symmetry

MDPI

Review

Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches

Abdullah M. Alnajim [1,*,†], Shabana Habib [1,†], Muhammad Islam [2,†], Hazim Saleh AlRawashdeh [3,†] and Muhammad Wasim [4,†]

[1] Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia; s.habibullah@qu.edu.sa
[2] Department of Electrical Engineering, College of Engineering, Qassim University, Unaizah 56452, Saudi Arabia; muha.khan@qu.edu.sa
[3] Department of Computer Science, College of Engineering and Information Technology, Onaizah Colleges, Onaizah 56447, Saudi Arabia; hazim@oc.edu.sa
[4] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan; m.wasim@icp.edu.pk
* Correspondence: najim@qu.edu.sa
† These authors contributed equally to this work.

Abstract: Considering the alarming increase in cyberattacks and their potential financial implications, the importance of cybersecurity education and training cannot be overstated. This paper presents a systematic literature review that examines different cybersecurity education and training techniques with a focus on symmetry. It primarily focuses on traditional cybersecurity education techniques and emerging technologies, such as virtual reality (VR) and augmented reality (AR), through the lens of symmetry. The main objective of this study is to explore the existing cybersecurity training techniques, identify the challenges involved, and assess the effectiveness of cybersecurity training based on VR and AR while emphasizing the concept of symmetry. Through careful selection criteria, 66 primary studies were selected from a total of 150 pertinent research studies. This article offers valuable insights into the pros and cons of conventional training approaches, explores the use of VR and AR in cybersecurity education concerning symmetry, and thoroughly discusses the challenges associated with these technologies. The findings of this review contribute significantly to the continuing efforts in cybersecurity education by offering recommendations for improving employees' knowledge, engagement, and motivation in cybersecurity training programs while maintaining symmetry in the learning process.

Keywords: security; education; traditional training techniques; virtual reality; augmented reality

Citation: Alnajim, A.M. ; Habib, S.; Islam, M.; AlRawashdeh, H.S.; Wasim, M. Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry* **2023**, *15*, 2175. https://doi.org/10.3390/sym15122175

Academic Editors: Tomohiro Inagaki, Christos Volos and Sergei D. Odintsov

Received: 19 August 2023
Revised: 19 September 2023
Accepted: 29 September 2023
Published: 7 December 2023

1. Introduction

Statistics of the last five to six years have reported that internet crime complaints have considerably increased, showing 515,612 complaints in 2020, while 162,091 complaints were reported previously [1]. In the year 2021, phishing and allied cyberattacks, business emails, and malware were the main sources of data breaches. According to recent statistics, in 2022, ransomware cyberattacks surpassed phishing attacks due to the primary reason of data compromises [2]. As end users, individuals play a vital role in defending against cyberattacks. However, the challenge is to identify the fake and malicious content and recognize it as an attack [3]. An IBM (2022) report declared that 25% of security breaches in industrial organizations occurred due to human errors [4]. The lack of effective staff training is the main cause of the success of these attacks [5,6].

In the realm of cybersecurity, occurrences of data breaches, cyberattacks, and widespread high-profile data compromises are prevalent. Thus, ensuring robust cybersecurity strategies is a critical need for both business and government organizations [7,8]. The sophisticated

and evolving nature of cyberattacks—especially those that use social engineering techniques (malware, phishing)—is a big challenge in the development of a robust cybersecurity system [9,10]. Employees represent the most vulnerable point in an organization's cybersecurity framework [11,12]. Thus, organizations should focus on effective training and education of employees and allocate the required resources [13], along with the development of a security awareness culture [14]. The use of the latest security technologies without effective cybersecurity training does not guarantee the mitigation of the recent cyberattacks [14]. According to IBM (2019) [15], human error remains the most significant aspect in causing security breaches, as employees increasingly fall victim to phishing attacks and misconfiguring servers. The rise in cost, sophistication, and frequency of cyberattacks demands comprehensive personnel training, and a security shield remains the foundation of organizations' cybersecurity strategies. Effective cybersecurity training of the employees is the most essential cybersecurity asset for any organization [16]. So, organizations must spend more and more on cybersecurity training to boost their employees' knowledge [17,18]. However, most cybersecurity training is underfunded [19,20]. In addition, most employees do not follow the organization's cybersecurity policies, which may disturb the effectiveness of a training program and may lead to frequent data and security breaches [21]. So, a robust cybersecurity training program that can lead to improved employee knowledge, motivation, and engagement is needed for organizations.

One of the most critical challenges arising with technological advancements is the protection of systems against cyberattacks [22]. There is a need to establish robust infrastructure security procedures, starting at the grassroots level and involving local governments. As a result, cybersecurity has become a fundamental aspect of information systems education, particularly due to the emergence of hacktivist groups, such as Anonymous, whose primary objective is to disrupt the information systems of various governments [23]. Within each organization, information system analysts bear the responsibility of educating and training employees about cyber risks, ensuring their awareness, and enabling them to make well-informed decisions that prioritize the organization's security [24].

To deal with these problems, education and training of an organization's employees regarding cybersecurity fundamentals, such as the identification of certain attacks and following the required countermeasures to deal with these attacks, are required. This paper aims to present a comprehensive analysis of the training techniques for cybersecurity education using a systematic literature review (SLR) methodology.

To the best of the authors' knowledge, the proposed study has the following distinctions over previous surveys:

1. We conducted a systematic literature review that covers almost all existing literature on cybersecurity training approaches.
2. We carried out a well-defined approach for searching articles, inclusion/exclusion, and data extraction while avoiding any possible bias.
3. We performed a detailed analysis of the conventional, VR, and AR cybersecurity training techniques.

1.1. Research Goals

The main goal of this study is to explore and analyze the current research regarding cybersecurity training methods, including traditional, VR, and AR-based techniques. The core of the study is based on four different research questions.

1. RQ1: What are the traditional cybersecurity training techniques?
2. RQ2: What are the main issues with traditional cybersecurity training techniques?
3. RQ3: What are the current trends in cybersecurity training techniques?
4. RQ4: What are the main challenges of AR and VR-based cybersecurity training techniques?

1.2. Contribution and Layout

This SLR contributes to the ongoing efforts for cybersecurity education and to enhance personal skills to effectively countermeasures against cyberattacks. The main contributions of the study can be summarized as:

1. We conducted an SLR in the area of cybersecurity education training and identified 66 primary studies out of 150 relevant articles (see Appendix A).
2. We classified these articles based on different conventional cybersecurity education techniques and discussed their pros and cons.
3. We also identified and discussed state-of-the-art recent VR and AR-based cybersecurity training systems.
4. We identified various issues associated with the implementation of recent VR and AR-based cybersecurity training approaches.

This study can be helpful for researchers to extend their knowledge in this area. Similarly, the presentation of advanced technology (AR and VR) for cybersecurity education along with their pros and cons will give researchers a basis for further advancement in this research area.

The paper is organized as follows: Section 2 presents the research methodology. Section 3 discusses the findings of the study, and, finally, Section 4 is the conclusion.

2. Research Methodology

We followed the SLR approach [25] due to its systematic and prevalent use in literature reviews. It involves a review of the literature using a predefined set of steps to identify, analyze, and interpret the available research related to the given research question [25,26]. The complete scenario of the SLR is depicted in Figure 1.

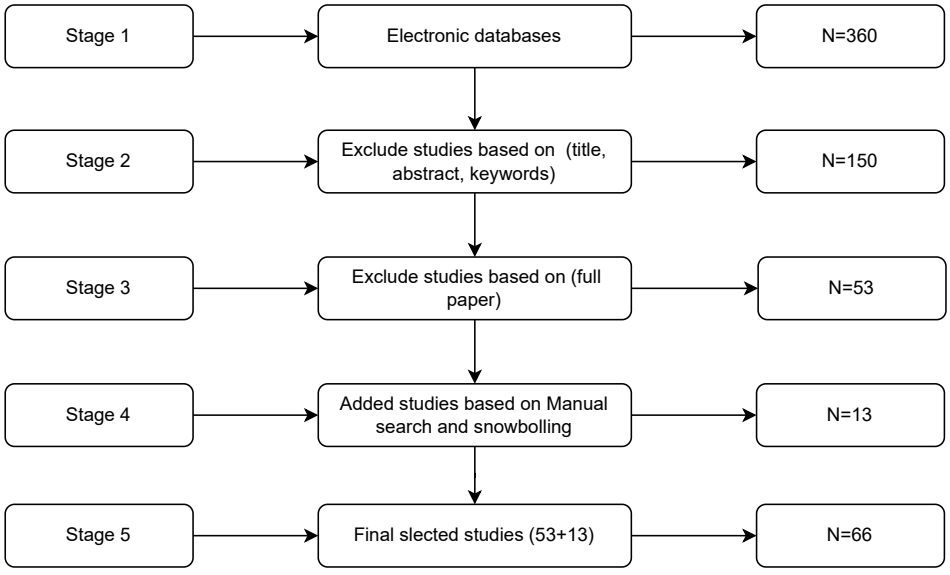


Figure 1. The complete scenario of article selection for the SLR.

2.1. Research Article Search Strategy

Searching for articles in online digital libraries is one of the critical steps in an SLR. First, we designed a search string according to the SLR recommendations [25]. For this purpose, we developed a search string consisting of the basic keywords along with necessary synonyms using different Boolean operators. The final search string for the selection of articles is given below.

$$(cybersecurity\ AND\ (virtualreality\ OR\ augmentedreality\ OR\ extendedreality) AND\ (training\ OR\ education)\ AND\ (methods\ OR\ techniques\ OR\ approaches))$$

To search for relevant articles using the above string, we searched six different online digital libraries: Google Scholar, IEEE Xplore, Science Direct, ACM, Springer, and Wiley (see Table 1). These well-known online databases are assumed to provide the necessary literature on this topic. Furthermore, we used a manual search and the snowballing approach [27] to search for further relevant articles. Using this search string, we identified a total of 360 articles in the above online databases.

Table 1. Articles Search Results.

Databases	First Filtration	Second Filtration	Third Filtration	Final Selected Studies	Percent Selected (%)
IEEE Xplore	68	35	22	14	21.2
Google Scholar	80	42	25	17	25.7
Science Direct	85	18	12	7	10.6
ACM	50	21	10	5	7.5
Springer	71	32	18	10	15.15
Wiley	6	2	0	0	0
Snowballing				9	13.6
Manual Search				4	6
Total	360	150	87	66	100

2.2. Article Selection Criteria

Different filters were applied for the selection of relevant research articles (see Table 2). In the first stage, different online databases were searched for research articles using a predefined set of keywords. The first stage identified a total of 360 articles from the six different databases. In the second stage, we reviewed these articles and included them based on the relevance of the title, abstract, and keywords of the articles. We selected a total of 150 relevant articles in this stage while excluding others. In the third stage, we read complete articles and followed the following inclusion/exclusion criteria:

1. The articles were specific to cybersecurity training techniques.
2. The papers were specific to traditional, VR-, AR-, or XR-based cybersecurity training methods.
3. We included articles that were peer-reviewed and written in English.
4. We included recent versions of studies.
5. We excluded duplicate articles.

