International Journal of Information Security (2023) 22:1531–1546
https://doi.org/10.1007/s10207-023-00704-z

REGULAR CONTRIBUTION

A personalized learning theory-based cyber-security training exercise

Nabin Chowdhury[1] · Vasileios Gkioulos[1]

Accepted: 3 May 2023 / Published online: 2 June 2023

Abstract

Current enterprises' needs for skilled cyber-security (CS) professionals have prompted the development of diverse CS training programs and offerings. It has been noted that even though enterprise staff is now more aware of security threats, the number of successful attacks against companies has all but decreased over the years. Several criticisms were raised against current CS training offerings, which often made them inadequate, or unable to change participants' behavior and security attitude. One of the main factors CS training programs are often not very effective is the lack of engagement or motivation of participants. This is often the result of training not being tailored to the needs or preferences of participants. In our previous work, we tackled this issue by developing a personalized learning theory-based model for developing CS training frameworks. In this work, we utilize the model to develop two CS training exercises: two game-based scenarios using the CS training video game Cyber CIEGE and one table-top team exercise. The exercises are later tested by involving a group of 12 students from the Norwegian Institute of Science and Technology (NTNU) Information Security master's degree program. According to the results of the experiment and the feedback from the students, students felt more engaged during the exercises due to having been participants in their development process. This has in turn motivated them to continue using the training tools independently in their spare time. Further research is recommended to establish whether the training development model is adequate for different target groups, as well as better performing than other models when developing full-fledged training programs.

Keywords Cyber-security · Personalized learning theory · Video game · Table-top

1 Introduction

The threat of cyber-attacks against service providing companies has steadily increased over the years. According to recent reports, it was found that over the last 10 years the number of successful malware attacks has steadily increased year-over-year [1], with damage caused by ransomware estimated to be exceeding $7.5 billion in 2019 alone [2]. Moreover, it is reported that cyber attacks costs totalled $6.5 trillion in 2021, with experts predicting this cost to exceed $10.5 trillion annually by 2025 [3]. One of the primary targets of these attacks are often private and public companies and enterprises. Due to the key roles some of these enterprises and businesses play in today's society, especially if they are involved in a nation's critical infrastructure, the damages caused by successful attacks can greatly impact national and international economies and functions.

An example of such an event are the 2017 cyber attacks on Ukraine, which targeted local organizations, including banks, ministries, newspapers and electricity firms [4]. The Petya malware, a type of ransomware malware, was utilized by the attackers. By using the exploit, the attackers were able to switch off the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant, in addition to affecting several Ukrainian ministries, banks, metro systems and state-owned enterprises.

One of the key factors to the success of many of these attacks has been identified as the lack of personnel CS awareness or of an adequate CS response team inside of a company. According to a recent IBM study, 95% of CS breaches are the result or can be traced to human error [5]. To prevent this issue, a great deal of effort has been put into advancing CS education and teaching (intended as theoretical and abstract activities to impart CS knowledge [6]) as well as CS training

✉ Nabin Chowdhury
nabin.chowdhury@ntnu.no

Vasileios Gkioulos
vasileios.gkioulos@ntnu.no

[1] Norwegian University of Science and Technology (NTNU), Teknologivegen 22, 2815 Gjøvik, Norway

(intended as practical, hands-on activities to develop abilities [6]).

In the industry, a majority of companies address the need for action to be taken to prevent cyber incidents in their CS strategy [7]. These strategies are a compilation of the most effective optimal course of actions available to ensure the success of a cyber operation [8].

According to most modern CS strategies, one of the fundamental measures to incorporate for CS are ensuring that a company's personnel has a sufficient awareness of CS threats and is well-trained to respond to these. In fact, many companies implemented internal CS awareness and training programs to educate and train staff against common attack vectors and prepare them in case of emergency scenarios. Over the years, CS training has evolved to adjust to newer, more complex attacks, but also to accommodate user needs and preferences, in both content and training format. Moreover, research has also been conducted to establish uniform, methodological design structures and models for developing various types of CS training and CS exercises [9–11].

Nevertheless, research has shown that many of these forms of training still fail to engage participants and motivate them toward learning [12]. Lack of user engagement has been indicated in the literature as one of the main detractors to the effectiveness of CS training programs [12]. Motives for lack of engagement or motivation in CS training cited in the literature include use of tedious training delivery methods [12, 13], such as classroom training, as well as lack of initial consultation with target training participants during the development of training for the decision on topics, material and training delivery options. The effects of motivation on training have long been studied, with several studies and meta-studies analyzing the correlation between increased motivation pre and during training, to training outcome [14, 15]. Recent studies have further demonstrated how motivation is a key aspect in installing a successful cyber culture [16]. These factors motivated researchers to focus on delivering training that is more engaging, by adopting more captivating training delivery methods, such as game-based and simulation-based training [17–19].

Engagement is not the only factor affecting the outcome of a training session. Factors, such as cognition & metacognition [20], adaptability, and learning styles [21] have all been well-documented in research as of great impact to the effectiveness and results of training exercises.

To account for these factors in CS education, researchers have started incorporating knowledge regarding learning theory and instructional design into CS curricula [22, 23]. Learning taxonomies for digital learning environments, such as Bloom's digital taxonomy [24] and Webb's taxonomy have also been used in the literature to enhance CS education [25]. Additionally, in recent years, significant progress has also been made in the area of Personalized Learning Theory (PLT), which refers to providing training that is tailored to a specific individual, based on their learning objectives, learner's profile and overall preferences in learning [26].

Research efforts on using the aforementioned theoretical concepts regarding learning theory are on the other hand either lacking or at very initial stages when it comes to CS training exercises. As a matter of fact, according to our previous study in Chowdhury and Gkioulos [27], none of the current CS training offerings extensively incorporates these concepts to the training activities offered, focusing instead on the technical knowledge and abilities set as acquisition goals of the exercises.

In this work, we propose two CS exercises developed by using a CS training development framework founded in PLT concepts. This work is a continuation of our previous work in Chowdhury, Katsikas, and Gkioulos [28], where we proposed a model for developing CS training frameworks and validated the model through the use of the Delphi process. To provide practical validation of the model, we tested the developed exercises by involving a group of Master's students from the Norwegian University of Science and Technology (NTNU) Information Security faculty.

Specifically, the exercise is evaluated by conducting an experiment with 12 students from the Norwegian Institute of Science and Technology (NTNU) Information Security master's degree program. By involving participants in the development of the exercises and by collecting continuous feedback regarding their experience with the novel approach, the exercise will provide an initial appraisal of the use of PLT in CS training exercises.

The remainder of the work is organized as it follows. In Sect. 2, we introduce the main objectives of this work, as well as outline the overall scope of the article. In Sect. 3, we discuss background work we previously conducted on CS training framework modelling, as well as findings from the literature when it comes to recommendations and best practices in developing CS exercises. In Sect. 4, we analyze articles found in the literature discussing design suggestions and methods for CS exercises, as well as pedagogical and educational considerations when developing such exercises. In Sect. 5 we discuss the methodology used to develop the proposed exercises. In Sect. 6 we present the results of the test cases developed and finally in Sect. 7 we discuss the main conclusions and future plans and direction for further research.

2 Scope & objectives

The main goal of the experiment described in this work is to evaluate the applicability and effectiveness of cyber-security training exercises developed using the framework proposed in Chowdhury, Katsikas, and Gkioulos [28]. Specifically, the combination of the revised ADDIE model proposed in the previous work, in combination with PLT concepts will be implemented and evaluated, with particular focus on evaluating their effects on participants' engagement and feedback. Additionally, the results of this evaluation will be compared to the feedback provided by participants to provide a qualitative, comparative analysis of the exercise developed using the framework to other, more traditional exercises experienced by the participants. This evaluation is limited to the assessment of the aforementioned components and properties of the framework. Evaluation of applicability of the framework to industrial personnel, and development of software-assisted forms of training are outside the scope of this work.

