World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:7, 2022

A VR Cybersecurity Training Knowledge-Based Ontology

Shaila Rana, Wasim Alhamdani

***Abstract*—**Effective cybersecurity learning relies on an engaging, interactive, and entertaining activity that fosters positive learning outcomes. VR cybersecurity training may provide a training format that is engaging, interactive, and entertaining. A methodological approach and framework are needed to allow trainers and educators to employ VR cybersecurity training methods to promote positive learning outcomes. Thus, this paper aims to create an approach that cybersecurity trainers can follow to create a VR cybersecurity training module. This methodology utilizes concepts from other cybersecurity training frameworks, such as NICE and CyTrONE. Other cybersecurity training frameworks do not incorporate the use of VR. VR training proposes unique challenges that cannot be addressed in current cybersecurity training frameworks. Subsequently, this ontology utilizes concepts to develop VR training to create a relevant methodology for creating VR cybersecurity training modules.

***Keywords*—**Virtual reality cybersecurity training, VR cybersecurity training, traditional cybersecurity training, ontology.

I. Introduction

EFFECTIVELY designed cybersecurity training programs are of the utmost importance. Poorly designed cybersecurity training programs result in insignificant improvements within a population [1]. Thus, specific and targeted training programs and frameworks need to be developed for an appropriately designed training module. Cybersecurity training frameworks, such as CyTrONE and NICE, exist; however, nuances within VR cybersecurity training must be addressed. VR cybersecurity training may be a mitigating factor to the problems found in traditional training methods. Furthermore, VR cybersecurity can extend game-based training to account for an immersive and highly interactive experience to support positive learning outcomes. VR cybersecurity training is an immature field with few studies focusing on its potential significance. Researchers studied the use of virtual reality to enforce cybersecurity principles, and it was found that VR and augmented reality tools can teach cybersecurity fundamentals effectively and support active learning [2]. Researchers have demonstrated traditional cybersecurity training methods as ineffective in changing user behavior and defending against cyber threats [3]. Furthermore, researchers have found that traditional training methods have been cited as "boring and tedious" and lack success in programs [4]. VR cybersecurity training was demonstrated to be a more engaging learning platform for cybersecurity education than traditional training methods [5]. VR systems allow students to learn cybersecurity principles in an interactive way [2]. VR training is utilized in other industries, such as in the healthcare industry, for medical training and is demonstrated as applicable [6]. Thus, the need for exploring VR cybersecurity training modules needs to be addressed. Consequently, a proposed ontology for the development of VR cybersecurity training may encourage additional research and usage of VR training simulations and games. Moreover, creating ontologies is significant for both the cybersecurity field and cybersecurity training field as it can contribute to assist decision-makers in need of effective cybersecurity training modules [7].

This paper aims to fill the gap in current cybersecurity training literature by providing a methodology for creating VR cybersecurity training. VR scenarios require additional planning and designing; thus, this methodology aims to incorporate the unique challenges of developing VR simulations. Some of these challenges include the stylistic components that are unique to VR simulations.

A. Research Contribution

The contribution of this study is to propose a framework to design a VR cybersecurity training program that is customized to the user. This framework proposes to create an engaging, interactive, and entertaining platform to encourage positive learning outcomes. This study aims to create an ontological model to create an effective cybersecurity training platform that equips users to defend against cyberattacks. The proposed ontology aims to support the creation of VR cybersecurity training programs, which are nuanced and differ from traditional cybersecurity training. The proposed methodology includes the idiosyncrasies involved in the production and creation of VR simulations and games.

II. Other Frameworks Compared to the Proposed Ontology

A. CyTrONE Cybersecurity Training Framework Compared to the Proposed Ontology

Researchers note that a methodology is necessary to disseminate the required knowledge in cybersecurity education programs [8]. Furthermore, a methodology can assist educational and training institutions in providing an appropriate cybersecurity training program to equip professionals adequately [8]. Frameworks can allow for a customized approach that incorporates both the students' knowledge and the cybersecurity industry's needs [8].

The framework that is proposed in this paper differs in that it is specifically aimed at developing VR simulations. VR simulations require a different development level and can be

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

either just a simulation or game-based training. Thus, some nuances create another layer beyond only cyber ranges.

