World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:1, 2021

Exploring the Need to Study the Efficacy of VR Training Compared to Traditional Cybersecurity Training

Shaila Rana, Wasim Alhamdani

***Abstract*—**Effective cybersecurity training is of the utmost importance, given the plethora of attacks that continue to increase in complexity and ubiquity. VR cybersecurity training remains a starkly understudied discipline. Studies that evaluated the effectiveness of VR cybersecurity training over traditional methods are required. An engaging and interactive platform can support knowledge retention of the training material. Consequently, an effective form of cybersecurity training is required to support a culture of cybersecurity awareness. Measurements of effectiveness varied throughout the studies, with surveys and observations being the two most utilized forms of evaluating effectiveness. Further research is needed to evaluate the effectiveness of VR cybersecurity training and traditional training. Additionally, research for evaluating if VR cybersecurity training is more effective than traditional methods is vital. This paper proposes a methodology to compare the two cybersecurity training methods and their effectiveness. The proposed framework includes developing both VR and traditional cybersecurity training methods and delivering them to at least 100 users. A quiz along with a survey will be administered and statistically analyzed to determine if there is a difference in knowledge retention and user satisfaction. The aim of this paper is to bring attention to the need to study VR cybersecurity training and its effectiveness compared to traditional training methods. This paper hopes to contribute to the cybersecurity training field by providing an effective way to train users for security awareness. If VR training is deemed more effective, this could create a new direction for cybersecurity training practices.

***Keywords*—**Virtual reality cybersecurity training, VR cybersecurity training, traditional cybersecurity training, evaluating efficacy.

I. Background

TRADITIONAL training methods include text-based, video-based, instructor-led, and game-based training. Unfortunately, there are pitfalls with current training techniques. Effective training is primarily described as methods that engage users and encourage interaction. Thus, this paper aims to bring attention to the need to explore the effectiveness of VR training and its ability to remediate the drawbacks of traditional training methods.

Effective training is noted as being a key component in creating security awareness [1]. Training should not be limited to those responsible for information infrastructures; rather, all members of an organization should be effectively training [1]. Thus, cybersecurity training is of the utmost importance, both for organizations and personal safety. Cybersecurity training is needed to train existing workforces and future ones [2]. It is widely accepted that humans are the weakest link within a security architecture. Thus, the primary way to combat this is to train any person that interacts with IT systems effectively. Traditional training methods include text-based, video-based, instructor-led, and game-based training. Unfortunately, there are pitfalls with current traditional training techniques. Effective training is primarily described as methods that engage users and encourage interaction.

VR simulation training and its potential to be more effective than traditional training methods needs to be further explored. There is little work focusing on utilizing VR as a training method and even less work comparing the effectiveness of VR training over traditional methods.

A necessary component for an effective cybersecurity training program is the inclusion of engaging and interactive activities to ensure that students learn to deal with real-world situations [3]. Consequently, training seminars, coupled with interactive, hands-on activities, are essential when crafting effective cybersecurity training. If VR training is deemed more engaging and interactive, it can contribute to the overall learning and retention of training modules.

II. Traditional Training

A. Current Training Methods

Cybersecurity awareness training comes in many forms. Most often, it is conducted by instructor-led training methods. Instructor-led training is done in a lecture-type setting with the main instructor that gives information to a classroom [4]. Instructor-led training can be considered a traditional training method, as many different topics, including cybersecurity topics, are taught in this manner. However, a mix of training methods was thought to be most effective in disseminating information to users to protect themselves against attacks that exploit human behavior [4]. The aforementioned mix of training methods includes text-based, video-based, and game-based education aimed at training users on how to guard themselves against being victims of phishing attempts [4]. Video-based training is a self-paced method that presents a selection of videos to users to present information on phishing attacks [4]. In a study conducted in 2019, researchers noted that participants preferred video-based training over text-based and game-based [4]. Game-based training is also a self-paced method that utilizes games to allow users to interact with

Shaila Rana is with the University of the Cumberlands, United States (e-mail: shailashifarana@gmail.com)

information to determine whether an email is received as a phishing attempt [4]. Finally, text-based training was also self-paced and relied upon educational information in text format that outlined best practices and other information on phishing attacks [4].