3 Background

To understand the methodology that is later used to develop the proposed CS exercises, in this section we introduce the model we previously proposed in Chowdhury, Katsikas, and Gkioulos [28] for developing CS training frameworks, together with additional considerations that influence the design of the proposed exercises. The overall methodology uses a revised version of the ADDIE (Analysis, Design, Development, Implementation, Evaluation) model, which had been integrated with key concepts of PLT and suggestions from expert stakeholders in the industry and academia, following a Delphi method evaluation.

While the overall design shown in Chowdhury, Katsikas, and Gkioulos [28] was developed for multimodular CS training, this design was adapted in this work for the development of individual CS exercises. More in detail, the following activities have been established as necessary during each phase of the ADDIE model:

- *Analysis Phase*: Establish training needs and goals. It is recommended to involve the selected target audience in the process, by both analyzing their preferences in training delivery, but also on whether the goals of training align with their current goals. Establish desired outcome establishment, pre-requirement definition, selection of possible learning environment and overall duration of training. Take in consideration any possible resource constraints. Revision should occur based on progressive feedback given by both training designers and participants on each established decision, until a majority agreement is reached on all attributes.
- *Design Phase*: Define overall structure of how the exercises will be conducted. Design phase must be both *systematic and specific* [29]. During the design phase, initial consideration for the following components should be made, which will later have to be completed during the development phase: decide type of training delivery method, making sure that take into consideration the individual-specific factors. Learning material should be developed based on the learning style of participants and their preferences.
- *Development Phase*: Develop an action plan, training resources and a pilot test, training scenarios and other hands-on activities that will be integrated in the training program, which will utilize the tools and learning environment selected in the previous phases. Consult with all of the involved stakeholders as well as the pilot test should be used.
- *Implementation Phase*: Engage participants in training; monitor the overall progress by collecting formative feedback.
- *Evaluation Phase*: Evaluation should be conducted formatively during design, development and implementation, with summative assessment to be conducted at the conclusion of the first implementation cycle and at any successive iteration.

Figure 1 summarizes the tasks to conduct during the revised ADDIE model

Additionally to overall methodology for design, development and implementation of training, several key attributes were highlighted as desirable when developing CS training exercises or CS training material. These attributes are listed below:

- Suitability
- Real-life experience
- Scalability & adaptability
- Accessibility
- Frequency of training and periodical updates
- Cost efficiency
- Consideration for the human factor

When it comes to training delivery methods, simulation-based and game-based solutions were suggested to be most effective in the literature [27, 30]. One of the main reasons these two methods were seen more advantageous than more traditional, classroom-based training were because they were found to be more engaging and consequentially more motivating [31, 32]. Tedious or non-engaging training solutions often fail to change employees' security behaviour and attitudes [33].

Finally, when it comes to training assessment, two methods in particular were noted to be more effective based on the findings of a panel of CS experts [28], these methods being feedback collection and comparison between pre and post-training performance. The combination of the two methods provides a complementary evaluation, as the former is a qualitative approach based on training participant input, while the

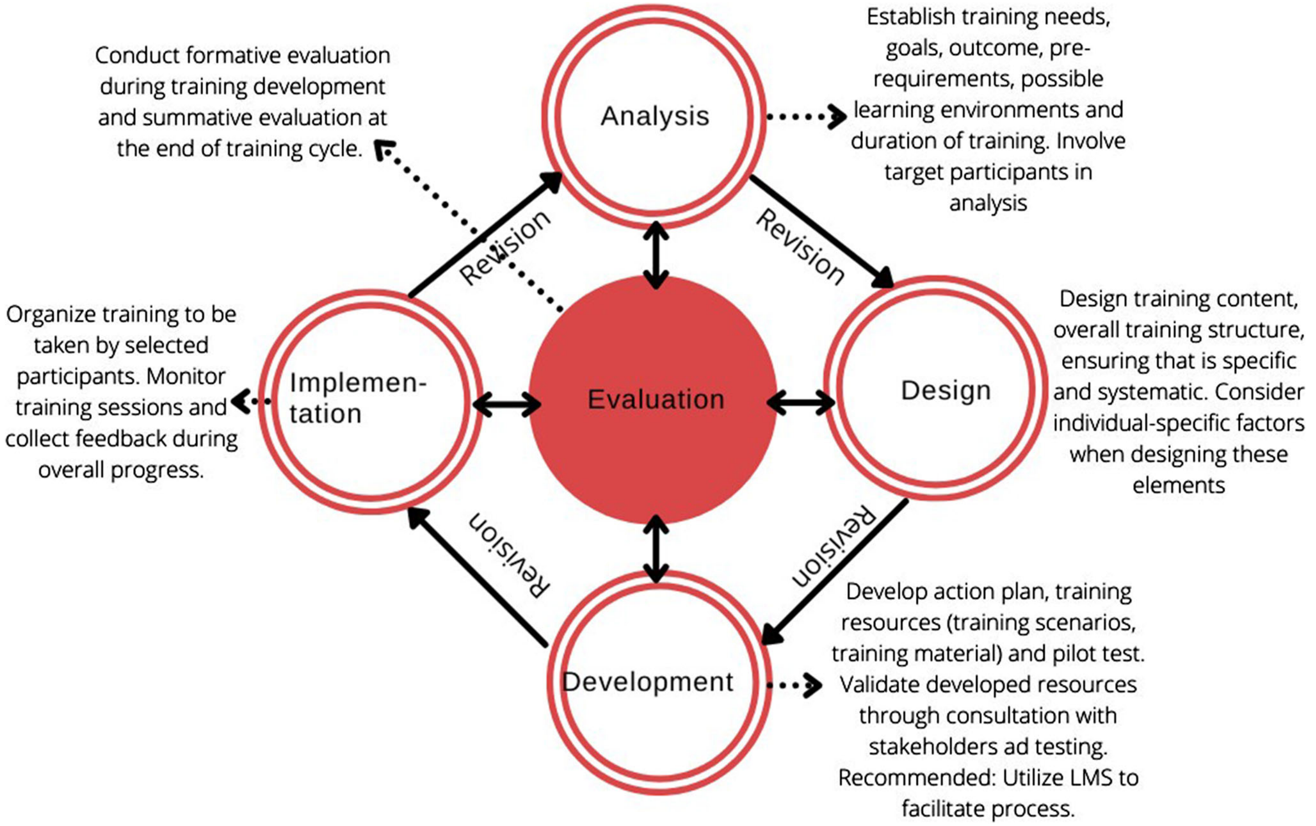

Analysis
Establish training needs, goals, outcome, pre-requirements, possible learning environments and duration of training. Involve target participants in analysis
Design
Design training content, overall training structure, ensuring that is specific and systematic. Consider individual-specific factors when designing these elements
Development
Develop action plan, training resources (training scenarios, training material) and pilot test. Validate developed resources through consultation with stakeholders ad testing. Recommended: Utilize LMS to facilitate process.
Implemen-tation
Organize training to be taken by selected participants. Monitor training sessions and collect feedback during overall progress.
Evaluation
Conduct formative evaluation during training development and summative evaluation at the end of training cycle.
Revision
Revision
Revision
Revision

Fig. 1 Revised ADDIE model, presented in Chowdhury, Katsikas, and Gkioulos [28]

latter is a quantitative approach that analyzes specific performance indicators (PI). Benefits of collecting feedback as an evaluation tool are many, including constant training program improvement based on learners' input, increase participants' motivation and performance [34].

The following five elements should always be included during post-training feedback collection, according to Andriotis [35]:

- *Effectiveness of training*: Effectiveness is a critical element to measure the performance of a training program as it establishes learners' perception of whether the course helped them attain their learning objectives and how relevant it was for them.
- *Comprehension*: Comprehension refers to the effectiveness of the course delivery and as such is focused about the way the course content was delivered. This element also includes the conciseness and clarity of content.
- *Attractiveness*: Attractiveness of a training program refers mostly to how the material and tools used during training looked and felt to the learners. It is especially relevant for software-based training, such as game-based, simulation-based or online training.
- *Engagement*: One of the most critical aspects in the success of a training program depends on user engagement. As overall training engagement is a multifaceted issue, evaluation of individual training components should be collected from participants to highlight any weak points.
- *Suggestions*: Suggestions for improvement from training participants should also be collected. Andriotis [35] notices that suggestions are often skipped during feedback surveys and for this reason recommends asking participants to include a minimum required number of suggestions.