Table 2. Article filtration stages.

Filtration Stage	Method	Assessment Criteria
First Filtration	Identifying relevant studies from online databases	Keywords
Second Filtration	Excluding studies based on title, abstract, and keywords	Title, abstract, and keywords
Third Filtration	Excluding studies based on the full paper	Full paper
Final Filtration	Obtaining selected papers	Final selected papers

We selected 53 articles that were the most relevant to the topic in this stage. In the fourth stage, thirteen (13) other articles were identified using the manual and snowballing approaches. So, finally, a total of 66 relevant articles were selected for this study. The searches were conducted on 15 June 2023, and all research up to this point was processed.

3. Results

3.1. RQ1: Traditional Cybersecurity Training Techniques

Training using some pre-built systems with fixed curricula is referred to as a conventional approach to training [28]. These systems are less flexible as they train users with the concept of "one for all". These techniques are often costlier, so they are not well suited for cybersecurity training [29]. These systems use both paper (i.e., newsletters, posters, and brochures) and electronic-based resources (mobile phones and computers) [30]. Print materials may convey information related to a single or multiple topics to a specific group [30].

In conventional training approaches, the replication of the real scenarios is very difficult [31]. Cybersecurity training is carried out to improve workers' skills by including recent topics, such as firewall management, encryption, virtual networks, etc., in traditional training approaches [31]. Common cybersecurity training may include lecture-based classes, emails, newsletters, virtual classes, web-based training, and teleconferencing [31,32]. Traditional approaches to conducting cybersecurity training include emails, posters, newsletters, training studies, web-based training, and instructor-led techniques [32].

3.1.1. Lecture-Based Training

This type of training consists of the delivery of information to a classroom by a field expert [33]. This approach is mostly based on presentations to a group of employees [30]. This type of training includes direct interaction with trainees, so it is considered better than paper-based training [34]. It is more expensive due to its lack of flexibility and a lack of up-to-date cybersecurity training information [30]. This type of training is also considered boring and ineffective [30]. The success of this type of training depends on the expertise of the instructor in the subject area, as well as the ability to engage trainees during the class [30,35]. So, students' engagement and interest in the class are necessary for the success of this type of training. Furthermore, most cybersecurity training approaches are considered passive due to poor communication skills and a lack of methods for assessment of the trainees' behavior [36].

Similarly, this type of training depends on the active interaction of trainees to practice the topics learned [37]. Active interaction is very necessary for effective memorization of the learned material [37]. A less engaged and chatty nature of the trainees may also affect the effectiveness of this type of training on cybersecurity [37]. So, to counter these issues, there is a need for improved social and motivational skills to engage trainees during training [34].

3.1.2. Text-Based Training

Text-based training is also self-paced and relies upon educational information that outlines best practices and other information on phishing attacks in text format [33].

3.1.3. Video-Based Training

Video-based training is another traditional cybersecurity training approach in which information is provided to trainees through educational videos [30]. It is mostly used to teach the principles and fundamentals of cybersecurity [34]. It can be less effective due to a lack of attention due to the long and boring topical materials of such videos [30]. This training is based on a self-teaching concept that allows users to select cybersecurity topics of their interest [33]. Video-based training is more effective than text- and game-based training [33].

3.1.4. Web-Based Training

Web-based user training is an online training approach that is a cost-effective and more flexible type of cybersecurity training application [30]. It is flexible in nature, can be sent, and goes at the user's pace. Email falls under this type of cybersecurity training, which is used for specific and time-sensitive matters. Different mobile learning platforms and screensavers are used to spread information related to cybersecurity training through web-based training [30]. This approach has various limitations, such as a lack of a methodology

for delivering online training. Similarly, users consider the training information boring, challenging, non-interactive, and unengaging. This results in a lack of motivation to continue and a lack of overall information retention. To deal with these problems, the training should be complemented with assessments, graphics, and some type of animation to make the material more engaging for trainees [30].

3.1.5. Combined Cybersecurity Training

This method attempts to combine more than one approach, such as text-, video-, and game-based training, in cybersecurity training, aiming to enhance user skills to guard against different types of cybersecurity attacks. Different methods should be applied in a cybersecurity training program to combine different self-paced methods with instructor-based training based on users' preferences [33].

A combination of various training approaches that depend on interactive and self-paced methods can improve trainees' knowledge and behavior. Effective cybersecurity training is important for behavioral changes and boosting users' learning of the basics of cybersecurity to safeguard against any type of cyberattack. Combined training approaches can consolidate the knowledge of users and improve their levels of interaction. However, a study showed that users favored instructor-led training in a classroom as compared to a combination of different training techniques (video-based, game-based, and text-based techniques) [33].

3.1.6. Simulation Training

Cybersecurity simulation training helps ease learning and has a positive effect on learning [38]. Simulation games also produce data for analysis that can be used to determine the learning effect of the simulation on the users [38]. Simulations are used in different areas for training and education purposes, such as in flight simulators, which are used to train novice pilots [38]. Further, they are used by cybersecurity professionals for the prediction of different types of cybersecurity threats, such as cyberattacks, data breaches, etc. The realistic nature of training in simulations prepares users to deal with realistic, uncertain cyberattacks and cybersecurity incidents [38].

The main problems inherent to simulation applications are the delay and feedback loops between an event and the response, resulting in complex and unpredictable solutions [38]. Further, cybersecurity simulation games should use some heuristics, along with the availability of users [38].

3.1.7. Cyber Ranges

Cyber ranges are cybersecurity training systems that allow users to practice different learned concepts in a realistic scenario [39]. They include instructor-led training in combination with a practical environment to exercise the learned concepts [40]. Cyber ranges are used by researchers in web-based learning systems [39]. The training should allow users to analyze tasks from different angles, mimic real-world activities, present complex situations, and have a realistic learning practice [39]. Similarly, cyber ranges allow interactive training experiences that provide perfect guidance and information [39].

Kirsi Aaltola [41] presented a detailed literature review on the current capabilities of cyber ranges and proposed various suggestions for cybersecurity education and training. Cyber ranges are becoming vital means of gaining knowledge and skills; similarly, they supplement, augment, and simulate human cognitive behavior for mental agents.

There are different problems associated with these cyber ranges, such as the fact that they are too long and affect users' interest in learning. Similarly, they are less helpful in learning for users with less IT knowledge and experience [39].

3.1.8. Virtual Environments

Virtual environments allow users to perform experiments and change different configurations to analyze the causes and effects of certain cyberattacks in a harmless and isolated

situation [31]. Facilitating users' ability to perform different types of experiments and configuration settings without any fear of IT system and configuration damage results in improved learning and understanding [31].

However, there are some limitations associated with virtual environments, including system performance, limited capacity, and obsolete virtual systems for experimentation [31]. Another issue is the time and effort required for the development of virtual environments. Similarly, cybersecurity scenarios are constantly evolving, changing, and becoming more complex. So, there is a need to update systems according to recent cyberattacks, threats, and IT systems, thus demanding high costs, time, and a large cyber workforce. Furthermore, replicating a real-world information system involves much complexity, and it is almost impossible to accurately mimic a real scene. In cybersecurity principles, it is unethical to deploy users to try or exercise learned material using an out-of-band virtual environment [31]. Similarly, the professionals who create and deploy virtual environments are responsible for informing users that trying certain actions in production or an uncontrolled environment has legal and harmful implications [34]. A list of traditional cybersecurity education techniques is listed in Table 3.

Table 3. Traditional cybersecurity education techniques.

References	Year	Training Type
Abawajy [30]	2014	Lecture-based training
Tschakert et al. [33]	2019	Lecture-based training
Rana et al. [34]	2021	Lecture-based training
Raman et al. [35]	2014	Lecture-based training
Nagarajan et al. [36]	2012	Lecture-based training
Corradini et al. [37]	2020	Lecture-based training
Tschakert et al. [33]	2019	Text-based training
Rana et al. [34]	2021	Video-based training
Tschakert et al. [33]	2019	Web-based training
Tschakert et al. [33]	2019	Combined cybersecurity training
Jalali et al. [38]	2019	Simulation training
Tang et al. [39]	2017	Cyber ranges
Beuran et al. [40]	2017	Cyber ranges
Aaltola et al. [41]	2021	Cyber ranges
Wahsheh et al. [31]	2019	Virtual environments
Rana et al. [34]	2021	Virtual environments
[42–58]		Game-based training

3.1.9. Game-Based Training

Computer games are also a traditional training technique, as they follow a fixed curriculum with a predefined set of learning modules [28]. This is a self-teaching method of training that allows users to interact with information, such as checking for an email or phishing attack [33]. It is a computer-based approach to cybersecurity training and education that allows users to learn and practice different cybersecurity concepts and theories in an interactive, entertaining, and interesting manner. It teaches how to deal with different attacks and make defenses against different situations in a dynamic environment. This type of learning equips users with cybersecurity skills more rapidly [59]. Awojana and Chou [60] proposed a game-based system for learning basic cybersecurity concepts. The proposed system is an interactive training system for students and faculty that enhances their attraction and motivation. Cybersecurity games allow users to follow a set of rules

and choices and compete to achieve a task [61]. They can select different strategies for dealing with different types of attacks.

The basic elements of games, i.e., aesthetics, mechanics, technology, and story, are closely related to cybersecurity education [62]. Attackers and defenders are the two basic stakeholders of cybersecurity activities; they are opposites and have an offensive and defensive relationship, creating a miniature of a global cybersecurity scene [63]. These stakeholders may have users from various sectors in a specific cybersecurity environment, occupying different positions in different events, which may be represented as attacking and defensive positions in a cybersecurity environment [63]. Cybersecurity education develops environments in which instructors give information to one or more users. Such a type of framework is suitable for multiplier games. Different settings of difficulty can be adjusted based on a player's cybersecurity knowledge. Complex games may be developed by having interactions and fighting in different areas. Complex game frameworks can explore philosophical, cultural, and moral themes through the cultural domain of cybersecurity information [63].

Research on game-based cybersecurity education has been a focus throughout the world for the last decade. Gestwicki and Stumbaugh (2015) examined approximately 20 cybersecurity education games from Europe and the United States. They were either based on less professional knowledge or had high-skill knowledge. The concerned issues may be used as developmental opportunities in cybersecurity education games. Elevation of Privilege (EoP), which was released by Microsoft [64], is a card game that enhances the identification of threats such as tampering, spoofing, information disclosure, repudiation, escalation of privilege, and denial-of-service attacks [65]. Other board games, such as Play2Prepare [61], "Decision & Disruption" [66], "Cyber Security-Requirements Awareness Game" [67], "[d0x3d!] a board game" [68], and "The Security Cards" [69], are used for cybersecurity education.

Similarly, the authors of [46] proposed a serious cybersecurity game framework that consisted of analysis, game design, development, game evaluation, deployment, and player evaluation. CyberCIEGE is a security training video game [43]. It is actually a simulation engine, scenario definition language, scenario production tool, video-enhanced encyclopedia, and unique security scenario. Indra [44] is an advanced cybersecurity simulator that is used for training in cyberthreats prevention, detection, reaction, forensic analysis, cyberattacks, cyber defense, and cyber warfare.