Traditional training methods, such as virtual learning platforms, train users based on a "one size fits all" approach that is not specific to a user [5]. Instead, all students take that same form of learning through a predefined course. Game-based training is included as a traditional training method, as it also has a predefined set and sequence of modules that follow a static curriculum [5]. When cybersecurity training methods stray from traditional methods that rely upon fixed curriculums and prebuilt systems, they are shown to be more effective [5]. Context-aware cybersecurity training goes beyond traditional training methods by avoiding preset modules and training materials; instead, relying on user input. Sensors, data storage devices, and receiving and analyzing data from sensors provide an experience that senses user behavior and adapts training to a specific user [5]. Essentially, context-aware user training relies upon sensing and analysis of user behavior and modifying training materials so that the user can understand cybersecurity training based on their specific skill set, thought process, reactions, and more. Devices that are a part of context-aware cybersecurity training also use user-specific data, such as social networks, public records, health and financial records, company records, and more [5]. This demonstrates the extreme customization to a specific user and being far from a "one size fits all" approach. Context-aware cybersecurity training utilizes a plethora of devices, such as mobile and pervasive computing devices, to be used in a context-aware training system [5]. This form of cybersecurity training was more effective than traditional methods that utilize predefined modules and training materials. Virtual environments, or virtual reality, can use forms of context-aware cybersecurity training. Context-aware training methods may be found to be more expensive in terms of costs, time, and resources for average organizations to implement for their users. Thus, the ability for it to be widely adopted remains dubious at this point. This form of training has been shown to be more effective because its ability to be specifically customized to a user emphasizes areas the user lacks in and identifies conditions where the training is most likely to be useful for the learner [5]. Additionally, the training is tailored to the specific threats the user may be facing in his or her current environment and prioritizing those threats and risks for training [5]. In general, more targeted training leads to more effective mitigation techniques for users [5]. In general, cybersecurity training techniques are looking to extend traditional methods for maximum effectiveness. In scenarios where traditional methods are looking to be extended, more interaction with the player and an immersive experience is usually sought after more effectiveness. A balance between the expenditure of time and resources balanced with effective methods to engage users in an interactive training method is needed.

Text-based, game-based, and video-based training methods are utilized for training users in cybersecurity principles and fundamentals. To have an end goal of security awareness, the delivery method that maximizes student learning and creates behaviors following best practices is critical. To not do so, it could mean that users are not prepared to deal with attacks they are faced with daily. Ignorant users are the leading source of data breaches that result in both tangible and intangible losses within organizations [6].

Traditional cybersecurity training is often expensive, resulting in a barrier for entry for cybersecurity professionals [7]. Therefore, an accessible way for cybersecurity training is required. One could argue that VR simulations offer a level of accessibility, as games can be utilized from personal headsets. Cybersecurity simulation training possesses a level of gamified elements [8]. Researchers note that costly infrastructure bars cybersecurity professionals from entering the field [7]. Thus, it is all the more vital that a personalized platform be readily available for students. Personalized and gamified cybersecurity training can alleviate the challenge of traditional training methods being too expensive. Consequently, gamified and personalized forms of cybersecurity training will allow more students to participate in cybersecurity training.

Traditional or conventional methods of cybersecurity training focus on both electronic resources (i.e., computers, mobile phones) and paper-based methods (i.e., leaflets, posters, newsletters) [6]. Posters, or a paper-based form, focus on one topic regarding specific issues [6]. On the other hand, newsletters carry several topics to convey to a specific group [6]. Both methods cannot guarantee that users are reading and comprehending the message(s) conveyed. Another traditional method of cybersecurity training is instructor-led presentations. Instructor-led training is usually in the form of a formal presentation, and a "top-down" approach wherein an expert instructs employees [6]. Instructor-led training can also be categorized as an expert-based approach, wherein a subject matter expert teaches a large group [6]. This cybersecurity training method may be more impactful than paper-based methods in that the instructor can interact with students. Expert-based instruction is expensive and can be thought of as providing a "one size fits all" approach for a continually evolving and complex cyber landscape [6]. Users also describe this traditional form of cybersecurity training as "boring and ineffective" [6]. Furthermore, the success of cybersecurity training with instructor-led training depends on the instructor's abilities in both subject matter and the ability to engage with students [6]. Thus, to combat this issue, student engagement and participation are necessary [6].

Web-based user training is an online method that goes at the user's pace and is more flexible [6]. This is a less costly form of cybersecurity training and can be sent at will. Emails fall under the umbrella of this form of training and are used for time-sensitive and specific matters [6]. Screensavers and other mobile learning platforms are utilized to disseminate cybersecurity training information in web-based user training [6]. This method also has shortcomings, such as an overall lack of a methodology to deliver online training [6].

Furthermore, the effectiveness of web-based user training has not been adequately measured. In web-based delivery methods, users find the training material monotonous, unchallenging, and not interactive [6]. All in all, this training method could be seen as unengaging. Consequently, this leads to a lack of motivation to continue training and a lack of overall material retention. A suggested solution for web-based training is to include graphics, assessments, and animations to make the content more engaging for users [6].

Video-based cybersecurity training is another conventional training method in which users watch educational videos [6]. This form of training is thought to be less effective in that it does not hold student attention long enough, especially for mundane topics [6]. On the other hand, simulation-based delivery methods are a more interactive and engaging form of training that requires user input [6]. In general, users who underwent simulation training were better able to discern phishing attacks than those given paper-based training [6].