As mentioned in Sect. 1, engagement has a significant effect on training outcome and training effectiveness. According to recent studies on training engagement theory, participants' engagement needs to be captured during three different phases: goal establishment, goal prioritization (meaning the prioritization of the goals of training over other goals) and goal persistence (meaning using a persistent approach until the goal is attained) [36].

When it comes to PIs and Key Performance Indicators (KPIs) for CS training, Samuel [37] suggests that these should measure one of the following attributes: Accuracy, Timeliness, Completeness and Authorization. Specific definition of each PI should depend on the type of exercise being developed, and should occur during initial development of the exercise itself.

As mentioned in Sect. 1, the framework developed is heavily based on concepts of PLT. This allows for both the optimization of the initial training modules, as well as tailoring based on participants' feedback. This allows for both the optimization of the initial training modules, as well as.

Additionally, elements of popular educational taxonomies such as Bloom's and Webb's taxonomies have been considered during development [25]. In particular, recent proposals of CS training based on such taxonomies have been consulted to allow for a progressive and constructive learning experience.

4 Related work

Over the last years, both models to design CS training frameworks and exercises as well as considerations for pedagogical and psychological aspects in CS education have been proposed in the literature. To the best of the author's knowledge, none of these proposals combine the latter considerations to the former models, to develop a CS exercise centered around individual-specific needs.

That being said, various guides and proposals for designing CS exercises have been proposed that outline key steps and design considerations when developing these types of offerings.

A number of these proposals have been consulted for the completion of this work and are described in this section.

Patriciu and Furtuna [11] proposed a guide on how to design a CS exercise, by outlining 7 key steps and several guidelines to follow. The steps outlined by the authors include defining the objectives, choosing an approach, designing network topology, creating a scenario, establishing a set of rules, choosing appropriate metrics and learning lessons, as shown in Fig. 2.

The guide proposed by the authors provides a useful initial roadmap for designing CS exercises, although its utility is limited by the lack of detail on action plans that need to occur at each step. More detail and exemplary information for the model is given in the authors' later work in Furtunˇa, Patriciu, and Bica [38], but lack of consideration for individual-specific factors still limits the perceivable effectiveness of the proposal.

Another step-based framework to aid in the development of CS skills is proposed by Brilingaite, Bukauskas, and Juozapaviˇcius [39]. The framework is specific for hybrid CS defense exercises (CDX), which indicate exercises that involve both expert and non-expert teams of participants. The framework consists of a sequence of steps including stages of formative assessment, team construction, determination of objectives for different types of teams, and the exercise flow. During assessment of the case study developed using the framework, the authors utilized a combination of monitoring, interviews and feedback collection to evaluate the effectiveness of the framework.

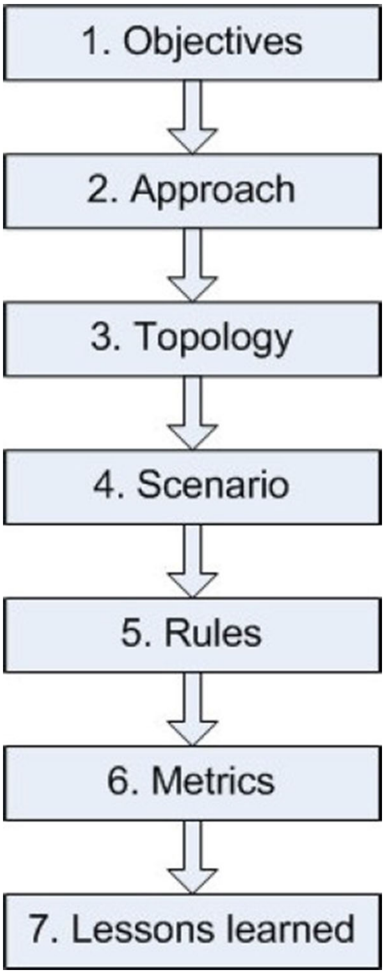


Fig. 2 Design Steps for a Cyber Security Exercise, proposed by Patriciu and Furtuna [11]

Karjalainen, Kokkonen, and Puuska [40] examine pedagogical issues related to CS exercises, from exercise design to training results and evaluation. For each of the three phases of exercise development (planning, implementation, feedback), the authors suggest the following improvements:

- *Planning Phase*: Use semi-structured interviews for data collection from participants to improve the quality of communication, thus improving the results obtained during the activities conducted in the planning phase;
- *Implementation Phase*: Maintain situation awareness on the exercise at all times. Theories relative to decision-making models in stressful situations should be used. Incident reporting and log analysis are also suggested as techniques to improve focusing;

- *Feedback Phase*: From the perspective of individuals' learning, the feedback phase is most important phase of the exercise. All actors of exercises need to participate in the feedback phase, and detail regarding both experience and execution need to be collected;

Overall, the authors suggest CS exercises to be goal-oriented during all phases of development, while suggesting to use the levels of learning and behavior in Kirkpatrick taxonomy [41] in the context of CSE for future research.

Another work focused on analyzing and incorporating, psychological and pedagogical approaches in CS education is conducted by Taylor-Jackson et al. [42]. According to the authors, 6 critical requirements for workplace learning that combines psychology and CS factors can be highlighted:

- Use immersive learning environment and material (videos, dramatization, etc.);
- Integrate psychologically backed game-design with intellectual challenges, and positive reinforcement techniques improves learner's engagement, to promote behavior change and knowledge retention;
- Allow learners to select preferred learning location and instrumentation, as well as pace of learning;
- Provide a combination of training activities to avoid tediousness and fatigue;
- Ensure that users are able to produce their own positive action plan against threats;
- Utilize a Learning Management Software (LMS) to allow participants to monitor their progress and performance.

Karjalainen, Kokkonen, and Puuska [40] discuss pedagogical issues relating to CS exercises, both in regard of design and development of the exercise, as well as its evaluation. The authors use previously gathered data from past exercises to assess how pedagogical aspects can influence the outcome of training and how these aspects can be integrated to the life-cycle of an exercise. In particular, it is noted that CS exercises should avoid over-stressing on technical phenomena and instead consider what the primary goals set for the exercise are. The authors suggest that more research should be conducted to understand how to conciliate individual focus in training development with organization constraints.

Frank, Leitner, and Pahi [43] proposed a CS testbed design life cycle and a methodology for their development, after conducting an extensive literature analysis of other testbeds. According to the authors, the design life cycle of a testbed should be composed of the following phases:

- Define, configure environment;
- Deploy environment;
- Define challenges;
- Deploy challenges;
- Conduct challenges;
- Maintain environment;
- Maintain challenges;

The final testbed design proposed by the authors is later validated in a case study. It must be noted that the authors do not take into consideration pedagogical aspects and individual-specific factors that should need to be considered in the development of educational testbeds. Also, the testbed design is only validated theoretically. Practical validation is recommended to ensure transferability of the concepts in real scenarios.

The use of game-based CS training has seen vast application and documentation in a variety of sectors.

In a study by Chukwudi, Udoka, and Charles [44], the authors reviews the application of game theory in CS. Six different varieties of games are noted: (1) perfect information games, (2) Bayesian games, (3) static/strategic games, (4) dynamic/extensive games, (5) stochastic games and (6) the game-type.

The authors additionally note the frequent use in the military of game-based information warfare.

Video games as a source of training, and CS training have in fact originated in the military sector, as noted in Herr and Allen [45]. With first applications dating back to 1962, the main purpose of these early tools was to provide a simulated and engaging environment to train future generations of personnel. This approach has been continued and adapted in later years for CS training as well. A recent example of video games for CS training in the military sector is the work proposed by Abadia Correa, Ortiz Paez, and Pen˜a Castiblicanco [46]. The authors It is divided into several interfaces: first, the game presentation, in which the system requests a username and a password; second, an interface in which information security is explained, which helps the user build knowledge from the learning virtual object. The third interface is a game in a, who wants to be a millionaire format, which will evaluate what was learned by using random questions that will display a grade when answered. The final interface shows the user's score. In the short-term, the degree of knowledge in cybersecurity of Emavi's staff will be evaluated to know if it is possible to perform a medium term pilot plan to apply such an strategy to CACOM 7, taking into account the results displayed in the first stage of interaction. The application was uploaded to the institution's virtual platform, which helped 60% of the staff use it and know both their advances in cybersecurity knowledge and tips to minimize risks in information security when using technology.

