Computer Science Review 40 (2021) 100361

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

Cyber security training for critical infrastructure protection: A literature review

Nabin Chowdhury *, Vasileios Gkioulos

Norwegian Institute of Science and Technology (NTNU), Teknologivegen 22, 2815, Gjøvik, Norway

ARTICLE INFO

Article history:
Received 16 September 2020
Received in revised form 27 December 2020
Accepted 13 January 2021
Available online xxxx

Keywords:
Review
Cybersecurity
Critical infrastructure
Training
Aviation
Energy
Nuclear

ABSTRACT

Introduction: Today, cyber-security curricula are available across educational types and levels, including a vast array of programs and modules tailored to specific sectors of industry and audiences, to allow more targeted delivery of knowledge. Nonetheless, general agreement on best measures and methods for cybersecurity training has yet to be reached.

Objective: In this study, we seek to establish the current state-of-the-art in cyber-security training offerings for critical infrastructure protection and the key performance indicators (KPIs) that allow evaluating their effectiveness. Particular focus is given in this study on the aviation, energy and nuclear sectors.

Methodology: Accordingly, the article presents the findings of a systematic literature review that collected relevant literature produced after 2000. The identified sources have been examined according to a formal data extraction form, allowing the analysis of relevant training solutions, methodologies, target groups and focus areas.

Results: The results show that solutions that provide hands-on experience, team skills development, high level of real-life fidelity are often preferred to other options, with simulation-based solutions showing the highest amount of research and development. Nonetheless, researchers have not reached agreements on optimal training delivery methods and design of cybersecurity exercises.

Conclusion: Consequently, research on improving current cybersecurity training offerings should be conducted, to demonstrate whether integrating advantageous attributes from different delivery methods could produce more comprehensive and effective solutions.

Contents

* Corresponding author.
E-mail addresses: nabin.chowdhury@ntnu.no (N. Chowdhury), vasileios.gkioulos@ntnu.no (V. Gkioulos).

https://doi.org/10.1016/j.cosrev.2021.100361

Abbreviations

CS	Cyber-security;
CI	Critical Infrastructure;
CIS	Critical Infrastructure Security;
CIP	Critical Infrastructure Protection;
IDS	Intrusion Detection System;
KPI	Key performance Indicator;
API	Application Programming Interface;
NIST	National Institute of Standards and Technology;
NICE	National Initiative for Cybersecurity Education;
ICS	Industrial Control System;
CCS	Central Control System;
CSS	Control and Supervision Substation;
PLC	Programmable Logic Controller;
I&C	Instrumentation and Control;
DNS	Domain Name System;
DDoS	Distributed Denial of Service;
LMS	Learning Management System;

1. Introduction

In the ongoing digital era, cyber-security threats have become considerable enough to have reached mainstream attention, with major cyber-attack cases reaching the headlines of multiple media outlets.

One of the major targets of cyber attacks in recent years have been critical infrastructures from all sides of the industry. For example, one of the most infamous cyber-attacks in recent years was a campaign against industrial control systems, known by the codename *Dragonfly*. According to technical reports, attackers exploited a variety of techniques, including attaching malware to third-party programs, e-mails and websites to gain access to numerous computer systems. By doing so, the attackers were able to mount sabotage operations that could have disrupted energy supplies across several European countries and the US [1,2].

Often, the success of such attacks was determined by user unawareness and lack of formal training of staff [3,4]. In a 2015 study, 31% of security breaches in industrial firms during that year were attributed to human errors [5]. In another study, it was found that the root cause of 80% of data breaches can be attributed to stolen data, often obtained through social engineering attacks such as e-mail phishing [6]. All these studies and reports show that one of the key factors in the success of many cyber-attacks is user awareness and training.

Many initiatives have taken place around the world to counter the issue of human unpreparedness to cyber attacks. The cybersecurity framework developed by the US National Institute of Standards and Technology (NIST) is arguably the most renowned and has been used as the basis for later national frameworks [7]. NIST was the main contributor to the development of the National Initiative for Cybersecurity Education (NICE) and the Cybersecurity Workforce Framework (NICE Framework). This framework has been instrumental to the development of many different awareness and training programs, tools and modules for CS personnel [8,9]. Nonetheless, criticism regarding the comprehensiveness and accuracy of the information given in the NICE documentation was raised by multiple researchers [10–12]. This criticism was raised due to the frameworks' inability to cover multiple groups of interdisciplinary workforce effectively, not providing a measurable outcome or metric [10] and not identifying or correctly classifying certain CS areas [11,12].

Since the development of the first frameworks for cybersecurity workforce education and awareness, significant amount of research has been conducted to establish training content, delivery methods and other key aspects of workforce training. Nonetheless, agreement on an overall best performing solution is yet to be reached, with most researchers being only able to identify specific advantages and disadvantages of individual training offerings [13,14], without being able to conclude on which are the optimal strategies for CS awareness training. This lack of agreement and the urgent need for well-prepared CS workforce was the motivation to conduct more research regarding current solutions when it comes to CS training for Critical Infrastructure protection (CIP).

In this work, we try to map and review all relevant findings regarding the state-of-the-art in training content and methodologies for CS awareness and training. While solutions for a variety of sectors of CI have been analyzed, particular focus was given to the aviation, energy and nuclear sectors.

As a continuation of our previous research in [15], which focused on reviewing the key competencies and skills to be acquired for CI CS, in this work more focus will be given to the understanding and evaluation of training delivery methods found in the literature. Moreover, we also conduct an analysis of metrics and key performance indicators (KPIs) necessary to evaluate CS training solutions suggested in the literature. Finally, suggestions regarding content and structure of future training solutions are given, based on the findings and analysis of the reviewed solutions.

The rest of this work is organized as it follows: in Section 2, we present relevant review works that have been conducted in the field of CI security assessment as well as security measures. In Section 3, we clarify the motivations that brought us to conduct this research. Following, in Section 4, we provide a thorough description of the research method utilized to search, screen and select the literature for this review. Next, in Section 5, we discuss all the papers that have been selected, focusing on their main findings and highlighting possible shortcomings. The literature is divided based on the sector of CI that it is focusing on. In Section 6 we then analyze possible evaluation metrics and KPIs to assess the performance of the training measures found in Section 5. In Section 7 we first discuss possible classification methods and metrics of CS training offerings and later provide a tabular classification of the training solutions discussed in the articles included in this review. We later conduct a comparative and quantitative analysis of the data, based on this classification. Finally, in Sections 8 and 9, we give our final remarks and summary of the work conducted in this paper and further discuss future research meant to overcome the limitations of this research and expand on them to allow for the development of effective CS training measures.

2. Related work

To the best of the authors' knowledge, a systematic literature review that analyzes and reviews current offerings in terms of awareness and training solutions for CS CIP has not been conducted yet. Nevertheless, several reviews and surveys have been conducted focusing on CI security assessment, defensive tools and measures, etc. These articles have provided useful insight into the state of the art regarding CI cyber-security, with some providing comprehensive related work sections and evaluation methodologies which were partially integrated into this work.

Al-Daeef et al. [16] reviewed users' training approaches as a non-technical solution to mitigate security threats. In particular, they examine training solutions against phishing attacks, identifying that training is most effective when integrated into daily activities and routines. Previous studies have also supported this proposition, with the approach being known as embedded training [17–19], which can be defined as training provided by capabilities built into or added onto operational systems or equipment, to enhance and maintain the skill proficiency of personnel. One of the main advantages of integrating training to daily activities is that it aids retaining information for longer than traditional training and that it allows this information to be transferred into other activities[20]. Other forms of training analyzed by the authors include classroom training, experiment-based training, interactive games, material sharing and user knowledge and intelligent measurement. The authors conclude that interactive methods have shown a greater degree of success in effectively training personnel and students. Embedded solutions, in particular, have shown to allow trainees to retain information for the longest. One criticism to the research conducted by the authors is that the data utilized come from different training sessions that included different material, modules and objectives. Standardization of all these attributes would be necessary to extrapolate objective conclusions about the advantages and disadvantages of each solution.

Alotaibi et al. [21] conducted a solution-specific review for CS awareness and training, focusing on gaming applications and the effectiveness of their usage in creating cybersecurity awareness. Among the many listed advantages of gaming applications as solutions for CS training, the authors cite the versatility, the fidelity of simulations and problem-solving tasks, and the adaptability of the game to suit almost every training subject possible. The authors reviewed a total of 12 papers discussing game-based solutions, concluding that although most of these solutions yielded positive results, the lack of comprehensive evaluation hinders the arguments for the usability of these solutions in large-scale applications.

Aldawood and Skinner [14] have conducted a comprehensive literature review of offerings and methods for raising awareness against social engineering attacks. The authors firstly discuss what the challenges in implementing a social engineering awareness program are. Additionally, innovating and traditional education and training techniques are discussed in their advantages and shortcomings. The authors conclude that further research is needed in user behavior as a factor of social engineering attacks success, and towards the evaluation of current offerings.

Abd Rahim et al. [22] analyze and survey approaches found in the literature for assessing cybersecurity awareness, also investigating which methodologies were applied, who was the target audience, and whether the coverage of previous assessment of cybersecurity awareness was comprehensive or not. During their literature search, the authors found 23 studies that matched the search criteria and the information about the authors, publication year, assessment method used, target audiences, coverage of assessment and assessment goals were extracted from each article. The authors found that younger audiences were not explored as a target of assessment as in-depth as it would be required. This is seen as particularly concerning due to the amount of exposure and damage that this target could incur into in case of security incidents. The authors call for both further research in identifying suitable approaches for this target and for the development of programs for CS awareness of the younger population.

Tweneboah-Koduah and Buchanan [23] conducted a comparative study of six existing CI security assessment frameworks, to investigate whether the current solutions are sufficient to assess the security risks exposure of the complexities associated with modern CI systems. In their study, they analyze modern institutional risk assessment standards, including the NIST risk assessment framework, ISO/IEC 27 005:2008 and Bs-7799-2006. These standards are compared with three other enterprise solutions, namely the OCTAVE risk assessment model, the Fair approach and Microsoft security risk management. The authors conclude that the analyzed solutions are not as useful to predict the complexities and dynamic nature of modern CI systems and their supporting technologies, as system interdependencies make defining boundaries more difficult. Finally, the authors propose a tailored solution for modeling and simulation of CI, developed specifically for assessing the security risks associated with controlled technologies supporting critical infrastructure systems.

3. Motivation

As digitalization spreads and influences an increasing number of occupations, the CS skills and knowledge requirements towards the workforce also evolve continuously and rapidly. Additionally, the lack of standardization on which methods and content should be prioritized when developing a CS training program suggests the need for more in-depth analysis. As stated earlier, to the best of the authors' knowledge, a systematic literature review that analyzes and reviews current offerings in terms of awareness and training solutions for CS CIP has not been conducted yet. These aspects motivated the development of this work, which is focused on providing a comprehensive systematic literature review of the current offerings for CS awareness and training for CIP, according to the research objectives presented in the following section. Thus, this study aims to provide useful insights towards a benchmark for the development of effective training modules and programs to increase cyber-security awareness and preparedness for CIP. The future development and methodical evaluation of comprehensive and effective training programs for CI CS.

4. Research method

The literature review was conducted based on the eight-step approach presented by Okoli and Schabram [24], which are presented and discussed in detail below in order to facilitate future extensions or updates:

- Establishing the purpose of the literature review;
- Protocol and training (for any review that employs more than one reviewer);
- Searching of the literature;
- Practical screen;
- Quality appraisal;
- Data extraction;
- Synthesis of studies;
- Writing the review.

4.1. Purpose of the review

The purpose of the review can be summarized as to *identify solutions and offerings for Critical Infrastructure Cyber-Security awareness and training, and also investigate key performance indicators for the evaluation of these solutions*. More specifically, the objectives of the literature review can be encapsulated in the following points:

- Research and identify papers reviewing CI CS training solutions. If any relevant paper is identified, analyze its content and the methodologies adopted. More specifically, the training solutions focused on the energy, nuclear and aviation sector.
- Identify the main target groups for training, focus areas and preferred methodologies within the literature and evaluate the dependencies or lack thereof between the suggested solutions.
- Identify the key performance indicators (KPIs) necessary to evaluate the comprehensiveness and efficacy of the training solutions reviewed;
- Suggest recommendations for future research.

4.2. Protocol and training

Before commencing the systematic literature review, we analyzed the most appropriate methodology to be adopted for this work. Okoli's approach was selected due to its comprehensiveness in research criteria and its standardized screening and data extraction methodologies. As Okoli's approach is defined generically for any SLR, several scientific papers that followed Okoli's approach in the field of computer science and information security had been consulted. It was found that the methodology adopted by Yamin et al. [25] shared research and methodology requirements that were needed in our literature review. Accordingly, this work's methodology has been based on the methodology of their work and adapted to our scope and evaluation criteria. There had been no need for training of other individuals to ensure protocol conformity, as one sole reviewer conducted the literature review.

