carried out. The students were asked to complete an online self-assessment form, which included evaluating changes in competencies and the training approach. Afterward, the students completed the team workload questionnaire and self-assessment manikin on paper.

The last measurement was a structured interview with each team, performed by the dedicated interviewer. The interview included the following questions:

Q1. Did the training video help to execute tasks?
Q2. How did you build teamwork for the task? What worked and what did not?
Q3. How did you evaluate the team's performance?
Q4. Other informal feedback on the game (what you liked, what you did not like, what could be improved).

The interview data was used to define the directions for game improvement.

The team applied statistical methods to analyze the data and triangulate it with qualitative data collected by the observers to get insights into the applicability of the CAPE approach.

Interviews with participants were conducted according to the established Code of Ethics for students, academic and administrative personnel of Riga Technical University (RTU) and the Code of Ethics of scientists published by the Charter of Latvian Academy of Sciences. All ethical principles were assured, and students' consent was collected as part of the registration form. The signs of ongoing photography were posted in the event area. All participants had the possibility to leave the game and stop the interviews at any time.

Table 1 Scoring metric based on tasks

Task	Maximal points
Task 1. CSIRT decomposition	4 points
Task 2. Incident detection and classification	5 points
Task 3. Incident recovery measures definition	5 points
Task 4. Security measures definition	3 points
Task 5. Crisis communication	8 points
Task completion time (escape from the room)	5 points

4 Competence Model

The CAPE approach follows the competence model design guidelines (Pirta-Dreimane et al., 2022). Thus, it considers technical skills, soft skills, and behavior to rely on in certain scenarios. This section reviews the role of the *Cyber Incident Responder*, associated tasks and competences, expected behavior, along with the game learning outcomes and evaluation criteria.

4.1 Cyber Incident Responder

The *Cyber Incident Responder* work role is the central element of the competence model. The role is defined by leading cybersecurity investigation institutions, such as the European Union Agency for Cybersecurity (ENISA) and the National Institute of Standards and Technology (NIST). *Cyber Incident Responder* is responsible for handling incidents and implementing security measures to ensure the continued operations of ICT systems. The complex role includes extensive tasks to oversee and manage cybersecurity incidents along their life-cycle (Lemay et al., 2015). The main task of a *Cyber Incident Responder* is incident identification, assessment, and mitigation. For proactive risk response, the role needs to assess and manage cybersecurity vulnerabilities. The incident results and handling aspects must be communicated and documented according to the legal and compliance requirements. The role must cooperate with stakeholders such as Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs). Effective task execution requires a diverse set of competences (see Fig. 3).

The model in the figure distinguishes the vital technical and operational competences defined by the ENISA and NIST. The role must master cybersecurity incident handling and

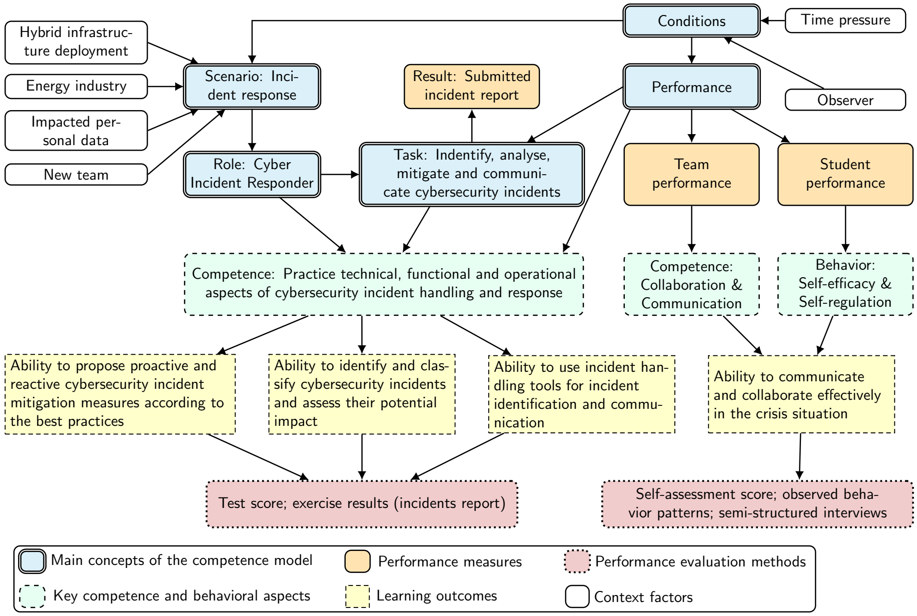

Conditions
Time pressure
Hybrid infrastruc-ture deployment
Energy industry
Impacted per-sonal data
New team
Scenario: Inci-dent response
Result: Submitted incident report
Performance
Observer
Role: Cyber Incident Responder
Task: Indentify, analyse, mitigate and communi-cate cybersecurity incidents
Team performance
Student performance
Competence: Practice technical, functional and operational aspects of cybersecurity incident handling and response
Competence: Collaboration & Communication
Behavior: Self-efficacy & Self-regulation
Ability to propose proactive and reactive cybersecurity incident mitigation measures according to the best practices
Ability to identify and clas-sify cybersecurity incidents and assess their potential impact
Ability to use incident han-dling tools for incident identification and commu-nication
Ability to communicate and collaborate effectively in the crisis situation
Test score; exercise results (incidents report)
Self-assessment score; observed beha-vior patterns; semi-structured interviews
Main concepts of the competence model
Performance measures
Performance evaluation methods
Key competence and behavioral aspects
Learning outcomes
Context factors

Fig. 3 CAPE competence model (a fragment)

response from functional, technical, and operational angles. It is essential to operate with heterogeneous IT environment components, e.g., operating systems, databases, servers, and cloud computing services. The role must know the communication procedures of incident handling. A deep understanding of computing networks and operating systems security is required along with knowledge of incident handling best practices.

Related studies (Chen et al., 2014; Steinke et al., 2015) and psychology experts pinpoint essential soft competences to enhance specialist performance in the cybersecurity incident response. Effective collaboration in the team promotes the execution of the incident-handling process. Communication, presentation, and reporting skills are essential to engage with internal and external stakeholders. Incidents typically relate to high-stress situations requiring quick decision-making and problem-solving. Therefore, the role must be able to work under pressure. Incident management can elicit a wide range of emotions and cognitive and behavioral changes, such as increased stress levels and difficulty concentrating. Thus, not only individual competences, but also behavioral aspects play a significant role in effective task execution. Self-regulation, confidence, and adaptability may raise individual performance in crises. Therefore, the competence model considers team and individual performance under time pressure (Conditions) in the incident response situation (Scenario) related to the defense of the critical infrastructure.

4.2 Expected Behavior

CAPE design includes tasks that mimic authentic situations and problems to be solved by the incident responder, having to make precise decision and act collaboratively while maintaining a composed state of mind in a stressful situation. People with higher metacognitive skills accurately and confidently assess their performance despite situational demands, i.e., workload and team workloads, and can better cope and adapt their behavior (Salas et al., 2008).

Metacognition is the awareness of one’s knowledge and the capacity to comprehend, regulate, and manipulate one’s cognitive processes (Meichenbaum, 1985). It is made up of three elements: self-awareness, situational awareness, and behavioral control techniques (Flavell, 1979). Examples of metacognitive knowledge skills include knowledge of the world, technology, and experience, as well as knowledge of oneself and awareness of one’s own abilities, such as self-efficacy, beliefs, such as confidence, and anticipated results (situational knowledge). The incident manager must have a deep understanding not only of their own behavior but also knowledge of the organization, its policies, stakeholders, and technical environment, along with personal knowledge and the team’s abilities to respond effectively to the incident. Metacognitive skills can help incident managers navigate complex organizational dynamics and make decisions that align with the organization’s overall goals and values, such as assessing investments in post-incident improvement measures and considering enterprise risk appetite.