Batzos et al. [70] presented a literature review on cybersecurity training techniques and frameworks. Similarly, it covered the field of serious games that were used for the improvement of knowledge among individuals, first respondents, and organizations. The CyberAware (cybersecurity education and awareness) mobile game-based system was proposed by [47]. The main purpose of the application was to convey cybersecurity concepts to K–6 students. Control-Alt-Hack is a computer security board game for learning computer security. The players are represented as employees of a security company. A mission related to computer security is assigned to the players to be completed [45]. Anit-Phishing Phil is an online game for teaching how to notice unusual URLs to avoid phishing cyberattacks [42]. The game was implemented using Flash 8. It includes training messages and URLs that are loaded from a file at the beginning of the game. A tower-defense-style game called Cloud Defense [58] was developed to teach the security protocols of Amazon Web Services (AWS). Players in the game have to defend their application against security attacks with different difficulty levels. Each level has a tower with a new challenge, allowing users to practice different protocols by permitting legal traffic to go through the web infrastructure while protecting against malicious cyberattacks. The Cyber Security Defender [48] game is used to teach about cyberattacks caused by viruses and hackers. In the Wecode Competition, this game won the gold medal for the structure program award (2015). The game involves players as the ball defenders for the protection of the core's center from different viruses and hackers. Firewalls are used to help the players by blocking the viruses for some time. The difficulty level increases with the lifetime of

the player. The Cyber Wellness and Cyber Security Awareness [52] game is used to teach nine (9) types of security awareness to users. The game was developed by Playware Studio (Singapore) for Cyber Security on Cyber Security Awareness Day in 2013 and was designed on a multi-touch table for users. The game can teach about various situations, such as virus protection, password creation, smartphone building and use, sending data, securing Wi-Fi from unauthorized access, checking for fraudulent websites, and interaction and response in each situation.

A list of various cybersecurity games is presented in Table 4.

Table 4. Cybersecurity training games.

References	Year	Domain	Description
Anit-Phishing Phil [42]	2007	Cybersecurity education	An online game for teaching how to notice unusual URLs to avoid phishing cyberattacks
CyberCIEGE [43]	2007	Cybersecurity training	An interactive video game for security training
Hernandez et al. [44]	2011	Cybersecurity training	An advanced simulator for CS training
Control-Alt-Hack [45]	2013	Cybersecurity training	A computer security board game for learning computer security
Le et al. [46]	2015	Cybersecurity training	A serious game for CS training
CyberAware [47]	2015	Cybersecurity training	Cybersecurity mobile game for conveying cybersecurity concepts to K–6 level students
Cyber Security Defender [48]	2015	Teaching about cyberattacks	Cyber Security Defender game is used to teach about cyberattacks caused by viruses and hackers
Gestwicki and Stumbaugh [49]	2015	Cybersecurity education	Reviewed about 20 games on cybersecurity education
Nicho et al. [50]	2017	Cybersecurity training	A serious game model for organizations to substantially enhance computer users' cybersecurity awareness
Sorace et al. [51]	2018	Cybersecurity survey	Survey of 181 games related to cybersecurity
The Cyber Wellness and Cyber Security Awareness [52]	2018	Cybersecurity awareness	The Cyber Wellness and Cyber Security Awareness game is used to teach nine (9) types of security awareness to users
Katsantonis et al. [53]	2019	Cybersecurity training	PeriHack is a board and card game simulating the struggle between a team of attackers and a team of defenders
Hill et al. [54]	2020	Cybersecurity survey	A review of 20 serious games for teaching cyber security at various levels
Jaffray et al. [55]	2021	Cybersecurity training	SHERLOCKED is a serious 2D top-down detective adventure game for supporting further engagement
Van et al. [56]	2021	Cybersecurity training	A serious cybersecurity game applicable for CS training
Filippidis et al. [57]	2022	Cybersecurity training	An interactive book and board game for optimizing learning procedures and understanding in an entertaining way
Cloud Defense [58]		Teaching the security protocols of Amazon Web Services (AWS)	A Cloud Defense game is used to teach the security protocols of Amazon Web Services (AWS)

3.2. RQ2: Main Issues with Traditional Cybersecurity Training Methods

Various problems are associated with conventional cybersecurity training methods (see Table 5). There is a short time to learn long materials, which affects knowledge retention [71]. Different types of learning models have been proposed to deal with these cybersecurity training problems, but there are still different problems associated with these training techniques [72]. The use of interactive content can improve the effectiveness of these training methods [19]. However, there are different personal and economic issues associated with cybersecurity training methods [19].

Table 5. Problems with traditional training techniques.

Problems	Effect	Solution
Personal issues	Lack of interest or motivation to be trained	Needs effective security training programs
Economic issues	High cost: A more interactive, engaging, and effective training program. Low cost: A less interactive, engaging, and effective training program	A balance should be found
Time constraint	Effect on understanding of learners	Training should be straightforward
Boringness, tediousness	Less effective outcomes	Entertaining and interactive activities need to be included in training programs
Lack of a realistic view of attacks and security issues	Ignorance of the latest attacks	Constant updates should be included in the training systems
Lack of mental stimulation and engagement	Lack of attention	Learners must also be mentally stimulated to learn and retain information
Isolated and custom-made testbeds for training purposes	Expensive, hard to maintain, and time-consuming to implement and deploy	Simulation models may be a solution
Ineffective cybersecurity training	Threat to organizations, puts assets at risk	Interactive, engaging, and entertaining training programs should be used

3.2.1. Personal and Economic Issues

Personal issues may include a lack of user interest, such as a lack of motivation to participate in the training program [19]. So, cybersecurity training programs should be effective, interactive, and entertaining to improve the motivation of uninterested users. Economic issues are associated with the cost of effective training techniques [19]. To achieve more interactive, effective, and engaging training, it will cost more, while a less interactive and engaging training program costs comparatively less. So, the big challenge for cybersecurity training programs is the need for the required funding to be available for an effective cybersecurity training program.

3.2.2. Time Constraints

Games and simulations, for example, require more time, resources, and, thus, money than traditional cybersecurity training methods. So, there is a need for a balance between interactive and engaging training and the associated budget. Furthermore, to avoid the additional time requirement for learning and understanding training modules, training must be simple and straightforward [19]. Simplicity in a cybersecurity training system lets organizations strike a balance between effective training and cost. Traditional training techniques are often referred to as tedious, and they have lower success rates [19]. However, the inclusion of entertaining content may encourage and motivate users to interact with the training content [19].

3.2.3. Lack of a Realistic and Dynamic View of Attacks

Due to their unrealistic nature [71], traditional training techniques are unable to realistically simulate recent attacks and security problems, as they have no ability to present real scenarios to users [19]. To retain content, users must be mentally prepared to learn the information [19]. In the absence of this, users may pay less attention during training, resulting in less engagement. Presently, no global standards are available for cybersecurity training [73]. Secure environments for cybersecurity training that allow practical activities are hazardous for organizations and their infrastructure [73].

Testbeds are mostly used for training, but they are costly in nature, and complexities are involved in their maintenance, implementation, and deployment [73]. A low-cost solution is required for a sandbox environment that involves users interactively. Simulations are suitable for solving this issue, but they are hard to implement [73]. A shortage of budgets and funds available for cybersecurity training pushes organizations to use available methods of paper-based conventional cybersecurity training, such as screensavers, manuals, and posters [19].

3.2.4. Lack of Effective Training

The most critical issue faced by organizations is due to the lack of cybersecurity awareness and training. This creates opportunities for cyber attackers to crash organizational systems [19]. This means that traditional cybersecurity methods are not effective compared to interactive training techniques. The lack of proper training causes terrible results that put organizations and assets at risk. This may cause different types of damages, such as loss of business, customers, and intellectual property, data breaches, etc. [19]. Inefficient training of users may cause data breaches that can damage an organization and its reputation, which leads to loss of time, resources, and money. So, there is a need for an interactive, engaging, and entertaining cybersecurity training program to deal with risks that may be caused by ineffectively trained users in an organization [19].

3.3. RQ3: Current Trends in Cybersecurity Training

Context-Aware Cybersecurity Training Systems

As opposed to traditional training techniques, context-aware training systems rely on user input, while they do not depend on fixed and pre-built training materials. Data from different sensors and storage devices are collected and analyzed; based on this information, the training is modified according to specific users [28]. Context-aware training is based on sensing and analyzing user behavior and adapting training resources to be easily understood by users according to their mental level, skills, reactions, etc. The devices used in cybersecurity training use user-related data, such as public records, social networks, financial and health records, company records, etc. [28]. This means that these types of training are completely user-specific while avoiding the use of a "one size fits all" methodology. Context-aware training systems include different types of devices, i.e., mobile and general computing devices [28]. This type of training is more effective because it focuses on user-specific needs and emphasizes the skill areas in which users need to be educated [28]. Further, the training may be designed to deal with a specific threat or risk faced by a user and follow a priority-based approach for that risk or threat [28]. Generally, these targeted training systems are more effective for users [28]. So, these training systems extend the traditional training techniques to achieve more effectiveness. Context-aware training systems are too expensive in terms of time, cost, and other resources for deployment in medium-sized organizations. So, these systems cannot be widely commercially adopted.

VR Cybersecurity Training

VR-based training is an extended form of game-based training in that it not only entertains and engages users during training, but also provides an immersive and realistic interactive experience. Due to its highly engaging, interactive, and immersive nature, it is considered the most effective training technique. VR cybersecurity training includes stylistic, thematic, and mechanical features that make it a digital agent in VR applications [74]. Cybersecurity training systems should also include visual aspects to deliver visual content along with stylistic modules and themes to enhance student learning. Virtualization is highly dependent upon delivering realistic training, along with being cost-effective, safe, low-maintenance, and reproducible [73]. Additionally, VR provides an even more realistic choice for providing cybersecurity training.

VR and AR applications can be used to teach cybersecurity principles and fundamentals to students who have no access to real data centers for physical cybersecurity training [75]. Similarly, these systems allow one to learn cybersecurity principles in an active, observational, and interactive fashion [75]. As compared to traditional training, VR training produces more effective cognitive activity. Active learning develops new ideas and experiences, as well as the skills to make hypotheses and create and experience solutions [75].

As active learning creates higher levels of learning, VR training applications allow students to experience a new technique of active learning of cybersecurity basics. VR systems provide more effective learning with a high level of information retention. VR cybersecurity systems are designed to enhance user retention, engagement, and sustainability [75]. Moreover, VR systems allow free navigation and 3D interaction with objects inside the

virtual environment [75]. Some improvements for VR cybersecurity systems have also been suggested by researchers, such as reducing confusion with controls and adding new approaches to ease access to and control of physical data centers [75]. Studies show that VR training systems are more effective for students' learning and understanding of data center security principles and procedures [75]. In terms of knowledge retention, the results showed that 80% of students remembered the principles learned from VR cybersecurity training [75]. Similarly, interview results showed that VR training was more beneficial, engaging, interactive, entertaining, easy, and great for learners [75].