4.3. Searching for the literature

To identify and collect scientific articles to be evaluated, the following databases were consulted for extraction of related literature: IEEE Xplore, ACM Digital Library, ResearchGate, Google Scholar, ScienceDirect, Scopus, ProQuest and Semantic Scholar. A combination of the following keywords was used to maximize the search output: cyber-security, critical infrastructure, aviation, energy, nuclear, training. The following conditional logic statement further describes how the keywords were combined to create the search combinations: ((Cyber-security OR Cybersecurity) AND (Critical Infrastructure OR Aviation OR Energy OR Nuclear) AND (TRAINING)). This produced a total of 8 keywords combinations. The initial database search produced a total of 106,211 entries. Although we expected the selected search key to produce a high amount of results, with a high likeliness of duplicates, or unrelated articles and, this was necessary to avoid omitting any relevant article as part of the review. Articles that were found to be non-valuable to the research were omitted during the next steps, as described below.

4.4. Practical screening

A set of inclusion and exclusion rules was put in place to screen the result of the literature search:

- Only articles written in English were selected.
- Duplicates found through multiple databases were excluded.
- Articles before the year 2000 were excluded, to avoid the use of antiquated data
- Only scientific articles published in peer-reviewed conferences, workshops and journals were selected.

Only articles that followed the complete list of rules were selected. Nevertheless, not all the results of the screening process are presented in this study, as many were discarded in the next steps, according to the process described below.

4.5. Quality appraisal

One more exclusion rule was set to facilitate the selection of papers. Articles that did not include the combination of keywords in their abstract, title or introduction were discarded. A second round of exclusion was conducted to eliminate further articles that did not contribute to the initial goal: "identify solutions and offerings for CI CS awareness and training or metrics for the evaluation of these solutions". For this purpose, any article that did not focus or extensively describe possible training offerings for CI CS awareness, or that did not provide a comprehensive discussion about possible evaluation criteria for these training offerings was excluded.

4.6. Data extraction

To extract and map the key findings of each paper that was utilized in this review, a data extraction review form was created. This form was organized as a table with eight columns representing key attributes that were deemed necessary and sufficient to identify and summarize each paper.

- Title and Year: title of the paper and year of publishing;
- Authors: List of contributing authors;
- Target: Group of individuals targeted by the training solutions;
- Areas: fields of study, cyber-security and industry areas that the research focuses on or identifies;
- Training method: Methods and tools discussed or developed in the research conducted in each individual paper;
- Evaluation Criteria and KPIs: Methods used for evaluation purposes of proposed solutions or metrics to evaluate its effectiveness.
- Description: Brief description of the content of the paper;
- Conclusions: Final conclusions and results discussed by the authors of the papers and our personal analysis of the results.

4.7. Synthesis of studies

For the synthesis of the studies, we utilized the qualitative material collected in the data extraction and the writing of the reviews. The data was later utilized to map training solutions and methodologies in Section 5. Observations on each category of this mapping are then given in the same sections.

4.8. Writing the review

Writing this systematic literature review has been conducted in accordance with the standard principles for writing research articles, utilizing the method described by Okoli and Schabram [24]. After the initial search, a total of 106,211 articles were found, using the combination of keywords indicated in Section 4.3. This significantly elevated number of results was caused by the lack in many of the database search engines of filters based on the previously mentioned screening criteria. After two rounds of practical screening, consisting of removing any articles that did not fulfill the requirements indicated in Section 4.4, the selection was narrowed down to 2,241 articles. The articles were then further manually checked, to establish their relevancy to the subject of the review. The manual check consisted of excluding articles that did not contain specific references to the keywords mentioned in 4.3. At the same time, articles that did not respect the second rule of the quality appraisal described in 4.5 were also excluded. After the quality appraisal, the final selection came down 68 articles as part of the literature review and 5 articles in the related work section. Many of the articles excluded during screening focused on CS awareness education or on application sectors that were not compatible with the focus of this research. Furthermore, during the quality appraisal, some articles were not considered exhaustive enough in the discussion of training delivery methods or evaluation methods to be included in this work.

5. Literature review

As stated in Section 3, the focus of the literature review will be for articles discussing CS training in the aviation, energy and nuclear sector. Additional papers discussing CS training solutions for CIP are also later discussed, as they provide relevant solutions, adaptable to the sectors mentioned previously.

5.1. Aviation sector

Aircraft manufacturers have integrated into modern aircraft packet switching devices, wireless interfaces and other technologies to reduce cost/size/weight/power, and increase connectivity [26]. These new features have introduced potential CS risks that may affect aircraft safety. Exploits such as morphing, zombies, malicious code, and BOTS/BOTNETS have been reported to be common occurrences both in aviation and other sectors.

De Cerchio and Riley [26] have conducted an analysis of these new risks and what has been developed as suitable countermeasures. Due to the novelty of CS in aviation, FAA (Federal Aircraft Administration) regulations, standards, and guides do not address cybersecurity vulnerabilities. Nonetheless, two CS training for aircraft security have been developed by the FAA: Aircraft Systems Cyber Security Designated Engineering Representative (DER) Seminar, Aircraft Systems Cyber Security Orientation in the electronic Learning Management System (eLMS). The authors later discuss the efforts of the Aerospace Network Security Simulator (ANSS) project to assess and identify network security threats in airborne network environments by integrating industry and government aeronautical simulators. The 3 phase approach of the ANSS project sees the last phase focused on skills development for CS personnel. Gaming technologies, scenario-based training and other solutions have all been discussed and possible methods to develop skills for the future CS workforce. Particular attention has been given to team-based training strategies, with exercises such as red–blue team and capture the flag games being suggested as being effective for achieving the training goals. The authors do not go into further details regarding the requirements of the training modules and the structure of the training.

Gopalakrishnan et al. [27] also discuss the needs for aviation cyber-security, with a focus on education and literacy for the security of U.S. airports. When it comes to CS education, the authors note how the focus should be shifted from the implementation of security controls and mechanisms at the application, operating system, network, or physical technology layers to the ones at the user-layer. The authors discuss how practical security education can be made accessible to airport users and airport employees with minimal technical backgrounds if computer security education is abstracted correctly. The authors conclude by stating that the best solution for airport security is a defense-in-depth or belt-and-suspenders approach (an approach that is not reliant on just one security mechanism, but a combination of mechanisms). As such, CS education should be supported with good CS measures, industry standards and best practices. The authors do not go into further detail regarding the content or the type of solution that would be best suited for CS training.

Kagalwalla and Churi [28] provide a comprehensive review of challenges and solutions on how to tackle issues in aviation cyber-security. When it comes to solutions, the authors cite staff training and skill development as one of the most critical components of aviation CS. It is noted that all personnel should undergo basic CS training, including employees that are not in charge of CS tasks. This is to guarantee all-around base-level security, against prevalent attacks such as phishing attacks. For CS personnel, training should be differentiated and developed at a department level, to ensure that personnel is trained specifically to the tasks they may need to complete. While the authors give a higher degree of detail in describing approaches for staff training, it is still not enough to understand how to best develop basic or specialized CS training programs.

Janisz et al. [29] propose a basic model for cybersecurity requirements definition based on regulatory international aviation security documents. The authors combine the requirements found different control aviation security documents (standards, guidance, and national programs) to form a plurality of all requirements, based on mathematical formulation. Of the seven sub-pluralities showcased by the authors, three of them (relative to administrative regulation, security control and organizational requirements respectively) cited training and retraining as fundamental elements for their model. Unfortunately, the authors only reference the documentation where the data had been extracted from, without providing further details on the type or content of the training.

A similar distinction between basic and specialized training requirements is made by Lykou et al. [30]. In their discussion on CS measures and best practices to improve airport CS resilience, the author surveys which methods have been suggested to be most useful for this specific goal. Providing basic security awareness training to all information system users was indicated to be one of the most needed and successful first measures against CS attacks. When it comes to specialized information security training, the authors indicate that role-based and security-related training should be required before authorizing access to IT systems. Training should also be conducted for personnel involved in incident response roles for the information system. This type of training should consist of user training in the identification and reporting of suspicious activities, both from external and internal sources. Additionally, testing and regular exercises of the airport incident response capability system should be conducted to determine their progressive effectiveness. Integrating the research conducted by the authors with some examples of training solutions would allow determining how to tackle the issue most effectively.

Schmitt et al. [31] offer a more direct cyber-security solution for aviation personnel training, in the form of a simulation-supported CS risk analysis tool. As stated by the authors, simulation scenarios are very effective withing training programs

to support and improve the development and implementation of codes of conduct to face potential cyber-attacks. The tool, which uses an air traffic simulation software called TrafficSim from DLR, allows for Separation and conflict detection, airport slot management, arrival and departure management and development of use case scenarios. Two different scenarios, focused on integrity and availability of flight plan data, have been developed by the authors. Field flight plans have been manipulated in both scenarios, to create inconsistencies. The case scenario demonstrated the usefulness of simulation tools, in aiding in predicting behavior in case of attacks, although significant simplifications were used. Further efforts should be taken in progressing the level of fidelity of simulation tools and integrating them more cohesively to training programs.

Yardley et al. [32] proposed a modular, hands-on and open Smart Grid cybersecurity educational training platform. An initial pedagogical approach is used to give a formal educational background to participants, which is based on 4 pillars: active learning, project-based learning, learn-by-doing posture and constructivism. Additionally, hands-on SCADA security modules are offered in lab-based training. Overall assessment of the education and training program has shown very positive feedback from participants.

5.2. Energy sector

Within the energy sector, many technological advances have occurred, especially when it comes to power distribution. Smart grids are nowadays commonly used for this function. These type of grids have several advantages over traditional power grids such as cost-effectiveness, better communication channels and many additional functionalities. Nonetheless, the digitalization of the power supply process has introduced a slew of cyber-vulnerabilities to these systems and the need for a well prepared CS incident prevention team.

Curtis and Mehravari [33] describe a CS capability maturity model (C2M2) and two tailored versions of this model for the energy and oil & natural gas sectors. These models are to be used to evaluate the overall CS capabilities of these CIs and suggest possible improvements or actions to be taken. The model architecture is composed of 10 domains. One of the domains, relative to workforce management, specifically addresses organizational training and awareness of staff. The model states that a company should establish and maintain plans, procedures, technologies and controls to ensure personnel competence. Evaluation of the training and of any other security-related activities that are to take place is measured using the maturity indicator levels. These levels go from an initial evaluation corresponding to a *not performed* activity to a fourth and final level of *managed*. An activity is considered managed if:

- It is guided by policy and governance;
- Guiding policies include compliance requirements for specified standards or guidelines;
- It is periodically reviewed for conformance to policy;
- Responsibility and authority for practices are assigned to personnel;
- Personnel performing the practice have adequate skills and knowledge.

Rob et al. [34] discuss the need to develop solutions to prevent cyber-attacks on grids and companies in the oil, gas and energy sector. The authors agree that to secure any of these systems, one of the fundamental steps is to create a strong internal policy plan, guidelines and have well-prepared personnel. When developing an awareness program, the authors note four main challenges:

- Selecting the appropriate program;
- Selecting the most effective delivery method;
- Applying an adaptive method to continuously evaluate and modify the program;
- Selecting the best available technology with the best tools to get the message across.

Unfortunately, aside from giving recommendations on how to develop effective awareness programs, the authors do not develop or suggest a tailored solution for their cases.

Strasser et al. [35] do instead develop a training solution for educating both students and power system professionals in complex smart grid applications. The solution is based on a simulation platform which divides the grid system into various parts, each coupled with domain-specific tools to allow for behavior simulation and control. The development of this simulation platform has been motivated by the authors as necessary for improving the understanding of power systems, control systems, communication networks principles, and standards by current and future operators. While the use of the platform is mostly as an educational tool for operational tasks, implementation of behavioral changes and injection of attacks to the simulation system would also allow for CS training.

Hahn et al. [36] give an overview of a smart grid security testbed. This includes a set of control, communication, and physical system components. The testbed under the scrutiny by the authors is the PowerCyber testbed from Iowa State University. The authors discuss the multiple applications of this testbed, which include educational and training purposes, and identifies how various components support these applications. The testbeds allow for both vulnerability assessment and evaluation of the impact of CS attacks. Some of the attacks evaluated are malicious breaker trip, SCADA observability DoS and remedial action scheme DoS. Future work considered by the authors includes the evaluation of the impacts from more sophisticated attacks along with various impact mitigation efforts through both cyber and physical approaches.

One more cyber–physical system (CPS) smart grid CS testbed is described by Oyewumi et al. [37]. ISAAC, the Idaho CPS Smart Grid Cybersecurity testbed, is a cross-domain, distributed, and reconfigurable testbed, which emulates a realistic power utility. While the testbed completion is still to be finished, many of its applications are already fully functional. For training purposes, ISAAC facilitates the use and reproduction of experimental environments. Examples cited by the authors of experimental environments include:

- simulation of holistic CPS organizational models
- simulation of real-world attack case studies, such as false data injection attacks and replay attacks;
- simulation of best-effort damage mitigation models;
- security evaluation of power grid using the RTDS.

The effectiveness of ISAAC as a training tool will only be determined after completion and adoption in educational environments.