Metacognitive knowledge, experience, and skills are the three facets where metacognition interacts with behavior. Metacognition is evident at each facet and is influenced by experiences at the situational level (Efklides, 2008, 2011). In addition to being essential for decision-making and problem-solving, metacognitive skills are also crucial for situational awareness and domain switching from socio-technical to tactical and strategic domains. In order to include emotional and behavioral aspects into flexible situational decision-making and problem-solving, it is necessary to be aware of how to control and modify them (Gross, 1998). The self-regulation process demonstrates how a person monitors and controls emotions and behaviors when interacting with the environment. When an incident occurs, there is often a sense of urgency and pressure to recover quickly. The incident manager must control their own behaviors (i.e. emotional states, communication styles) as they can negatively impact decision-making ability and interactions with other stakeholders involved in incident response. Macrocognitive aspects must be considered to fully understand how metacognition enhances performance in order to notice and explain interactions with situational factors. Macrocognition is addressed as a complement to microcognitive approaches, i.e., metacognition, by incorporating both individual and team processes Smieszek and Rußwinkel (2013) and refers to high-level mental processes at a team level to create new knowledge during complex collaborative problem-solving (Letsky et al., 2007).

Several distinctive characteristics within the macrocognitive environment that make up the context in which naturalistic decision-making typically occurs have been identified (Klein et al., 2003). Uncertainty, ambiguity, and missing data are these characteristics, along with shifting and competing goals, dynamic and constantly changing conditions, action-feedback loops (real-time reactions to changed conditions), time pressure, high stakes, multiple players, organizational goals and norms, and experienced decision makers Wolf et al. (1991). These factors are typical for incident management processes. The incident manager must possess a deep understanding of the incident and be able to make informed decisions based on incomplete or limited information while maximizing the efficiency of resources.

Therefore, based on the processes described above, we expect that individual self-regulation and confidence (self-efficacy) factors and situational factors, such as communication and cooperation, will impact team performance in this exercise, focusing on the incident management process.

4.3 Learning Outcomes and Evaluation Criteria

Learning outcomes (LOs) refer to the student's hard and soft skills and expected behavior after completing the program. Evaluation incorporates three key aspects: students' competence evaluation, students' behavior analysis, and training approach assessment. The overview of the learning outcomes and evaluation methodology is presented in Table 2. We break down the four learning outcomes of the competence model (see Fig. 3) into learning outcomes LO1–LO7 to align with applied measurements. Additionally, we define learning outcomes LO8–LO9 to identify the impact of the CAPE educational method on student engagement in cybersecurity and individual growth (generic competences).

The student assessment schema is based on student performance in task execution and self-assessment (pre- and post-event questionnaires, exit interviews), as provided in Fig. 2. Trainers conduct evaluations using qualitative and quantitative parameters and apply some monitoring tools. For example, measurement M4 considers message contents and receiver lists, and measurement M5 relates to monitoring tools because trainees have to use incident handling tools (LO5). Team assessment is used for student behavior evaluation to identify factors that may influence communication and performance at the individual and team level, along with the situational awareness of the individuals. Psychological questionnaires support behavioral analysis (Sellers et al., 2014; Bradley & Lang, 1994a) as listed in measurements M6–M7. Student feedback is a central element for the training approach evaluation (see measurements M8–M9).

Table 2 Evaluation methodology

Learning outcome / Evaluation criteria	Measurement
Student competence (RO1)	
To identify and classify cybersecurity incidents (LO1)	Detected and classified incidents, assessed their potential impact (trainer evaluation) (M1)
To reactively mitigate cybersecurity incidents (LO2)	Identified incident reaction measures and contained incidents (trainer evaluation using monitoring tools) (M2)
To proactively mitigate cybersecurity incidents (LO3)	Identified post-incident improvement measures (trainer evaluation) (M3)
To communicate confidently in a crisis situation (LO4)	Identified stakeholders, prepared personalized crisis communication messages (trainer evaluation) (M4)
To use incident handling tools (LO5)	Infrastructure monitoring tool usage for incident identification, analysis and mitigation (trainer evaluation using monitoring tools) (M5)
Student behavior (RO2)	
To collaborate effectively in a crisis situation (LO6)	Defined team structure, effective interaction between team members (psychologist evaluation using The Team Workload Questionnaire (TWLQ), observers notes and interviews) (M6)
To self-regulate and adapt in a crisis situation (LO7)	Individuals situational awareness (psychologist evaluation using Self-Assessment Manikin (SAM), observers notes and interviews) (M7)
Training approach (RO3)	
Engagement increase (LO8)	Students interest in cybersecurity (self-assessment) (M8)
Competence increase (LO9)	Students competences in the incident management (self-assessment, interviews) (M9)

5 Game Scenario Overview

Scenario-based learning enables student skill development by performing authentic tasks in a real-world context, which is vital in cybersecurity (Ghosh & Francia, 2021). This section covers the game scenario context that requires performing specific tasks to gain new competences and reach the learning outcomes.

5.1 Learning Scenario Context

The CAPE learning scenario presents a fictional mid-size energy sector company recently facing cybersecurity incidents. The central component of the enterprise is the Hydroelectric power station. Thus, the critical infrastructure is located near the river and is affected by changing seasons and weather conditions. The enterprise operates with industry-specific IT assets, such as SCADA (supervisory control and data acquisition), CRM (customer relationship management), billing systems, customer portal and website. The enterprise processes large amounts of customers' data each day. The CAPE participants take the role of the newly established CSIRT in the company and perform specific tasks across the information security incident management lifestyle.

Throughout the scenario, the story evolves and reflects cybersecurity concerns in the daily operations of the enterprise. First of all, the IT manager and human resources (HR) manager welcome the CSIRT team. They introduce the team to the company's operational model, structure and resources, and the expected team's role and capabilities. The communication manager presents the communication policy of the enterprise. During the game, the team gradually faces different contextual events in the enterprise's operation, such as customer and employee complaints, unavailable services, and external factors (such as floods and social engineering).

During the scenario, the team interacts with typical organizational roles, such as IT department manager, HR manager, communication manager, IT support, and service staff. Each role is represented by a fictional character (persona), having specific personality traits, attitudes, and behaviors.

As CAPE is a serious game, the designed scenario creates realistic situations that allow participants to develop knowledge and skills transferable to real situations.

5.2 Incident Management Tasks

The game represents the incident response life-cycle defined in NIST computer security incident handling recommendations (Cichonski et al., 2012). The NIST suggests four phases of incident reaction process: preparation, detection & analysis, containment eradication & recovery and post-incident activity. Participant teams are required to complete specific tasks in each phase (see Fig. 4).

The initial phase emphasizes the preparation for future incidents. It concerns the establishment of incident management capability, including the definition of relevant policies, roles, and responsibilities, and acquiring the necessary resources and tools. The first participant task is to form a CSIRT team and define the team structure, roles, and responsibilities. The CAPE is a hybrid exercise incorporating both table-top exercises and virtual exercises that require determining roles and responsibilities, considering the team size. The team must know the typical CSIRT structure and split responsibilities among its members

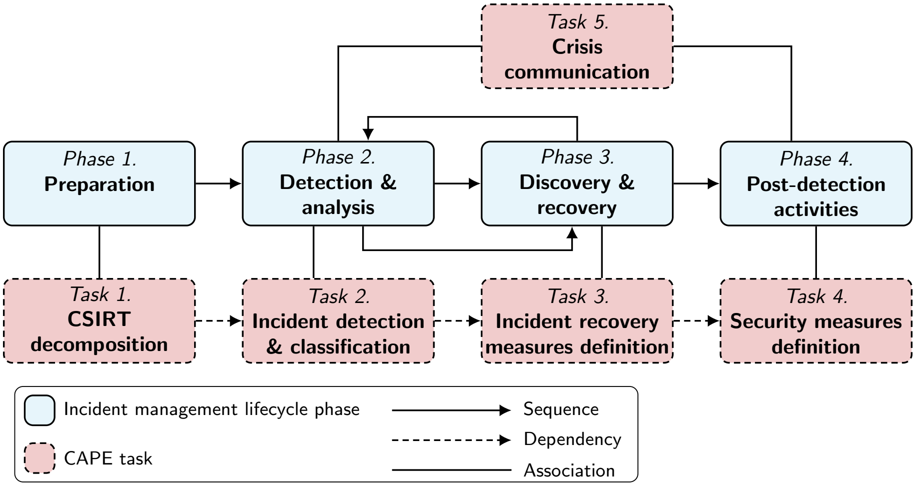


Fig. 4 Workflow of CAPE tasks

to ensure effective collaboration, considering group collaboration, individual performance, and behavioral factors (related to LO6 and LO7).