The most common cybersecurity training forms include virtual classrooms, teleconferencing sessions, instructor-led sessions, posters, email messages, and newsletters [9]. It is found that these traditional forms of cybersecurity training come with limitations. Most importantly, too many topics in too little time will not allow users to retain all the information. Instructors can be bad communicators, methods of measurement of user behavior are lacking, and many cybersecurity training methods are considered passive [9]. Consequently, to combat this, researchers found that cybersecurity training programs must grab and hold user attention and communicate material effectively in a certain amount of time [9]. Previous traditional cybersecurity training methods were found not to retain user attention and could not adequately teach cybersecurity training information in a limited amount of time. Therefore, future cybersecurity training techniques must interact and hold student attention while using time appropriately. Game-based training, or video games, can address the problems mentioned above with interactive and immersive content.

Utilizing a combination of different training methods that rely on interactive and self-paced techniques can consolidate knowledge to users and potentially invoke desired behaviors. Effective cybersecurity training is imperative to change behaviors and encourage users to understand cybersecurity fundamentals to protect themselves in their work and personal lives. Combining different training methods may bring different levels of interaction and consolidation of knowledge. However, in a study conducted, it was found that there was no specific combination of training methods proved to be more effective than instructor-led training [4]. On the contrary, it was seen that participants in this study favored instructor-led training in a classroom experience rather than a combination of the different training methods [4]. It was noted that training did lower the rate at which users fell victim to phishing attacks. However, a significant combination of self-paced training (i.e., game-based, video-based, and text-based) was not noted to be more effective than the traditional method of instructor-led training [4]. Furthermore, it is important to note that cybersecurity training programs should consider the students and create a training method based on the target group [4]. In other words, a variety of methods should be implemented within cybersecurity training programs to include a mix of instructor-led training and self-paced methods based on student preferences [4]. Essentially, this study highlights the importance of further exploration of the most effective methods of cybersecurity training.

Conventional methods, such as instructor-led methods, also rely on an interactive component, such as working groups, to practice concepts learned [10]. A hands-on activity is assumed to be more effective because it restructures and consolidates concepts [10]. However, the shortcomings of interactive activities with traditional methods are that users may be less engaged and extroverted than others, which works against its overall effectiveness [10]. Inevitably, social skills play a significant factor in this form of interactive activity with conventional cybersecurity training methods [10]. Therefore, there should be a customized method for interaction with individual students to counter the aforementioned issue to engage users. A "one size fits all" approach does not yield the most effective results, especially when dealing with users with different social skills. Subsequently, a flexible, customized, and interactive method may be more effective than traditional training methods, which are relatively inflexible and depersonalized.

Traditional training methods have been deemed unsuitable for cybersecurity in that an academic approach is not realistic to train students effectively [11]. Instead, cybersecurity training requires practical experience with hands-on activities and interaction to consolidate and retain knowledge [11]. Traditional training methods include lectures and instructor-led sessions in which students are not applying the knowledge acquired in practical and interactive activities. Instructor-led training can be enhanced by using exploratory learning in which students have hands-on training through virtual labs [11]. Hands-on activities in the cybersecurity field may be destructive by introducing vulnerabilities, threats, illegal attacks, and more to a system [11]. Hence, a balance between interactive, real-world activities and a safe environment is required to train students in cybersecurity principles. Labs are traditionally used for practical exercises to reduce the risk of ineffective training or attacks and vulnerabilities being introduced into a system [11]. However, these labs have difficulties and drawbacks, such as immobility, cost, and complexity in sandboxing environments [11]. Creating an interactive feature with traditional training methods was demonstrated to be costly, difficult, complex, and dangerous. A training feature that allows for an isolated environment is essential to train students effectively. VR simulations may deliver an isolated environment that addresses issues brought forth with traditional learning methods and labs.

Cyber ranges are a hands-on way to practice concepts learned in cybersecurity training through activities that mimic real-world scenarios [12]. Researchers have used cyber ranges through web-based learning platforms [12]. The training activity should have real-world relevance, have complex tasks,

allow students to examine tasks from different perspectives, have opportunities to reflect, and have an authentic learning experience [12]. Students responded positively to interactive cyber range training activities, stating that interactive interfaces provided clear information and guidance [12]. However, participants also indicated that training formats in current interactive formats, or cyber ranges, were too long. Furthermore, participants with less IT experience were not sure they were learning anything from these cyber ranges [12]. Therefore, there needs to be an interactive and tailored format to the participant's IT and cybersecurity experience level. VR cybersecurity training may remedy the issues found in cyber ranges; however, not enough studies have been conducted on this topic.