An additional educational training solution utilizing a virtual security testbed is proposed by Stites et al. [38]. Their cloud-based solution, namely ThunderCloud, consists of virtual machines connected using a virtual internal network. Remote accessibility to the platform gives it additional training benefits, as it allows students to use it from any location. The training attacks and exercises designed in the platform are based on real and well known CS vulnerabilities and attacks. During the case study conducted by the authors, they asked students to perform reconnaissance on a series of websites created for TLU. Evaluation through surveys indicated that the vast majority of students reported being more

knowledgeable after the use of the testbeds and more prepared against attacks. To confirm the results obtained by the survey, a secondary evaluation process should be conducted to verify whether students were really more well-prepared after using the instrument.

Jauhar et al. [39] developed a model-based process for assessing the security risks from the US National Electric Sector Cybersecurity Organization Resource (NESCOR) failure scenarios. The NESCOR failure scenarios consist of 111 unique cyber-incidents that could negatively impact an electric utility. To support the use of these scenarios, the authors use the CyberSecurity Argument Graph Evaluation (CyberSAGE) approach and software tool. The scenarios show usefulness in determining which instances may require technical intervention as a security measure and which other instances see personnel training as a more successful solution. For example, it was determined by the authors that training personnel on securing networking requirements can reduce the failure probability for two of the modeled attacker settings, the hacker and industrial spy. For the third setting, an inept installer, training was seen as being less useful. This was motivated by how the installer gains access, which is through physical means instead of network means. This model, like other similar models in this domain, can provide useful insight in determining which scenarios should be used for training purposes and how to use the scenarios for this purpose effectively.

Another training simulator for CPS security is discussed by Vellaithurai et al. [40]. Their solution, called SECPSIM, is a user-friendly framework based on mathematical models of corrective control actions against various intrusions and failure scenarios. The two major phases of SECPSIM involve learning from simulation and training operators. One critical feature of SECPSIM is the capability of learning from expert administrators, although also a scripted list of suitable control actions in various simulated cyber–physical intrusion states can be used. The solution was evaluated to be effective in training operators without using or damaging real systems.

Holm et al. [41] developed and tested two experiments to discuss the effects of phishing exercises on smart grid security awareness. The experiments were conducted in collaboration with a business in the electrical power domain industry and involved sending emails with a hyperlink to the victims, camouflaged as update notifications for locally installed software. By observing the results of the attacks, the author noted that more context-aware phishing attempts generated more traffic to malicious websites, but also more reporting of the attacks by the victims. More generic attacks, while generating just a fraction of the traffic of the other one, was not disclosed to the management. This suggests that more efforts should be taken to educate personnel in reporting suspicious emails and possible security breaches. The findings of the research provide useful information in the development of evaluation exercises to be conducted after training periods.

5.3. Nuclear sector

When it comes to nuclear facilities security, often the attention and efforts are reserved on securing physical aspects of the plants Masood [42]. As with the other sectors, the increased digitalization of the control and communication systems of these platforms meant that new efforts should be put on securing the digital and cyber aspects of these infrastructures, with particular focus on training personnel in CS awareness Gupta and Bajramovic [43],Gupta et al. [44].

Masood [42] provides a detailed review of cyber challenges and security incidents that put nuclear power facilities at CS risk and follows it with a discussion on initiatives taken by multiple governmental and regulatory institutions to mitigate the issue. The author states that in past recent nuclear plant accidents, one of the major motives that led to the success of the training could be reconducted to the lack of CS training and knowledge of the personnel. Training procedures that are cited as lacking by the author include internal communication training, CS drills, and large-scale incident response. The authors cite the International Atomic Energy Agency (IAEA) and the World Institute for Nuclear Security (WINS) as major contributors to the development of standardized training strategies for nuclear facility security. The EU has taken similar efforts to aid in the development and training of nuclear plant personnel. While the authors highlight areas that should be the focus of CS training, they do not describe or propose any direct solution.

Kang and Chong [45] develop a methodology for CS assessment for the instrumentation and control (I & C) systems in nuclear power plants. The methodology has the goal of providing qualitative assessments useful to formulate recommendations to bridge the security risk gap. The assessment covers the following managerial, technical, organizational and operational areas of cybersecurity features on I & C systems: cybersecurity policy and plans, organizational security, asset classification and control, personnel security, physical and environmental security, communication and operation management, access control, system development and maintenance, compliance. The personnel or human aspect of CS is assessed through twenty-six questions, relating to responsibilities, training programs, personnel screening, etc. Regarding training, the questions focus on the comprehensiveness and availability training to all personnel and also 3rd party users. Also, the authors note that training should be periodic, as additional information may be needed with the development or adoption of new software, systems, etc. While the methodology provides a holistic tool for CS assessment, it would be not suitable for a thorough evaluation of the training solutions adopted in nuclear facilities, as not enough detail is put in interrogating the structure and content of the training programs. Similarly, more information should be gathered to be given as possible suggestions for the improvement of existing solutions evaluated by the assessment methodology.

Ahn et al. [46] develop cyber-attack scenarios that reflect the characteristics of nuclear power plants (NPPs) using a type of attack model known as scenario graphs. CS regulatory guidelines for NPP established that attack scenarios should be developed and used for tests and training regarding contingency plans. These scenarios are an aid to understand the nature of attacks, potential venues used by the attack, to develop design basis threats, countermeasures and implement CS plans for risk management and penetration testing. The scenarios developed by the authors are based on directed graphs, where the nodes represent, respectively: attackers, events and goals. The edges of the graph represent the relationship between an initial node and a terminal node. Each path must start from an attacker node and end to a goal node. The authors then develop case studies by adopting the model to real cyber-attack cases. This type of solution is an efficient way of providing practical training to CS personnel, especially if supported by simulation tools and previous technical training and assessment.

Kim et al. [47] discuss possible ways to establish CS policies for digital instruments and controls in NPPs. the outlined security setup involves six steps:

- Establishing the organization and system;
- Mapping the basic guidelines;
- Analyzing the risk;
- Formulating the standard of measures;
- Deciding the policy;

Table 1
Abbreviations for assign responsibilities used in RACI charts.

Code	Responsibility
R	Responsible for the realization of an activity
A	Accountable for the realization of an activity
C	Consulted during the realization of an activity
I	Informed of the realization of an activity

Table 2
CS training types identified by the authors and the training target groups associated to each training type.

Type of CS training	Trainees
Awareness training	All employees
Technical training	System engineers and CST
Specialized CS training	CST and CSIRT
Incident response and Recovery Training	CSIRT and System engineers

- Formulating the implementation procedure.

User training should be based on the established security policy, as part o the operation management and human security. Unfortunately, the authors do not detail further about the requirements needed to be present in the CS policies to regulate training.

Rice [48] describes measures to be taken in order to ensure the security of NPPs simulators. When discussing possible entry points for attacks, the author cites multiple digital instruments, communication channels and technologies and lack of training of personnel regarding risks and incident reporting. When it comes to training, Rice states that it needs not only to be implemented at the corporate level, but it needs to be conducted for SCADA or simulation environment as well. Training should be supplemented to best practices and policies to mitigate incidents in the infrastructures effectively. The author does not investigate deeper regarding the requirements of training for simulation environments for NPPs.

Khattak et al. [49] provides a review of articles discussing CS applications in nuclear power plants. In their review, the authors summarize the history of CS and cyber-attacks against NPPs. When it comes to policies, the authors discuss the RG. 1.152–2011 issued by the United States Nuclear Regulatory Commission (USNRC). The document provides a top-down methodology of actions to build up multiple layers of CS assurance. 2 main sections are highlighted: CS program establishment and CS program maintaining. The training plan that should be implemented for the training of the NPP personnel should be defined in the first section, while possible modifications and additions should be conducted during the maintenance.

Gupta and Bajramovic [43] discuss all aspects relating to security culture in nuclear facilities. When discussing training, the authors firstly focus on the necessity for training to ensure proper reporting of security incidents. When it comes to more focused CS training, the authors distinguish requirements for technical staff to be given separately from general CS training. The authors use the acronym RACI to distinguish four main roles that should be receiving differentiated and focused training. Two other types of training described by the authors include security awareness training and technical security training. The former has the goal of providing employees with a better understanding of security risks, while the latter is to be used to extend the skills and qualifications of the security team. Some of the main areas cited for technical security training include network defense, prevalent attack vectors, and advanced security technologies. Annual security testing should also be conducted as a method of evaluation of the training sessions.

In a later work by Gupta et al. [44], the authors provide a more in-depth justification of occasions and sectors of NPP security that justified the need for more CS training. During integrated safety and security training, the authors state that the personnel should receive both awareness training and technical training. The motive and result of the first should be to give a general better understanding of safety and security (S&S) risks, as all personnel should be responsible to a certain degree for S&S. Technical training should be used to extend current skills and qualifications, but also to better identify the roles of individuals. The main areas that should be impacted by the technical training are security testing on safety and the effects on safety by using security controls. Unfortunately, the authors do not highlight any specific training program or methods to achieve the identified goals (see Tables 1 and 2).

Lee et al. [50] conduct a study on nuclear facility CS awareness and training programs. The authors distinguish 4 types of CS training and 4 associated targets for the training.

The authors list the items shown in Table 3 for each category of training as the main content to be taught.

While the authors offer a comprehensive analysis of different types of training, targets and content of training, one limitation of their work is the lack of discussion regarding methods for training and evaluation.

5.4. Critical infrastructure

In this section, we review papers relating to training requirements and solutions for CI CS. Although the papers discussed in this section are not specific to the sectors of aviation, nuclear and energy, they provided relevant insights on CI CS, with findings that could be easily incorporated or adapted to the requirements of the aforementioned sectors.

Pollet and Cummins [51] discussed an all-hazard approach for assessing the readiness of CI against cyber-attacks and threats. The motivation for the approach came from what the authors cited as a lack of effectiveness from previous approaches. This ineffectiveness was motivated by the tendency of previous approaches to focus on evaluating single elements of security at a time, instead of giving a holistic evaluation. Ensuring effective personnel, by offering structured and comprehensive training, was considered to be one of the key factors in CIP. The authors list the following sub-systems as being supportive in guaranteeing effective training: Health and Safety, Onsite Medical Capabilities, Security Training, Job-related Training, Policy Framework, Change Management, Governance, Information Classification, Clear and Repeatable Procedures, Proper Division of Labor, Internal Morale, Systems Management/Asset Inventory. Two other cited recommendations are having a strong situational awareness and verifying the state of emergency management readiness.

Skarga-Bandurova et al. [52] conducted a report on the implementation of an educational program in risk analysis and resilience of critical infrastructures. Four main modules were selected as part of the educational program: foundation of CI security and resilience, security risk analysis techniques and standards, enterprise CS and risk management, ICS security and resilience. The course combines lectures, seminars, and laboratory exercises to provide a comprehensive initial understanding of CI CS awareness. Evaluation of the results from the course showed positive feedback and concrete improvement of students' skills and knowledge. When it comes to challenges, the authors mentioned inadequate equipment and the freeware that had to be used for practical experimentation. Adapting such courses to major industries would most likely guarantee access to better equipment and software, solidifying the effectiveness of such courses.

Table 3
Types of cyber security training and trainees.

Awareness training	Technical training	Specialized CS training	Incident response and Recovery Training
General cyber threats. Methods, attack techniques; Cyber attack cases; Meaning of CIA(confidentiality, integrity, availability) and potential risks from compromising CIA; Five attack vectors (network, wireless, portable media and mobile devices, supply chain, and physical access); Elements of CSP; Technical, operational, and management security controls of RS-015; Organizational contacts to whom to report; Terminologies;	Identification of critical systems (CS) and critical digital assets (CDAs); Security level assignment under the defense-in-depth(DiD) strategy; Assessment of CDAs' compliance with security control requirements in RS-015; Application of required security controls; Performing cyber security activities related to CDAs after the implementation of security controls; Change control; Supports for cyber security incident response;	Developed based on the CDAs of nuclear facilities	Incident handling, incident monitoring, recovery, and reconfiguration

Table 4
Topics for CIS students and engineering students.

CIS students	Engineering students
ICS hardware	Principles and core concepts of CS
ICS software	Commercial solutions for network security
ICS Networks	Security principles in corporate environments
Industrial Environment	

Jarmakiewicz et al. [53] propose a CI testbed for SCADA CS evaluation and assessment. The testbed consisted of one control center CCS and one substation CSS. A communication subsystem modeled in the form of switch and router is used to provide communication within the power station. As with many other testbeds, the authors' proposal can function as a vulnerability assessment tool as well as a comprehensive security training tool. Unfortunately, the authors did not conduct experimentation involving the use of the testbeds for this latter purpose, although they indicate that this is part of their future plans.