The incident detection and analysis phase concerns identifying security breaches using various sources, such as alerts of monitoring tools, people, and logs. The incidents must be assessed, validated, and prioritized, considering their severity. The CSIRT team must record the facts related to the incident and notify relevant parties. The second task of the participants is to detect incidents hidden in the physical and digital environment: a denial of service attack, data loss caused by a natural disaster, and phishing, and to document and classify them by specifying the incident name, short description, type (logical, physical, or organizational), category (incident sub-type), and its impact (low, medium, high, or critical) (related to LO1 and LO5).

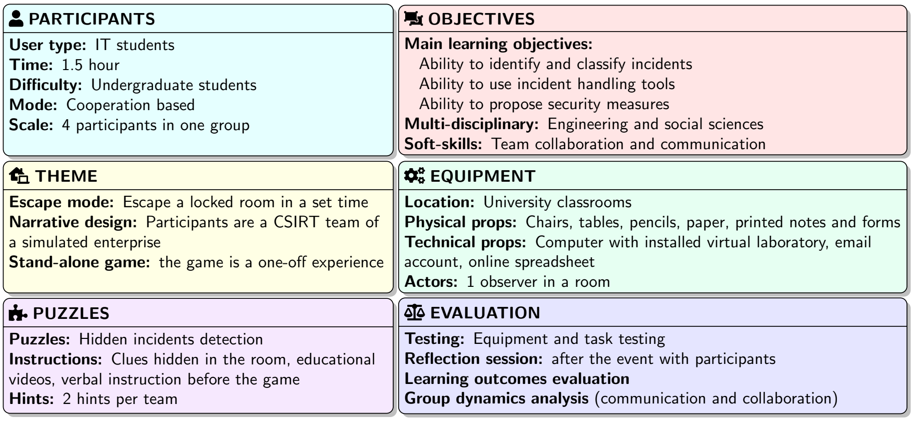
The incident containment, eradication, and recovery phase aims to resolve the cybersecurity incident. The phase requires decision-making on incident containment (server disconnect, shut-down of the system, etc.), evidence gathering, and recovery from the incident. The third task of the students is to identify the root cause of the incident and associated vulnerabilities and to choose, apply, and describe immediate incident containment actions (related to LO2 and LO5). The fourth task is to reflect on the incident and propose control measures to minimize identified vulnerabilities in the future (related to LO3). It is associated with the last phase of the incident management life-cycle, i.e., post-detection activities.

Crisis communication is an essential part of all incident management life-cycle phases. The incident communication plan and communication channels (e.g., email, website, phone call, in person) are defined in the incident preparation phase to help CSIRT report the incidents to the relevant roles, such as CIO (Chief information officer), head of information security, system owner, and others. The actual crisis communication is ongoing through incident detection and analysis, discovery and recovery, and post-incident phases. The last task for the students is to create an incident report and choose the appropriate communication channel and internal and external report recipients (related to LO4).

6 Physical and Digital Environment

Figure 5 illustrates the CAPE pilot setup and key features. The research team executed the event for undergraduate students making groups of four members. Each group was located in a separate room and monitored by a dedicated observer. The participants had access to the virtual laboratory and office tools (email, online collaboration tools). An email address was created for each team. The organizers recorded five videos (less than 10 min each), and students could watch them before the event execution. The videos provided instructions, e.g., correctly filling the incident classification table, an overview of the incident response roles according to the NIST Incident Management Guide (Cichonski et al., 2012), or crisis communication recommendations supplemented by A Guide to Effective Incident Management Communications (Manley and McIntire, 2021). Also, the E-learning course included supplementary training material.

The game itself included various gamification elements described by Al-Rayes et al. (2022): feedback, points, rewards, leaderboards, challenges and quests, customization, and unlockable content. The participants could choose their role in the CSIRT team and act according to it to solve challenges. Some of the challenges could be solved only by completing the previous steps. The point system was introduced to evaluate the progress of



PARTICIPANTS

User type: IT students
Time: 1.5 hour
Difficulty: Undergraduate students
Mode: Cooperation based
Scale: 4 participants in one group

OBJECTIVES

Main learning objectives:
Ability to identify and classify incidents
Ability to use incident handling tools
Ability to propose security measures
Multi-disciplinary: Engineering and social sciences
Soft-skills: Team collaboration and communication

THEME

Escape mode: Escape a locked room in a set time
Narrative design: Participants are a CSIRT team of a simulated enterprise
Stand-alone game: the game is a one-off experience

EQUIPMENT

Location: University classrooms
Physical props: Chairs, tables, pencils, paper, printed notes and forms
Technical props: Computer with installed virtual laboratory, email account, online spreadsheet
Actors: 1 observer in a room

PUZZLES

Puzzles: Hidden incidents detection
Instructions: Clues hidden in the room, educational videos, verbal instruction before the game
Hints: 2 hints per team

EVALUATION

Testing: Equipment and task testing
Reflection session: after the event with participants
Learning outcomes evaluation
Group dynamics analysis (communication and collaboration)

Fig. 5 Setup of the CAPE pilot CyberEscape 1.0 (adapted from Clarke et al. (2017))

each task, indicate the team's place on a leaderboard, and show which team got the prize. Each task was worth a different number of points. The highest point score was associated with the crisis communication, while the role assignment was worth the lowest amount. Another challenging component of the game was limited time and the observer's presence in the room. It added the stress factor to the game. After the game, all teams received feedback on how good their performance was and what they missed during the game.

According to the scenario, the students got an overview of the fictional company, and the company staff (see Sect. 5.1) sent tasks and clues as notes or emails. Each team had to find hidden clues (physical, digital) and solve the tasks. The provided notes were insufficient to identify the incidents. Therefore, participants used Lego pieces hidden in the room to reconstruct the physical company infrastructure and determine that the company data storage and server room were in a flooded river area.

The phishing email contained a link to a form asking the receiver to apply for the training and to fill in the sensitive data. The email initiated the phishing campaign; thus, the team received complaint messages from the company employees, claiming their data had been leaked. The team had to reason that these events were linked.

The virtual laboratory, central CAPE component, utilized bare metal virtualization and nested virtualization technologies (see Fig. 6). The bare metal virtualization used the open-source Proxmox Virtual Environment (Proxmox VE) as a hypervisor based on the KVM hypervisor and Linux containers (LXC). Proxmox VE supported all the infrastructure necessary for a Denial-of-Service (DoS) simulation, e.g., virtual machines, containers, virtual networks, network rate limit, and centralized management of DoS scripts. The DoS attack was performed against the fictional company environment developed using nested virtualization. Each student group had an Ubuntu Desktop virtual machine with the Apache Web server deployed in a dedicated nested Proxmox VE hypervisor. Any remote communication with the virtual machine was lost during a DoS attack, and services like VNC and SSH were unavailable. Therefore, nested virtualization enabled direct connection to the virtual machine from the Proxmox VE hypervisor console.

Event participants could trace and analyze this DoS attack using the network protocol analyzer Wireshark. This incident required performing an additional task to decrypt a password using a hidden key for the virtual machine. Participants were expected to block the attack