5 Methodology

As mentioned in Sect. 3, the methodology adopted to develop the proposed CS exercises is an adaptation of the methodology we previously developed in Chowdhury, Katsikas, and Gkioulos [28]. As previously stated, the overall model follows the revised ADDIE model shown in Fig. 1.

In the following sections we describe in more detail the actions conducted for each phase of the Delphi.

5.1 Analysis phase

The first step that had to be completed during the analysis phase was to select the target audience for the exercise. Due to greater availability and easiness in coordination, the selection came to involving 12 master's students at the Norwegian University of Science and Technology (NTNU) enrolled in the Information Security degree program. Further development of the exercise is influenced by the selection of this as the target audiences, as the knowledge and needs of the students may differ from the ones of trained professionals and general audience. Specifically, the master's students are familiar with most of the basic concepts and areas of CS, unlike most general audience, with advanced knowledge in specific subjects. They may lack in the practical experience and preparedness of security professionals, which encourages the use of active, hands-on training that simulates real emergency scenarios. To motivate voluntary participation, participants were offered 3 gift cards to be given to randomly selected participants to the exercises. A total of 12 students agreed to participate to the first exercise. Of these 12 students, 8 participated to the second exercise. The decrease in number of students for the second exercise was due unavailability or impossibility for physical presence, which was required for the second exercise.

Participants were then sent out two initial surveys, one focused on allowing them to self-express their level of knowledge and confidence in different CS areas, while the other one had the goal of collecting preferences on different design and development attributes of the training. Table 1, Figs. 3 and 4 summarize both questions and answers to the two surveys.

In Fig. 3, the y-axis represents the self-assessment grading given by the students, which starts at 1 (indicating no knowledge of the subject) up to 10 (indicating full expertise on the subject, comparable to that of a senior expert), while the x-axis represents the number of respondents. Based on the responses from the surveys shown in Fig. 3, it can be seen that most participants expressed having a limited grasp of many basic CS areas and have also not participated to previous CS exercises, aside from two participant. One of the reasons of this, as explained by the students, was that they felt their technical knowledge on the subject was not matched by practical education and training, which made them feel not having the adequate skillset.

Table 1 Summary of the results from the first part of survey 1

Question	Answers
Survey 1	
Have you ever conducted any form of CS risk assessment	YES (50%)–NO (50%)
Have you ever participated to a CS exercise?	YES (16.7%)–NO (83.3%)
If Yes, what type of exercise have you participated to?	Game-based exercise (2 students)–Risk assessment exercise (1 student)

When it comes to preferences on the objectives and design of the exercise, participants expressed primarily wanting to increase their team skills and ability to respond to attacks. Additionally, when it comes to preferred type of exercise, red team vs blue team exercise were slightly preferred over scenario-based exercise, while both game-based and simulation-based exercises were equally favoured by students. These factors were kept in consideration during the later phases of design and development of the adapted ADDIE model used to build up the exercises.

5.2 Design phase

During the design phase, we utilized the results of the two surveys to establish the main components that will compose the exercises. Due to many participants stating they felt inexperienced and were not confident about their knowledge level in several key CS areas, an initial game-based exercise was suggested. Cyber-CIEGE [47], one of the more well-known video games for CS training, was suggested to the participants. The motivation behind the choice of Cyber-CIEGE came from its ease of use and understanding and effectiveness in training both students and industrial personnel in basic CS concepts [48]. Additionally, Cyber-CIEGE provides logs of the exercises after each successful or failed attempt, which can be used both as a form of assessment and to establish areas of concern.

Participants to the exercise were given the possibility of familiarizing themselves with the video game, by completing initial test scenarios offered in Cyber-CIEGE. After completing these, another survey was sent to establish whether they agreed on conducting further exercises using the platform.

Cyber-CIEGE offers a selection of different scenarios from the following 5 campaigns: encryption campaign, identity management campaign, mandatory access control campaign, network traffic analysis campaign. After consulting with the students and agreeing on using Cyber-CIEGE as the platform of choice, they were asked to express their

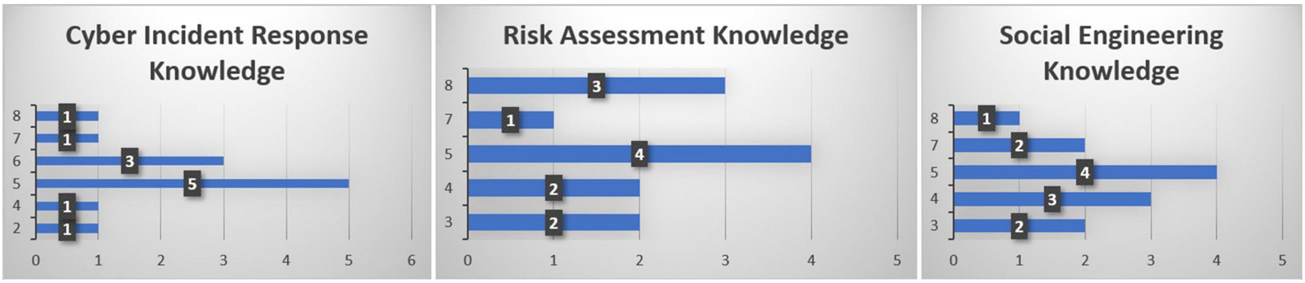


Fig. 3 Students' self-assessment of knowledge in cyber-incident response, social engineering and risk assessment, graded between 1 and 10

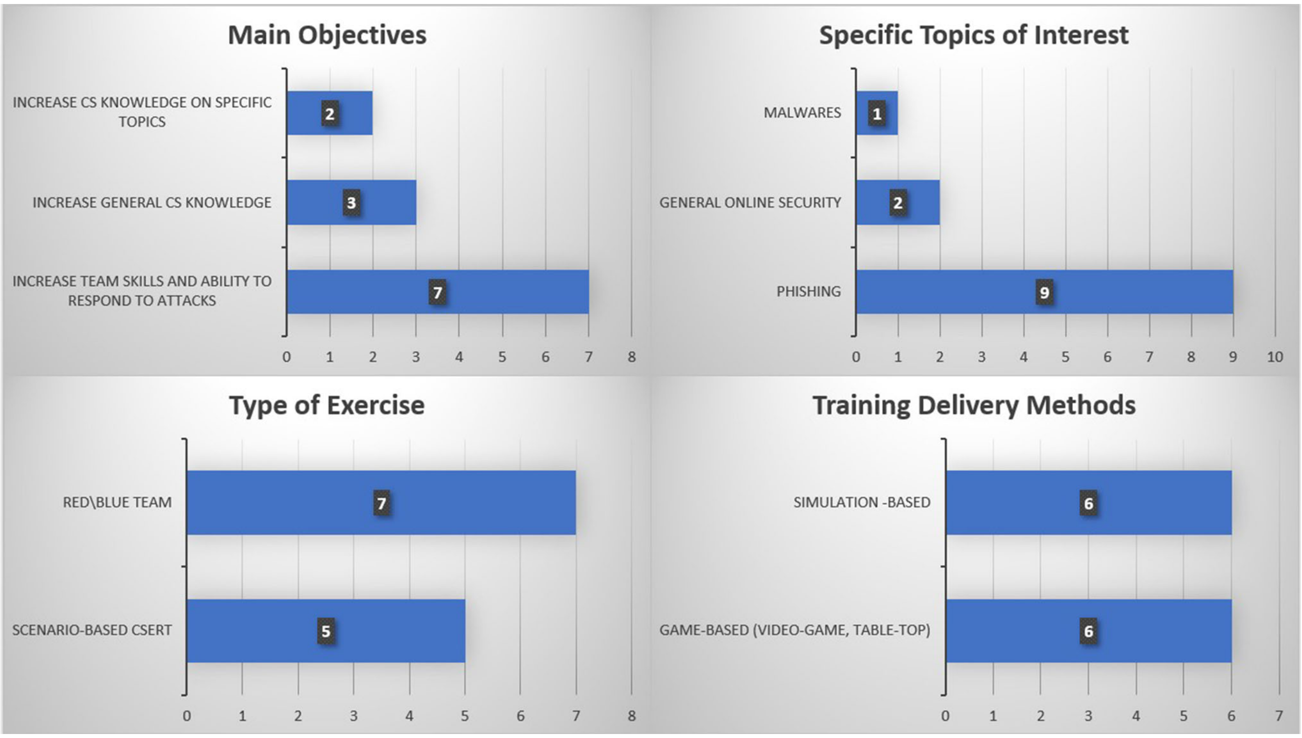


Fig. 4 Preferences of students when it comes to exercise objectives, topics, type of exercise and training delivery methods

preferences between the campaigns, to reach an agreement on two different training scenarios.