Foreman et al. [54] develop educational modules with the objective of providing knowledge both from the CIS and ICS disciplines as a solution for ICS CS education limitations. The topics for the courses are divided between students coming from a CIS background and students from an engineering background. Table Table 4 summarizes the topics proposed for each category of student. Practical exercises in laboratory facilities supported these training modules. The facilities included ICS components such as PLCs, Input/Output devices (I/O), network hardware, computing platforms and software used in industrial settings. The exercises conducted ranged from preliminary exercises to demonstrate hardware and software practices, to final exercises consisting of red team/blue team competitions. The evaluation was conducted through a survey sent before and after the course presentation, to understand how the knowledge of participants had changed. Overall, the solution presented by the author is comprehensive in its components. Training and evaluation methods are also well designed, although, for more accurate evaluation, there may be the need to collect direct reports during the experiments and possibly also from written tests.

Mishra et al. [55] propose a training framework for integrating CIP into cybersecurity training. The framework is built upon multiple, self-contained training modules, with each module having its distinct target. For each training module, an overview, learning outcome, training material, sample questions and assignments component is defined. This modular approach presents multiple benefits, including the ability to integrate with existing lessons, the ability for instructors to add new modules and modify or remove existing ones easily. The authors state that future efforts will be focused on the development of more advanced modules and on evaluating the effectiveness of this modular approach.

Dominguez et al. [56] propose a CS training solution in the mean of a laboratory of CIs CS (CICLab). The lab allows for the simulation of different settings and scenarios in four CI sectors: industry, energy management, building management and smart cities. The activities at the lab are focused on identifying and understanding the elements, network architectures, industrial protocols and field-buses found in automation. Control and monitoring systems, together with network management tools, are made available to allow users to create and configure realistic security scenarios in control systems.

Yoon et al. [57] propose evaluation criteria to assess the readiness of cyber first responders for CIP. The evaluation is a scenario-based series of CS exercises, all with the purpose to assess the responders' team ability to defend against a specific cyber attack. These exercises used a simulated environment of hardware and physical processes, to maintain high levels of fidelity to real systems. A total of five scenarios were designed. For evaluation, a set of criteria derived from the NFPA 1410 concepts was used.

5.5. CS training solutions

In this section, we present an analysis of training solutions for CS found in the literature. These proposals, while not being explicitly developed for CI sectors, present relevant examples of modules, programs and tools developed for the training of CS skills and abilities. Integration or adaptation of the content of these proposals to CI sectors would allow them to be easily incorporated into CS training for CIP. Table Table 5 lists all the works found in the literature that fell in this category of training solutions and provide a brief description of each solution.

6. KPIs and metrics for CS training evaluation

Before commencing the classification and analysis of the CS training solutions discussed in Section 5, we examine evaluation metrics and KPIs identified in the literature for measuring the effectiveness of these solutions. Identification of these KPIs is required to allow the evaluation of the comprehensiveness and effectiveness of the training programs. Additionally, methods and other criteria useful for the measurement of the KPIs are also discussed. The comprehensiveness of a training program can be evaluated before its application, while effectiveness can only be evaluated after completion of the training sessions. As such, the metrics are distinguished based on whether they allow for evaluation of the former or the latter. Another consideration to be made before discussing the evaluation metrics and KPIs is the distinction between effectiveness and efficacy. Effectiveness can be defined as the measure of the degree of beneficial effects under "real world" settings, while efficacy is the measure of results under ideal circumstances [58]. Due to the many factors that can influence the outcomes of CS training, it is necessary that evaluation is conducted on real sessions or experimentation instead of hypothetical, theoretical scenarios.

Unfortunately, there is no formal consensus when it comes to KPIs for CS training, although a number of articles have tried to determine methods for evaluation of training programs.

Table 5
Description of training solutions for CS awareness.

Work	Proposed solution	Description
Willems et al. [59]	Tele-lab: system for hands-on IT security training in a remote virtual lab environment	Web-based tutoring and training environment built on virtual machines. Information is presented in the form of text, multimedia and practice exercises. Each learning unit starts with general information, followed by a more detailed description of tools and procedures and culminates in practical exercises.
Acosta et al. [60]	EmuBox: lightweight CS testbed to facilitates the creation of heterogeneous scenarios; ECEL: extensible software package that enables centralized data acquisition and management.	EmuBox uses multiple tool components to process scenario VMs as *Workshop Units* (WU) and *Workshop Groups* (WG). WU contain the sets of VMs that make up a single scenario. ECEL is a centralized management system that uses a plugin to capture and format evaluator data. The purpose of these two tools is to allow evaluators to develop training scenarios and save the data from training experiments for later evaluation.
Toth and Klein [61]	CS Learning Continuum (CSLC): progressive curriculum for CS education and training.	CSLC is based on the idea that education and training should start out as more generic as possible, to be suited for all users, and culminate in specialized education and experience, specific to selected roles. Important distinction between role-based and topic-based training.
Le Compte et al. [62]	Framework for designing serious games for CS training	The framework is based on a step-by-step approach: preliminary analysis, design, development, game assessment, deployment, player assessment. To integrate CS skills in serious games, the authors extracted the most relevant competences from online CS frameworks.
Cone et al. [63]	CyberCIEGE: interactive video game for security training	CyberCIEGE is composed of a unique simulation engine, a domain-specific scenario definition language, a scenario development tool, and a video-enhanced encyclopedia. Each scenario developed is based on one selected security topic. Certain scenarios may be specific to one specific IT-related job.
Hernández-Ardieta et al. [64]	Indra: Advance Simulator for CS Training	Indra has been designed to enhance 5 skills: prevention, detection/reaction, forensic analysis and attack. 4 different exercises are also supported: forensic analysis, cyber-defense, cyber-attack and cyber-warfare.
Martin and Woodward [65]	Remote Lab	Remote labs provide an accessible solution, which also only has an initial cost overhead and low maintenance costs. The main advantage over simulators is that it allows to observe non-programmed behavior from the system.
Fouché and Mangle [66]	CodeHunt: Platform for Gamification of CS training	Interactive educational gaming platform. Initial introductory texts are used to familiarize participants to the subjects and tools. An incremental approach that introduces new topics and exercises one-by-one is selected. Additional support material is suggested to be integrated to better support participants.
Tioh et al. [67]	Serious Games in CS (Survey of different solutions)	The authors justify the use of serious games for CS training as it combines the benefits of traditional training (cost-effectiveness, low risk, standardized assessments) to the ones of hands-on training (high engagement, tailored learning pace, immediate feedback, skill transferability, active engagement). 13 different serious games are analyzed and evaluated. While all games received positive feedback from the participants of the evaluation experiment, not all produced significant improvement to awareness.
Katsantonis et al. [68]	Game-based approaches for CS training (conceptualization map)	The authors map the key elements of game-based learning in 78 concepts, organized in 8 segments that share 14 links. The key concepts included are: adaptability, analysis, architecture, assessment and feedback, design, game mechanics, learning outcome and pedagogical considerations.
Rajamäki et al. [69]	Prosilience EF: Holistic Cyber Resilience and Security Framework	Framework for education and training of healthcare workers, based on the principle of interactivity, guidance, and relevancy to users' operational environment. Training scheme for the proposed framework can summarized in 5 points: Development of learning concept; Creation of an online module(s) content and delivery; Piloting: joint exercises for IT departments, user and manager education); Hospitals as testbeds/demos; Evaluation on learning achievements;
Adams and Makramalla [70]	Attacker-centric Gamified Approach	Gamification approach for CS training. 4 elements must be respected: progress mechanics, player control, problem solving, story. Additionally, games can be categorized based on 4 aspects: awareness, defensive strategy, offensive strategy and attacker centricity.
Gonzalez et al. [71]	Cybersecurity Training Resources Taxonomy	The presented taxonomy identifies the following resources for CS training through gamification: content oriented, skills developed, tech. resources, game format and target audience.
Hoffman et al. [72]	Holistic Approach to Workforce Development	The approach considers both technical and non-technical aspects of CS compliance. Such an approach needs to include activities defined by workforce structure, continuous professional development and educational opportunities.

(*continued on next page*)

Table 5 (*continued*).

Work	Proposed solution	Description
Jin et al. [73]	Game-based Learning	4 different games had been developed for high school students. Topics selected included social engineering, secure online behavior and 10 CS principles.
Kim et al. [74]	CS training Education and Training System	The system developed is composed of multiple parts, each with a specific purpose. A mail server for education, personal computers, agent system, web server for monitoring & reporting, web server for virtual security threat education.
Urias et al. [75]	CS training platform	The developed platform is built on the standard criteria evidenced in previous solutions. The different types of training offered include appliance training, specific task reinforcement, targeted scenarios, certification/technique training and team studies. The developed training was based on simulated scenarios, with high levels of fidelity and interactivity. One important aspect was the result collection and data output, for evaluation purposes.
Sawyer et al. [76]	Email testbed for evaluating CS training	The email testbed experiment was run in 4 variants. An initial variant that included no training or awareness activity and three variants that included different forms and levels of awareness and training. A second experiment was developed using the testbed, which involved participants having to download certain files, some of which were malicious. Both experiments showcased the efficacy of training.
Beyer and Brummel [77]	Effective CS training implementation	Seven requirements are indicated. SMEs must examine the job and specific cybersecurity functions by level for employees in the organization. I–O psychologists must conduct analysis and guide SMEs. Assess through analysis if the personnel is conducting tasks appropriately. Develop objectives that impart specified knowledge, skills and attitude levels commensurate with task requirements. SMEs must determine which methods best support objectives and conduct training. SMEs must evaluate training effectiveness and determine whether it has produced anticipated outcomes. Data is used to adapt training or adopt non-training solutions.
Korpela [78]	Use of Data Analytic to Improve CS Training	Data sources identified include: LMS, firewall logs, email server audit and activity logs, surveys, phishing simulators, anti-virus alerts, awareness campaigns. Benefits cited include cost and resource efficiency, improved general and targeted training and support to trainees.
Nagarajan et al. [8]	CyberNEXS: CS gaming tool	CyberNEXS, offers on-site and remote training. 5 gaming modes are included to teach about cyber defense and penetration testing. Increasing flexibility, scalability and adaptability of the system is suggested to improve the game modes.
Silva et al. [79]	Tracer FIRE: Competitive CS exercise	Initial series of lectures concerning pertinent topics , followed by a multi-day competitive event. Multi-topic, *Jeopardy-styled* questions.
Amorim et al. [80]	Gamification of Training for CS	Authors take efforts in understanding whether gamification of training is the most effective approach to CS training. Approaches based on the Agile methods that promote continuous change and adaptation of the model are suggested.
Jin et al. [81]	Game-based CS training	The training targeted high-school students and focused on educating on the following topics: social engineering and information security, secure online behavior, cyber-defense.
Antonioli et al. [82]	SWaT Security Showdown (S3): ICS security game	A water treatment testbed is developed. Two PLCs and a remote input–output (RIO) are used. A capture-the-flag event is used for training, based on *jeopardy*-styled and attack-defense mechanisms.
Patriciu and Furtuna [83]	Guide for Designing CS exercises	Guide proposed to homogenize the design of CS training exercises. 7 steps: objectives, approach, topology, scenario, rules, metrics and lesson learned. Objectives can be split into offensive and defensive security. Each step determines the design of the following step.
Salah [84]	Cloud-based CS Teaching	Cloud-based solutions present the advantage of having pre-configured tools and accessibility Amazon AWS cloud is used. Exercises offered with the cloud include packet sniffing, network footprinting and port scanning, vulnerability assessment and pen-testing, backdoor establishment, firewalls, snort NIDS, Dionaea Honeypot, OpenSSL. One main limitation of this solution is the high initial overhead of knowledge needed to use the offerings.
McClain et al. [85]	Tracer FIRE: Forensic and Incident Response Exercise. Analysis of Human Performance during CS Exercises	Use of Tracer FIRE for team-based exercises. Performance is later analyzed through questionnaires and tools available in Tracer FIRE. Due to the team-based nature of the exercise, the member with highest experience were reported to be the one taking charge and submitting the results.

(*continued on next page*)

Table 5 (*continued*).