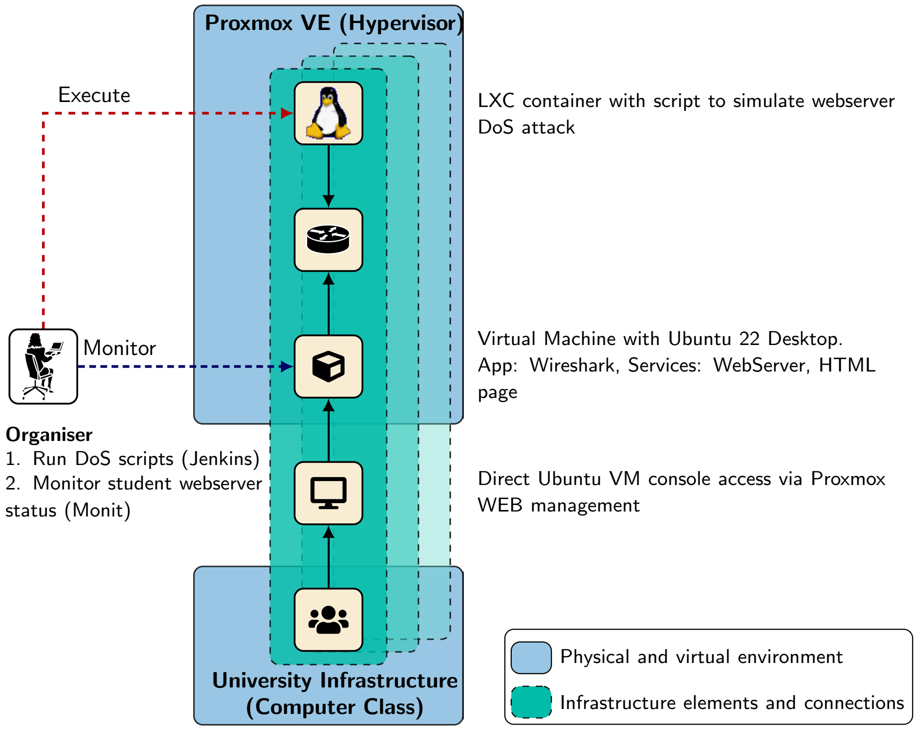

Proxmox VE (Hypervisor)
Execute
LXC container with script to simulate webserver DoS attack
Monitor
Virtual Machine with Ubuntu 22 Desktop. App: Wireshark, Services: WebServer, HTML page
Organiser
1. Run DoS scripts (Jenkins)
2. Monitor student webserver status (Monit)
Direct Ubuntu VM console access via Proxmox WEB management
University Infrastructure (Computer Class)
Physical and virtual environment
Infrastructure elements and connections

Fig. 6 Virtual laboratory architecture

using a virtual machine hypervisor firewall that simulated the company's main firewall in real life. The organizers executed DoS scripts from specially created LXC containers. Each LXC container attacked the specified hypervisor and the Ubuntu Apache Web server. The organizers managed the DoS attack from a separate virtual machine with the open-source automation server Jenkins installed. The dedicated Jenkins servers allowed to configure individual automatically executed scripts to perform different scenarios and set attack parameters for each student group, e.g., at specific and predefined time intervals.

The Hping3 network tool was used to simulate a Web server SYN Flood Attack—the most common and effective way to attack a Web server and make its services unavailable. The attack also made the entire virtual machine network adapter and all protocols unavailable. The open-source process supervision tool Monit enabled monitoring of the progress of the attack and the effectiveness of blocking.

The chosen architecture ensured a scalable, completely isolated environment for a safe DoS attack execution. Users could access it from any place via the Internet, and the attack automatization enabled the implementation of dynamic scenarios.

7 CyberEscape Delivery Results

Students were invited to participate and compete in the CAPE pilot, and five groups applied, with four students in each. The prerequisites for the students included: (1) Each student was associated with an undergraduate computer science or information technology study programme; (2) They completed at least the first semester of their studies; (3) Their study experience included foundational courses in computer science and information technology (computer networks and operating systems, algorithms and programming).

The study included a quantitative and qualitative assessment according to the evaluation methodology presented in Table 2. All defined evaluation criteria and measurements were applied, considering the main areas of the results: student competence (related to the LO1, LO2, LO3, LO4, and LO5), student behavior (LO6 and L07), and training approach (LO8 and LO9).

7.1 Student Competence

Students demonstrated the ability to solve practical tasks with an average score of 60% and the best score of 80%. Table 3 provides the scores of the groups per task. The scores are

Table 3 Competence, task, and score (% of total score)

Competence / Task	Score (% of total score)
To identify and classify cybersecurity incidents (LO1)	Team 1: 66%
Task 2: Incident detection and classification	Team 2: 100%
	Team 3: 50%
	Team 4: 60%
	Team 5: 63%
To reactively mitigate cybersecurity incidents (LO2)	Team 1: 100%
Task 3: Incident recovery measures definition	Team 2: 0%
	Team 3: 100%
	Team 4: 0%
	Team 5: 100%
To proactively mitigate cybersecurity incidents (LO3)	Team 1: 33%
Task 4: Security measures definition	Team 2: 100%
	Team 3: 33%
	Team 4: 0%
	Team 5: 67%
To communicate confidently in a crisis situation (LO4)	Team 1: 65%
Task 5: Crisis communication	Team 2: 100%
	Team 3: 38%
	Team 4: 81%
	Team 5: 69%
To use incident handling tools (LO5)	Team 1: 100%
Task 2: Incident detection and classification (logical incident)	Team 2: 50%
Task 4: Security measures definition (logical incident)	Team 3: 100%
	Team 4: 50%
	Team 5: 50%

based on M1–5, considering trainer qualitative evaluation (M1, M3, and M4) and trainer evaluation using monitoring tools (M2 and M5). For example, three teams performed well in defining recovery measures for reactive incident mitigation, but two failed.

The result was perceived as good, given the students' low competences in the study field before the assignment and the time constraints. The majority of the students declared low previous knowledge about cybersecurity and incident response.

The students filled out questionnaires to perform competence screening before and after the CyberEscape pilot execution, as presented in the data collection phases (see Fig. 2). The self-assessment questionnaire included ten questions that represented knowledge topic groups, and each group was mapped to the learning outcomes:

K-01 Team collaboration in a crisis situation (LO6)
K-02 Typical incidents, threats, and vulnerabilities (L02)
K-03 Crisis communication (LO4)
K-04 Incident response roles (L06)
K-05 Operating systems, servers, clouds, and infrastructures (LO1–LO2)
K-06 Incident handling tools (LO5)
K-07 Incident response (LO1–LO3)
K-08 Computer networks and operating systems security (LO1–LO2)
K-09 Incident handling standards, methodologies, and frameworks (LO1–LO4, LO6)
K-10 Cybersecurity related laws, regulations, and legislations (LO4)

The 10-point scale was used for competence self-reporting, where value 1 meant low competence level, and value 10 – high. Self-assessment reports (M9) of the students showed an improvement in all considered competences, as presented in Fig. 7. The figure shows mean values.

Table 4 provides the statistical results of the Welch Two Sample *t* test.

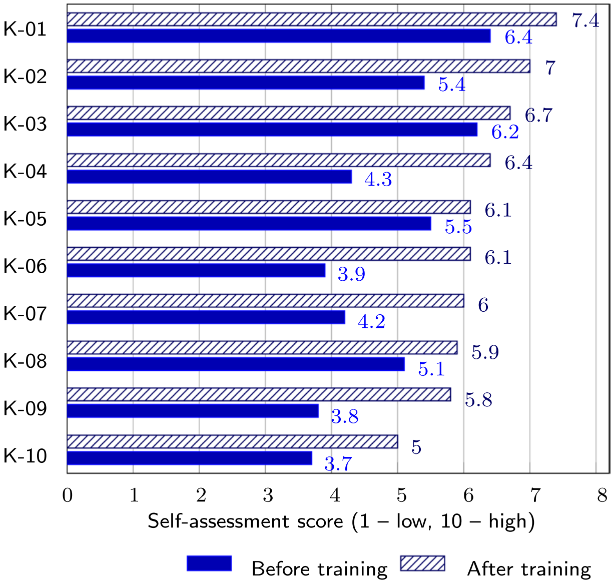


Fig. 7 Student competences self-assessment (N=20 before CyberEscape, N=19 after CyberEscape)

Table 4 Standard deviations (SD) in responses before (B) and after (A) CyberEscape and *p* values according to Welch Two Sample *t* test

	K-01	K-02	K-03	K-04	K-05	K-06	K-07	K-08	K-09	K-10
SD (B)	2.68	2.81	2.65	2.59	2.42	2.73	2.29	2.4	2.63	2.32
SD (A)	2.5	1.96	2.7	2.12	2.26	1.93	1.86	2.23	2.14	2.29
p	0.251	**0.047***	0.576	**0.007***	0.387	**0.007***	**0.01***	0.292	**0.011***	0.076

*p <=0.005

The most considerable increase was observed in improving the knowledge of the Incident response roles (K-04) and management of Incident handling tools (K-06). Statistical analysis shows a significant change, $p<0.05$ (see Table 4). The incident management team setup was integrated in the practical task of roles and responsibilities definition of the CSIRT team (Task 1). The practical tasks of incident detection and recovery required applying incident handling tools as part of the virtual laboratory (Tasks 2–3). Statistically, a significant change was observed in Incident response (K-07) and Incident handling standards, methodologies, and frameworks (K-09).