Unfortunately, VR-based cybersecurity training is an understudied and immature field. However, there are some systems available; for example, Walmart and Fidelity presented a cybersecurity training system named "STRIVR" [76]. The proposed system provides improved user satisfaction, while less time (about fifteen minutes to eight hours) is required in training than with traditional training techniques [77]. In addition, according to the VP of US Learning at Walmart, this VR cybersecurity training provides highly significant knowledge retention [77]. Another cybersecurity training company (NNIT) carried out experiments that allowed participants to spot security cracks in a usual office environment [78]. They observed that VR scenes and gamification of cybersecurity training enhanced effectiveness and knowledge retention among users [78]. A VR cybersecurity training vendor (Security Quotient) observed high customization, adaptability, and engagement when using VR cybersecurity training [78]. These benefits found in various studies are significant for effective training. Some features of VR cybersecurity training comprise 3D images and scenarios that help users spot security threats easily [78]. InfoSequre proposed a VR cybersecurity training game called Escape Rooms [79]. According to InfoSequre notes, VR cybersecurity training is an entertaining and highly engaging experience for users [79]. SixGen, a VR cybersecurity training company, is devoted to assessing the higher retention levels of its users [80]. VR cybersecurity training is highly effective due to its highly entertaining, engaging, and interactive features compared to those in traditional training. Further studies are required to assess the other benefits of VR cybersecurity training systems.

Rana et al. [34] carried out a comparative study of VR and traditional cybersecurity training techniques in terms of effectiveness. Both VR and traditional training systems were developed and analyzed by 100 users. The objective was to train users in cybersecurity awareness in an effective manner to contribute to cybersecurity training. If VR training is more effective, it will be a new track for cybersecurity training. Makransky et al. [81] presented a comparative study of workplace safety training in three different modes (standard, computerized, and VR). The experiments showed that the VR group achieved more significant enjoyment, along with other affective measures, than the standard and computerized groups did, while a significant recall effect was reported. VR also showed considerably greater behavioral changes. Adinolf et al. [74] carried out a study aiming to enhance the relationship among different partners of VR training agents by using different workshops related to cybersecurity training concepts. The results were categorized as stylistic (less realistic art), mechanical (VR gestures), and thematic (use of different metaphors for the translation of cybersecurity topics). Users reported high feasibility and utility in these workshops. The workings of VR training and practice have been favored over traditional training by users [82]. They observed that VR training systems had a negative correlation with users' ages. According to McMahan et al. [83], the user interface, display, and response had a great impact on users' performance and strategies, as well as their assessments of engagement, presence, and usability. Ulsamer et al. [84] reported that VR-based storytelling enhanced user awareness of cybersecurity concepts. A comparative study was carried out between a VR environment (3D storytelling video) and a non-VR platform that used a traditional e-learning (no video) platform. The results showed improved cybersecurity awareness and material retention for the VR system. Alberto Giaretta [85] presented the current state of VR security and privacy, the potential threats and issues, and the sources and impacts of these identified threats. They also discussed the application of VR in cybersecurity, such as in teaching cybersecurity or evaluating the usability of security solutions.

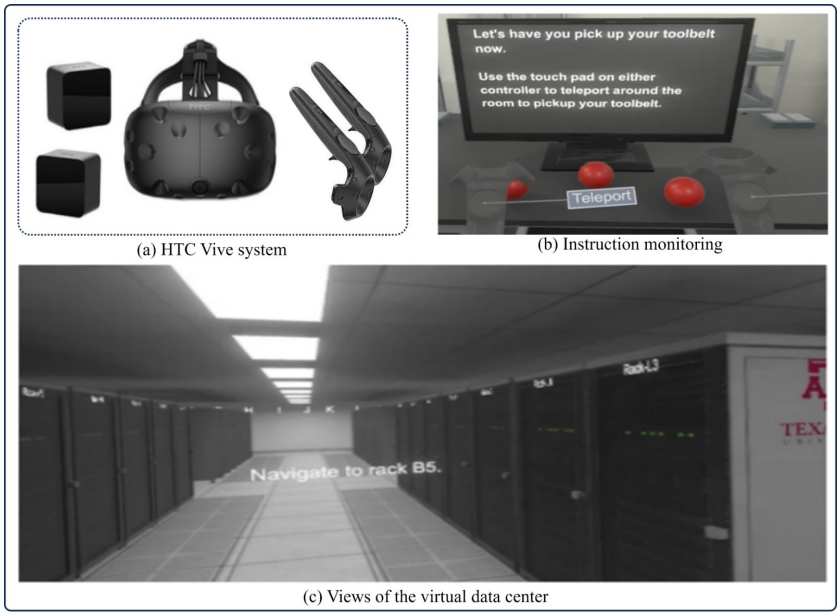
A VR cybersecurity program (CiSE-ProS) was proposed by Seo et al. [75] to help users learn cybersecurity fundamentals by using active and immersive tasks in a virtual data center environment. The proposed system allowed users to study and practice cybersecurity with highly interactive display technology in an innovative learning scenario (see Figure 2). Further, the system was designed with the intent of providing the principles of training, engagement, sustainability, and retention to encourage cyber-infrastructure as a professional field. An immersive virtual environment was designed with Unit 2017, while the HTC Vive system, including a headset, two motion-tracking sensors, and two handheld controllers, was used for navigation, selection, and manipulation of objects inside the virtual data center. There were four main activities: a tutorial, entrance/exit, inspection, and replacement of hardware components inside the virtual data center. The results showed that 90% of the students remembered the data center's physical security layers and the procedure for fixing broken RAM. A week after the initial experiment, 80% of the students still remembered the security checkpoints and hardware replacement procedure. Similarly, the students argued that VR would be helpful in education due to its realistic visualization and its immersive and interactive nature.

Chekhovskoy et al. [86] proposed an educational and laboratory complex for cybersecurity education. Their study intended to provide a detailed implementation of current cyberattacks and their countermeasures. The system included a VR testbed and algorithmic support, and it was tested at the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute). The proposed VR environment was designed in Unity, while the algorithm presented different cyberattacks and strategies for protection against them. The results showed that the highest interest was in VR training, while 89% scored for the adaptation of material according to the test results. However, there were some problems with the visualization of some elements during interactions and an unclear interconnection between the virtual environment and the applied cyberattacks.

A serious VR game called Lord of Secure was proposed by Visoottiviseth et al. [87]. Users were challenged using different cybersecurity topics, such as flooding, IP spoofing, firewalls, TCP convert channels, honeypots, and intrusion detection and prevention systems. The objective of the game was to make theoretical cybersecurity topics easier for students and to evaluate their understanding of the core concepts. The results showed that 90% of the students reported that they understood the topics in the game, while 82% claimed that this approach gave a better understanding than traditional lessons via text and visualization. Similarly, the results showed that 70% of the students improved their learning, and the game provided a high level of enjoyment.

Veneruso et al. [88] proposed CyberVR, a VR-based interactive cybersecurity learning game. The CyberVR was developed using the Unreal Engine to design the virtual environment, the Oculus Rift for immersive visualization of the virtual environment, and Leap Motion for interaction with the virtual environment using hand gestures. A comparative study was carried out in which CyberVR was compared with traditional textbook-based learning. The experimental results showed improved engagement while being equally as effective as traditional learning methods.

Dattel et al. [89] proposed an immersive Cybersecurity Virtual Reality Trainer (CyVR-T) application for a destroyer in the US Navy. This research investigated the training of U.S. Navy midshipmen enrolled in the Reserve Officer Training Corps (ROTC) at Embry-Riddle Aeronautical University (ERAU) to identify cyber and security threats on a simulated bridge of a Navy vessel [89]. Midshipmen received classroom instruction, as well as training in a virtual reality bridge simulator. This study intended to train midshipmen to be better prepared to identify cybersecurity threats in their future positions and careers following graduation from the program. The specific VR application was designed to be sustainable for further utilization in the future Naval curriculum and other applications. The results showed significant cyber threat performance and enhanced knowledge improvement. Additionally, the CyVR-T is the best tool for the identification of cyberattacks and can be used in more complex scenarios.



(a) HTC Vive system (b) Instruction monitoring

(c) Views of the virtual data center

Figure 2. CiSE-ProS: [75] (**a**) The HTC Vive system, including headsets, motion trackers, and handheld controllers. (**b**) The tutorial room had an instruction monitor. (**c**) Views of the virtual data center.

Puttawong et al. [90] proposed a VR-based application called VRFiWall (Virtual Reality Edutainment for Firewall) to teach the concept of firewalls in network security. The proposed game was developed using Unity3D to teach graduate-level students as an alternative to lecture-based teaching. The proposed game was also implemented using Google Cardboard, while interactions were carried out using head gestures. The users could also practice the security concepts on their desktops and mobile phones. The game was based on the concept of a fantasy role-playing game in which the player interacts with non-player characters, obtains different items, and fights monsters.

AR Cybersecurity Training

Alqahtani et al. [91] developed an AR -based mobile application, "Cybersecurity Awareness using Augmented Reality" (CybAR), for teaching the fundamental concepts of cybersecurity. They also presented the results of real cyberattacks through feedback. A subjective study of 91 participants was carried out to assess the effectiveness of the CybAR game. The results showed that 88% of the participants reported a high level of understanding of cybersecurity concepts. The results for the proposed application indicated the usefulness of CybAR in terms of understanding vulnerabilities and cyberattacks.

CS:NO [92] is an extended reality (XR)-based educational tool for teaching the fundamentals of cybersecurity in an easy, concrete, and engaging manner. A virtual environment was used for the visualization of the data flow over a network that allows real-time interaction (audio, visual, and haptic) with virtual data packets. The goal was to give a better understanding of intangible cybersecurity concepts, such as cryptography, malicious data, and firewalls. A Peltier thermoelectric sensor and Arduino Uno were used in the experiments to achieve a high level of immersion in the XR environment. Further evaluation of the experiments was presented, along with possible new directions.

An XR-based experiential and immersive cybersecurity learning (XR-CEIL) application was developed by Gračanin et al. [93]. The proposed system was used for cybersecurity learning and training using an XR-based immersive cybersecurity environment. The application was used for data exploration and immersive analysis of cybersecurity data with a multi-dimensional, heterogeneous nature. XR for cybersecurity is used for visualization, which allows users to visualize and analyze cyber threats in an extremely different fashion, thus increasing cybersecurity education, training, and analytical abilities. A survey of the AR and VR cybersecurity training systems is presented in Table 6.

Table 6. Survey of the state-of-the-art cybersecurity training techniques.