Replicating real-world scenarios is difficult, especially for traditional training methods [13]. Cybersecurity training aims at reducing skill gaps within a cybersecurity workforce; thus, traditional training methods include topics ranging from encryption to firewall management to vulnerability scanning and virtual networks [13]. Some cybersecurity training tutorials are designed for two-hour instructor-led laboratory sessions, as a hands-on environment is required [13]. This demonstrates the requirement of real-world scenarios to train a cybersecurity workforce to instill principles that will lessen skill gaps between employees. Other ways that employees and students educate themselves to be up to par with cybersecurity requirements are studying networking concepts externally because of a lack of documentation within organizations and the lack of documentation for the laboratory exercises [13]. It is predicted that real-world scenarios coupled with virtual laboratory modules will assist students looking to be a part of a cybersecurity workforce and companies who accept students to work for them and deploy virtual laboratories [13].

Virtual environments deployed for students allows them to experiment and change configurations to determine cause and effect in a safe and isolated environment [13]. Allowing students the ability to explore environments and configurations with-out the fear of damaging an IT system and configuration allows for a greater under-standing [13].

Some limitations of virtual environments are the limited capacity, system performance, and virtual IT systems designed for experimentation becoming outdated [13]. The amount of time and effort creating virtual laboratories should not be under-estimated. Additionally, the cybersecurity landscape is continuously changing, evolving, and becoming more complex. Consequently, the amount that virtual environments will need to be updated and revised to reflect the current state of threats, attacks, the organization's IT systems, and more will cost organizations a lot of time, money, and workforce. Moreover, creating a virtual environment that accurately reflects the complexity of deployed information systems may be a limitation because the real complexity may not be replicated within a virtual environment. It is noted that virtual cybersecurity exercises' ethical issues include students attempting to try out what they learned in a virtual environment in other out of band environments [13]. Therefore, those creating and deploying virtual environments to students to communicate that there could be legal and other detrimental implications if attempting to try certain actions in an uncontrolled or production environment is the responsibility of those creating and deploying virtual environments.

Cybersecurity training environments are frequently referred to as cyber ranges [3]. In cyber ranges, practical training includes instructor-led training combined with environments to practice skills learned, such as digital forensics [3]. Including an interactive component to allow users to practice the skills acquired in cybersecurity training may be vital to solidifying the knowledge gained in an instructor-led format. Cybersecurity training and other training rely on disseminating information to students and then allowing students to practice and demonstrate this knowledge. Thus, creating environments to enable students to have real-world uses of this acquired knowledge may prove beneficial in training techniques. In other words, realistic training techniques could equip users with practical knowledge to protect themselves and organizations from cyber-attacks and practice safe cybersecurity behaviors. Some cybersecurity roles highly dependent on realistic and well-developed training are first responders and security professionals [14].

Cybersecurity training simulations are found to facilitate learning and bring about positive learning effects [15]. Simulations can also yield some amount of data for analysis to determine whether or not users are experiencing positive learning effects [15]. Simulations are also used for pilots for flight simulations before flying a jet [15]. Similarly, cybersecurity professionals can utilize simulations before dealing with real-world scenarios of data breaches, cyber-attacks, and more. The uncertainty faced in cyber-attacks requires that students undergo simulation type training that is realistic; thus, equipping users to deal with real-world cybersecurity incidents [15]. Some problems faced with simulations include time delays and feedback loops between cause and effects that created complex outcomes that are difficult for researchers to predict [15]. Additionally, heuristics and availability of users should be utilized for the development of simulation cybersecurity training games [15].

Investing in new technologies for cybersecurity training is becoming commonplace for certain organizations, especially organizations that collect, house, and utilize sensitive and personal information [16]. Attacks against personal data are frequent and negatively affect organizations regarding tangible and intangible costs [16]. Therefore, organizations are looking to utilize cybersecurity training methods that effectively communicate policies and procedures to employees and users, who are the weakest link in cybersecurity infrastructures [16]. Traditional approaches to conduct cybersecurity training include emails, posters, newsletters, training studies, web-based training, and instructor-led techniques [16]. However, in traditional approaches, students may not understand the gravity of the negative consequences of incidents, security breaches, and breaches in security policies and procedures [16]. Moreover, traditional cybersecurity training methods are described as being "unauthentic, unintuitive, and unattractive

to users" [16]. As a remedy, cybersecurity training methods must create a visual platform to engage users, entertain them, and create an immersive experience that allows them to retain the knowledge acquired through a hands-on training approach.