Aside from the aforementioned exercises, an additional table-top exercise was set-up, based on the preferences expressed by the participants during the analysis and design phase. This latest exercise was designed to utilize some of the concepts learnt from the two selected scenarios of CyberCIEGE as well as concepts where some participants showed limited knowledge. The selection of a table-top game as a delivery method for the second exercise came due to different reasons:

- Ease of Implementation: table-top exercises are easier to implement than most other group exercises, due to not requiring particular tools and because of their straightforward instructions.
- Increased engagement: it has been demonstrated that by offering an interacting and enjoyable table-top exercise, participants engagement and motivation are increased [49].
- Skill Acquisition: additional to improving participants' knowledge on selected CS topics, table-top exercises aid in acquiring both technical and non-technical skills [49].

There are also certain limitations to table-top exercises, such as limited remote accessibility (unless they were run in online live sessions) and time constraints depending on participants' availability and duration of the exercise. These were resolved in our case as all students were present at the same campus and a time-slot to conduct the exercise was agreed by all participants.

5.3 Development phase

Development for the scenarios run through Cyber-CIEGE was simplified thanks to the platform already including all instrumentation necessary to run the exercise and conduct assessment through log analysis. Two scenarios were selected to be completed for the exercise, based on participants' preferences: the *Link Encryptors* scenario from the encryption campaign and the *Network Traffic Analysis* scenario from the network traffic analysis campaign.

Development of the table-top exercise on the other hand required extensive work and further consultation with the participants. Additionally, evaluation and feedback from the Cyber-CIEGE exercises were also partly utilized to the develop the table-top exercise. In particular, later assessment showed that the second scenario focused on network traffic analysis proved to be more challenging to students. To remedy this and to create an appropriate learning path toward overcoming this gap as recommended in personalized learning theory models [26], we ensured that the following table-top exercise focused on network analysis and security.

Initial consultation was conducted to establish preferences in regard of format for the exercise and general outline. Once agreement was reached on using a traditional, discussion-based table-top format and a red-team vs blue-team scenario, further development on the exercise was conducted before it being run. The MITRE playbook [50] was followed for initial definition of design and development requirements for the exercise. According to the playbook, the following tasks must be conducted for a successful table-top exercise:

- Define objectives and learning outcomes: objectives and learning outcomes should be defined during initial planning meetings/activities [50]. Further development shall be conducted in-between further planning activities;
- Clearly define cyber exercise scenario: while participants may be let free to explore different approaches for solving different cyber exercise scenarios, the overall scenario structure and description should be clearly defined, to avoid confusion during implementation;
- Ensure smooth running of exercise: the instructor should ensure that the cyber exercise is run smoothly, by controlling the flow of the exercise, ensuring participants are active, communicative and engaged;
- Observe and keep logs during execution: the instructor should observe how each participant behaves and responds during the exercise, and keep logs of all the activities conducted during the exercise;
- Evaluate exercise after completion: conduct assessment and collect feedback from participants to understand whether the exercise was successful and if there were any issues.

Additionally to design the cyber-exercise scenario, we utilized the recommendations presented in Ottis [51] for creating red-team vs blue-team scenarios. Initial description of the overall scenario was sent to all participants, which were then allowed to select which teams they would prefer being participants of. Once participants were made familiar with the scenario and overall instructions for the cyber exercise, this was implemented in a live session.

5.4 Implementation phase

Implementation of the two exercises run with Cyber-CIEGE occurred with limited input from the instructor, as the majority of instructions were already provided by Cyber-CIEGE. Participants were sent out initial instructions regarding the installation and use of the software application, as well as recommended to run initial test scenarios meant to familiarize themselves with the platform. Once these were completed and evaluated, the results were utilized to further define the following table-top exercise.

When it comes to the cyber table-top exercise, this was implemented in a more interactive manner, to allow open discussion between teams, as well as consultation of online sources. This was done to ensure that participants were not discouraged in case they lacked the background knowledge to respond to the opponent team's actions. Additionally, this allowed for the exercise to further build participants' technical knowledge, while also improving their team-skills and responsiveness.

The facilitator introduced to the participants the roles and objectives of both teams and of each individual participant. Members of the blue team were allowed to choose between a variety of roles, both of technical and non-technical nature, at different levels of a fictional security device and software manufacturing company. The red team instead represented an international cyber-crime group with the goal of obtaining confidential data from the servers of the company and/or from its key managers.

The game started by allowing the teams to conduct initial internal consultation to determine the key requirements shown in Table 2.

Members of the red team were encouraged to come up with techniques that could take advantage of network security vulnerabilities over other exploits. This was done in order to ensure that participants focused on the knowledge gaps revealed from the previous Cyber-CIEGE exercise. Likewise, the blue-team were encouraged to think of and research both vulnerabilities and security measures to install against network security threats and attacks.

Once the initial consultation phase was concluded, the exercise was commenced. This was conducted in a turn-based setting, with the red-team starting, following the scheme shown in Fig. 5.

Table 2 Initial requirements to be determined by both teams

Blue team requirements	Red team requirements
Establish roles for each participant;	Determine three different techniques to achieve your goals;
Determine security measures that company should have in place;	Use the MITRE ATT&CK Matri or the Lockheed Martin Cyber Kill Chain to determine all tactics and steps of your attack;
Determine possible vulnerabilities;	Determine possible countermeasures to your attacks and ways to circumvent them;
Generic cyber-incident response plan;	

Three runs of the exercise were completed, where a round consisted of a complete sequence of the turns shown in Fig. 5, which meant that each run lasted from a minimum of six turns to a maximum of 10 turns, in case further responsive actions were suggested by either team. During each turn, the team active for the turn had to respond to the actions from the opposing team conducted in the previous turn, by either explaining what procedures they had already put in place or by thinking of responsive actions in a 10 minutes window of time.

Each runs of the table-top game was declared concluded once either team could not come up with an appropriate response measure, or if either team successfully reached their objectives. Once all three runs of the exercise were completed, the overall experience and the results were discussed with the participants.