Features	VTFiWall	Lord of Secure	CyberVR	Shaila Rana	CyVR-T	CiSE-ProS	Chekhovskoy	CybAR	CS:NO	XR-CEIL
Technology	Desktop VR, VR, Android smartphone	VR	VR	VR	VR	VR	VR	Mobile AR	XR	XR
Software	Unity 3D, Blender, Google VR SDK, Android SDK	Unity 3D, Blender, Android Studio	Unreal Engine	Unity VR		Unity 3D	Unity and Unreal Engine 4	Unity 3D, Vuforia SDK	Unity 3D	
Hardware	HTC Vive, VR Box, Google cardboard	HMD	Oculus Rift, Leap Motion	Google Cardboard, VR headset	Oculus Rift	HTC Vive, headset		Android smartphone	Oculus Rift, Arduino Uno Rev 3, Proto Shield	
Interaction	Head gestures and pointing	Pointing	Hand gestures		Hand controllers	Motion-tracking sensors, handheld controllers	Mouse	Touchscreen	Visual, audio, and haptic thermal feedback	
Cybersecurity contents	Firewall	Flooding, IP spoofing, firewalls, TCP convert channels, honeypots, and intrusion detection and prevention systems	Six mini-games Information flow, code injection, patch management, dynamic SW Analysis, privilege escalation, public-key cryptography	Physical security concepts, such as locked devices, keeping passwords and sensitive files secured, keeping doors locked, and keeping keys secured	Voyage management system, radar detection system, and automatic identification system	Tutorial, entrance/exit, inspection, and replacement of hardware	Network attacks	Teaching the fundamental concepts of cybersecurity	Encryption and decryption, firewalls, malicious data, network traffic	Exploration of immersive multi-dimensional data of a heterogeneous nature

3.4. RQ4: AR and VR in Cybersecurity Education: Challenges and Limitations

The use of VR cybersecurity in education and training faces various challenges.

3.4.1. Technical Challenges

The implementation of VR in cybersecurity education involves various technical challenges, such as the need for high-speed hardware (powerful computers and graphics processing units) for smooth VR experiences. McMahan et al. [83] surveyed VR learning environments' technical infrastructures and limitations. Furthermore, skilled professionals are required for the development of VR software and 3D content creation. Another important challenge is the availability of high-speed networking infrastructure for handling the data-intensive nature of VR. Overwhelming these challenges is essential for achieving a realistic VR environment for cybersecurity education.

3.4.2. Cost and Accessibility Challenges

The required cost for the implementation of an immersive VR cybersecurity education system is another crucial challenge. The cost of the required VR hardware (visualization, interaction, and locomotion hardware), development tools, and software licenses can be a problem, especially for educational organizations with low budgets. Similarly, the required maintenance of and updates to a VR system may require an additional budget. In addition, the accessibility of VR systems to learners, especially those with disabilities, needs cautious consideration. Discovering low-cost solutions and procedures for the widespread adoption of VR experiences depends on making VR experiences more accessible to a wide range of learners.

3.4.3. Ethical and Risk Considerations

The implementation of VR cybersecurity education systems promotes ethical and potential risk considerations. Alberto Giaretta et al. [85] carried out a comprehensive analysis of the current state of VR security and privacy, their related issues and threats, and their causes and effects. The VR systems for cyberattacks and defense strategies may be carefully designed to avoid any misuse or accidental results. Responsible use and ethical protocols have a vital role in the effectiveness of VR cybersecurity education and training systems. Similarly, the privacy of personal data in VR systems is also a very crucial problem. So, ensuring the use of ethical guidelines and security is the most critical factor in the implementation of VR cybersecurity education systems.

3.4.4. User Comfort

VR systems may cause user discomfort and motion sickness, which may affect the learning experience. Different issues, such as eyestrain, disorientation, and simulator sickness, need to be considered to achieve high user comfort in VR cybersecurity training. The use of high-quality VR devices, high tracking accuracy, and data with a high response may improve user comfort during the VR experience.

3.4.5. Interoperability and Standardization Problems

The problems associated with the lack of interoperability and standardization of different platforms and VR technologies pose challenges in VR cybersecurity education and training. Compatibility issues arise due to the different natures of software, hardware, and data formats, which may lead to integration problems in the deployment of a VR cybersecurity education system. Using common protocols and standards may facilitate the effective integration and broad implementation of VR cybersecurity education and training systems.

3.4.6. Global Challenges, Policies, and Standardizations

The main objective of cybersecurity is to safeguard the reliability, availability, and security of computer systems. One example of such defensive procedures is the employment of security policies designed to defend a corporation's digital space [94].

In this regard, Mishra et al. [94] examined five different industries: finance, healthcare, aviation, education, and e-commerce. Different common cybersecurity challenges, such as privacy protection, website security, cloud computing security, email security, physical security, information security, network security, data retention, access control, and data protection, were identified. Different significant legislative acts have been recognized as essential to cybersecurity efforts. These include the Gramm–Leach–Bliley Act, which protects financial information, the Family Educational Rights and Privacy Act, which secures individual students' data, the Health Insurance Portability and Accountability Act, which protects personal health information, and the Fair Credit Reporting Act, which protects credit information. Attaining a balance between employing security measures and defending individual rights, such as when installing body-scanning devices at airports, is necessary [94]. Additionally, data security regulations should include all kinds of personal information related to customers, which can be categorized into two types: recognizable and non-recognizable information. These regulations are critical for sustaining the privacy and security of people's data. Mishra et al. (2022) [95] identified various common attributes of cybersecurity policies, i.e., cloud computing, e-commerce, identity theft, network, online banking, privacy, smart grid, and telecommunication, across seven different regions, namely, Australia, China, Canada, Europe, India, Malaysia, and the USA. Furthermore, Weiss and Biermann [96] analyzed the international legal regulations regarding privacy and security, especially in areas such as healthcare, education, and banking. In another study, London [97] discovered different features of information technology and studied the results of a lack of awareness in this area. The study focused on data security, data protection, and regulations associated with information confidentiality in five different countries. Furthermore, an analysis of the availability of security-improving technologies was conducted, particularly under US regulations, such as the Gramm–Leach–Bililey Act, the Health Insurance Portability and Accountability Act, and the Family Educational Rights and Privacy Act. Yoo [98] characterized breaches of personal identity information into social, financial, and medical classes. This study also identified the particular privacy protection laws necessary for each group. These involved acts such as the Gramm–Leach–Billey Act, the Health Insurance Portability and Accountability Act, and the Economic and Clinical Health ("HITECH") Act. Liu et al. [99] suggested the employment of authentication and access control procedures to deal with security and privacy issues on the internet. Alotaibi et al. [100] presented the challenges faced by organizations during the implementation of information security policies. Similarly, Persadha et al. [101] carried out a comparison of the assignment of duties in cyber activities, classifying them through three (3) different countries.

4. Conclusions

Cybersecurity education and training have a significant role in response to the increasing cyber threats and their prospective financial impacts on different business and government organizations. In this article, we presented a comprehensive SLR of various cybersecurity education and training techniques. The main objective of this study was to analyze the current cybersecurity training approaches, identify their associated challenges, and evaluate the effectiveness of AR- and VR-based cybersecurity training systems. Using stringent selection criteria, we selected 66 primary articles from a total of 150 relevant articles for detailed analysis and data extraction. We classified the articles based on the different techniques used for cybersecurity training, such as traditional lecture-based, textual, video-based, web-based, video-game-based, and simulation-based techniques, as well as virtual environments and cyber ranges, and we described their pros and cons. Similarly, we also presented and analyzed the advanced AR- and VR-based approaches used for

cybersecurity education. Finally, a detailed description of different challenges associated with the implementation of AR and VR cybersecurity training systems was presented.

Author Contributions: Conceptualization, A.M.A. and M.W.; methodology, A.M.A., M.W., and M.I.; software, A.M.A., M.W. and M.I.; validation, S.H., M.I., and A.M.A.; formal analysis, M.I., H.S.A. and S.H.; investigation, A.M.A., M.I., M.W. and H.S.A.; resources, S.H., A.M.A. and M.I.; data curation, A.M.A., M.I. and S.H.A.; writing—original draft preparation, A.M.A., M.W. and S.H.; writing—review and editing, A.M.A., M.I. and S.H.; visualization, M.I., M.W. and S.H.; supervision, S.H. and M.I.; project administration, H.S.A. and M.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The researchers would like to thank the Deanship of Scientific Research Qassim University for funding the publication of this project.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Selected studies for this SLR.

Reference	Description
[28]	Sadeh-Koniecpol, N.; Wescoe, K.; Brubaker, J.; Hong, J. Method and system for controlling context-aware cybersecurity training, 2016. US Patent 9,373,267.
[29]	Fouché, S.; Mangle, A.H. Code hunt as platform for gamification of cybersecurity training. In Proceedings of the Proceedings of the 1st international workshop on code hunt workshop on educational software engineering, 2015, pp. 9–11.
[30]	Abawajy, J. User preference of cyber security awareness delivery methods. Behaviour & Information Technology 2014, 33, 237–248.
[31]	Wahsheh, L.A.; Mekonnen, B. Practical cyber security training exercises. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2019, pp. 48–53.
[32]	Nguyen, T.A.; Pham, H. A design theory-based gamification approach for information security training. In Proceedings of the 2020 RIVF International Conference on Computing and Communication Technologies (RIVF). IEEE, 2020, pp. 1–4.
[33]	Tschakert, K.F.; Ngamsuriyaroj, S. Effectiveness of and user preferences for security awareness training methodologies. Heliyon 2019, 5.
[34]	Rana, S.; Alhamdani, W. Exploring the Need to Study the Efficacy of VR Training Compared to Traditional Cybersecurity Training. International Journal of Computer and Information Engineering 2021, 15, 10–17.
[35]	Raman, R.; Lal, A.; Achuthan, K. Serious games based approach to cyber security concept learning: Indian context. In Proceedings of the 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE). IEEE, 2014, pp. 1–5.
[36]	Nagarajan, A.; Allbeck, J.M.; Sood, A.; Janssen, T.L. Exploring game design for cybersecurity training. In Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER). IEEE, 2012, pp. 256–262.
[37]	Corradini, I.; Corradini, I. Training methods. Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology 2020, pp. 115–133.
[38]	Jalali, M.S.; Siegel, M.; Madnick, S. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. The Journal of Strategic Information Systems 2019, 28, 66–82.
[39]	Tang, D.; Pham, C.; Chinen, K.I.; Beuran, R. Interactive cybersecurity defense training inspired by web-based learning theory. In Proceedings of the 2017 IEEE 9th International Conference on Engineering Education (ICEED). IEEE, 2017, pp. 90–95.
[40]	Beuran, R.; Pham, C.; Tang, D.; Chinen, K.i.; Tan, Y.; Shinoda, Y. Cytrone: An integrated cybersecurity training framework 2017.