B. Problems with Traditional Training Methods

Learning models have been developed in order to deal with the issue of cybersecurity training [17]. However, issues are still ever-present in cybersecurity training tactics [17]. It is widely understood that training modules are more effective if they include interactive content [18]. However, to this day, cybersecurity training programs face a plethora of difficulties. Such problems include personal and economic issues [18]. Personal issues include the lack of interest in learners, such as a lack of motivation to be trained [18]. This highlights the need for security training programs that are of interest, entertaining, and interactive to tackle unmotivated and uninterested users. Economic issues include balancing costs with an effective training program [18]. The more interactive, engaging, and effective a training program is, the more costly it will be. On the other hand, the less engaging and interactive, the more budget-friendly the cybersecurity training program is. This is a challenge for cybersecurity training because an adequate budget needs to be readily available for organizations and cybersecurity trainers to train students effectively. Furthermore, "modern" cybersecurity training techniques, such as simulations and games, are thought to be time-consuming [18]. Due to this categorization of being time-consuming, cybersecurity training practices may be further thought to exhaust resources, time, and money. Thus, a balance between engaging and interactive training practices and budget needs to be met. Additionally, to avoid additional time attempting to learn and understand a training module, training practices must be straightforward and simple [18]. Simplicity in training modules may allow organizations to meet the balance between costs and an effective training program.

Traditional training methods are often categorized as "boring and tedious" and lack overall success in programs [18]. This generalized and formal method does not produce effective outcomes for learners [18]. Instead, entertaining activities need to be included in training programs to encourage employees to interact with the training material [18]. Additionally, traditional methods lack a realistic view of attacks and security issues, as they do not expose users to real-world scenarios [18]. Learners must also be mentally stimulated to learn and retain information [18]. Without doing so, learners may not pay attention to training sessions that are not engaging and mentally stimulating. All in all, this demonstrates a strong need for entertaining, engaging, and interactive methods for cybersecurity training. This is in stark contrast to traditional training methods that are generalized, boring, formal, and not interactive.

Currently, there is no standardization of training methods in cybersecurity training [14]. Secure environments to train and allow hands-on activities are perilous to an organization and its IT infrastructure [14]. Thus, isolated and custom-made testbeds are utilized for training purposes [14]. However, these testbeds are not often used in that they are expensive, hard to maintain, and time-consuming to implement and deploy [14]. A cost-effective solution that provides a sandboxed environment that engages users in an interactive format is required. Simulation models may be a solution for this; however, more simulations need to be developed [14].

The overall shortage of funds and budgets available for cybersecurity training pushes organizations to rely heavily on traditional, paper-based training methods, such as posters, screensavers, and manual reminders [18]. The lack of training creates opportunities for attackers, such as social engineering-based attackers, to breach organizational systems [18]. Essentially, this demonstrates that traditional methods are not as effective as interactive training programs.

The lack of effective training programs has dire consequences. This poses a threat to organizations and puts assets at risk. Damages range from data breaches, loss of business reputation, loss of customers, loss of intellectual properties, and more [18]. In general, the overall security posture of organizations is at risk when cybersecurity training programs are ineffective. The threat of data, personnel, and IT infra-structure is at risk when users are not adequately and appropriately trained [18]. An inadequately trained user may result in a successful data breach that can severely damage an organization. Reputational damage and the loss of money, time, and resources coupled together are consequences of ineffectively trained users. There must be an interactive, entertaining, and engaging training program to counter the risk that ineffectively trained users present to an organization [18].

III. Virtual Reality

VR training is an extension of game-based training in that it engages with and entertains the user but goes a step further to create an immersive and highly interactive scene. Game-based training has been demonstrated to be more effective than paper-based and instructor-led training; however, VR training may show to be even more effective due to its highly interactive, engaging, and immersive nature. Thus, further studies regarding the ability of VR simulations to effectively train cybersecurity learners need to be conducted.

VR applications for cybersecurity training include thematic, stylistic, and mechanical aspects [19]. These design insights create cybersecurity training with a digital agent in VR applications [19]. As aforementioned, cybersecurity training programs should include visual aspects. VR applications provide a way to deliver visual elements while invoking stylistic components and themes to promote student learning. Virtualization is heavily relied upon to provide realistic training, and they are low-cost, low-maintenance, safe, and easily reproducible [14]. Furthermore, virtual reality may encompass the aforementioned factors and provide an even more realistic way to deliver cybersecurity training.

Virtual reality and augmented reality tools can teach cybersecurity principles to students, particularly undergraduate students, who do not have access to physical

data centers for physical cybersecurity learning [20]. Additionally, VR systems allow students to learn cybersecurity fundamentals in an observation, interactive, and active way [20]. Active learning is demonstrated to produce higher metacognitive activity levels over traditional training [20]. Active learning includes processing ideas, new experiences, and the ability to hypothesize and create and try out solutions [20]. As demonstrated, active learning produces higher learning levels; therefore, VR systems allow students a method of active learning of cybersecurity fundamentals. The use of VR systems can allow for more effective learning for students and a higher retainment of information. VR systems for cybersecurity also are designed to promote engagement, retention, and sustainability [20].

Virtual reality is a system that allows for the divulgence of information and video games [20]. Additionally, VR systems allow users to navigate a virtual environment [20]. For VR cybersecurity training, researchers determined that there could be some improvements. Some improvements include reducing confusion with controls and including new program elements to extend data center physical access control training [20].