CyTrONE is a framework that includes a training database to create training content and the necessary environment within a cyber range for training [9]. These cyber ranges are administered on virtual machines for users. VR simulations differ from virtual machines in that users wear a VR headset and are immersed within the scene or game. On the other hand, virtual machines are administered on a computer or device. VR simulations include another layer of human interactivity and human input, including head and eye movements. For instance, the proposed ontology includes an additional testing phase before the VR simulation or game is administered. Thus, the proposed framework for CyTrONE, while highly flexible and configurable, is not complete for VR cybersecurity training modules. Instead, additional steps need to be included in the framework to account for human input and gestures, the subject in question, and extensive testing.

B. NICE Framework Compared to the Proposed Ontology

The ontology proposed in this paper, discussed below, differs from the NICE framework in that the NICE framework focuses on cybersecurity job roles and the development of cybersecurity professionals. Work roles are an inherent part of the NICE framework. On the other hand, VR cybersecurity training can apply to many audiences, including non-cyber security users. Thus, this study's proposed ontology aims to be a more inclusive framework that targets a broad audience and can be used outside government, educational institutions, and private organizations. Furthermore, this ontology focuses on VR development, which includes an immersive training platform requiring more testing and development than traditional training methods. Contrastingly, the NICE framework is primarily focused on traditional cybersecurity training methods. While this ontology builds upon the components proposed in the NICE framework, it extends it by including specificities found in VR simulations and games.