Table A1. *Cont.*

Reference	Description
[41]	Aaltola, K. Empirical study on cyber range capabilities, interactions and learning features. Digital Transformation, Cyber Security and Resilience of Modern Societies 2021, pp. 413–428.
[42]	Sheng, S.; Magnien, B.; Kumaraguru, P.; Acquisti, A.; Cranor, L.F.; Hong, J.; Nunge, E. Anti- 724 phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In Proceedings of the Proceedings of the 3rd symposium on Usable privacy and security, 2007, pp. 88–99.
[43]	Cone, B.D.; Irvine, C.E.; Thompson, M.F.; Nguyen, T.D. A video game for cyber security training and awareness. computers & security 2007, 26, 63–72.
[44]	Hernández-Ardieta, J.L.; Santos, D.; Parra, P.; Tapiador, J.E.; Peris-López, P.; López, J.; Navarrete, G.F. An Intelligent and adaptive live Simulator: A new concept for Cybersecurity Training. Indra, Madrid 2011.
[45]	Denning, T.; Lerner, A.; Shostack, A.; Kohno, T. Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In Proceedings of the Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 915–928.
[46]	Le Compte, A.; Elizondo, D.; Watson, T. A renewed approach to serious games for cyber security. In Proceedings of the 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. IEEE, 2015, pp. 203–216.
[47]	Giannakas, F.; Kambourakis, G.; Gritzalis, S. CyberAware: A mobile game-based app for cybersecurity education and awareness. In Proceedings of the 2015 International conference on interactive mobile communication technologies and learning (IMCL). IEEE, 2015, pp. 54–58.
[48]	Chai, P. Cyber Security Defender, 2015 WeCode National Competition : Cyber Security Game. https://www.youtube.com/watch?v=Bb_gGq1QMUU. In comment section, accessed on 7 June 2023.
[49]	Gestwicki, P.; Stumbaugh, K. Observations and opportunities in cybersecurity education game design. In Proceedings of the 2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAMES). IEEE, 2015, pp. 131–137.
[50]	Nicho, M. Modelling serous games for enhancing end user cyber security awareness. IADIS Int. J. Comput. Sci. Inf. Syst 2017, 15, 91–106.
[51]	Sorace, S.; Quercia, E.; La Mattina, E.; Patrikakis, C.Z.; Bacon, L.; Loukas, G.; Mackinnon, L. Serious games: an attractive approach to improve awareness. Community-Oriented Policing and Technological Innovations 2018, pp. 1–9.
[52]	Chai, P. Cyber Wellness and Cyber Security game for the IDA. https://www.youtube.com/watch?v=g7Mz9vFceMU. In comment section, accessed on 7 June 2023.
[53]	Katsantonis, N.M.; Kotini, I.; Fouliras, P.; Mavridis, I. Conceptual framework for developing cyber security serious games. In Proceedings of the 2019 IEEE global engineering education conference (EDUCON). IEEE, 2019, pp. 872–881.
[54]	Hill, W.; Fanuel, M.; Yuan, X. Comparing serious games for cyber security education. In Proceedings of the 2020 ASEE Southeastern Section Conference, 2020.
[55]	Jaffray, A.; Finn, C.; Nurse, J.R. Sherlocked: A detective-themed serious game for cyber security education. In Proceedings of the Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15. Springer, 2021, pp. 35–45.
[56]	van Steen, T.; Deeleman, J.R. Successful gamification of cybersecurity training. Cyberpsychology, Behavior, and Social Networking 2021, 24, 593–598.
[57]	FILIPPIDIS, A.; Lagkas, T.; Mouratidis, H.; Nifakos, S.; Grigoriou, E.; Sarigiannidis, P. Enhancing information security awareness programs through collaborative learning. In Proceedings of the European Conference on Games Based Learning, 2022, Vol. 16, pp. 803–810.
[58]	Intuit Cyber security game. https://www.youtube.com/watch?v=_3VLx0pXSYs. In comment section, accessed on 7 June 2023.
[59]	Trickel, E.; Disperati, F.; Gustafson, E.; Kalantari, F.; Mabey, M.; Tiwari, N.; Safaei, Y.; Doupé, A.; Vigna, G. Shell We Play A Game?CTF-as-a-service for Security Education. In Proceedings of the 2017 USENIX Workshop on Advances in Security Education (ASE 17), 2017.
[60]	Awojana, T.; Chou, T.S. Overview of learning cybersecurity through game based systems. In Proceedings of the 2019 CIEC, 2019.

Table A1. *Cont.*

Reference	Description
[61]	Graffer, I.; Bartnes, M.; Bernsmed, K. Play2prepare: A board game supporting it security preparedness exercises for industrial control organizations 2015.
[62]	Bond, J.G. Introduction to Game Design, Prototyping, and Development: From Concept to Playable Game with Unity and C#, Addison-Wesley Professional 2017.
[63]	Xiao, H.; Hao, W.; Liao, Q.; Ye, Q.; Cao, C.; Zhong, Y. Exploring the gamification of cybersecurity education in higher education institutions: An analytical study. In Proceedings of the SHS Web of Conferences. EDP Sciences, 2023, Vol. 166.
[64]	Shostack, A. Elevation of privilege: Drawing developers into threat modeling. In Proceedings of the 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.
[65]	Potter, B. Microsoft SDL threat modelling tool. Network Security 2009, 2009, 15–18.
[66]	Frey, S.; Rashid, A.; Anthonysamy, P.; Pinto-Albuquerque, M.; Naqvi, S.A. The good, the badand the ugly: a study of security decisions in a cyber-physical systems game. IEEE Transactionson Software Engineering 2017, 45, 521–536.
[67]	Yasin, A.; Liu, L.; Li, T.; Fatima, R.; Jianmin, W. Improving software security awareness using a serious game. IET Software 2019, 13, 159–169.
[68]	Gondree, M.; Peterson, Z.N. Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game. In Proceedings of the 6th Workshop on Cyber Security Experimentation and Test (CSET 13), 2013.
[69]	Denning, T.; Friedman, B.; Kohno, T. The Security Cards: A Security Threat Brainstorming Toolkit. Univ. of Washington, http://securitycards. cs. washington. edu 2013.
[70]	Batzos, Z.; Saoulidis, T.; Margounakis, D.; Fountoukidis, E.; Grigoriou, E.; Moukoulis, A.; Sarigiannidis, A.; Liatifis, A.; Karypidis, P.A.; Bibi, S.; et al. Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview 2023.
[72]	Thakong, M.; Phimoltares, S.; Jaiyen, S.; Lursinsap, C. One-pass-throw-away learning for cybersecurity in streaming non-stationary environments by dynamic stratum network. PloS one 2018, 13, e0202937
[73]	Urias, V.E.; Van Leeuwen, B.; Stout, W.M.; Lin, H.W. Dynamic cybersecurity training environments for an evolving cyber workforce. In Proceedings of the 2017 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE, 2017, pp. 1–6.
[74]	Adinolf, S.; Wyeth, P.; Brown, R.; Altizer, R. Towards designing agent based virtual reality applications for cybersecurity training. In Proceedings of the Proceedings of the 31st Australian Conference on Human-Computer-Interaction, 2019, pp. 452–456.
[75]	Seo, J.H.; Bruner, M.; Payne, A.; Gober, N.; McMullen, D.; Chakravorty, D.K. Using virtual reality to enforce principles of cybersecurity. The Journal of Computational Science Education 2019, 10.
[76]	Booth, J.; COMMAND, A.; States, S.C.M.A.A.M.A.U. The Use of Virtual and Augumented Realities in Air Force Training; Air Command and Staff College, 2019.
[77]	Elevate performance through immersive experience. https://www.strivr.com/lp/elevateperformance-through-immersiveexperience/?utm_medium=Paid-Search. In comment section, accessed on 7 June 2023.
[78]	VR Cybersecurity Training. https://www.nnit.com/our-solutions/cybersecurity/vrcybersecuritytraining/. In comment section, accessed on 7 June 2023.
[79]	Security awareness game. https://www.infosequre.com/security-awareness-game. In comment section, accessed on 7 June 2023.
[80]	Virtual Reality Training powered by SixGen. https://www.sixgen.io/course. In comment section, accessed on 7 June 2023.
[81]	Makransky, G.; Borre-Gude, S.; Mayer, R.E. Motivational and cognitive benefits of training in immersive virtual reality based on multiple assessments. Journal of Computer Assisted Learning 2019, 35, 691–707.
[82]	Meldrum, D.; Glennon, A.; Herdman, S.; Murray, D.; McConn-Walsh, R. Virtual reality rehabilitation of balance: assessment of the usability of the Nintendo Wii® Fit Plus. Disability and rehabilitation: assistive technology 2012, 7, 205–210.
[83]	McMahan, R.P.; Bowman, D.A.; Zielinski, D.J.; Brady, R.B. Evaluating display fidelity and interaction fidelity in a virtual reality game. IEEE transactions on visualization and computer graphics 2012, 18, 626–633.

Table A1. *Cont.*

Reference	Description
[84]	Ulsamer, P.; Schütz, A.; Fertig, T.; Keller, L. Immersive storytelling for information security awareness training in virtual reality 2021.
[85]	Giaretta, A. Security and Privacy in Virtual Reality–A Literature Survey. arXiv preprint arXiv:2205.00208 2022.
[87]	Visoottiviseth, V.; Phungphat, A.; Puttawong, N.; Chantaraumporn, P.; Haga, J. Lord of secure: the virtual reality game for educating network security. In Proceedings of the 2018 seventh ict international student project conference (ict-ispc). IEEE, 2018, pp. 1–6.
[88]	Veneruso, S.V.; Ferro, L.S.; Marrella, A.; Mecella, M.; Catarci, T. CyberVR: an interactive learning experience in virtual reality for cybersecurity related issues. In Proceedings of the Proceedings of the International Conference on Advanced Visual Interfaces, 2020, pp. 1–8.
[89]	Dattel, A.; Ochoa, O.; Friedenzohn, D.; Goodwin, T.; Brodeen, H. Using Virtual Reality to Identify Cybersecurity Threats for Navy Midshipmen 2022.
[90]	Puttawong, N.; Visoottiviseth, V.; Haga, J. VRFiWall virtual reality edutainment for firewall security concepts. In Proceedings of the 2017 2nd international conference on information technology (INCIT). IEEE, 2017, pp. 1–6.
[91]	Alqahtani, H.; Kavakli-Thorne, M. Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information 2020, 11, 121.
[92]	Bernsland, M.; Moshfegh, A.; Lindén, K.; Bajin, S.; Quintero, L.; Solsona Belenguer, J.; Rostami, A. CS: NO–an Extended Reality Experience for Cyber Security Education. In Proceedings of the ACM International Conference on Interactive Media Experiences, 2022, pp. 287–292.
[93]	Gračanin, D.; Park, J.; Eltoweissy, M. XR-CEIL: Extended reality for cybersecurity experiential and immersive learning. In Proceedings of the International Conference on Human-Computer Interaction. Springer, 2022, pp. 487–492.