VR training is utilized in other industries, such as in the healthcare industry, for medical training and is found to be largely useful [21]. Students noted a difference between screen-projected simulations over immersive and interactive VR environments [21]. Although both are simulations, students noted a preference for immersive and interactive environments over screen projectors. This hints towards a more widespread use for VR technologies in other industries to enhance student experiences for better learning and retention of information over traditional and more widely used learning methods, such as screen projectors. Unfortunately, the effectiveness of VR cybersecurity training is staggeringly understudied. Traditional methods (i.e., video-based, text-based, and instructor-led training) are more often studied, especially when compared to VR training. In general, cybersecurity training remains an immature and understudied field.

A. VR Cybersecurity Training

TABLE I
NUMBER OF STUDIES FOR CYBERSECURITY TRAINING METHODS

Training Method	Studies
Traditional Methods	59
Virtual Reality	4

Fig. 1 The number of studies for traditional training methods and VR cybersecurity training. VR cybersecurity training remains understudied, especially when compared to traditional training methods

B. VR Training in Healthcare

VR training is seen to be effective in the medical field, as the use of VR simulations reduces errors and trains skills required in operating rooms [22]. A study was done between VR trained students and non-VR trained students to determine the effectiveness of VR training over traditional forms [22]. Researchers observed that errors were less likely to occur in gallbladder dissections in VR trained students than non-VR trained students [22]. Thus, VR simulations have been shown to be effective in other fields, such as the medical field, in that the transfer of training skills was more advanced. Error reduction was the means of measuring effectiveness, as is the case when measuring cybersecurity training effectiveness. The amount of times users clicked on phishing links could equate to the number of errors experienced depending upon training format. Principally, researchers have found VR training to be effective in other industries. Therefore, VR training may show to be effective if utilized more ubiquitously in the cybersecurity training realm.

In general, VR training has been utilized in the healthcare industry more so than in other industries. Studies on the effectiveness of VR training remain primarily limited to the healthcare industry. However, it was demonstrated to be an effective form of training. Subsequently, the effectiveness of VR simulations in cybersecurity training should be explored to cover difficulties presented by traditional forms of training.

C. Measuring VR Cybersecurity Training Effectiveness

To measure the effectiveness of VR systems for cybersecurity training, researchers tested students regarding data center physical security principles and procedures [20]. Additionally, students were tested again, one week after training to demonstrate the retention of knowledge, and 80% of participants remembered the fundamentals learned in the VR training [20]. Student experiences were also recorded through interviews, and students mentioned that VR was considered beneficial [20]. Some student responses included that the VR systems were interactive, kept them engaged, easy, fun to use, and great for visual learners [20]. When interviewed, the positive reaction from students, coupled with high scores after taking VR training and one week after training, illustrates the potential effectiveness of VR training as opposed to traditional or procedural training. However, the effectiveness of VR training compared to traditional training needs to be further explored to determine if one is indeed more successful than the other.

D. Commercial Cybersecurity Training

Out of 51 commercial cybersecurity vendors researched, numbers of VR cybersecurity training in the commercial field remains low, with only five vendors noted. STRIVR, a VR cybersecurity training company, has found success in large companies like Walmart and Fidelity [23]. Additionally, STRIVR found a reduction in training from eight hours to fifteen minutes and an increase in customer satisfaction with VR training methods, as opposed to traditional methods [23]. Furthermore, this VR cybersecurity training company found

that knowledge retention is significantly higher, according to the VP of US Learning at Walmart [23]. NNIT, another cybersecurity VR training firm, focused on allowing users to spot security breaches in a typical office environment [24]. NNIT notes that gamification of cybersecurity training and VR simulations increase knowledge retention and increase effectiveness [24]. Security Quotient, the third VR cybersecurity training vendor, has an advantage over traditional training methods, like online classes [25]. Security Quotient notes that VR cybersecurity training invokes deeper engagement, customization, and adaptability. All of the aforementioned benefits were noted as being important for effective training in peer-reviewed and researched studies. Some aspects of virtual reality cybersecurity training include 360-degree pictures where users are meant to spot potential security vulnerabilities [24]. Other types of VR cybersecurity training include games, such as escape rooms employed by InfoSequre [26]. InfoSequre notes that VR cybersecurity training is an engaging and entertaining experience for students [26]. The last of the five cybersecurity VR training firms is SixGen, noting higher user retention levels [27]. The aforementioned confirms the assumption that VR cybersecurity training can be more effective in that it is more engaging, entertaining, and interactive than traditional platforms. However, this claim has yet to be studied, as demonstrated by the lack of literature surrounding VR cybersecurity training.