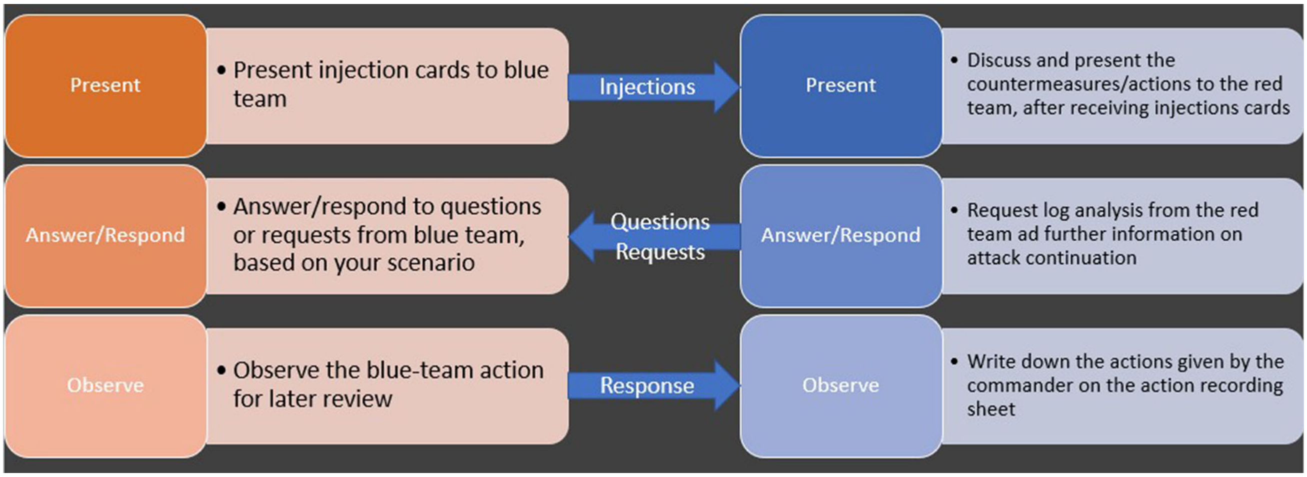
5.5 Evaluation phase

Evaluation of the two exercises conducted with CyberCIEGE was based off log analysis and feedback assessment, via questionnaire. These combinations of forms of assessment provide a vital qualitative and quantitative evaluation of the overall effectiveness of the exercise, as well as an understanding of whether participants felt engaged and motivated during the exercise [27]. Duration to successful completion, number of attempts and percentage of successful completion are the three main metrics collected in the logs of CyberCIEGE.

To evaluate the table-top cyber exercise, a qualitative approach based on open discussion with the participants was combined with feedback collection.

Aside from the aforementioned forms of summative evaluation, formative evaluation in the way of feedback surveys was conducted during each phase of the ADDIE, as suggested in Chowdhury, Katsikas, and Gkioulos [28]. While the formative evaluation was utilized to aid in the development of the exercises, the summative evaluation provided the overall assessment of the effectiveness of the exercises.

Additionally, a follow-up feedback collection was later conducted via unstructured group interviews, to compare the results and overall experience with the table-top exercise conducted to another, large-scale red-team vs blue-team exercise conducted externally by the same group of participants, as well as compare the learning experience with the exercises to classroom and video education and training.


Present

- Present injection cards to blue team

Injections

Present

- Discuss and present the countermeasures/actions to the red team, after receiving injections cards

Answer/Respond

- Answer/respond to questions or requests from blue team, based on your scenario

Questions Requests

Answer/Respond

- Request log analysis from the red team ad further information on attack continuation

Observe

- Observe the blue-team action for later review

Response

Observe

- Write down the actions given by the commander on the action recording sheet

Fig. 5 Turn-based actions to be conducted by each team, with the Red team actions shown in the left and blue team actions shown in the right

Table 3 Actions conducted for each of the ADDIE model phase

Phase	List of actions	Action's result

Analysis	Target audience selection;
	Goal & Objectives establishment;
	Pre-requisite definition;
	Initial design abstraction;
		12 Information Security Master Student's;
		Cyber attack Incident Response, team skills development;
		Low complexity threshold;
		Preferences for game-based methods;

Design	Exercise structure definition;
	Training environment selection;
	Content selection;
	Assessment criteria development (KPI definition);
		Game-based structure (both video-game and table-top game);
		Cyber-CIEGE scenarios + table-top;
		Encryption, Network Traffic Analysis;
		KPI exercise 1: completion rate, average time to completion, number of attempts. KPI exercise 2: turn duration, team objective success;

Development	Develop action plan;
	Develop pre-requirement test;
	Develop/Integrate exercise resources;
	Develop test case;
		Two-exercise action plan developed in collaboration of participants;
		Survey-based pre-requirement assessment;
		Preemptive testing of Cyber-CIEGE scenarios;
		Development of table-top exercise based on literature recommendations and input from participants;

Implementation	Run per-requirement test;
	Run exercise;
		Cyber-CIEGE pilot scenarios run over one week;
		Cyber-CIEGE base scenarios run over one additional week. Table-top exercise run in one live day session;

Evaluation	Continuous feedback collection during exercise development; Monitoring of participants during exercise; Summative feedback collection at the end of the exercise; Post-training evaluation;	Survey-based feedback collection during all phases of ADDIE; Log collection in Cyber-CIEGE for monitoring. In-person monitoring for table-top exercise; Survey, questionnaires, and open discussion at the conclusion of the exercise;

Table 4 Results from the log analysis for the Cyber-CIEGE scenarios

Metric	Results
Percentage of participants who completed successfully 1st scenario	83%
Percentage of participants who completed successfully 2nd scenario	66%
Average time to completion for 1st scenario	9 min 43 s
Average time to completion for 2nd scenario	32 min 7 s
Number of attempts to successful completion 1st scenario	3, 5
Number of attempts to successful completion 2nd scenario	5, 6

6 Results

The results of the feedback collection and the action taken during each phase of the ADDIE described in Sect. 5 are summarized in Table 3.

The results from the log analysis conducted for the Cyber-CIEGE exercises can be seen in Table 4, while Table 5 summarizes the results from the feedback collection surveys for both the Cyber-CIEGE exercise and the table-top exercise.

The second survey for the assessment of the table-top exercise was simplified based on the feedback from the participants in regards of the format of the previous assessment survey. Specifically, most questions were changed to multiple answer questions, as open-ended questions were described as tedious.

Overall, both exercises were received positively by participants.

When it comes to the two scenarios run through Cyber-CIEGE, as it can be seen from Table 4, the second scenario focused on network traffic analysis was found to be overall more complex, difficult and longer to complete than the first one. Participants indicated that some lack of prior knowledge of the topic influenced their overall ability to complete successfully the exercise, which also explained the increased number of trials needed on average to complete. It must be noted that the scenario itself was also longer to complete due to the increased workload and number of actions needed to be performed.

When it comes to the table-top exercise, each run of the exercise lasted between 45 minutes and 1 hour each, with a 10 minute break between each. An initial hour was also spent

Table 5 Answer to summative feedback survey after Cyber-CIEGE exercises

Question	Answers
Survey 1	
Did you find the exercise to be useful to the initial goals you had?	91% YES
Did you enjoy the format of the exercise? If not, what other type of format would have preferred?	100% YES
Did you enjoy the topics selected from the exercise or would you have preferred other topics (from the ones available in Cyber-CIEGE)?	83% YES–17% PARTLY
Did you feel more involved/engaged in the exercises, due to having been able to express preferences in its design?	83% YES
Did you find tedious answering to the surveys? If so, do you have suggestions for other feedback and evaluation collecting strategies?	91% NO
Did you try out other training scenarios in Cyber-CIEGE, aside from the ones required?	66% YES–17% INTERESTED–17% NO
Do you believe the exercises may have helped you understand concepts of Encryption and Network Traffic Analysis that you previously did not understand/possess?	33% YES–41% PARTLY–26& NO
Do you believe Cyber-CIEGE could be improved? If so, how?	Improvement of the GUI; additional scenarios;
Is there anything you would like to suggest or highlight as feedback of the exercise development phase?	Simpler evaluation survey (Use more multiple choice questions)
Survey 2	
Did you find the exercise to be useful to the initial goals you had?	75% YES–25% PARTLY
Did you enjoy the format of the exercise? If not, what other type of format would have preferred?	100% YES
Did you enjoy the topics selected from the exercise or would you have preferred other topics?	75% YES–25% PARTLY
Did you feel more involved/engaged in the exercises, due to having been able to express preferences in its design?	75% YES–25% PARTLY
Do you believe the exercises may have helped you understand concepts that you previously did not understand/possess?	50% YES–50% PARTLY
Is there anything you would like to suggest or highlight as feedback of the exercise development phase?	No recommendations

to give further detail on the exercise execution and setting up the teams. It was noted that participants expressed feeling fatigued after the first two runs and showed less focus and responsiveness during the last run. Fatigue is an important consideration in training, as studies have shown that fatiguing training may have an adverse effect on trainees and worsen their CS knowledge and skills [52]. It is thus recommended to consider duration of the exercises as a significant parameter during the design and development of training, and to possibly spit long exercises in multiple sessions. That being said, participants expressed that the open discussion and active research they had to conduct during the exercise aided them in knowledge acquisition, improving their responsiveness abilities and team-work skills.