Work	Proposed solution	Description
Beuran et al. [86]	CyTrONE: integrated cybersecurity training framework	Categories of training: attack-oriented, defense-oriented, forensic analysis. Two goals: easy to manage and modify training content and automated creation of training environments. Scenarios are based on the competences and skills previously captured of the participant. Assessment is based on coverage of relevant NIST guidelines.
Tang et al. [87]	Interactive Cybersecurity Defense Training Inspired by Web-based Learning Theory	Training based on the two modules used by CyTrONE Beuran et al. [86]. Use of multiple databases for setup: vulnerability, exploit, instantiation databases. Training over LMS, allows participants to choose a scenario or attack and train.
Proctor [88]	CS Awareness Training Program Efficacy Evaluation	Study evidences the need to understands audience needs and stratification. Additionally, CS training should be integrated to existing or future installations of other CS measures.
Boopathi et al. [89]	Gamification for Learning CS	Level-based CS training game. Each level tests students knowledge at a different knowledge depth. Capture-the-Flag exercises conducted. Case studies and number of breaches should be used to measure a program's effectiveness. User's response, including emotional evaluation should be taken in consideration.
Willems and Meinel [90]	CS Training in Virtual Lab	Assessment of practical exercises in online lab, based on virtual machine technology. After parameterizing the scenarios, they are dynamically imported to the virtual environment.
Dodge et al. [91]	CDX: Cyber Defense Exercise	Well-established educational exercise aimed at students, giving both education and hands-on training. One particular note is that these team based exercises promote development of leadership skills in certain individuals.
Aldawood and Skinner [92]	Review of CS Social Engineering Programs	Challenges that have been noted in development and installation of a successful CS training program include business environmental factors, social, constitutional, organizational, economical and personal factors.
Raman et al. [93]	Serious Game-based Approach to CS Concept Learning	Development of game with multiple scenarios to support CS concept learning. The assessment was conducted through two control groups, one which was trained using the game-based approach and one that was not. The first group showed much higher knowledge and efficacy in combating CS threats.
Pastor et al. [94]	Simulation Systems for CS Education, Training and Awareness. State-of-the-art	13 simulation systems were found and reviewed by the authors. The systems were categorized by their technical features: remote usability, virtualization, scalability and license. Additionally, target audience, teaching objectives and learning curve of each solution was considered.
Kercher and Rowe [95]	Training CS Workforce Using Student Red Teams	Offer penetration testing through red teams to local organization. Teams of up to 5 students and a faculty advisor. Highlighted the importance of mentoring.
Aoyama et al. [96]	CS Training for Cyber Incident Resilience	Blue/Red team exercise, with blue team with about double the number of participants from red team. Exercise showed that lack of communication and information sharing, distrust of management and lack of experience led to the blue team to lose against the red team.
Nicholson et al. [97]	(1) 3D gaming environment, a virtual Cyber Security Instruction Environment (CYSTINE), Red-team verse blue-team, live simulation, exercises	The 3D gaming environment is developed and used for insider threat training. CYSTINE is used for penetration testing with cognitive agent defenders. Lastly, live simulation and red-team/blue-team exercises are used as realistic, challenging experiences for computer network defense.
Tunc et al. [98]	CLaaS: Cybersecurity Lab as a Service	CLaaS offers virtual CS experiments accessible from remote. The testbeds available include a DNS attack scenario, network packet sniffing experiment scenario, DDoS attack scenario.
Salah et al. [99]	Cloud Computing for CS Teaching	Use of Cloud (Amazon AWS) to teach two CS courses across two different campuses. Centralized control is given to one instructor. Eight labs were used with the cloud: packet sniffing, network footprinting and port scanning, vulnerability assessment and penetration testing, backdoor establishment, firewalls-EC2, Dionaea honeypot, OpenSSL.
Abawajy [13]	CS Awareness Delivery Methods: User Preferences	The authors first identify the different types of awareness delivery methods, categorizing them as conventional methods, instructor-led methods, online delivery methods, game-based, video-based and simulation based delivery methods. From experimentation, the authors found that many of the methods had their own advantages and should be integrated to offer an effective and user-approved awareness training.

(*continued on next page*)

Proctor [88] conducted an investigation with the aim of understanding the effectiveness of CS training programs. The authors agreed that finding accurate metrics for determining the performance of these programs can be challenging, but have suggested a few criteria. One first example was statistical data regarding

Table 5 (*continued*).

Work	Proposed solution	Description
Herr and Allen [100]	Videogames for CS training	The authors cited video games' ability to reach a larger audience, comprising also individuals not familiar or interested in CS, as one of the main appeals in using video games for training. It is an especially effective tool for the teaching of undergraduate and graduate students. Highlighted attributes for successful training video games are realism, ability to reinforce key concepts and skills, complexity scale and clear ability to identify goals and learning objectives.
Olano et al. [101]	SecurityEmpire: Digital Game for CS Education and Training	Digital game with core narrative to teach IA concepts. It uses central server to run the game and web-based access to allow students to join. For evaluation, review of gameplay metrics, player surveys about their experiences playing the game, observations of research team during game play sessions, open ended questionnaires, and semi-structured group interviews were all used.
Beuran et al. [102]	Evaluation of Practices and Methodologies for CS Education and Training	Training programs were classified based on training content, activities, target participants, level of complexity, availability and frequency. A list of criteria is established to correctly analyze the effectiveness of each training program.

breaches or other CS incidents before and after the implementation of training programs. Evidence-based on this type of data can be hard to retrieve due to the secretiveness nature of such information, usually kept confidential by companies and firms to avoid the occurrence of more attacks. Furthermore, a decrease in number of breaches or attacks cannot be directly linked as the outcome of CS training, as other security implementations may have also affected the breach and incidents statistics.

An additional method for evaluation described by the author consists of conducting experiments to assess personnel preparedness and ability to detect and report attacks. An example of such type of experiment is the West Point Carronade case study [103], where students had been randomly sent emails containing malicious links and attachments. A similar experiment was conducted by Sawyer et al. (2015) [76]. In their experiment, the authors used an email testbed that was able to automatically generate malicious and non-malicious emails to evaluate the results of CS training. The evaluation consisted of collecting data about different populations of students, each trained to a different extent, on their ability to detect malicious emails. Two indicators in particular were collected by the authors: the number of students opening the malicious emails and the number of students reporting cases of malicious emails. For both instances, it was noted that students that had received practical training were more likely to detect the malicious emails and also report them, with low numbers of false-positive reporting. Bowen et al. [104] conducted a similar experiment in which participants were also sent malicious emails. The participants that failed to detect the malicious emails were informed about their oversight and then selected to be sent ulterior emails until they would be able to detect the attack attempts. After four rounds, all 2000 participants were able to report the malicious mail.

Psychological principles that can influence the outcome of training should also be considered. Research by Gragg [105] showed that overloading information, relation with authoritative figures and carelessness in training procedures could all negatively impact the psyche of participants, decreasing the effectiveness of training. Gratian et al. [106] discuss how certain personality traits and predispositions can affect individual's performance in CS behavior intention, which can also be assumed to be valid during training procedures. To have a better understanding of personnel's point of view on CS training, a popular method is collecting feedback, in the form of surveys, questionnaires and interviews. The main use of this feedback is to understand both the perceived improvement of participants in their ability and their personal evaluation of the training content and delivery method. This is particularly important as user's engagement is often an indicator or a motivating factor behind the success of CS training programs [92,107]. Abawajy [13] conducted a study on user preference for CS awareness delivery methods. After training participants using different delivery methods, the authors analyzed the performance of the participants and also their preferences. The majority of participants declared that their preferred method of training was the video-based training, although also the other methods were reported to be enjoyed by most participants. A similar study was conducted later by Ricci et al. [107]. In their study, the authors focused on finding not only audience's fields of interests in CS, but also willingness to participate in different awareness and training programs. The study showed that although the majority of respondents was willing to participate in training sessions, the amount of time they would like to dedicate to these sessions was often the minimum option.

Beuran et al. [102] conduct an analysis of the effectiveness of training programs and offerings at a national level in Japan. After categorizing each training program, a set of requirements is listed by the authors to ensure the effectiveness of CS education and training:

- Training content should be appropriate for the target audience(in terms of knowledge and ability levels);
- Training content should be in accordance with the skills that the program aims to develop;
- Training programs should use hands-on activities for developing practical abilities, to ensure that trainees can deal with real-life incidents;
- Training programs should reach the largest audiences possible;
- Training programs should have good cost/performance characteristics, to ensure long-term sustainability.

These requirements are aligned with the findings of Proctor and can also be translated as requiring training platforms to have two key features: the ability to modify and add training content, ability to generate automatically and manage the training environment.

Establishing data collection procedures and aiding data collection from training experiments is also crucial in the evaluation of a training program. This can be achieved with the use of data acquisition software [60] or data and log analytics [78,108]. Potential data sources for analytics include LMS, firewall logs, awareness campaigns, anti-virus alerts, phishing simulations, activity logs and surveys [78]. In the case of data logs retrieved directly from CS exercises, metrics for the evaluation of the data should be carefully established, especially in the case of team-based experimentation. The risk that could occur is that the

Table 6
Metrics categories identified from the literature. Abbreviations: Quant.: quantitative; Qual.: qualitative; Eff.: Effectiveness; Comp: comprehensiveness.

Metrics and KPIs cat.	Type	Classification	Measurement units	Data source
CS incident records	Quant.	Eff.	Number of data breaches or other incidents that occurred before and after training.	Internal Reports on attacks and incidents.
User Performance	Quant.	Eff.	Outcome of CS exercises and tests; Comparison of pre-training and post-training test results; Evaluation of threats detection, prevention and report rates, from tests and real-life occurrences	Data analytics from exercises; reports from evaluators; analytics about threat detection and reporting times.
User Feedback	Qual.	Eff. & Compr.	User evaluation of training program's content, delivery methods, accessibility, usability; Improvement suggestions	Surveys; Questionnaires; Interviews.
Compliance to User Needs and Roles	Quant.	Compr.	Results of maturity models scoring; Internal evaluation (User feedback & user performance evaluation methods);	Standard certification evaluation; Company or National standard/guidelines/ best practices compliance;
Compliance to Companies' Requirements	Quant.	Compr.	Results of maturity models scoring; User Performance evaluation methods; Standard certification evaluation;	Maturity Models; Company or National standard/guidelines/ best practices compliance;

evaluation of a group of participants could be based on the results obtained by one or a few selected members of the group [85].

In addition to exercises, maturity models have also been proposed as an evaluation metric, although they are often used for broader security evaluation. On example is the model described by Curtis and Mehravari [33], which is developed for evaluating the security capability of companies in the electricity and oil & natural gas sectors. The model is used for the evaluation of 10 domains of CS practices, one of which being workforce management (which includes personnel training). The same evaluation indicators are used for all domains. A domain is considered managed if all activities and best practices defined are respected. This includes compliance to policies, periodical revision, role assignment and personnel adequacy. Another model found in the literature is the one proposed by Parsons et al. [109]. In their model, the authors try to evaluate respondents' knowledge, behavior and abilities (KBAs) on different focus areas of information security awareness by developing the Human Aspects of Information Security Questionnaire (HAIS-Q). While the overall goal of the authors was to understand the relationship between knowledge of policies and procedures and behavior when using computers, the evaluation classification could be adapted for CS training evaluation.

An additional metric often taken into consideration when evaluating the effectiveness of a CS training program or of the personnel is adherence to national and company standards, policies and guidelines. Yoon et al. [57] for examples adapt the NFPA 1410 standards used to assess the readiness of firefighter first responders and develop exercises for evaluating first responders in CIP. For this purpose, a blend of simulated environments and physical systems was used to develop an evaluation environment. Several scenarios, characterized by an objective, a type of attack and specific evaluation criteria were developed in the environment. The criteria were based on real-life requirements in case of attacks, such as specific detection and report time windows, removal of the threat and recovery of the system. The team tasked with evaluating the participants had to determine deficiencies in abilities, provide focused feedback, identify key indicators used by the participants to respond to attacks and evaluate the effectiveness of procedures and action plans.

When talking about the comprehensiveness of a CS training program, a few criteria have been cited. While basic awareness courses may be suitable for general staff, more specialized training should be personalized for target groups, covering certain roles and tasked to complete similar actions [72]. This can be translated as the ability of a training program to satisfy the specific needs of single or groups of users, based on their existence competencies and knowledge, roles and actions performed and other individual factors. For firms, alignment should be done based on previous and existing threats. Additional to personnel requirements, firm-specific requirements should also be considered. This means that training should take into consideration both workforce structure, known vulnerabilities and prior incidents. A more detailed description of the recommended design considerations for CS training programs is given in the following section. (See Tables 4 and 5.)

In Table 6, the metrics and KPIs collected from the literature have been grouped in categories, based on the type of measurement. For each group, measurement units, possible data sources and metric type (whether they are quantitative or qualitative, measures of comprehensiveness or effectiveness) were also identified.

The list of KPIs and metrics groups shown in Table 6 is supposed to provide a general instrument for evaluation of CS training programs. A few considerations should be made before using these metrics for evaluation purposes. Exact goals, values and frequency of measurement should be set when determining KPIs. These values should be based on the desired outcome of each training program and session. Values or value ranges should correspond to levels of comprehensiveness and effectiveness reached by the CS training solution. This in turn should be dependent on the design of the CS exercise. Patriciu and Furtuna [83] have described in their 7-step design of CS exercises how evaluation of results of the exercises and collecting feedback from the participants is a fundamental last step in the design of a CS exercise and should be based on the previous steps. In their design methodology, the authors distinguish 7 forward chaining steps.

As it can be seen from Fig. 1, the first step consists on defining the objectives of the exercise. Based on these objectives, the appropriate approach will then need to be decided. The infrastructure and systems to be used should subsequently be agreed upon, and the topology should reflect this choice. At this point, the scenarios to present to the participants must be defined, in a

Fig. 1. 7 steps identified by Patriciu and Furtuna [83] for designing CS exercises.

Table 7
Examples of learning objectives and possible metrics for effectiveness, as presented by Patriciu and Furtuna [83].