The CyberEscape session did not significantly improve the knowledge areas of Crisis communication (K-03) and Operating systems, servers, clouds, and infrastructures (K-05). The practical task required preparing the communication message and selecting recipients as a crisis communication activity (Task 5). Students self-reported being highly skilled in crisis communication before the event. However, the interviews revealed they had not applied during the event. The slight competence increase may be due to an overly high initial assessment. Another knowledge area, Operating systems, servers, clouds, and infrastructures (K-05), was a prerequisite for training (see prerequisites at the beginning of Sect. 7).

7.2 Student Behavior

Pilot participants admitted an increase in relevant competences. However, team collaboration (LO6) was a critical success factor, requiring more team cooperation experience, measured by observers' notes and interviews (M7). Each team nominated a leader, and observers identified mostly servant-leadership style, one of the suggested leadership styles in cybersecurity (Cleveland and Cleveland, 2018). Teams with previous experience working together demonstrated more efficient execution of tasks, which is a typical pattern in team collaboration. This feature indicates the importance of teamwork requiring exercises in cybersecurity education.

TWLQ (Sellers et al., 2014) was used to measure team workload demands (M6). The TWLQ Items are scored on an 11-point Likert scale (from very low to very high), with higher scores indicating higher levels of subjective workload. The TWLQ has two dimensions, the Teamwork component (communication, coordination, team performance monitoring) and the Task-Team component (time-share, team emotion, team support). The TWLQ shows good reliability on all subscales (Cronbach's a > .70) and also for this research (Teamwork Cronbach's a = .673; Task-team Cronbach's a = .626). Statistical analysis was done with JASP version 0.16.1. for Windows operating system. All variables were not normally distributed; therefore, non-parametric analyses were used. Alpha levels for hypothesis testing were set at the 0.05 level. A multiple linear regression was computed with the TWLQ entered as predictors and the score of the teams as the dependent variable.

The participants rated team collaboration and communication effectiveness as good, 8.6 and 8 points of 10, respectively.

However, the teams have faced some difficulties, such as time-share demand, e.g., sharing and managing time between task-work (work done individually) and team-work (work done as a team). Table 5 provides descriptive statistics and correlations (ρ) for the outcome score and workload items.

To see the influence of team workloads on performance, hierarchical multiple regressions were performed where Team Workloads were entered in the first step and Task-team workloads entered in the second step. Performance outcome variable was computed from combining the total score with the time taken. Team workloads (Communication $\beta = -.249$, Coordination $\beta = .543$, Team Performance Monitoring $\beta = .090$) positively predicted team performance in the exercise ($R^2 = .560$, $F = 6.36$, $p = .005$) but task-team workloads factors (team support $\beta = .522$, team emotional demand $\beta = -.058$, time share demands $\beta = .098311$) were not significant in influencing performance ($\Delta R^2 = .152$, $F = 2.12$, $p = .152$).

Metacognitive aspects (mood, judgment of performance) were measured for understanding how individual aspects influenced performance. To measure initial emotional states a SAM was used (Bradley & Lang, 1994b) where mood (negative to positive), physiological activation (not activated—over activated), and control (no control—dominance) was measured on a 9-point Likert-scale (−5 to +5) and is used in performance research across domains and populations, including cyber settings (DeFalco et al., 2018; Paquette et al., 2016) (measurement M7).

The emotion demand was rated below average (3.0 points out of 10), and the majority of the students stated that they did not have to control their emotions. The students reflected that they mainly faced positive emotions (excitement, joy) as the game integrated funny character descriptions. Meanwhile, the technical task execution was also related to some negative emotions, such as hopelessness. Team members' encouragement helped peers deal with emotions. Team support difficulties were rated below the average (4.4 points). Most students stated that it was not difficult to provide and receive support from team members (providing guidance, helping team members, etc.). The performance monitor demand (individual and team) was rated as average (5.8 and 4.1, respectively). Individual performance monitoring was more required than team performance monitoring. Team leaders

Table 5 Descriptive statistics and correlations (ρ) (19 responses)

Item	Mean	SD	1	2	3	4	5	6	7
Outcome score	31.98	21.15	–						
Communication d	8.00	1.92	.125	–					
Coordination d	6.32	2.50	.527*	.519*	–				
Team Perf. Monit. d	4.11	2.58	.274	.311	.480*				
Time Share d	5.79	3.14	.581*	.033	.520*	.450	–		
Team Support	4.37	3.22	.147	-.170	.096	.300	.519*	–	
Team Emotion d	3.05	2.97	.366	.423	.346	.330	.605**	.253	–

$^{*}p < .05$, $^{**}p < .01$, $^{***}p < 0.001$

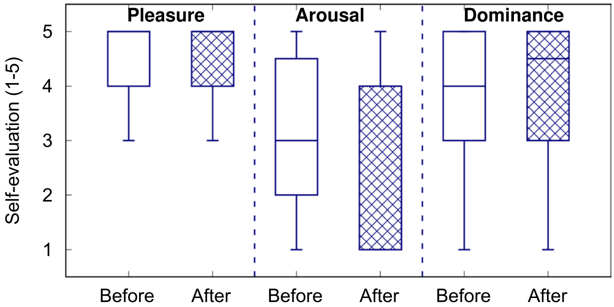


Fig. 8 Participant emotions before and after the execution (19 responses)

Table 6 Group means on initial states (SAM) and total scores

Group	Mood	Activation	Control	Total score
1	4.25	2.50	4.00	20.80
2	4.00	2.25	3.25	27.50
3	5.00	2.75	4.75	70.00
4	4.50	3.50	3.25	19.30
5	4.50	4.75	3.50	18.00

rated team performance monitoring slightly higher than team members (0.8 points). The average performance monitor demand might be related to relatively low team maturity. The teams' dissatisfaction level was low (2.4 points).

The SAM results show that the participants emotions have been similar before and after the exercise (see Fig. 8).

The level of pleasure remained at approximately the same level (median stays at value 5), the excitement level decreased a bit after the game (from 3.9 to 3.75 points as a mean, but the median increases), the control level remained unchanged (3.15 points, but the median is higher after the game). The observers did not note typical psychical signs of the stress (Whitehouse et al., 2022), such as groom, hand-to-face, hand-to-mouth, scratching, yawning, fumbling, twisting the mouth, licking lips and biting lips. To see the impact of initial states (mood, activation, control) on performance, group means of SAM scores and performance were explored (see Table 6).

Mean activation of a group was inversely related to performance scores. Being too overly activated is related to anxious states and this has been shown to negatively influence performance in cyber domain (Ask et al., 2021). Team #3, which performed best, also had the highest mood and control means, while reporting lower of physiological activation. To further analyse the influence of initial states, the group scores were ranked as the highest score was significantly larger than all other scores. A logistic regression was performed to ascertain the effects of initial states on the team ranking. The model was statistically significant, $\chi^2(3) = 9.23, p = .026$). The model explained 38.5 percent (Nagelkerke R^2) of the variance in ranking where only physiological activation significantly predicted the participant's ranking ($\beta = .895, p = .009$). Participants metacognitive judgments of performance was also calculated with a multiple regression where initial judgement of performance scores were controlled for and their post exercise judgment of performance was entered in the second step. Metacognitive judgements could predict performance scores

($R^2 = .362, F = 3.12, p = .043$ 1-tailed) and post exercise metacognitive judgements was significant ($\beta = .644, t = 2.54, p = .032$). Post exercise reflection on performance could explain 36% of the participants score. Taken together, individual factors, both initial states and metacognition had significant influence on their performance.

7.3 Training Approach

The questionnaire included retrospective questions regarding CAPE-promoted student engagement (LO8) and self-efficacy (LO7). The results demonstrated a high student engagement. The student engagement was measured using self-assessment questionnaires (M8). The questionnaire included a statement, "The game increased my interest in cybersecurity," and students were asked to rate the statement using the 5-point Likert scale. Nearly 90% of the students stated that the CAPE game had increased their interest in cybersecurity. The interview data supported this result as students indicated they would be interested in similar future activities and inquired about further possibilities to study cybersecurity. All student groups admitted that the game was exciting and had a good atmosphere.