References

1. Federal Bureau of Investigation, U.S. Internet Crime Report 2020. 2021. Available online: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3rpeort.pdf (accessed on 7 June 2023).
2. WSAV. Data Brechers, Annual Report. 2022. Available online: https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (accessed on 7 June 2023).
3. Alnajim, A.M.; Habib, S.; Islam, M.; Albelaihi, R.; Alabdulatif, A. Mitigating the Risks of Malware Attacks with Deep Learning Techniques. *Electronics* **2023**, 12, 3166.. [CrossRef]
4. Federal Bureau of Investigation, U.S. 2022 Internet Crime Report. 2022. Available online: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics (accessed on 7 June 2023).
5. Chowdhury, N.; Gkioulos, V. Cyber security training for critical infrastructure protection: A literature review. *Comput. Sci. Rev.* **2021**, *40*, 100361. [CrossRef]
6. Agbo-ola, A. Motivating Cybersecurity Awareness within an Organisation: An Explorative Study from an Awareness Practitioner's Perspective. Master Thesis, Luleå University of Technology, Luleå, Sweden, 2022, Digitala Vetenskapliga Arkivet. Available online: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1667742&dswid=1938 (accessed on 7 June 2023).
7. Shin, D.H. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interact. Comput.* **2010**, *22*, 428–438. [CrossRef]
8. Ponnusamy, V.; Selvam, L.M.P.; Rafique, K. Cybersecurity governance on social engineering awareness. In *Employing Recent Technologies for Improved Digital Governance*; IGI Global: Hershey, PA, USA, 2020; pp. 210–236. [CrossRef]
9. Conteh, N.Y.; Schmick, P.J. Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*; IGI Global: Hershey, PA, USA, 2021; pp. 19–31. [CrossRef]
10. Yaokumah, W.; Walker, D.O.; Kumah, P. SETA and security behavior: Mediating role of employee relations, monitoring, and accountability. *J. Glob. Inf. Manag. (JGIM)* **2019**, *27*, 102–121. [CrossRef]
11. Teh, P.L.; Ahmed, P.K.; D'Arcy, J. What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory. *J. Glob. Inf. Manag. (JGIM)* **2015**, *23*, 44–64. [CrossRef]
12. De Maggio, M.C.; Mastrapasqua, M.; Tesei, M.; Chittaro, A.; Setola, R. How to improve the security awareness in complex organizations. *Eur. J. Secur. Res.* **2019**, *4*, 33–49. [CrossRef]
13. Chatterjee, D. Should executives go to jail over cybersecurity breaches? *J. Organ. Comput. Electron. Commer.* **2019**, *29*, 1–3. [CrossRef]
14. Norris, D.F.; Mateczun, L.; Joshi, A.; Finin, T. Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. *Public Adm. Rev.* **2019**, *79*, 895–904. [CrossRef]

15. Majeed, A.; Alnajim, A.M.; Waseem, A.; Khaliq, A.; Naveed, A.; Habib, S.; Islam, M.; Khan, S. Deep Learning-Based Symptomizing Cyber Threats Using Adaptive 5G Shared Slice Security Approaches. *Future Internet* **2023**, 15, 193. [CrossRef]
16. Disparte, D.; Furlow, C. The best cybersecurity investment you can make is better training. *Harv. Bus. Rev.* **2017**, *5*. Available online: https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training (accessed on 7 June 2023).
17. Ergen, A.; Ünal, A.N.; Saygili, M.S. Is it possible to change the cyber security behaviours of employees? Barriers and promoters. *Acad. J. Interdiscip. Stud.* **2021**, *10*, 210. [CrossRef]
18. Schmidt, M.B.; Johnston, A.C.; Arnett, K.P.; Chen, J.Q.; Li, S. A cross-cultural comparison of US and Chinese computer security awareness. *J. Glob. Inf. Manag. (JGIM)* **2008**, *16*, 91–103. [CrossRef]
19. Aldawood, H.; Skinner, G. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet* **2019**, *11*, 73. [CrossRef]
20. Mejia, G. Examining the Impact of Major Security Breaches on Organizational Performance: Should Investing in Cybersecurity Be a Requirement for Companies? Ph.D. Thesis, Utica College, Utica, NY, USA, 2019.
21. Kweon, E.; Lee, H.; Chai, S.; Yoo, K. The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Inf. Syst. Front.* **2021**, *23*, 361–373. [CrossRef]
22. Lin, W.C.; Saebeler, D. Risk-Based v. Compliance-Based Utility Cybersecurity—A False Dichotomy. *Energy LJ* **2019**, *40*, 243.
23. Norris, D.F.; Mateczun, L.; Joshi, A.; Finin, T. Cybersecurity at the grassroots: American local governments and the challenges of internet security. *J. Homel. Secur. Emerg. Manag.* **2018**, *15*, 20170048. [CrossRef]
24. Pawlowski, S.D.; Jung, Y. Social representations of cybersecurity by university students and implications for instructional design. *J. Inf. Syst. Educ.* **2015**, *26*, 281–294.
25. Zuhaib, M.; Shaikh, F.A.; Tanweer, W.; Alnajim, A.M.; Alyahya, S.; Khan, S.; Usman, M.; Islam, M.; Hasan, M.K. Faults Feature Extraction Using Discrete Wavelet Transform and Artificial Neural Network for Induction Motor Availability Monitoring—Internet of Things Enabled Environment. *Energies* **2022**, *15*, 7888. [CrossRef]
26. Alzoubi, Y.I.; Gill, A.Q.; Al-Ani, A. Empirical studies of geographically distributed agile development communication challenges: A systematic review. *Inf. Manag.* **2016**, *53*, 22–37. [CrossRef]
27. Ibrahim, K.; Alnajim, A.M.; Naveed Malik, A.; Waseem, A.; Alyahya, S.; Islam, M.; Khan, S. Entice to Trap: Enhanced Protection against a Rate-Aware Intelligent Jammer in Cognitive Radio Networks. *Sustainability* **2022**, *14*, 2957. [CrossRef]
28. Sadeh-Koniecpol, N.; Wescoe, K.; Brubaker, J.; Hong, J. Method and System for Controlling Context-Aware Cybersecurity Training. U.S. Patent 9,373,267, 21 June 2016.
29. Fouché, S.; Mangle, A.H. Code hunt as platform for gamification of cybersecurity training. In Proceedings of the 1st International Workshop on Code Hunt Workshop on Educational Software Engineering, Baltimore, MD, USA, 14 July 2015; pp. 9–11.
30. Abawajy, J. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* **2014**, *33*, 237–248. [CrossRef]
31. Wahsheh, L.A.; Mekonnen, B. Practical cyber security training exercises. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA , 5–7 December 2019; pp. 48–53.
32. Nguyen, T.A.; Pham, H. A design theory-based gamification approach for information security training. In Proceedings of the 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), Ho Chi Minh City, Vietnam, 14–15 October 2020; pp. 1–4.
33. Tschakert, K.F.; Ngamsuriyaroj, S. Effectiveness of and user preferences for security awareness training methodologies. *Heliyon* **2019**, *5*, e02010. [CrossRef]
34. Rana, S.; Alhamdani, W. Exploring the Need to Study the Efficacy of VR Training Compared to Traditional Cybersecurity Training. *Int. J. Comput. Inf. Eng.* **2021**, *15*, 10–17.
35. Raman, R.; Lal, A.; Achuthan, K. Serious games based approach to cyber security concept learning: Indian context. In Proceedings of the 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), 2014; pp. 1–5.
36. Nagarajan, A.; Allbeck, J.M.; Sood, A.; Janssen, T.L. Exploring game design for cybersecurity training. In Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Coimbatore, India, 6–8 March 2012; pp. 256–262.
37. Corradini, I. Training methods. In *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology*; Springer Nature: Chan, Switzerland, 2020; pp. 115–133.
38. Jalali, M.S.; Siegel, M.; Madnick, S. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *J. Strateg. Inf. Syst.* **2019**, *28*, 66–82. [CrossRef]
39. Tang, D.; Pham, C.; Chinen, K.I.; Beuran, R. Interactive cybersecurity defense training inspired by web-based learning theory. In Proceedings of the 2017 IEEE 9th International Conference on Engineering Education (ICEED), Kanazawa, Japan, 9–10 November 2017; pp. 90–95.
40. Beuran, R.; Pham, C.; Tang, D.; Chinen, K.i.; Tan, Y.; Shinoda, Y. *Cytrone: An Integrated Cybersecurity Training Framework*; SciTePress—Science and Technology Publications: Setúbal, Portugal, 2017.
41. Aaltola, K. Empirical study on cyber range capabilities, interactions and learning features. *Digital Transformation, Cyber Security and Resilience of Modern Societies*; Springer: Cham, Switzerland, 2021; pp. 413–428.
42. Sheng, S.; Magnien, B.; Kumaraguru, P.; Acquisti, A.; Cranor, L.F.; Hong, J.; Nunge, E. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA. USA, 18–20 July 2007; pp. 88–99.

43. Cone, B.D.; Irvine, C.E.; Thompson, M.F.; Nguyen, T.D. A video game for cyber security training and awareness. *Comput. Secur.* **2007**, *26*, 63–72. [CrossRef]
44. Hernández-Ardieta, J.L.; Santos, D.; Parra, P.; Tapiador, J.E.; Peris-López, P.; López, J.; Navarrete, G.F. *An Intelligent and Adaptive Live Simulator: A New Concept for Cybersecurity Training*; Indra: Madrid, Spain, 2011.
45. Denning, T.; Lerner, A.; Shostack, A.; Kohno, T. Control-Alt-Hack: The design and evaluation of a card game for computer security awareness and education. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 915–928.
46. Le Compte, A.; Elizondo, D.; Watson, T. A renewed approach to serious games for cyber security. In Proceedings of the 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, Tallinn, Estonia, 26–29 May 2015; pp. 203–216.
47. Giannakas, F.; Kambourakis, G.; Gritzalis, S. CyberAware: A mobile game-based app for cybersecurity education and awareness. In Proceedings of the 2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL), Thessaloniki, Greece, 19–20 November 2015; pp. 54–58.
48. Chai, P. Cyber Security Defender, 2015 WeCode National Competition: Cyber Security Game. Available online: https://www.youtube.com/watch?v=Bb_gGq1QMUU (accessed on 7 June 2023).
49. Gestwicki, P.; Stumbaugh, K. Observations and opportunities in cybersecurity education game design. In Proceedings of the 2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAMES), Louisville, KY, USA, 27–29 July 2015; pp. 131–137.
50. Nicho, M. Modelling serous games for enhancing end user cyber security awareness. *IADIS Int. J. Comput. Sci. Inf. Syst.* **2017**, *15*, 91–106.
51. Sorace, S.; Quercia, E.; La Mattina, E.; Patrikakis, C.Z.; Bacon, L.; Loukas, G.; Mackinnon, L. Serious games: An attractive approach to improve awareness. In *Community-Oriented Policing and Technological Innovations*; Springer: Cham, Switzerland, 2018; pp. 1–9.
52. Chai, P. Cyber Wellness and Cyber Security Game for the IDA. Available online: https://www.youtube.com/watch?v=g7Mz9vFceMU (accessed on 7 June 2023).
53. Katsantonis, N.M.; Kotini, I.; Fouliras, P.; Mavridis, I. Conceptual framework for developing cyber security serious games. In Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON), Dubai, United Arab Emirates, 8–11 April 2019; pp. 872–881.
54. Hill, W.; Fanuel, M.; Yuan, X. Comparing serious games for cyber security education. In Proceedings of the 2020 ASEE Southeastern Section Conference, Auburn, AL, USA, 8–9 March 2020.
55. Jaffray, A.; Finn, C.; Nurse, J.R. Sherlocked: A detective-themed serious game for cyber security education. In Proceedings of the Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, 7–9 July 2021; Proceedings 15; Springer: Berlin/Heidelberg, Germany, 2021; pp. 35–45.
56. van Steen, T.; Deeleman, J.R. Successful gamification of cybersecurity training. *Cyberpsychol. Behav. Soc. Netw.* **2021**, *24*, 593–598. [CrossRef]
57. FILIPPIDIS, A.; Lagkas, T.; Mouratidis, H.; Nifakos, S.; Grigoriou, E.; Sarigiannidis, P. Enhancing information security awareness programs through collaborative learning. In Proceedings of the European Conference on Games Based Learning, Lisbon, Portugal, 6–7 October 2022; Volume 16, pp. 803–810.
58. Intuit Cyber Security Game. Available online: https://www.youtube.com/watch?v=_3VLx0pXSYs (accessed on 7 June 2023).
59. Trickel, E.; Disperati, F.; Gustafson, E.; Kalantari, F.; Mabey, M.; Tiwari, N.; Safaei, Y.; Doupé, A.; Vigna, G. Shell We Play A Game? {CTF-as-a-service} for Security Education. In Proceedings of the 2017 USENIX Workshop on Advances in Security Education (ASE 17), Vancouver, BC, Canada, 15 August 2017.
60. Awojana, T.; Chou, T.S. Overview of learning cybersecurity through game based systems. In Proceedings of the 2019 CIEC, New Orleans, LA, USA, 1 February 2019.
61. Graffer, I.; Bartnes, M.; Bernsmed, K. Play2prepare: A board game supporting it security preparedness exercises for industrial control organizations. In Proceedings of the Norwegian Information Security Conference 2015 (NISK-2015), Ålesund, Norway, 23–25 November 2015.
62. Bond, J.G. *Introduction to Game Design, Prototyping, and Development: From Concept to Playable Game with Unity and C#*; Addison-Wesley Professional; Game Design Series; Pearson Education: Singapore, 2014. ISBN 9780133439625. Available online: https://books.google.com.pk/books?id=40T1AwAAQBAJ (accessed on 7 June 2023).
63. Xiao, H.; Hao, W.; Liao, Q.; Ye, Q.; Cao, C.; Zhong, Y. Exploring the gamification of cybersecurity education in higher education institutions: An analytical study. In Proceedings of the SHS Web of Conferences, Sanya, China, 22–23 December 2023; Volume 166.
64. Shostack, A. Elevation of privilege: Drawing developers into threat modeling. In Proceedings of the 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA, USA, 18 August 2014.
65. Potter, B. Microsoft SDL threat modelling tool. *Netw. Secur.* **2009**, *2009*, 15–18. [CrossRef]
66. Frey, S.; Rashid, A.; Anthonysamy, P.; Pinto-Albuquerque, M.; Naqvi, S.A. The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. *IEEE Trans. Softw. Eng.* **2017**, *45*, 521–536. [CrossRef]
67. Yasin, A.; Liu, L.; Li, T.; Fatima, R.; Jianmin, W. Improving software security awareness using a serious game. *IET Softw.* **2019**, *13*, 159–169. [CrossRef]