Learning objective	Metric for effectiveness
Implement security configurations on a specific system	Number of successful attacks performed by the attacker teams on that system
Systems' security monitoring	Percentage of detected attacks over the total number of attacks performed.
Incident handling/response	Time taken to recover from a successful attack
Log analysis and forensics	Number of attacks correctly identified
Scanning and enumeration	Percentage of open ports/services detected over the total number of open ports (pre-configured)
DDoS	Downtime of the attacked service compared to attack duration
Cover tracks and place backdoors	Number of successful accesses to target systems kept until the end of the exercise

way that is realistic and stimulating to the users. A set of rules, which should include scoring system, eligibility, legal issues and limitations should also be put in place, based on the scenario. Appropriate metrics for the evaluation of the exercise should then be defined, which should be tightly related to the initial objectives. Finally, evaluators should try to receive feedback from users about the lesson learned during the exercises. As noted by the author, specific metrics should be established based on the learning objectives and the design of the exercise. Examples of objective-specific metrics given by Patriciu and Furtuna [83] are shown in Table 7.

Since training instructors and evaluators are often consulted in designing and implementing CS training exercises, they should be also consulted in determining precise KPIs and desired outcome values for the evaluation of the training sessions. This would further allow the alignment of learning objectives and metrics for effectiveness.

7. Classification & analysis of CS awareness training solutions

To compare CS awareness programs, training awareness programs must be first classified based on distinguishing attributes. Various CS training taxonomies have been found in the literature. Beauran et al. (2016)[102] suggested multiple methodologies for determining CS training taxonomies. Based on the authors' observations, training can be classified based on content, activities, participants, level, availability or frequency. Gonzalez et al. [71] propose an upgraded version of the classification by Beuran et al. [102], by adding resources employed as a criterion and substituting participants with target audience.

When classifying by content, a popular categorization subdivides training offerings in attack-oriented, defense-oriented and analysis/forensic-oriented training. Attack-oriented training is focused on how to reproduce exploits on known vulnerabilities [86], while defense-oriented training builds skills related to vulnerability patching and how to protect the systems [86]. Finally, forensic analysis training tries to provide a deeper understanding of the attack and its consequences by identifying targeted attack campaigns and other information [86,102].

Further attributes to distinguish training methods are accessibility and usability [94]. Accessibility determines whether a training solution can be accessed remotely or needs physical presence in the location of the training or the experimentation tools. Usability is a qualitative criterion that tries to classify training solutions based on how well users are able to use the material and tools required to perform the training activities. Due to its

Table 8
Classification of CS training methods, with examples found in the literature and associated advantages and disadvantages.

Delivery method	Examples	Advantages	Disadvantages
Conventional Methods	On-site courses; Paper-based teaching and exercises; Presentations & Conferences; On-site training sessions;	Usability; Familiarity of format; Multiple messages can be conveyed at once; Ease of communication between instructor and participants; Real-time resolution of issues; (Possible) team skills development;	No guarantee of personnel active participation; Can be perceived as tedious [110]; Does not always provide hands-on experience; Provides a static solution for a fluid problem [111]; High cost and resource overhead; Time consuming;
Online and Software-based	Online courses; Cloud-based training; Web-accessible training material and software; E-mail tests;	Remote and multi-modal accessibility [13]; Industry-wide standard use; Cost-effective; Hands-on exercises; (Possible) team skills development;	Users may undermine the value/pay less attention; Not always very scalable and adaptable; High cost and resource overhead, if personalized solution is needed; Does not provide instructor assistance;
Game-based	Serious Games for CS Awareness and Training	Team skills development, Engaging to users; Hands-on exercises, Demonstrated effectiveness [82,86,86]; Adaptability; (Possible) Remote Usability; (Possible) High scalability;	Older audiences may not be familiar with mechanics; Time consuming; May not reflect real-life processes. High initial development cost and resource overhead;
Video-based	Educational videos	Accessibility, Usability; Cost-efficient; Time efficient;	Limited content. Lack of interactivity with other trainees or instructors. Lack of hands-on experience. No guarantee of personnel active participation; Requires constant integration and updates for scalability;
Simulation and virtualization-based	Testbeds, Simulation platforms, Simulated Laboratory exercises	Team skill development; Hands-on experience; Replication of real-life incidents; Adaptability; (Possible) Remote Usability; (Possible) High scalability;	Hard to coordinate [112]; Requires pre-existing knowledge; Time consuming; High initial development cost and resource overhead;

qualitative nature, this attribute is better used as an evaluation criterion rather than a classification of CS awareness training.

Beuran et al. [102] suggested that training activities should be chosen based on what type of skills the training is aiming to develop, be it individual skills, team skills or Computer Security Incident Response Team (CSIRT) skills.

Based on the research of [113], providing authentic learning environments allow students to capture knowledge and engage in activities with many more benefits than traditional theorical learning. Ten fundamental characteristics [114] are cited for a learning environment or activity to be considered "authentic":

- Authentic activities (AA) have real-world relevance;
- AA are ill-defined, requiring students to define the tasks needed to complete the activity;
- AA comprise complex tasks to be investigated by students over a sustained period of time;
- AA provide the opportunity for students to examine the task from different perspective;
- AA provide the opportunity to collaborate;
- AA provide the opportunity to reflect;
- AA can be used in different areas and lead beyond domain-specific outcomes;
- AA are seamlessly integrated with assessment;
- AA activities create polished products valuable in their own right;
- AA allow competing solutions and diversity of outcomes.

When it comes to activities, multiple training and teaching delivery methods have been identified in the literature. The classification proposed by Abawajy (2014) [13] groups the methods in 6 categories: Conventional, Instructor-led, online-based, game-based, video-based and simulation-based methods. In this paper, we modify the classification proposed by Abawajy [13], to follow the findings of the literature review. In Table 8, we divide delivery methods in 5 categories and list their respective advantages and disadvantages.

Table 9
Delivery methods used by the solutions identified in the literature, for each CI sector.

	Aviation	Nuclear	Energy	Others	Total
Conventional	4	4	1	8	17
Online/ Software-based	1	/	3	7	11
Game-based	/	/	/	16	16
Video-based	/	/	/	/	/
Simulation /virtualization-based	2	1	4	13	20

In Table 9, the number of solutions that adopted any of the previously mentioned categories of delivery methods is reported. Both the total number and the number for each highlighted sector of CI are shown.

As it can be seen from Table 9, the majority of solutions proposed in the literature suggest simulation and virtualization techniques as the preferred delivery methods. This preference can be justified by the numerous advantageous attributes that distinguish simulation and virtualization systems. As mentioned by Pastor et al. [94], these types of systems can be used both for educational and training purposes, by providing hands-on experience to users. As the systems simulate with a high level of fidelity CI systems, the exercises developed provide realistic CI threat scenarios. Many of these solutions also allow for remote usability, by means of custom made clients, APIs and real-world network connections [94]. High levels of scalability, usability and detail, adequate learning curves are additional advantages that simulation systems can offer [94]. Not all simulation systems provide the same levels of advantageous properties. In fact, to guarantee completeness of a system, high scalability and usability, a great deal of initial cost and resource overhead may be required.

Conventional methods and game based methods also were found to be well represented in the literature, but for opposite

reasons. Conventional teaching and training, consisting of on-site activities has retained popularity due to the familiarity of its format and ease of development due to its standardization. Game based methods are instead a more recent development. As it can be seen from Table 9, specific serious games have yet to be developed for individual sectors of CI. Instead, the majority of CS games have been developed for the teaching and training of generic CS concepts and often target either the general public or students in academia [93,115]. The main advantages of game based training is high engagement with users, practical application and exercises and the ability to develop team skills [73,80]. Unfortunately, this type of solution is still in is infancy when it comes to application to aviation, energy, nuclear and other CI industry sectors. Further development would be needed to render game-based training solutions more appropriate for personnel training in specific sectors.

None of the articles analyzed in the literature review developed video-based CS training offerings. Nonetheless, [13] have found in their study that video-based teaching has often high user engagement and as such could find application. Integrating educational videos to conventional solutions would allow to increase user engagement. Additionally, educational videos could be used together with game-based and simulation-based solutions to provide background knowledge and technical aspects necessary for completion of the CS exercises offered.

From this analysis, it could be suggested that for offering practical CS training for CIP, simulation and virtualization platforms and systems present a higher number of advantages than other solutions. These types of solution satisfy the criteria for authentic activity theory developed by Reeves et al. [114], offer highly scalable and adaptable scenarios and exercises. Depending on their specific implementation, they can also satisfy the majority if not all requirements established by Beuran et al. [102], shown in Section 6. Additionally, this type of solution has already been well established as a training tool for CS training for different CI sectors, as shown in Table 9. Nonetheless, research on development and improvement of these types of platform should be continued to allow for better targeting of CS roles, offering realistic and up-to-date attack and defense scenarios and to increase scalability and accessibility for users.

Unfortunately, the financial cost and resources to be allocated for the establishment of comprehensive training programs is often an obstacle for most firms. As such, consideration should be taken in finding well-rounded and cost-efficient solutions. Challenges do not only come in the form of economic limitations; social, business environmental, organizational and personal challenges have also been often reported in the literature[92]. Depending on the established business environment and organization structure of a company, implementing a new solution may be challenged by personnel unfamiliarity, distrust in effectiveness or anxiety of failure [92]. A possible solution for these challenges, especially in the case of simulation-based and game-based training solutions, is to support participants by siding non-expert personnel with CS experts or senior personnel.

8. Limitations

Although in this study we tried to conduct a comprehensive literature review of CS training solutions for CIP and to discuss the optimal evaluation criteria and methods for these training solutions, a few limitations have been denoted:

- Evaluation metrics and KPIs value range determination: the metrics and KPIs identified in this work have been determined from the literature search and articles discussing the effectiveness of CS awareness training solutions. What has been noted during the analysis of these articles was the lack of exact values corresponding to different evaluation results for the metrics and KPIs applied. It is recommended that in future work, exact values or results corresponding to effectiveness and comprehensiveness levels of the CS training solutions are determined, similarly to the 4-level evaluation table used in the maturity model proposed by Curtis and Mehravari [33]. Additionally, it is important that these value ranges are determined based on the distinguishing properties of the training offering that is being evaluated.
- Interdependencies between KPIs and metrics: As stated by, [88], there is no universally agreed method for evaluating a CS training solution and determining the effectiveness of a solution can be challenging. The KPIs and metrics shown in Table 6 provide a comprehensive list of evaluation criteria found in the literature. Unfortunately, the adequacy of these criteria has not been formally determined. Additionally, which combination of evaluation criteria is best suited for the evaluation of specific training programs has also not been determined. Future research should focus on conducting a study on the adequacy and interdependencies of these criteria when evaluation a CS training solution.
- Interdependencies between CS awareness training and other security measures for CIP: CS training is only one of the lines of defense to be used for CS incident preparedness and CIP. Formulating standards, policies and guidelines [116], implementing security procedures and defense tools [117] to protect the systems, the network and any other component of CI is also necessary. All these defensive measures should be implemented to be complementary to each other. As such, when developing and implementing a CS awareness and training program specific to a firm, other security measures that have been implemented and future measures should also be considered.
- Firm-specific limitations: As mentioned in Section 7, there may be a number of obstacles in the implementation of an optimal CS training solution inside of a company, due to budget/resource thresholds or other limitations. Multiple studies have been conducted to determine these challenges [92,118,119]. These challenges may obstacle achieving optimal training solutions and as such they need to be considered when developing a CS training program. A direct consultation with industry personnel should be required to solidify knowledge on these challenges and which attributes may need prioritization when developing and implementing a firm-specific CS training program.

9. Conclusions & future work

The human element has been indicated as one of the greatest vulnerabilities to CIP [120]. Many of the modern cyber incidents are caused by the lack of knowledge and preparedness of personnel in detecting and preventing cyber attacks [3,4]. In our previous work [15], we conducted a systematic literature review with the purpose of investigating and analyzing key competencies and skills required for CS in CI. As stated in [15], there is still no agreement when it comes to optimal delivery methods for acquiring the skills and competencies extrapolated and there is also a lack of studies focusing on identifying and analyzing training offerings for CI CS. For this reason, in this work, we conducted a systematic literature review of proposed solutions for CS training, with a focus on solutions for the aviation, energy and nuclear sector. In Section 5, methods of delivery, target audiences, advantages and disadvantages of groups of solutions have also been discussed. Additionally, in Section 6, we conducted an analysis of evaluation criteria for these solutions, by reporting metrics and KPIs that could be used to assess a training program's

effectiveness and comprehensiveness. Evaluation methods and data sources for these metrics have also been discussed. Based on the findings of the literature review, it was found that delivery methods that offered hands-on experience, in the form of training scenarios and team-based exercises were often preferred over traditional or alternative methods. Simulation and virtualization platforms and systems in particular were shown to be a popular CS training tool, both for CI-sector specific training and general CS concept training. The main advantages offered by this category of solutions are fidelity to real-life CS procedures, hands-on training, team skills development, scalability and adaptability [94]. Nonetheless, agreement on which solution should be considered optimal has not been reached by researchers and all of the solutions analyzed presented a number of disadvantageous features. Further research should be conducted to establish whether integrating different beneficial attributes found across different proposals could produce a more effective and comprehensive solution. A more in-depth study of sector and firm-specific challenges should also be conducted, to determine which challenges may hinder the development of effective and comprehensive CS training solutions and which attributes should be prioritized. Finally, further studies should focus on analyzing the effectiveness of the metrics and KPIs highlighted in this work as evaluation measures for CS training. In future work, we plan on tackling all these limitations by developing training scenarios and exercises, and using training delivery methods mentioned in this work for CI personnel testing. This should also allow further research on establishing value-specific KPIs and metrics for the evaluation of the exercises' output.