In addition, students reported increased self-efficacy and rated the game higher than the theoretical videos. Approximately 89% of students agreed that the CAPE improved IT incident management knowledge. Meanwhile, the value of the videos in competence improvement was acknowledged by app. 61% of students. Students suggested that the videos could include more technical tutorials, subtitles, and English terms to increase their perception. However, the participants evaluated the flipped learning approach positively. The participants also mentioned that they found the phishing incident distracting. However, this attack demonstrated possible situations from real life.

8 Discussion

Several key outcomes support the CAPE design. The integration of gamification elements, problem-based learning, and flipped classroom principles has proven effective in fostering crucial skills such as crisis communication, collaboration, self-regulation, and technical competencies within incident management scenarios. These educational strategies have significantly enhanced the engagement and practical skills of students, as evidenced by the study outcomes. Students' reflections and performance metrics further support the validity of the CAPE design. High levels of student engagement were reported, with about 90% of participants expressing increased interest in cybersecurity, validating the design's effectiveness in capturing student interest and enhancing educational outcomes. Moreover, assessments of student performance revealed improvements in IT incident management knowledge and self-efficacy, which were notably higher compared to traditional theoretical instruction methods.

The CAPE design differs from other innovative teaching methodologies in cybersecurity education, integrating multiple educational strategies. For instance, CyberCIEGE and other virtual platforms offer interactive environments where students can apply security policies in a controlled, simulated setting (Thompson & Irvine, 2015). However, these methods often focus more on individual learning. They cannot provide the same level of team-based problem-solving and communication training as CAPE's escape room approach offers. The CAPE approach also differs from traditional escape rooms (see Beguin et al. (2019)) as it can measure the usefulness of the exercises through feedback, student engagement, and soft skill outcomes compared to previous methods (Mello-Stark et al., 2020).

The case study (Long et al., 2017) emphasized that not all students successfully prepared before classes in a flipped classroom approach, and we observed this tendency in the performance of the CAPE pilot, CyberEscape, participants. Therefore, some pre-class assignments, e.g., quizzes, would be useful to prevent this problem but were not included in this game version to ensure the balance between the gaming experience and the learning process.

CAPE's effectiveness in improving competences in crisis communication, collaboration, self-regulation, and technical skills is a significant advancement over more traditional, non-interactive learning methods, which may not equally address the psychological and behavioral aspects important in cybersecurity professions. In conclusion, the CAPE design effectively enhances educational outcomes by utilizing engaging, practical approaches that improve both soft and hard skills necessary for incident management. The positive reflections and performance improvements of the students provide strong validation for the CAPE design's effectiveness.

9 Conclusions, Limitations, and Future Work

This paper proposed a reusable educational approach CAPE to advance diverse cybersecurity skills. The paper presented its design and preliminary evaluation to provide adaptable knowledge for other cybersecurity educational programs in similar environments. Despite the existence of numerous educational games, their designs often lack detailed descriptions of their underlying concepts. Our experiences can provide valuable insights for educators designing and implementing similar approaches. Meanwhile, the study also includes several limitations that need to be addressed in the future work.

9.1 Conclusions

The cybersecurity-focused escape room approach promotes field-specific competence development, integrating hard and soft skills. During the pilot execution, the students demonstrated enhanced proficiency in competencies related to incident response roles and tools. Solving complex cyber puzzles and tasks demanded efficient communication and collaboration, stimulated creative and critical thinking, and kept participants engaged. Additionally, engaging and humorous storytelling helped to maintain a positive atmosphere during the game. The game increased student interest in cybersecurity, potentially catalyzing them to consider related career paths.

The implementation of the game emphasized the significance of different psychological aspects related to incident managers. Participants' initial affective states, alongside metacognitive processes, were associated with group outcomes. Also, team workload demands focusing on communication, cooperation, and team performance monitoring were significant in team outcomes. Given the complex decision-making involved in cybersecurity management and operations, which often takes place in a dynamic environment, it is essential to consider both emotional and behavioral factors, as well as situational aspects (i.e., team workload demands) when devising flexible strategies for situational decision-making and problem-solving in designing cyber exercises.

9.2 Limitations

While innovative in integrating gamification and real-life simulation for cybersecurity education, the CAPE does present certain limitations, as highlighted in the paper. The setup of the CAPE methodology is time-consuming and requires both human and specific technical resources. Although considered a minor limitation due to its high adaptability and scalability, this feature could pose challenges in environments where resources are limited or rapid deployment is necessary. One significant limitation is the unbalanced distribution of skill application within small student groups. This point could lead to uneven learning experiences and outcomes among participants, as not all students may have equal opportunities to engage deeply with all aspects of the training scenario.

Another limitation of the research is the use of a self-made questionnaire for evaluating certain aspects of the program. Unlike the TWLQ and SAM, which have established external validity and have been validated by other studies, the self-made questionnaire lacks such validation. This absence of external validation makes interpretation of the results more challenging and should be reported as a limitation. Future research should aim to validate this instrument against established measures to improve the robustness of the findings.

Moreover, the CAPE design currently lacks mechanisms to track individual development comparably to traditional learning methods. This constraint makes it difficult to measure individual progress and effectively tailor educational interventions to individual needs. Lastly, the number of trainees was relatively small. Thus, the results should be treated as potential indications.

The listed limitations suggest areas for future development in the CAPE design, particularly in enhancing its resource efficiency, ensuring equitable skill development among all participants, and improving the tracking of individual learning outcomes.

9.3 Future Work

In the future, the CAPE design will be complemented with learning analytics components powered by computer vision and data science to identify participant behavior features automatically. Additionally, more comprehensive evaluation approach and indicators will be developed, taking into account factors such as student performance in practical tasks, tests, combined with observers questionnaires and other relevant aspects to avoid biased evaluation results.

Additionally, the CAPE design and study results demonstrate an opportunity for future research. The student self-assessment method enabled insights into student competence changes. Similarly, the results of questionnaires revealed the level of metacognitive skills. In the future, the analysis could be enhanced by incorporating structured results from the observer questionnaires and data from tools for analyzing emotions. The updated CAPE measures would help assess the performance of individual participants and identify the team's joint skill level.

Finally, there is a long-term vision to develop an international module for easy game replication in different educational environments.

Acknowledgements The authors thank the whole ADVANCES team for their feedback and support.

Funding 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).

Data Availability Upon request.

References

Aggarwal, A., & Dhurkari, R. K. (2023). Association between stress and information security policy noncompliance behavior: A meta-analysis. *Computers & Security, 124*, 102991. https://doi.org/10.1016/j.cose.2022.102991

Al-Rayes, S., Al Yaqoub, F. A., Alfayez, A., Alsalman, D., Alanezi, F., Alyousef, S., & Alanzi, T. M. (2022). Gaming elements, applications, and challenges of gamification in healthcare. *Informatics in Medicine Unlocked, 31*, 100974. https://doi.org/10.1016/j.imu.2022.100974

Ashley, T. D., Kwon, R., Gourisetti, S. N. G., Katsis, C., Bonebrake, C. A., & Boyd, P. A. (2022). Gamification of cybersecurity for workforce development in critical infrastructure. *IEEE Access, 10*, 112487–112501. https://doi.org/10.1109/access.2022.3216711

Ask, T.F., Sütterlin, S., Knox, B.J., Lugo, R.G. (2021). Situational states influence on team workload demands in cyber defense exercise. Hci international 2021-late breaking papers: Cognition, inclusion, learning, and culture: 23rd hci international conference (pp. 3–20).

Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Don’t wanna cry: A cyber crisis table top exercise for assessing the preparedness against eminent threats. *International Journal of Engineering and Advanced Technology, 9*, 3705–3710. https://doi.org/10.35940/ijeat.A9893.109119

Baig, M., & Yadegaridehkordi, E. (2023). Flipped classroom in higher education: A systematic literature review and research challenges. *International Journal of Educational Technology in Higher Education, 20*, 61. https://doi.org/10.1186/s41239-023-00430-5

Beguin, E., Besnard, S., Cros, A., Joannes, B., Leclerc-Istria, O., Noel, A., & Alata, E. (2019). Computer security oriented escape room. *IEEE Security & Privacy, 17*(4), 78–83. https://doi.org/10.1109/MSEC.2019.2912700

Beuran, R., Tang, D., Pham, C., Chinen, K., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: Cytrone. *Computers & Security, 78*, 43–59. https://doi.org/10.1016/j.cose.2018.06.001

Braad, E., Degens, N., IJsselsteijn, W.W. (2019). Meco: A digital card game to enhance metacognitive awareness. *Proceedings of the 12th European conference on game based learning*, ECGBL (pp. 92–100).