IV. Proposed Framework

1. First, a VR simulation regarding physical cybersecurity training concepts that will be utilized on the Google Cardboard VR headset will be developed. The VR simulation will be programmed in Unity VR. The physical security concepts will include desirable behaviors regarding locked devices, leaving passwords written down, and tailgating. The VR simulation is programmed from the user's point of view in an office. Physical security concepts will be based on generalized office policies regarding locked devices, keeping passwords and sensitive files secured, keeping doors locked, and keeping keys secured.
2. A video-based format will be developed regarding differing physical cybersecurity training concepts. The video-based format will use a graphic PowerPoint slide with voiceover. The video-based training will be 5 minutes in length. The concepts will include shoulder surfing, physical access controls, surveillance, deterrence, and perimeter security.
3. VR simulation training will be given to at least 100 participants. The participants will be randomly selected through a cybersecurity training company that typically provides training to educational organizations.
4. The video-based training will be given to the same 100 participants selected for VR simulation training.

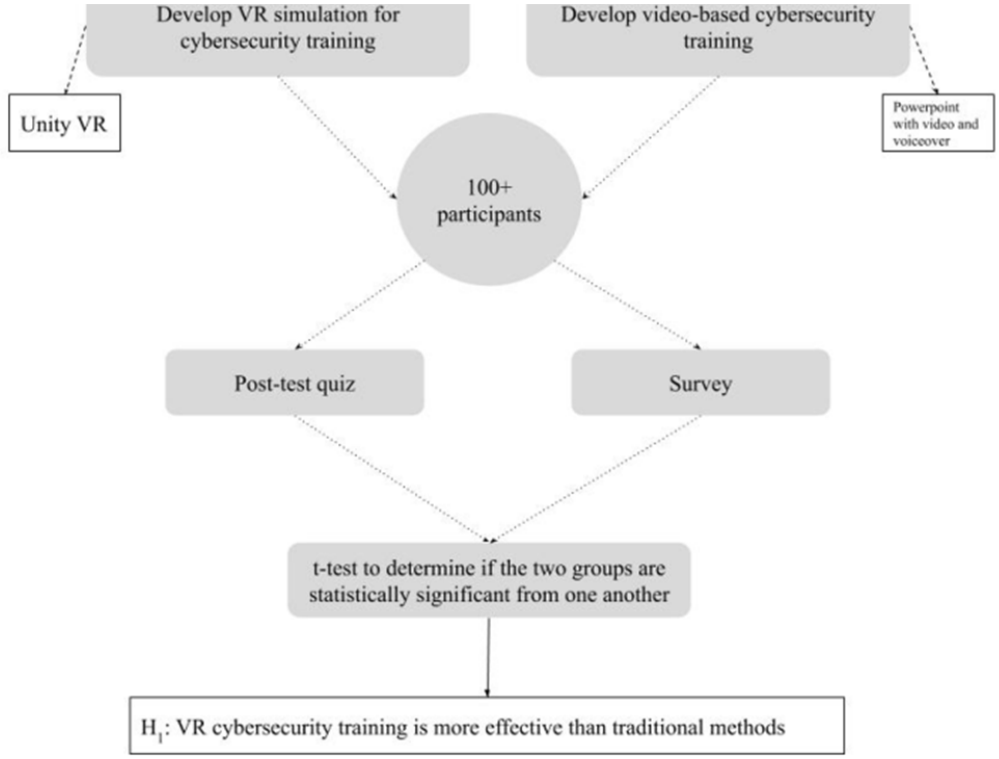

Fig. 2 The proposed framework to determine a difference in efficacy

5. After participants have undergone both VR training and video-based training, a post-test quiz will be delivered to all 100 participants that will measure the concepts taught in both VR and video-based training questions. The quiz will be sent on an online platform, such as SurveyMonkey. The quiz will consist of five questions

regarding what best practices are for physical cybersecurity. The quiz must be answered within one hour after the training.

6. After participants have undergone both VR training and video-based training, a survey will be delivered to all 100 participants asking to rate both training method's interactivity and engagement factors. The survey will be delivered on an online platform, such as SurveyMonkey. The survey will consist of four questions asking participants to rate both training form's engagement, entertainment, interactivity, and effectiveness.
7. The post-test quiz scores will be compared between video-based and VR training to see which group scored higher. Statistical analysis will be conducted to determine if VR cybersecurity training is more effective than traditional methods. A t-test test will be utilized to determine which group scored higher and whether or not the two groups are statistically significant from one another. The quiz scores will determine if VR cybersecurity training is more effective than traditional training methods.
8. The survey scores will be statistically analyzed to determine if there is a statistical significance between the two training groups. The significance will determine if one method of cybersecurity training is more engaging and interactive than another. The statistical significance test will be determined through a t-test to determine if the two groups are different from one another. If there is a difference, it can determine if VR cybersecurity training is more or less effective than video-based methods or traditional cybersecurity training.