68. Gondree, M.; Peterson, Z.N. Valuing Security by Getting {[d0x3d!]}: Experiences with a Network Security Board Game. In Proceedings of the 6th Workshop on Cyber Security Experimentation and Test (CSET 13), Washington, DC, USA, 12 August 2013.
69. Denning, T.; Friedman, B.; Kohno, T. *The Security Cards: A Security Threat Brainstorming Toolkit*; University of Washington: Washington, DC, USA, 2013.
70. Batzos, Z.; Saoulidis, T.; Margounakis, D.; Fountoukidis, E.; Grigoriou, E.; Moukoulis, A.; Sarigiannidis, A.; Liatifis, A.; Karypidis, P.A.; Bibi, S.; et al. Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview. 2023. pre-print. Available online: https://https://www.techrxiv.org/articles/preprint/Gamification_and_Serious_Games_for_Cybersecurity_Awareness_and_First_Responders_Training_An_overview/22650952 (accessed on 7 June 2023).
71. Willems, C.; Klingbeil, T.; Radvilavicius, L.; Cenys, A.; Meinel, C. A distributed virtual laboratory architecture for cybersecurity training. In Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 11–14 December 2011; pp. 408–415.
72. Thakong, M.; Phimoltares, S.; Jaiyen, S.; Lursinsap, C. One-pass-throw-away learning for cybersecurity in streaming non-stationary environments by dynamic stratum network. *PLoS ONE* **2018**, *13*, e0202937. [CrossRef]
73. Urias, V.E.; Van Leeuwen, B.; Stout, W.M.; Lin, H.W. Dynamic cybersecurity training environments for an evolving cyber workforce. In Proceedings of the 2017 IEEE International Symposium on Technologies for Homeland Security (HST), Greater Boston, MA, USA, 25–26 April 2017; pp. 1–6.
74. Adinolf, S.; Wyeth, P.; Brown, R.; Altizer, R. Towards designing agent based virtual reality applications for cybersecurity training. In Proceedings of the 31st Australian Conference on Human-Computer-Interaction, Fremantle, WA, Australia, 2–5 December 2019, pp. 452–456.
75. Seo, J.H.; Bruner, M.; Payne, A.; Gober, N.; McMullen, D.; Chakravorty, D.K. Using virtual reality to enforce principles of cybersecurity. *J. Comput. Sci. Educ.* **2019**, *10*, 81–87. [CrossRef] [PubMed]
76. Booth, J.; Air Command and Staff Coll Maxwell AFB Al Maxwell AFB United States. *The Use of Virtual and Augumented Realities in Air Force Training*; Air Command and Staff College: Montgomery, AL, USA, 2019.
77. Elevate Performance through Immersive Experience. Available online: https://www.strivr.com/lp/elevate-performance-through-immersiveexperience/?utm_medium=Paid-Search (accessed on 7 June 2023).
78. VR Cybersecurity Training. Available online: https://www.nnit.com/our-solutions/cybersecurity/vr-cybersecuritytraining/ (accessed on 7 June 2023).
79. Security Awareness Game. Available online: https://www.infosequre.com/security-awareness-game (accessed on 7 June 2023).
80. Virtual Reality Training Powered by SixGen. Available online: https://www.sixgen.io/course (accessed on 7 June 2023).
81. Makransky, G.; Borre-Gude, S.; Mayer, R.E. Motivational and cognitive benefits of training in immersive virtual reality based on multiple assessments. *J. Comput. Assist. Learn.* **2019**, *35*, 691–707. [CrossRef]
82. Meldrum, D.; Glennon, A.; Herdman, S.; Murray, D.; McConn-Walsh, R. Virtual reality rehabilitation of balance: Assessment of the usability of the Nintendo Wii® Fit Plus. *Disabil. Rehabil. Assist. Technol.* **2012**, *7*, 205–210. [CrossRef] [PubMed]
83. McMahan, R.P.; Bowman, D.A.; Zielinski, D.J.; Brady, R.B. Evaluating display fidelity and interaction fidelity in a virtual reality game. *IEEE Trans. Vis. Comput. Graph.* **2012**, *18*, 626–633. [CrossRef] [PubMed]
84. Ulsamer, P.; Schütz, A.; Fertig, T.; Keller, L. Immersive storytelling for information security awareness training in virtual reality. In Proceedings of the Hawaii International Conference on System Sciences, Kauai, HI, USA, 5 January 2021. Available online: https://api.semanticscholar.org/CorpusID:232414345 (accessed on 7 June 2023).
85. Giaretta, A. Security and Privacy in Virtual Reality—A Literature Survey. *arXiv* **2022**, arXiv:2205.00208.
86. Chekhovskoy, Y.; Plaksiy, K.; Nikiforov, A.; Miloslavskaya, N. The Use of Virtual Reality Technologies in the Specialists' Training in the Field of Information Security. *Procedia Comput. Sci.* **2022**, *213*, 223–231. [CrossRef]
87. Visoottiviseth, V.; Phungphat, A.; Puttawong, N.; Chantaraumporn, P.; Haga, J. Lord of secure: The virtual reality game for educating network security. In Proceedings of the 2018 seventh ict international student project conference (ict-ispc), Nakhon Pathom, Thailand, 11–13 July 2018; pp. 1–6.
88. Veneruso, S.V.; Ferro, L.S.; Marrella, A.; Mecella, M.; Catarci, T. CyberVR: An interactive learning experience in virtual reality for cybersecurity related issues. In Proceedings of the International Conference on Advanced Visual Interfaces, Salerno, Italy, 28 September–2 October 2020; pp. 1–8.
89. Dattel, A.; Ochoa, O.; Friedenzohn, D.; Goodwin, T.; Brodeen, H. Using Virtual Reality to Identify Cybersecurity Threats for Navy Midshipmen. 2022. Available online: https://commons.erau.edu/faculty-research-projects/21/ (accessed on 7 June 2023).
90. Puttawong, N.; Visoottiviseth, V.; Haga, J. VRFiWall virtual reality edutainment for firewall security concepts. In Proceedings of the 2017 2nd international conference on information technology (INCIT), Nakhonpathom, Thailand, 2–3 November 2017; pp. 1–6.
91. Alqahtani, H.; Kavakli-Thorne, M. Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information* **2020**, *11*, 121. [CrossRef]
92. Bernsland, M.; Moshfegh, A.; Lindén, K.; Bajin, S.; Quintero, L.; Solsona Belenguer, J.; Rostami, A. CS: NO—An Extended Reality Experience for Cyber Security Education. In Proceedings of the ACM International Conference on Interactive Media Experiences, Aveiro, Portugal, 22 June–24 June 2022; pp. 287–292.
93. Gračanin, D.; Park, J.; Eltoweissy, M. XR-CEIL: Extended reality for cybersecurity experiential and immersive learning. In *Proceedings of the International Conference on Human-Computer Interaction*; Springer: Cham, Switzerland, 2022; pp. 487–492.

94. Mishra, A.; Alzoubi, Y.I.; Gill, A.Q.; Anwar, M.J. Cybersecurity enterprises policies: A comparative study. *Sensors* **2022**, *22*, 538. [CrossRef]
95. Mishra, A.; Alzoubi, Y.I.; Anwar, M.J.; Gill, A.Q. Attributes impacting cybersecurity policy development: An evidence from seven nations. *Comput. Secur.* **2022**, *120*, 102820. [CrossRef]
96. Weiss, M.; Biermann, F. Cyberspace and the protection of critical national infrastructure. *J. Econ. Policy Reform* **2021**, *26*, 250–267. [CrossRef]
97. London, R.W. Comparative Data Protection and Security: A Critical Evaluation of Legal Standards. Ph.D. Thesis, University of South Africa, Pretoria, South Africa, 2014.
98. Yoo, R. An Expected Harm Approach to Compensating Consumers for Unauthorized Information Disclosures. *Rich. JL Tech.* **2012**, *19*, 1.
99. Liu, J.; Xiao, Y.; Chen, C.P. Authentication and access control in the internet of things. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 588–592.
100. Alotaibi, M.; Furnell, S.; Clarke, N. Information security policies: A review of challenges and influencing factors. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016; pp. 352–358.
101. Persadha, P.; Waskita, A.; Yazid, S. Comparative study of cyber security policies among malaysia, australia, indonesia: A responsibility perspective. In Proceedings of the 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, Indonesia, 29–31 October 2015; pp. 146–150.