Bradley, M. M., & Lang, P. J. (1994). Measuring emotion: The self-assessment manikin and the semantic differential. *Journal of Behavior Therapy and Experimental Psychiatry, 25*(1), 49–59. https://doi.org/10.1016/0005-7916(94)90063-9

Bradley, M. M., & Lang, P. J. (1994). Measuring emotion: The self-assessment manikin and the semantic differential. *Journal of Behavior Therapy and Experimental Psychiatry, 25*(1), 49–59. https://doi.org/10.1016/0005-7916(94)90063-9

Budimir, S., Fontaine, J., Huijts, N., Haans, A., Loukas, G., & Roesch, E. (2020). Emotional reactions to cybersecurity breach situations: A scenario-based survey study. *Journal of Medical Internet Research, 23*, e24879. https://doi.org/10.2196/24879

Calvano, M. , Caruso, F. , Curci, A. , Piccinno, A., Rossano, V. (2023). A rapid review on serious games for cybersecurity education: Are “serious” and gaming aspects well balanced? Joint proceedings of the workshops, work in progress demos and doctoral consortium at the IS-EUD 2023 co-located with the 9th international symposium on end-user development, IS-EUD (vol. 3408). CEUR-WS.org. https://ceur-ws.org/Vol-3408/short-s3-05.pdf

Center for Infrastructure Assurance & Security (2023). Cyber Threat Defender – The UTSA CIAS. University of Texas at San Antonio. https://cias.utsa.edu/ctd/ Accessed: February 1, 2023.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy, 12*(5), 61–67. https://doi.org/10.1109/MSP.2014.85

Cho, H., Zhao, K., Lee, C., Runshe, D., & Krousgrill, C. (2021). Active learning through flipped classroom in mechanical engineering: Improving students' perception of learning and performance. *International Journal of STEM Education*. https://doi.org/10.1186/s40594-021-00302-2

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security, 97*, 101931. https://doi.org/10.1016/j.cose.2020.101931

Cichonski, P., Millar, T., Grance, T., Scarfone, K. (2012). Computer security incident handling guide NIST Special Publication 800-61 Revision. National Institute of Standards and Technology.

Clarke, S. J., Peel, D. J., Arnab, S., Morini, L., Keegan, H., & Wood, O. (2017). EscapED: A framework for creating educational escape rooms and interactive games to for higher/further education. *International Journal of Serious Games, 4*, 3. https://doi.org/10.17083/ijsg.v4i3.180

Cleveland, S., & Cleveland, M. (2018). Toward cybersecurity leadership framework. The thirteenth midwest association for information systems conference proc. (pp. 49). Retrieved May 17, 2023 from https://aisel.aisnet.org/mwais2018/49.

Debello, J.E. , Schmeelk, S. , Dragos, D.M. , Troja, E., & Truong, L.M. (2022). Teaching effective cybersecurity through escape the classroom paradigm. *IEEE global engineering education conference* (pp. 17–23).

Decusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., & Mah, B. (2022). A cybersecurity awareness escape room using gamification design principles. In *12th IEEE annual computing and communication workshop and conference* (pp. 765–770).

DeFalco, J. A., Rowe, J. P., Paquette, L., Georgoulas-Sherry, V., Brawner, K., Mott, B. W., & Lester, J. C. (2018). Detecting and addressing frustration in a serious game for military training. *International Journal of Artificial Intelligence in Education, 28*, 152–193. https://doi.org/10.1007/s40593-017-0152-1

Department of Defense (2023). Cyber Protect—DoD Cyber Exchange. Retrieved February 1, 2023 from https://public.cyber.mil/training/cyber-protect/.

Dörner, R., Göbel, S., Effelsberg, W., & Wiemeyer, J. (2016). Introduction. In R. Dörner, S. Göbel, W. Effelsberg, & J. Wiemeyer (Eds.), *Serious games: Foundations, concepts and practice* (pp. 1–34). Cham: Springer International Publishing.

Duncan, K. (2020). Examining the effects of immersive game-based learning on student engagement and the development of collaboration, communication, creativity and critical thinking. *TechTrends, 64*, 514–524. https://doi.org/10.1007/s11528-020-00500-9

Efklides, A. (2008). Metacognition: Defining its facets and levels of functioning in relation to self-regulation and co-regulation. *European Psychologist, 13*(4), 277–287. https://doi.org/10.1027/1016-9040.13.4.277

Efklides, A. (2011). Interactions of metacognition with motivation and affect in self-regulated learning: The MASRL model. *Educational Psychologist, 46*(1), 6–25. https://doi.org/10.1080/00461520.2011.538645

European Union Agency for Cybersecurity (2022). European cybersecurity skills framework (ECSF). ENISA reports. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles Accessed: February 1, 2023.

Flavell, J. H. (1979). Metacognition and cognitive monitoring: A new area of cognitive-developmental inquiry. *American Psychologist, 34*(10), 906. https://doi.org/10.1037/0003-066X.34.10.906

Ghosh, T., & Francia, G. (2021). Assessing competencies using scenario-based learning in cybersecurity. *Journal of Cybersecurity and Privacy, 1*(4), 539–552. https://doi.org/10.3390/jcp1040027

Gilboy, M. B., Heinerichs, S., & Pazzaglia, G. (2015). Enhancing student engagement using the flipped classroom. *Journal of Nutrition Education and Behavior, 47*(1), 109–114. https://doi.org/10.1016/j.jneb.2014.08.008

Gordillo, A., & López-Fernández, D. (2024). Are educational escape rooms more effective than traditional lectures for teaching software engineering? A randomized controlled trial. *IEEE Transactions on Education*. https://doi.org/10.1109/TE.2024.3403913

Greene, J. C. (2012). Engaging critical issues in social inquiry by mixing methods. *American Behavioral Scientist, 56*(6), 755–773. https://doi.org/10.1177/0002764211433794

Gross, J. J. (1998). The emerging field of emotion regulation: An integrative review. *Review of General Psychology, 2*(3), 271–299. https://doi.org/10.1037/1089-2680.2.3.27

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems, 19*(2), 87–92.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

Hew, K. F., Bai, S., Dawson, P., & Lo, C. K. (2021). Meta-analyses of flipped classroom studies: A review of methodology. *Educational Research Review, 33*, 100393. https://doi.org/10.1016/j.edurev.2021.100393

Hmelo-Silver, C. (2004). Problem-based learning: What and how do students learn? *Educational Psychology Review, 16*, 235–266. https://doi.org/10.1023/B:EDPR.0000034022.16470.f3

IEEE (2017). Guide to the enterprise information technology body of knowledge (EITBOK) [Computer software manual]. Retrieved May 17, 2023 from http://eitbokwiki.org/Main_Page.

Klein, G., Ross, K. G., Moon, B. M., Klein, D. E., Hoffman, R. R., & Hollnagel, E. (2003). Macrocognition. *IEEE Intelligent Systems, 18*(3), 81–85. https://doi.org/10.1109/MIS.2003.1200735

Krath, J., Schürmann, L., & von Korflesch, H. F. (2021). Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. *Computers in Human Behavior, 125*, 106963. https://doi.org/10.1016/j.chb.2021.106963

Kuckartz, U. (2014). *Qualitative text analysis: A guide to methods, practice & using software*. SAGE Publications Ltd.

Kvietinskaitė, G., Bukauskas, L., & Krinickij, V. (2022). Cyber security table-top exercise gamification with dynamic scenario for qualification assessment. *Communications in Computer and Information Science, 1654*, 54–62. https://doi.org/10.1007/978-3-031-19679-98

Kyytsöen, M., Ikonen, J., Aalto, A. M., & Vehko, T. (2022). The self-assessed information security skills of the finnish population: A regression analysis. *Computers & Security, 118*, 102732. https://doi.org/10.1016/j.cose.2022.102732

Lemay, A. , Leblanc, S.P., de Jesus, T. (2015). Lessons from the strategic corporal: Implications of cyber incident response. *Proc. of the ACM Sigmis conference on computers and people research* (pp. 61–66).