V. Summary

Cybersecurity training remains an immature field; however, its importance should not be understated. Currently, cybersecurity training relies on traditional methods. However, there are significant difficulties and drawbacks to conventional training methods. Cybersecurity principles cannot be effectively taught without hands-on, engaging, and realistic scenarios. Thus, a training methkdsfsod that entertainingly encompasses interactive and engaging components is required. A simple, real-world, and engaging platform may be able to be utilized in VR simulations. As of now, the use of VR simulations in cybersecurity training remains understudied.

References

[1] Esteves, R. (2017). To Improve Cybersecurity, Think Like a Hacker. *MIT Sloan Management Review*, *58*(3), 71–.

[2] Beuran, R., Inoue, T., Tan, Y., & Shinoda, Y. (2019, June). Realistic Cybersecurity Training via Scenario Progression Management. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 67-76). IEEE.

[3] Beuran, R., Pham, C., Tang, D., Chinen, K. I., Tan, Y., & Shinoda, Y. (2017). Cytrone: An integrated cybersecurity training framework

[4] Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, *5*(6), e02010.

[5] Sadeh-Koniecpol, N., Wescoe, K., Brubaker, J., & Hong, J. (2016). *U.S. Patent No. 9,373,267*. Washington, DC: U.S. Patent and Trademark Office.

[6] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

[7] Fouché, M. (2015). *Code hunt as platform for gamification of cybersecurity training*. 9–11. https://doi.org/10.1145/2792404.2792406

[8] Maennel, K. (2020, September). Learning Analytics Perspective: Evidencing Learning from Digital Datasets in Cybersecurity Exercises. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 27-36). IEEE.

[9] Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)* (pp. 256-262). IEEE.

[10] Corradini, I. (2020). Training Methods. In *Building a Cybersecurity Culture in Organizations* (pp. 115-133). Springer, Cham.

[11] Willems, C., Klingbeil, T., Radvilavicius, L., Cenys, A., & Meinel, C. (2011, December). A distributed virtual laboratory architecture for cybersecurity training. In *2011 International Conference for Internet Technology and Secured Transactions* (pp. 408-415). IEEE.

[12] Tang, D., Pham, C., Chinen, K. I., & Beuran, R. (2017, November). Interactive cybersecurity defense training inspired by web-based learning theory. In 2017 IEEE 9th International Conference on Engineering Education (ICEED) (pp. 90-95). IEEE.

[13] Wahsheh, L.A. & Mekonnen, B., "Practical Cyber Security Training Exercises," *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2019, pp. 48-53. doi: 10.1109/CSCI49370.2019.00015

[14] Urias, V. E., Van Leeuwen, B., Stout, W. M., & Lin, H. W. (2017, April). Dynamic cybersecurity training environments for an evolving cyber workforce. In *2017 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-6). IEEE.

[15] Jalali, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

[16] Nguyen, T. A., & Pham, H. (2020, October). A Design Theory-Based Gamification Approach for Information Security Training. In *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)* (pp. 1-4). IEEE.

[17] Thakong, M., Phimoltares, S., Jaiyen, S., & Lursinsap, C. (2018). One-pass-throw-away learning for cybersecurity in streaming non-stationary environments by dynamic stratum network. *PloS one*, *13*(9), e0202937.

[18] Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73.

[19] Adinolf, S., Wyeth, P., Brown, R., & Altizer, R. (2019, December). Towards designing agent based virtual reality applications for cybersecurity training. In *Proceedings of the 31st Australian Conference on Human-Computer-Interaction* (pp. 452-456).

[20] Seo, J. H., Bruner, M., Payne, A., Gober, N., & McMullen, D. (2019). Using virtual reality to enforce principles of cybersecurity. The Journal of Computational Science Education, 10(1).

[21] Kasurinen, J. (2017). Usability issues of virtual reality learning simulator in healthcare and cybersecurity. *Procedia computer science*, *119*, 341-349.

[22] Seymour, N. E., Gallagher, A. G., Roman, S. A., O'brien, M. K., Bansal, V. K., Andersen, D. K., & Satava, R. M. (2002). Virtual reality training improves operating room performance: results of a randomized, double-blinded study. Annals of Surgery, 236(4), 458.

[23] Elevate performance through immersive experience. (2020, February 20). Retrieved November 10, 2020, from https://www.strivr.com/lp/elevate-performance-through-immersive-experience/?utm_medium=Paid-Search

[24] VR Cybersecurity Training. (n.d.). Retrieved November 10, 2020, from https://www.nnit.com/our-solutions/cybersecurity/vr-cybersecurity-training/

[25] Virtual Reality (VR) Cyber Security Awareness Training. (n.d.). Retrieved November 10, 2020, from https://securityquotient.io/security-awareness-training/virtual-reality.html

[26] Security awareness game. (n.d.). Retrieved November 12, 2020, from https://www.infosequre.com/security-awareness-game

[27] Virtual Reality Training powered by SixGen. (n.d.). Retrieved November 12, 2020, from https://www.sixgen.io/course