CRediT authorship contribution statement

Nabin Chowdhury: Conceptualization, Formal analysis, Investigation, Methodology, Writing - original draft, Data curation, Validation. **Vasileios Gkioulos:** Supervision, Writing - review & editing, Validation.

Declaration of competing 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.

Funding

This work was supported by the Norwegian Institute of Science and Technology (NTNU).

References

[1] Symantec Security Response, Dragonfly: Cyberespionage Attacks Against Energy Suppliers, 2014, v.1.21. URL: https://www.broadcom.com,
[2] H. MacKenzie, How Dragonfly hackers and RAT malware threaten ICS security, 2014, Belden, Indianapolis, Indiana: Industrial Security Blog.
[3] Jessica Davis, Ransomware, Phishing Attacks Compromised Half US Orgs in 2019, 2020, URL: https://healthitsecurity.com/news/ransomware-phishing-attacks-compromised-half-us-orgs-in-2019. [Online; posted 28-January-2020],
[4] I. Ghafir, V. Prenosil, J. Svoboda, M. Hammoudeh, A survey on network security monitoring systems, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2016, pp. 77–82, http://dx.doi.org/10.1109/W-FiCloud.2016.30.
[5] IRM, Amateyrs attack technology. Professional hackers target people, 2015, www.irmplc.com. URL: www.irmplc.com/issues/human-behaviour.
[6] Debo Chris, Preventing cyberattacks and data breaches via employee awareness training and phishing simulations, schneiderdowns (2015) URL: https://www.schneiderdowns.com/our-thoughts-on/.
[7] European Commission, in: European Commission (Ed.), July Infringements Package: Key Decisions, 2018.
[8] Ajay Nagarajan, Jan M. Allbeck, Arun Sood, Terry L. Janssen, Exploring game design for cybersecurity training, in: 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), IEEE, 2012, pp. 256–262.
[9] Wonhyung Park, Seongjin Ahn, Enhancing education curriculum of cyber security based on NICE, KIPS Trans. Comput. Commun. Syst. 6 (7) (2017) 321–328.
[10] Johanna Jacob, Wei Wei, Kewei Sha, Sadegh Davari, T Andrew Yang, Is the NICE cybersecurity workforce framework (NCWF) effective for a workforce comprised of interdisciplinary majors?, in: Proceedings of the International Conference on Scientific Computing (CSC), The Steering Committee of The World Congress in Computer Science, Computer …, 2018, pp. 124–130.
[11] Keith S. Jones, Akbar Siami Namin, Miriam E. Armstrong, The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals, ACM Trans. Comput. Educ. (TOCE) 18 (3) (2018) 1–12.
[12] Barbara Krumay, Edward W.N. Bernroider, Roman Walser, Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework, in: Nordic Conference on Secure IT Systems, Springer, 2018, pp. 369–384.
[13] Jemal Abawajy, User preference of cyber security awareness delivery methods, Behav. Inf. Technol. 33 (3) (2014) 237–248.
[14] Hussain Aldawood, Geoff Skinner, Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues, Future Internet 11 (2019) 73, http://dx.doi.org/10.3390/fi11030073.
[15] Nabin Chowdhury, Vasileios Gkioulos, Key competencies for critical infrastructure cyber-security: a review, in: Unpublished Results, Submitted After Minor Revision before Acceptance, Unpublished results, 2020.
[16] Melad Mohamed Al-Daeef, Nurlida Basir, Madihah Mohd Saudi, Security awareness training: A review, in: Proceedings of the World Congress on Engineering, vol. 1, 2017, pp. 5–7.
[17] Ponnurangam Kumaraguru, Yong Rhee, Steve Sheng, Sharique Hasan, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Getting users to pay attention to anti-phishing education: evaluation of retention and transfer, in: Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit, 2007, pp. 70–81.
[18] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge, Protecting people from phishing: the design and evaluation of an embedded training email system, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2007, pp. 905–914.
[19] John R. Anderson, Lynne M. Reder, Herbert A. Simon, Situated learning and education, Educ. Res. 25 (4) (1996) 5–11.
[20] Abdullah Alnajim, Malcolm Munro, An evaluation of users' anti-phishing knowledge retention, in: 2009 International Conference on Information Management and Engineering, IEEE, 2009, pp. 210–214.
[21] Faisal Alotaibi, Steven Furnell, Ingo Stengel, Maria Papadaki, A review of using gaming technology for cyber-security awareness, Int. J. Inf. Secur. Res.(IJISR) 6 (2) (2016) 660–666.
[22] Noor Hayani Abd Rahim, Suraya Hamid, Miss Laiha Mat Kiah, Shahabodin Shamshirband, Steven Furnell, A systematic review of approaches to assessing cybersecurity awareness, Kybernetes (2015).
[23] Samuel Tweneboah-Koduah, William J. Buchanan, Security risk assessment of critical infrastructure systems: A comparative study, Comput. J. 61 (9) (2018) 1389–1406.
[24] Chitu Okoli, Kira Schabram, A guide to conducting a systematic literature review of information systems research, SSRN Electron. J. 10 (2010) http://dx.doi.org/10.2139/ssrn.1954824.
[25] Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos, Cyber ranges and security testbeds: Scenarios, functions, tools and architecture, Comput. Secur. (ISSN: 0167-4048) 88 (2020) 101636, http://dx.doi.org/10.1016/j.cose.2019.101636, URL: http://www.sciencedirect.com/.
[26] Raymond De Cerchio, Chris Riley, Aircraft systems cyber security, in: 2011 IEEE/AIAA 30th Digital Avionics Systems Conference, IEEE, 2011, pp. 1C3–1.
[27] Kasthurirangan Gopalakrishnan, Manimaran Govindarasu, Doug W. Jacobson, Brent M. Phares, Cyber security for airports, Int. J. Traffic Transp. Eng. 3 (4) (2013) 365–376.
[28] Navid Kagalwalla, Prathamesh P. Churi, Cybersecurity in aviation: An intrinsic review, in: 2019 5th International Conference on Computing, Communication, Control and Automation (ICCUBEA), IEEE, 2019, pp. 1–6.
[29] Karina Janisz, Oleksandr Korchenko, Sergiy Gnatyuk, Roman Odarchenko, Model for cybersecurity requirements definition in civil aviation, Autobusy: Tech. Eksploatacja Syst. Transp. 17 (12) (2016) 630–634.
[30] Georgia Lykou, Argiro Anagnostopoulou, Dimitris Gritzalis, Implementing cyber-security measures in airports to improve cyber-resilience, in: 2018 Global Internet of Things Summit (GIoTS), IEEE, 2018, pp. 1–6.
[31] Angela R. Schmitt, Christiane Edinger, Thomas Mayer, Josef Niederl, Tobias Kiesling, Simulation-supported aviation cyber-security risk analysis: a case study, CEAS Aeronaut. J. 10 (2) (2019) 517–530.

[32] Tim Yardley, Suleyman Uludag, Klara Nahrstedt, Pete Sauer, Developing a smart grid cybersecurity education platform and a preliminary assessment of its first application, in: 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, IEEE, 2014, pp. 1–9.
[33] Pamela D. Curtis, Nader Mehravari, Evaluating and improving cybersecurity capabilities of the energy critical infrastructure, in: 2015 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE, 2015, pp. 1–6.
[34] Rafat Rob, Tolga Tural, Gareth W McLorn, Abdullah Sheikh, Ahmad Hassan, Addressing cyber security for the oil, gas and energy sector, in: 2014 North American Power Symposium (NAPS), IEEE, 2014, pp. 1–8.
[35] Thomas Strasser, Matthias Stifter, Filip Andrén, Peter Palensky, Co-simulation training platform for smart grids, IEEE Trans. Power Syst. 29 (4) (2014) 1989–1997.
[36] Adam Hahn, Aditya Ashok, Siddharth Sridhar, Manimaran Govindarasu, Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid, IEEE Trans. Smart Grid 4 (2) (2013) 847–855.
[37] Ibukun A. Oyewumi, Ananth A. Jillepalli, Philip Richardson, Mohammad Ashrafuzzaman, Brian K. Johnson, Yacine Chakhchoukh, Michael A. Haney, Frederick T. Sheldon, Daniel Conte de Leon, Isaac: The idaho cps smart grid cybersecurity testbed, in: 2019 IEEE Texas Power and Energy Conference (TPEC), IEEE, 2019, pp. 1–6.
[38] Joseph Stites, Ambareen Siraj, Eric L. Brown, Smart grid security educational training with thundercloud: a virtual security test bed, in: Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, 2013, pp. 105–110.
[39] Sumeet Jauhar, Binbin Chen, William G. Temple, Xinshu Dong, Zbigniew Kalbarczyk, William H. Sanders, David M. Nicol, Model-based cybersecurity assessment with nescor smart grid failure scenarios, in: 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC), IEEE, 2015, pp. 319–324.
[40] Ceeman Vellaithurai, Anurag Srivastava, Saman Zonouz, SECPSIM: A training simulator for cyber-power infrastructure security, in: 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2013, pp. 61–66.
[41] Hannes Holm, Waldo Rocha Flores, Göran Ericsson, Cyber security for a smart grid-what about phishing? in: IEEE PES ISGT Europe 2013, IEEE, 2013, pp. 1–5.
[42] Rahat Masood, Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives, Cybersecurity and Privacy Research Institute the George Washington University, 2016.
[43] Deeksha Gupta, Edita Bajramovic, Security culture for nuclear facilities, in: AIP Conference Proceedings, vol. 1799, AIP Publishing LLC, 2017, 050014.
[44] Deeksha Gupta, Edita Bajramovic, Holger Hoppe, Antonio Ciriello, The need for integrated cybersecurity and safety training, J. Nucl. Eng. Radiat. Sci. 4 (4) (2018).
[45] Young-Doo Kang, Kil To Chong, Development of cyber security assessment methodology for the instrumentation & control systems in nuclear power plants, J. Korea Acad.-Ind. Coop. Soc. 11 (9) (2010) 3451–3457.
[46] Woogeun Ahn, Manhyun Chung, Byung-Gil Min, Jungtaek Seo, Development of cyber-attack scenarios for nuclear power plants using scenario graphs, Int. J. Distrib. Sens. Netw. 11 (9) (2015) 836258.
[47] Zeen Kim, Jangseong Kim, Youngdoo Kang, Kwangjo Kim, Dai I. Kim, Choong Heui Jeong, Guideline of cyber security policy for digital i&c systems in nuclear power plant, in: Transactions of the Korean Nuclear Society Autumn Meeting, vol. 10, 2007.
[48] Brandon Rice, Nuclear Power Plant Simulation and Cybersecurity, Tech. Rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.
[49] Muhammad Adil Khattak, Muhammad Khairy Harmaini Shaharuddin, Muhammad Saiful Islam, Muhammad Hakimi Nik Ahmad, Review of cyber security applications in nuclear power plants, J. Adv. Res. Appl. Sci. Eng. Technol. 7 (1) (2017) 43–54.
[50] Jung-Woon Lee, Jae-Gu Song, Cheol-Kwon Lee, Study on nuclear facility cyber security awareness and training programs, 2016.
[51] Jonathan Pollet, Joe Cummins, All hazards approach for assessing readiness of critical infrastructure, in: 2009 IEEE Conference on Technologies for Homeland Security, IEEE, 2009, pp. 366–372.
[52] Inna Skarga-Bandurova, Alexandr Ryazantsev, Katerina Kiryushatova, An experience report on education and training programme in cybersecurity of critical infrastructures, Inf. Secur. Int. J. 35 (2016) 123–132.
[53] Jacek Jarmakiewicz, Krzysztof Maślanka, Krzysztof Parobczak, Development of cyber security testbed for critical infrastructure, in: 2015 International Conference on Military Communications and Information Systems (ICMCIS), IEEE, 2015, pp. 1–10.
[54] Chris Foreman, M. Turner, K. Perusich, Educational modules in industrial control systems for critical infrastruc-ture cyber security, in ASEE Annual Conference and Exposition, Conference Proceedings, vol. 122, 2015, p. 01.
[55] Sumita Mishra, Rajendra K. Raj, Carol J. Romanowski, Jennifer Schneider, Anthony Critelli, On building cybersecurity expertise in critical infrastructure protection, in: 2015 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE, 2015, pp. 1–6.
[56] Manuel Dominguez, Miguel A. Prada, Perfecto Reguera, Juan J. Fuertes, Serafin Alonso, Antonio Moran, Cybersecurity training in control systems using real equipment, IFAC-PapersOnLine 50 (1) (2017) 12179–12184.
[57] Jungsang Yoon, Stephen Dunlap, Jonathan Butts, Mason Rice, Benjamin Ramsey, Evaluating the readiness of cyber first responders responsible for critical infrastructure protection, Int. J. Crit. Infrastruct. Prot. 13 (2016) 19–27.
[58] Gerald Gartlehner, Richard A. Hansen, Daniel Nissman, Kathleen N. Lohr, Timothy S. Carey, Criteria for distinguishing effectiveness from efficacy trials in systematic reviews, 2006.
[59] Christian Willems, Thomas Klingbeil, Lukas Radvilavicius, Antanas Cenys, Christoph Meinel, A distributed virtual laboratory architecture for cybersecurity training, in: 2011 International Conference for Internet Technology and Secured Transactions, IEEE, 2011, pp. 408–415.
[60] Jaime C. Acosta, Joshua McKee, Alexander Fielder, Salamah Salamah, A platform for evaluator-centric cybersecurity training and data acquisition, in: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), IEEE, 2017, pp. 394–399.
[61] Patricia Toth, Penny Klein, A role-based model for federal information technology/cyber security training, NIST Specl. Publ. 800 (16) (2013) 1–152.
[62] Alexis Le Compte, David Elizondo, Tim Watson, A renewed approach to serious games for cyber security, in: 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, IEEE, 2015, pp. 203–216.
[63] Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, Thuy D. Nguyen, A video game for cyber security training and awareness, Comput. Secur. 26 (1) (2007) 63–72.
[64] Jorge L. Hernández-Ardieta, David Santos, Pascual Parra, Juan E. Tapiador, Pedro Peris-López, Javier López, Gerardo Fernández Navarrete, An Intelligent and adaptive live Simulator: A new concept for Cybersecurity Training, 2011, Indra, Madrid.
[65] Nancy L. Martin, Belle Woodward, Building a cybersecurity workforce with remote labs, Inf. Syst. Educ. J. 11 (2) (2013) 57.
[66] Sandro Fouché, Andrew H. Mangle, Code hunt as platform for gamification of cybersecurity training, in: Proceedings of the 1st International Workshop on Code Hunt Workshop on Educational Software Engineering, 2015, pp. 9–11.
[67] Jin-Ning Tioh, Mani Mina, Douglas W. Jacobson, Cyber security training a survey of serious games in cyber security, in: 2017 IEEE Frontiers in Education Conference (FIE), IEEE, 2017, pp. 1–5.
[68] Menelaos N. Katsantonis, Panayotis Fouliras, Ioannis Mavridis, Conceptualization of game based approaches for learning and training on cyber security, in: Proceedings of the 21st Pan-Hellenic Conference on Informatics, 2017, pp. 1–2.
[69] Jyri Rajamäki, Julia Nevmerzhitskaya, Csaba Virág, Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF), in: 2018 IEEE Global Engineering Education Conference (EDUCON), IEEE, 2018, pp. 2042–2046.
[70] Mackenzie Adams, Maged Makramalla, Cybersecurity skills training: an attacker-centric gamified approach, Technol. Innov. Manag. Rev. 5 (1) (2015).
[71] Hugo Gonzalez, Rafael Llamas, Francisco Ordaz, Cybersecurity teaching through gamification: Aligning training resources to our syllabus, Res. Comput. Sci. 146 (2017) 35–43.
[72] Lance Hoffman, Diana Burley, Costis Toregas, Holistically building the cybersecurity workforce, IEEE Secur. Privacy 10 (2) (2011) 33–39.
[73] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, Jonathan White, Evaluation of game-based learning in cybersecurity education for high school students, J. Educ. Learn. (EduLearn) 12 (1) (2018) 150–158.
[74] Bong-Hyun Kim, Ki-Chan Kim, Sung-Eon Hong, Sang-Young Oh, Development of cyber information security education and training system, Multimedia Tools Appl. 76 (4) (2017) 6051–6064.
[75] Vincent E. Urias, Brian Van Leeuwen, William M.S. Stout, Han W. Lin, Dynamic cybersecurity training environments for an evolving cyber workforce, in: 2017 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE, 2017, pp. 1–6.
[76] Ben D. Sawyer, Victor S. Finomore, Greg J. Funke, Vincent F. Mancuso, Brent Miller, Joel Warm, P.A. Hancock, Evaluating cybersecurity vulnerabilities with the email testbed: Effects of training, in: Proceedings 19th Triennial Congress of the IEA, vol. 9, 2015, p. 14.
[77] Richard E. Beyer, B.J. Brummel, Implementing effective cyber security training for end users of computer networks, in: SHRM-SIOP Science of HR Series: Promoting Evidence-Based HR, 2015.
[78] Karina Korpela, Improving cyber security awareness and training programs with data analytics, Inf. Secur. J.: Glob. Perspect. 24 (1–3) (2015) 72–77.
[79] Austin Ray Silva, Jonathan T. McClain, Benjamin Robert Anderson, Kevin S. Nauer, Robert Abbott, James C. Forsythe, Factors Impacting Performance in Competitive Cyber Exercises, Tech. Rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2014.