Additionally, further evaluation of the table-top exercise was conducted through another round of feedback collection after the students participated and completed an external, large-scale red-team versus blue-team exercise run as part of a CS education activity offered by their faculty, as well as by comparing the experience and knowledge acquired during the two exercises with their academic coursework learning methods. According to the later feedback provided, participants expressed overwhelmingly preferring the first table-top exercise conducted using the model described in Sect. 3 to the large-scale exercise. Reasons for their preference were being more actively involved during both the development of the exercise and its implementation. More in detail, having a smaller group of participants and additional liberty in the actions to be conducted during each turn increased both their engagement and the amount of new information and knowledge collected. When comparing the knowledge acquisition and experience during the exercise to the one in classroom and online exercises, the students highlighted advantages and disadvantages of the exercise over traditional educational methods. These are reported in Table 6.

As indicated in Table 6, the exercise was indicated by the students to be more engaging than traditional assessment methods.

Table 6 Advantages and disadvantages of the personalized table-top exercise over traditional exercise methods, for knowledge acquisition and assessment

Advantages	Disadvantages
Increased engagement	More challenging and complex set-up
Increased knowledge retention	Higher knowledge pre-requirements

Another interesting finding reported by the students was that the knowledge acquired during the table-top exercise was easier to remember and recall than the one from quizzes and other online assessment methods. Participants indicated that feedback collection during exercise development and the scenario-based approach of the table-top exercise had both contributed to increase their engagement during the running of the exercise, as well as provide an exercise more tailored to their preferences, as suggested by research on training engagement [36]. Participants also indicated that the exercise required a higher level of knowledge prior to its running than other types of exercises conducted, while also being significantly more challenging to set-up and conduct than individual-based online assessment exercises. As such, they could be considered as a supplementary tool for academic education, to be integrated to the traditional learning formats. Overall, participants indicated that they found the exercises useful to their initial goals. They also indicated having mostly enjoyed both the topics of exercises the their formats. As expected, most participants reported feeling more engaged in the exercises due to having participated to their design and development.

Interestingly, this had also motivated them to continue training with Cyber-CIEGE, by conducting further scenarios independently in their spare time. This suggests that by allowing participants to be more involved in the selection of preferred methods of training delivery and in the overall development of training, this may motivate them to continue their training formation autonomously. As many participants indicated not having felt as they acquired major new knowledge during the Cyber-CIEGE exercise, the table-top exercise was designed to focus on both knowledge gaps and the initial topics of interest, indicated in the first feedback collection survey.

Overall, the students expressed preferring the interactive format of exercises provided by Cyber-CIEGE and the table-top exercise over more traditional methods of training. More interestingly, they also agreed that the table-top exercise was more engaging than the exercises conducted in Cyber-CIEGE, due to the collaborative aspect of the tasks and the discussion-based approach.

7 Conclusion & future research

There are multiple factors that can determine the success of CS training offerings. Previous studies had shown that participants' motivation and engagement in training are of vital importance to increase the effectiveness of training [12, 53, 54]. As such, offering training and training exercises that is found engaging by participants is critical. One strategy that had been suggested in the literature in other areas of study to increase engagement is personalization, as part of PLT.

In this work, we developed two different formats of CS training exercises, involving a group of 12 master students from the information security faculty at NTNU. The exercises were developed by using the PLT-based CS training framework development model presented in Chowdhury, Katsikas, and Gkioulos [28]. According to the model, by involving participants in the selection of training delivery methods, topics of training and other components of the training, it would be possible to increase overall engagement and consequently overall effectiveness of the exercises.

By collecting continuous formative feedback from participants, two different types of exercises were selected and developed: (1) two scenarios in Cyber-CIEGE, a game-based CS training software and (2) a physical table-top red-team vs blue-team exercise. Final assessment and feedback from the participants confirmed that they felt more engaged during both exercises due to having been involved in their development. Participation to the goal definition and design of the exercise was indicated as the main contributing factor to the increased engagement, which is in accordance to the framework and to key concepts of training engagement theory [36]. In particular, participants reporting having continued training independently with Cyber-CIEGE, as the video-game was reported to be an engaging and useful tool for learning basic CS concepts. Additionally, by evaluating the limitations in knowledge of network traffic analysis shown after the conclusion of the Cyber-CIEGE exercises, it was possible to develop a learning path-oriented table-top exercise. This decision was also reported positively by participants, which described feeling as having acquired both knowledge in the topic during the exercise, as well as practical skills and abilities when it comes to incident response and team-work.

It was noted that during the table-top exercise, participants felt fatigued after the first two runs. Consequently, they showed less responsiveness and engagement. For this reason, it is recommended to take into consideration duration of exercises during the development of training programs. Overall, the PLT-based training development model was shown to have a beneficial impact on the engagement and motivation of participants, as well as comparing favorably to other, more traditional assessment methods, according to the feedback given by the students. This suggests that involvement of participants during training development has significant benefits on participants' engagement, and that utilizing more interactive training delivery methods as supplementary tools to CS education and training may be more beneficial, in terms of engagement, than traditional assessment methods, such as quizzes and reports.

While this initial effort had the objective of receiving a formal validation of the framework developed in Chowdhury, Katsikas, and Gkioulos [28], additional work need to be conducted, both to further validate the framework and extend it to consider for additional key concepts of training.

Additional experimentation using the framework has been conducted and described in Chowdhury, Gkioulos, and Nystad [55]. These experiments have been conducted in collaboration with CI personnel and utilize an updated version of the framework, refined based on the results obtained in this work. Specifically, two additional experiments have been conducted, one with CS personnel from an energy company and one with technical personnel from nuclear power plants. Particular focus has been put in designing exercises that accounted for organization and trainee requirements, as well as considerations for time and resource constraints. The results obtained in the follow-up exercises provide further confirmation of the usability and effectiveness of the proposed framework. Moreover, the framework is demonstrated to be flexible and adaptable to the needs of heterogeneous groups of participants, ranging from students to cybersecurity professionals.

That said, the model should also be tested within larger target groups and for the development of more extensive training programs, to understand whether it is appropriate in those settings and provides overall better results than traditional training programs. Further work should be also conducted to develop tailored variants of the training framework, to be proposed to technical staff in various critical infrastructure industry sectors. Additionally, aside from evaluating training results based on engagement, further evaluation should be conducted to establish whether the training exercises developed using PLT-based frameworks have also more benefits in skills and knowledge acquisition than traditional methods.

Currently, more substantial training programs are currently being developed targeting international SOC (Security Operation Centre) and CERT (Computer Emergency Response Team) teams working in the nuclear sector and in the energy sector.

Author contributions Author NC wrote the main manuscript and all of its components. Additionally, he was in charge of the design, development and implementation of the experiments conducted and described in the manuscript. Author VG was in charge of supervision of the work, its reviewing and suggestions for further improvement in design and implementation.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital).

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Human or animal rights This article does not contain any studies involving animals performed by any of the authors.

Informed consent Informed consent was obtained from all individual participants involved in the study. Identity of participants in the experiment described in the article is kept anonymous for privacy purposes.