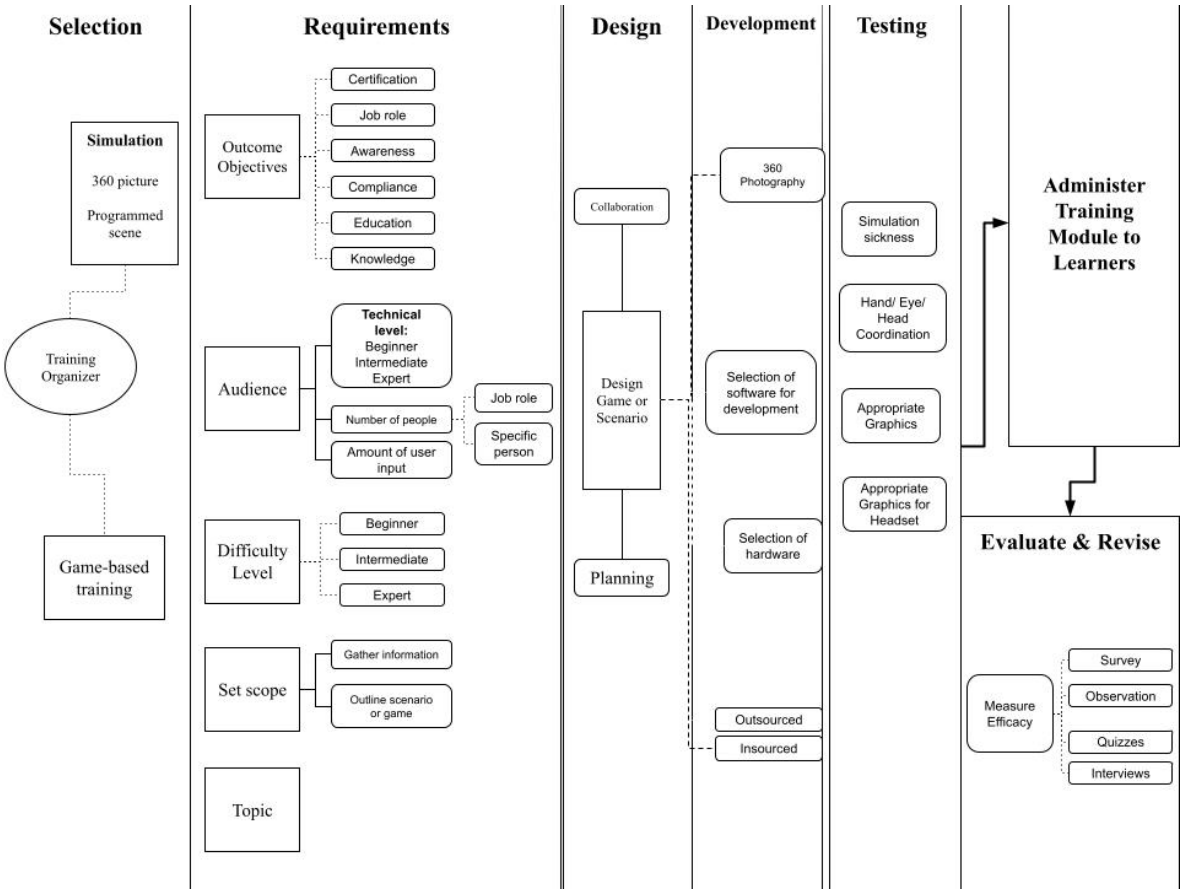

Fig. 1 Proposed Ontology with 7 Distinct Phases

III. Proposed Ontology

A. Stage I: Selection

The first stage of the ontology is the selection done by the training organizer. The training organizer can be one entity or a committee that can communicate, administer, and support the cybersecurity training program. The training organizer is the point of contact for setting the requirements for the VR cybersecurity training program. In the selection stage, the training organizer must decide the direction of the VR training content. VR training content can be created as either simulation or game-based training. Simulation training will allow a user to be immersed in a scenario or scene, walk around, explore, and interact with the scene. On the other

hand, game-based training requires more user input. Depending upon user actions and selections, the user will experience different scenarios and challenges.

Users have the option to interact with the environment or merely observe. Scenario-based VR training can be developed through software, or it can be done through 360-degree photographs. This is a less expensive way to create VR-based training while allowing the user to be immersed within a scene. The 360-degree photographs may be appropriate for allowing users to spot security infractions or relying on observation-based training. This is a less interactive form of training and may be appropriate for a wider audience, depending on technical skill level and the amount of interaction and time required for training. Alternatively, a scenario-based simulation may allow the user to interact with the surroundings, like holding objects and moving objects around. This will be most costly than 360-degree photographs but less expensive than developing game-based training.

Game-based training can have different game types such as role-play, adventure, action, strategy, puzzles, board games, and network simulations; consequently, VR simulation game-based training can include the aforementioned or a combination of these game types [10]. It is important to note that most game-based target audiences include students ranging from children to teenagers [10]. Essentially, game-based training design should heavily depend on the target demographic of cybersecurity learners. Demographics include but are not limited to the skill level, age, and gender of users. Game-based VR training may not be appropriate for a wide range of audiences; however, the nature of high user engagement and interactivity can produce more positive learning outcomes. Furthermore, game-based training allows users to view challenges in different ways and scenarios [11]. In general, game-based training is an "excellent platform" to train users [12]. Developing and implementing VR game-based training will be more costly in terms of time, resources, and finances. Furthermore, there is a higher likelihood that game-based VR training development will be outsourced to third-party vendors. Thus, the training organizer must decide whether the VR development will be simulation or scenario-based training or game-based training.

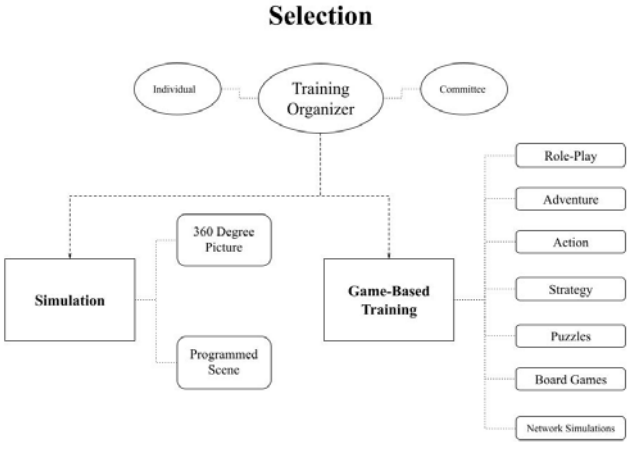

Fig. 2 Selection Stage

B. Stage II: Requirements

The second stage consists of building and setting requirements for the VR simulation or game-based training. This stage is relatively laborious compared to the other six stages; however, several factors need to be considered when designing and creating VR training. First, the training organizer(s) must decide the topic of cybersecurity training to be conducted. If the training is meant to be administered to office members, physical cybersecurity policies may be the topic in focus. If the training is meant to be delivered to university students exploring network security, the topic will differ. Some examples of regularly discussed cybersecurity training topics include physical cybersecurity concepts, incident response, social engineering, malware, patch management, password management, compliance, critical infrastructure, and many more. Selecting a topic will depend upon the audience, outcome objective, difficulty level, and overall scope. Additionally, there may be multiple topics covered in one VR simulation or game. Essentially, this will vary significantly between training organizers and organizations.

The outcome objective needs to be defined by the training organizer(s) to select the topic. There are different outcome objectives for cybersecurity training. Outcome objectives can range from training for a learner to certification, a job or work role, cybersecurity awareness, compliance, education, or merely obtaining knowledge. The goal of VR training will depend upon what the desired outcome objectives are. Depending on those objectives, VR cybersecurity training requirements will be drafted to develop, develop, test, and administer.