Letsky, M. , Warner, N. , Fiore, S.M. , Rosen, M., Salas, E. (2007). Macrocognition in complex team problem solving (Tech. Rep.). Office of Naval Research Arlington VA. Retrieved May 17, 2023 from https://apps.dtic.mil/sti/citations/ADA481422.

Long, T., Cummins, J., & Waugh, M. (2017). Use of the flipped classroom instructional model in higher education: Instructors' perspectives. *Journal of Computing in Higher Education, 29*, 179–200. https://doi.org/10.1007/s12528-016-9119-8

López-Belmonte, J., Segura-Robles, A., Fuentes-Cabrera, A., & Parra-González, M. E. (2020). Evaluating activation and absence of negative effect: Gamification and escape rooms for learning. *International Journal of Environmental Research and Public Health, 17*, 7. https://doi.org/10.3390/ijerph17072224

Löffler, E., Schneider, B., Asprion, P. M., & Zanwar, T. (2021). CySecEscape 2.0–A virtual escape room to raise cybersecurity awareness. *International Journal of Serious Games, 8*, 59–70. https://doi.org/10.17083/ijsg.v8i1.413

Malone, M., Wang, Y., James, K., Anderegg, M., Werner, J., & Monrose, F. (2021). To Gamify or Not? On leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention. *Proc. of the 52nd acm technical symposium on computer science education* (pp. 1135–1141).

Manley, B., & McIntire, D. (2021). A guide to effective incident management communications [Computer software manual]. Retrieved May 17, 2023 from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651816.

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security, 112*, 102526. https://doi.org/10.1016/j.cose.2021.102526

Meichenbaum, D. (1985). Metacognitive methods of instruction: Current status and future prospects. *Special Services in the Schools, 3*(1–2), 23–32. https://doi.org/10.1300/J008v03n01_03

Mello-Stark, S., VanValkenburg, M.A., & Hao, E. (2020). Thinking outside the box: Using escape room games to increase interest in cyber security. Innovations in cybersecurity education (pp. 39–53). Springer.

Murphree, C., & Vafa, S. (2020). Use of escape rooms in education. Proc. of society for information technology & teacher education international conference (pp. 1837–1842). Retrieved February 1, 2023 from https://www.learntechlib.org/p/215961.

Nieto-Escamez, F. A., & Roldán-Tapia, M. D. (2021). Gamification as online teaching strategy during COVID-19: A mini-review. *Frontiers in Psychology*. https://doi.org/10.3389/fpsyg.2021.648552

Ogbanufe, O., & Ge, L. (2023). A comparative evaluation of behavioral security motives: Protection, intrinsic, and identity motivations. *Computers & Security, 128*, 103136. https://doi.org/10.1016/j.cose.2023.103136

Onwubiko, C., & Ouazzane, K. (2022). Soter: A playbook for cybersecurity incident management. *EEE Transactions on Engineering Management, 69*(6), 3771–3791. https://doi.org/10.1109/TEM.2020.2979832

Papaioannou, T., Tsohou, A., Bounias, G., & Karagiannis, S. (2022). A constructive approach for raising information privacy competences: The case of escape room games. Trust, privacy and security in digital business, TrustBus (pp. 33–49).

Paquette, L., Rowe, J., Baker, R., Mott, B., Lester, J., DeFalco, J., & Georgoulas, V. (2016). Sensor-free or sensor-full: A comparison of data modalities in multi-channel affect detection. (pp. 93–100). ERIC. Retrieved May 17, 2023 from https://eric.ed.gov/?id=ED560545.

Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B. J., Lapin, K., Parish, K., & Lugo, R. G. (2022). Application of intervention mapping in cybersecurity education design. *Frontiers in Education*. https://doi.org/10.3389/feduc.2022.998335

Pouralvar, K., Sekhavat, Y.A., & Roohi, S. (2019). The interplay between metacognitive strategies and learning styles in learning via serious games. 2019 international serious games symposium, ISGS (pp. 129–134).

Salas, E., DiazGranados, D., Klein, C., Burke, C. S., Stagl, K. C., Goodwin, G. F., & Halpin, S. M. (2008). Does team training improve team performance? A meta-analysis. *Human Factors, 50*(6), 903–933. https://doi.org/10.1518/001872008X375009

Sellers, J., Helton, W. S., Näswall, K., Funke, G. J., & Knott, B. A. (2014). Development of the team workload questionnaire (TWLQ). *Proc. of the Human Factors and Ergonomics Society 58th Annual Meeting, 58*(1), 989–993. https://doi.org/10.1177/1541931214581207

Shah, A., Ganesan, R., Jajodia, S., Cam, H., & Hutchinson, S. (2023). A novel team formation framework based on performance in a cybersecurity operations center. *IEEE Transactions on Services Computing, 13*, 1–13. https://doi.org/10.1109/TSC.2023.3253307

Smieszek, H., & Rußwinkel, N. (2013). Micro-cognition and macro-cognition: trying to bridge the gap. Proc. of the 10th berlin workshop on human-machine systems: Foundations and applications of human-machine interaction (pp. 335–341).

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy, 13*(4), 20–29. https://doi.org/10.1109/MSP.2015.71

Subhash, S., & Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. *Computers in Human Behavior, 87*, 192–206. https://doi.org/10.1016/j.chb.2018.05.028

Thompson, M. F., & Irvine, C. E. (2015). CyberCIEGE: A video game for constructive cyber security education. *Call Signs, 6*(2), 4–8. https://doi.org/10.1016/j.cose.2006.10.005

Vykopal, J., Čeleda, P., Seda, P. , Švábenský, V., Tovarňák, D. (2021). Scalable learning environments for teaching cybersecurity hands-on. IEEE Frontiers in Education Conference, FIE (pp. 1–9).

Weickert, T. D., Joinson, A., & Craggs, B. (2023). Is cybersecurity research missing a trick? Integrating insights from the psychology of habit into research and practice. *Computers & Security, 128*, 103130. https://doi.org/10.1016/j.cose.2023.103130

Whitehouse, J., Milward, S. J., Parker, M. O., Kavanagh, E., & Waller, B. M. (2022). Signal value of stress behaviour. *Evolution and Human Behavior, 43*(4), 325–333. https://doi.org/10.1016/j.evolhumbehav.2022.04.001

Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Springer.

Wolf, S., Klein, G., Thordsen, M., & Klinger, D. (1991). Factors affecting the decision making of fire direction officers (Tech. Rep. No. Final Technical Report prepared under Contract DAAA15-90-C-1054). Yellow Springs, OH:Klein Associates, Inc.

Wolfenden, B. (2019). Gamification as a winning cyber security strategy. *Computer Fraud & Security, 2019*(5), 9–12. https://doi.org/10.1016/S1361-3723(19)30052-1

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Computers & Security, 110*, 102450. https://doi.org/10.1016/j.cose.2021.102450

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review, 55*, 1029–1053. https://doi.org/10.1007/s10462-021-09976-0

Zumbach, J., Rammerstorfer, L., & Deibl, I. (2020). Cognitive and metacognitive support in learning with a serious game about demographic change. *Computers in Human Behavior, 103*, 120–129. https://doi.org/10.1016/j.chb.2019.09.026

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security, 102*, 102154. https://doi.org/10.1016/j.cose.2020.102154

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Rūta Pirta-Dreimane[1] · Agnė Brilingaitė[2] · Evita Roponena[1] · Karen Parish[3] · Jānis Grabis[1] · Ricardo Gregorio Lugo[4] · Mārtiņš Bonders[1]

✉ Rūta Pirta-Dreimane
Ruta.Pirta-Dreimane@rtu.lv

Agnė Brilingaitė
Agne.Brilingaite@mif.vu.lt

Evita Roponena
Evita.Roponena@rtu.lv

Karen Parish
Karen.Parish@inn.no

Jānis Grabis
Grabis@rtu.lv

Ricardo Gregorio Lugo
Ricardo.G.Lugo@hiof.no

Mārtiņš Bonders
Martins.Bonders@rtu.lv

[1] Institute of Information Technology, Riga Technical University, Zunda Krastmala 10, Riga 1048, Latvia

[2] Institute of Computer Science, Vilnius University, Didlaukio str. 47, 08303 Vilnius, Lithuania

[3] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Postboks 191, 2802 Gjøvik, Norway

[4] Faculty of Health, Welfare and Organisation, Østfold University College, B.R.A. Veien 4, 1757 Halden, Norway