References

1. PurpleSec. 2021 Cyber Security Statistics The Ultimate List Of Stats, Data Trends. (2021). https://purplesec.us/resources/cyber-security-statistics/
2. Safe at Last. 22 Shocking Ransomware Statistics for Cybersecurity in 2021. (2021). https://safeatlast.co/blog/ransomwarestatistics/#gref
3. Morgan, S.: Cybercrime to cost the world $10.5 trillion annually by 2025. In: Cybersecurity Ventures (2020). https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
4. Rothwell, J.: Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down. In: The telegraph (2017)
5. Madiba, T.: The role of human error in cybersecurity breach. In: (2022)
6. MacRae, I.: Teaching is different from training: how to use both effectively. In: trainingindustry.com (2017). https://trainingindustry.com/articles/workforce-development/teachingis-different-from-training-how-to-use-botheffectively/#:~:text=Teaching%20seeks%20to%20impart%20knowledge,make%20them%20a%20good%20swimmer.
7. Chabinsky, S.R.: Cybersecurity strategy: a primer for policy makers and those on the front line. J. Natl. Sec. L. Poly. **4**, 27 (2010)
8. Chen, J.Q.: A framework for cybersecurity strategy formation. Int. J. Cyber Warf. Terror. (IJCWT) **4**(3), 1–10 (2014)

9. González-Manzano, L., de Fuentes, J.M.: Design recommendations for online cybersecurity courses. Comput. Secur. **80**, 238–256 (2019)
10. Mouheb, D., Abbas, S., Merabti, M.: Cybersecurity curriculum design: a survey. In: Transactions on Edutainment XV. Springer, pp. 93–107 (2019)
11. Patriciu, V.-V., Furtuna, A.C.: Guide for designing cyber security exercises. In: Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy. World Scientific, Engineering Academy, and Society (WSEAS), pp. 172–177. (2009)
12. Bada, M., Sasse, A., Nurse, J.: Cyber security awareness campaigns: Why do they fail to change behaviour? comput. Sci. pp. 118-131 (2019)
13. Haney, J.M., Lutters, W.G.: It's scary. It's confusing. It's dull": how cybersecurity advocates overcome negative perceptions of security. In: Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018), pp. 411–425. USENIX Association (2018)
14. Colquitt, J.A., LePine, J.A., Noe, R.A.: Toward an integrative theory of training motivation: a meta-analytic path analysis of 20 years of research. J. Appl. Psychol. **85**(5), 678 (2000)
15. Tai, W.-T.: Effects of training framing, general self-efficacy and training motivation on trainees' training effectiveness. Pers. Rev. **35**(1), 51–65 (2006). https://doi.org/10.1108/00483480610636786
16. Fisher, R., Porod, C., Peterson, S.: Motivating employees and organizations to adopt a cybersecurity-focused culture. J. Organ. Psychol. **21**(1), 114–131 (2021)
17. Beuran, R. et al. Cytrone: an integrated cybersecurity training framework. In: (2017)
18. Hendrix, M., Al-Sherbaz, A., Victoria, B.: Game based cyber security training: are serious games suitable for cyber security training? Int. J. Serious Games **3** (2016). https://doi.org/10.17083/ijsg.v3i1.107
19. Nagarajan, A. et al. Exploring game design for cybersecurity training. In: 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 256–262. IEEE (2012)
20. Miller, T.M., Geraci, L.: Training metacognition in the classroom: The influence of incentives and feedback on exam predictions. In: Metacognition and Learning 6.3, pp. 303–314 (2011)
21. Cekada, T.L.: Training a multigenerational workforce: understanding key needs & learning styles. Prof. Saf. **57**(03), 40–44 (2012)
22. WA Conklin, RE Cline, T Roosa: Re-engineering cybersecurity education in the US: an analysis of the critical factors. In: 2014 47th Hawaii International Conference on System Sciences, pp. 2006–2014. IEEE (2014)
23. Morris, T., Vaughn, R., Dandass, Y.: A testbed for SCADA control system cybersecurity research and pedagogy. In: ACM International Conference Proceeding Series (2011). https://doi.org/10.1145/2179298.2179327
24. Churches, A.: Bloom's digital taxonomy (2010)
25. Harris, M.A., et al.: Using Bloom's and Webb's taxonomies to integrate emerging cybersecurity topics into a computic curriculum. J. Inf. Syst. Educ. **26**(3), 219–234 (2015)
26. Morin, A.: Personalized learning: what you need to know. In: (2020)
27. Chowdhury, N., Gkioulos, V.: Cyber security training for critical infrastructure protection: a literature review. Comput. Sci. Rev. **40**, 100361 (2021)
28. Chowdhury, N., Katsikas, S., Gkioulos, V.: Modeling effective cybersecurity training frameworks: a Delphi method-based study. Comput. Secur. (2021)
29. Design Instructional. ADDIE model. In: Instructional design (2021)
30. Abawajy, J.: User preference of cyber security awareness delivery methods. Behav. Inf. Technol. **33**(3), 237–248 (2014). https://doi.org/10.1080/0144929X.2012.708787
31. Jin, G., et al.: Evaluation of game-based learning in cybersecurity education for high school students. J. Educ. Learn. (EduLearn) **12**(1), 150–158 (2018)
32. Pastor, V., Diaz, G., Castro, M.: State-of-the-art simulation systems for information security education, training and awareness. In: IEEE EDUCON 2010 Conference, pp. 1907–1916. IEEE (2010)
33. He, W., Zhang, Z.: Enterprise cybersecurity training and awareness programs: recommendations for success. J. Organ. Comput. Electronic Commerce **29**(4), 249–257 (2019)
34. DeFranzo, S.: 5 Reasons why feedback is important. In: Snap Surveys (2018)
35. Andriotis, N.: 5 Elements to include in any post training evaluation questionnaire. In: Efront Learning (2018). https://www.efrontlearning.com/blog/2017/12/element-postevaluation-training-questionnaire.html
36. Sitzmann, T., Weinhardt, J.M.: Training engagement theory: a multilevel perspective on the effectiveness of work-related training. J. Manag. **44**(2), 732–756 (2018)
37. Samuel, J.: Cyber security—key performance indicators. In: Infosec Write-ups (2019)
38. Furtun˘a, A., Patriciu, V.-V., Bica, I.: A structured approach for implementing cyber security exercises. In: 2010 8th International Conference on Communications, pp. 415–418. IEEE (2010). https://doi.org/10.1109/ICCOMM.2010.5509123
39. Brilingaite, A., Bukauskas, L., Juozapavičius, A.: A framework for competence development and assessment in hybrid cybersecurity exercises. Comput. Secur. **88**, 101607 (2020). https://doi.org/10.1016/j.cose.2019.101607
40. Karjalainen, M., Kokkonen, T., Puuska, S.: Pedagogical aspects of cyber security exercises. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 103–108 (2019). https://doi.org/10.1109/EuroSPW.2019.00018
41. Kirkpatrick, D.L.: Techniques for evaluating training programs. In: Training and development journal (1979)
42. Taylor-Jackson, J. et al.: Incorporating psychology into cyber security education: a pedagogical approach. In: International Conference on Financial Cryptography and Data Security, pp. 207–217. Springer (2020). https://doi.org/10.1007/978-3-030-54455-3_15
43. Frank, M., Leitner, M., Pahi, T.: Design considerations for cyber security testbeds: a case study on a cyber security testbed for education. In: 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th International Conference on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress, pp. 38–46 (2017). https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23
44. Chukwudi, A.E., Udoka, E., Charles, I.: Game theory basics and its application in cyber security. Adv. Wirel. Commun. Netw. **3**(4), 45–49 (2017)
45. Herr, C., Allen, D.: Video games as a training tool to prepare the next generation of cyber warriors. In: Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, pp. 23–29. (2015)
46. Abadia Correa, J., Ortiz Paez, L., Pen˜a Castiblicanco, N.: Development of a training game to provide awareness in cybersecurity to the staff of the aviation military school "Marco Fidel Su´arez" of the Colombian Air Force in the city of Cali. In: (2021)
47. Irvine, C.E., Thompson, M.F., Allen, K.: Cyber-CIEGE: gaming for information assurance. IEEE Secur. Priv. **3**(3), 61–64 (2005)
48. Thompson, M., Irvine, C.: Active learning with the Cyber-CIEGE video game. In: (2011)

49. Angafor, G.N., Yevseyeva, I., He, Y.: Game-based learning: a review of tabletop exercises for cybersecurity incident response training. Secur. Priv. **3**(6), e126 (2020)
50. Kick, J.: Cyber Exercise Playbook, The MITRE Corporation, 2014 (2018)
51. Ottis, R.: Light weight tabletop exercise for cybersecurity education. J. Homel. Secur. Emerg. Manag. **11**(4), 579–592 (2014)
52. Reeves, A., Delfabbro, P., Calic, D.: Encouraging employee engagement with cybersecurity: how to tackle cyber fatigue. SAGE Open **11**(1), 21582440211000050 (2021)
53. Gross, A.: Effective security training requires change in employee behavior (2018)
54. Kostadinov, D.: The components of a successful security awareness program. (2018)
55. Chowdhury, N., Gkioulos, V., Nystad, E.: Benefits of PLT for cybersecurity training (in Review). Int. J. Inf. Secur. (2023)

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