[80] Joni A. Amorim, Maurice Hendrix, Sten F. Andler, Per M. Gustavsson, Gamified training for cyber defence: Methods and automated tools for situation and threat assessment, in: NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111), 2013.
[81] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, Jonathan White, Game based cybersecurity training for high school students, in: Proceedings of the 49th ACM Technical Symposium on Computer Science Education, 2018, pp. 68–73.
[82] Daniele Antonioli, Hamid Reza Ghaeini, Sridhar Adepu, Martin Ochoa, Nils Ole Tippenhauer, Gamifying ICS security training and research: Design, implementation, and results of S3, in: Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, 2017, pp. 93–102.
[83] Victor-Valeriu Patriciu, Adrian Constantin Furtuna, Guide for designing cyber security exercises, in: Proceedings of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy, World Scientific and Engineering Academy and Society (WSEAS), 2009, pp. 172–177.
[84] Khaled Salah, Harnessing the cloud for teaching cybersecurity, in: Proceedings of the 45th ACM Technical Symposium on Computer Science Education, 2014, pp. 529–534.
[85] Jonathan McClain, Austin Silva, Glory Emmanuel, Benjamin Anderson, Kevin Nauer, Robert Abbott, Chris Forsythe, Human performance factors in cyber security forensic analysis, Proc. Manuf. 3 (2015) 5301–5307.
[86] Razvan Beuran, Dat Tang, Cuong Pham, Ken-ichi Chinen, Yasuo Tan, Yoichi Shinoda, Integrated framework for hands-on cybersecurity training: CyTrONE, Comput. Secur. 78 (2018) 43–59.
[87] Dat Tang, Cuong Pham, Ken-ichi Chinen, Razvan Beuran, Interactive cybersecurity defense training inspired by web-based learning theory, in: 2017 IEEE 9th International Conference on Engineering Education (ICEED), IEEE, 2017, pp. 90–95.
[88] Wesley R. Proctor, Investigating the Efficacy of Cybersecurity Awareness Training Programs (Ph.D. thesis), Utica College, 2016.
[89] K. Boopathi, S. Sreejith, A. Bithin, Learning cyber security through gamification, Indian J. Sci. Technol. 8 (7) (2015) 642–649.
[90] Christian Willems, Christoph Meinel, Online assessment for hands-on cyber security training in a virtual lab, in: Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON), IEEE, 2012, pp. 1–10.
[91] R.C. Dodge, Daniel J. Ragsdale, Charles Reynolds, Organization and training of a cyber security team, in: SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483), vol. 5, IEEE, 2003, pp. 4311–4316.
[92] Hussain Aldawood, Geoffrey Skinner, Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues, Future Internet 11 (3) (2019) 73.
[93] Raghu Raman, Athira Lal, Krishnashree Achuthan, Serious games based approach to cyber security concept learning: Indian context, in: 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), IEEE, 2014, pp. 1–5.
[94] Vicente Pastor, Gabriel Diaz, Manuel Castro, State-of-the-art simulation systems for information security education, training and awareness, in: IEEE EDUCON 2010 Conference, IEEE, 2010, pp. 1907–1916.
[95] Kellie E. Kercher, Dale C. Rowe, Risks, rewards and raising awareness: training a cyber workforce using student red teams, in: Proceedings of the 13th Annual Conference on Information Technology Education, 2012, pp. 75–80.
[96] Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Wataru Machii, Kohei Seki, Studying resilient cyber incident management from large-scale cyber security training, in: 2015 10th Asian Control Conference (ASCC), IEEE, 2015, pp. 1–4.
[97] Denise Nicholson, Lauren Massey, R. O'Grady, E. Ortiz, Tailored Cyber-security training in LVC environments, in: MODSIM World Conference, Virginia Beach, VA, 2016.
[98] Cihan Tunc, Salim Hariri, Fabian De La Peña Montero, Farah Fargo, Pratik Satam, Youssif Al-Nashif, Teaching and training cybersecurity as a cloud service, in: 2015 International Conference on Cloud and Autonomic Computing, IEEE, 2015, pp. 302–308.
[99] Khaled Salah, Mohammad Hammoud, Sherali Zeadally, Teaching cybersecurity using the cloud, IEEE Trans. Learn. Technol. 8 (4) (2015) 383–392.
[100] Christopher Herr, Dennis Allen, 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, 2015, pp. 23–29.
[101] Marc Olano, Alan Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac Sohn, Donna Thomas, SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education, in: 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), USENIX Association, San Diego, CA, 2014, URL: https://www.usenix.org/conference/3gse14/summit-program/presentation/olano.
[102] Razvan Beuran, Ken-ichi Chinen, Yasuo Tan, Yoichi Shinoda, Towards effective cybersecurity education and training, in: Research report (School of Information Science, Graduate School of Advanced Science and Technology, Japan Advanced Institute of Science and Technology), IS-RR-2016-003, 2016.
[103] Aaron J. Ferguson, Fostering e-mail security awareness: The west point carronade, Educ. Q. 28 (1) (2005) 54–57.
[104] Brian M. Bowen, Ramaswamy Devarajan, Salvatore Stolfo, Measuring the human factor of cyber security, in: 2011 IEEE International Conference on Technologies for Homeland Security (HST), IEEE, 2011, pp. 230–235.
[105] David Gragg, A multi-level defense against social engineering, SANS Reading Room 13 (2003).
[106] Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, Amy Ginther, Correlating human traits and cyber security behavior intentions, Comput. Secur. 73 (2018) 345–358.
[107] Joseph Ricci, Frank Breitinger, Ibrahim Baggili, Survey results on adults and cybersecurity education, Educ. Inf. Technol. 24 (1) (2019) 231–249.
[108] Robert G. Abbott, Jonathan McClain, Benjamin Anderson, Kevin Nauer, Austin Silva, Chris Forsythe, Log analysis of cyber security training exercises, Proc. Manuf. 3 (2015) 5088–5094.
[109] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, Cate Jerram, Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q), Comput. Secur. 42 (2014) 165–176.
[110] John Leach, Improving user security behaviour, Comput. Secur. 22 (8) (2003) 685–692.
[111] J. Andrew Valentine, Enhancing the employee security awareness model, Comput. Fraud Secur. 2006 (6) (2006) 17–19.
[112] Anshul Kumar, Mansi Chaudhary, Nagresh Kumar, Social engineering threats and awareness: a survey, Eur. J. Adv. Eng. Technol. 2 (11) (2015) 15–19.
[113] Jan Herrington, Thomas C. Reeves, Ron Oliver, Authentic learning environments, in: Handbook of Research on Educational Communications and Technology, Springer, 2014, pp. 401–412.
[114] Thomas C. Reeves, Jan Herrington, Ron Oliver, Authentic Activities and Online Learning, Higher Education Research and Development Society of Australasia, Inc, 2002.
[115] Maurice Hendrix, Ali Al-Sherbaz, Bloom Victoria, Game based cyber security training: are serious games suitable for cyber security training? Int. J. Ser. Games 3 (1) (2016) 53–61.
[116] Adam Sedgewick, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, Tech. Rep., 2014.
[117] William Hurst, Madjid Merabti, Paul Fergus, A survey of critical infrastructure security, in: International Conference on Critical Infrastructure Protection, Springer, 2014, pp. 127–138.
[118] Hussain Aldawood, Geoffrey Skinner, Challenges of implementing training and awareness programs targeting cyber security social engineering, in: 2019 Cybersecurity and Cyberforensics Conference (CCC), IEEE, 2019, pp. 111–117.
[119] Henrique Santos, Teresa Pereira, Isabel Mendes, Challenges and reflections in designing cyber security curriculum, in: 2017 IEEE World Engineering Education Conference (EDUNINE), IEEE, 2017, pp. 47–51.
[120] Ibrahim Ghafir, Jibran Saleem, Mohammad Hammoudeh, Hanan Faour, Vaclav Prenosil, Sardar Jaf, Sohail Jabbar, Thar Baker, Security threats to critical infrastructure: the human factor, J. Supercomput. 74 (10) (2018) 4986–5002.