The audience is another consideration to take into account when outlining the requirements for VR cybersecurity training. The target audience's technical prowess level should be defined to avoid administering too complex training for their knowledge or too simple to extract useful learning from the training module. Thus, the training organizer needs to define what the technical capacity level is for the target audience. Furthermore, the number of people who will receive this training needs to be considered and whether the training is meant for a specific person and job role. These factors will contribute to outlining applicable and appropriate requirements for the VR cybersecurity training module. As mentioned, VR cybersecurity training creates an immersive experience for a learner, given that a headset will be placed on them only to view the scene created by the training organizer. However, the amount of user input can vary greatly. As mentioned in stage 1, the training organizer must select whether the VR training module will be a simulation or game-based training. Subsequently, there will be different levels of human input and interaction. The training organizer(s) must also consider how much user input is required in the requirements stage. If the training module is simply a simulation or scenario, it should be defined as picking up objects and interacting with the scenario. It is essential to define the amount of user input before designing and developing the game.

The scope of the VR simulation or game should also be considered in the requirements stage. Depending upon the topic(s) selected by the training organizer, the scope will differ amongst training modules. Additionally, the overall objectives of the training module will influence the scope of the VR training module. To set the scope, the training organizer must gather information regarding the overall outcome objectives. If the outcome objective is to spread awareness simply, the scope may be set within a scene in an office focusing on commonplace office policies. On the other hand, if the scope is to create incident response training, the scope will encumber more scenes, principles to be taught, and human interaction.

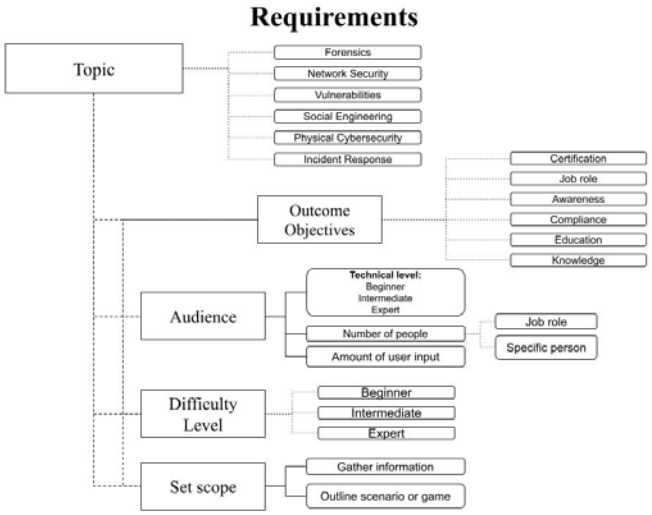

Fig. 3 Requirements stage

C. Stage III: Design

Designing the VR training module will take stages one and two and translate it into an overall simulation design. The outputs of stage one include whether the VR training module will be a simulation or game. The outputs of stage two are the overall requirements for the training module. These outputs include the outcome objectives, target audience, scope, difficulty level, and cybersecurity topic. The design stage is a natural next step from the requirements stage. Designing a VR training module will require planning and possibly collaboration. For gamified VR cybersecurity training, designers with past game experience may be necessary. The training organizer(s) must evaluate whether or not a dedicated designer is required. Collaboration can also include gathering input from other stakeholders. Stakeholders can range from the learner to members within an organization or even possibly third parties. This will heavily depend on the training organizer's goals for the cybersecurity training module, scope, target audience, outcome objectives, and difficulty level.

In the design stage, the elements of the game will be outlined. Elements may include the scene in which the game or simulation will occur, how the user will interact with the VR simulation, and how topic information will be disseminated to the user. If text is utilized for training the user, the way that text will be displayed must also be addressed in this stage. On the other hand, if sound, music, or voiceovers are utilized in the VR game or simulation, these must be appropriately addressed in this stage. The design stage will outline the key elements that will be passed on to developers.

Design and development may be outsourced to third parties to ensure the VR training module can support the requirements and selections made in the previous two stages. Depending upon the outputs of stages one and two, outsourcing to third-party vendors may be deemed appropriate. Ultimately, this will depend upon the training organizer whether or not a collaboration with external vendors is required. Overall, focused planning should occur in this stage to create a blueprint for developing a VR simulation or game. The design phase's output will allow developers to create a simulation or game that supports the requirements delineated in stage two.

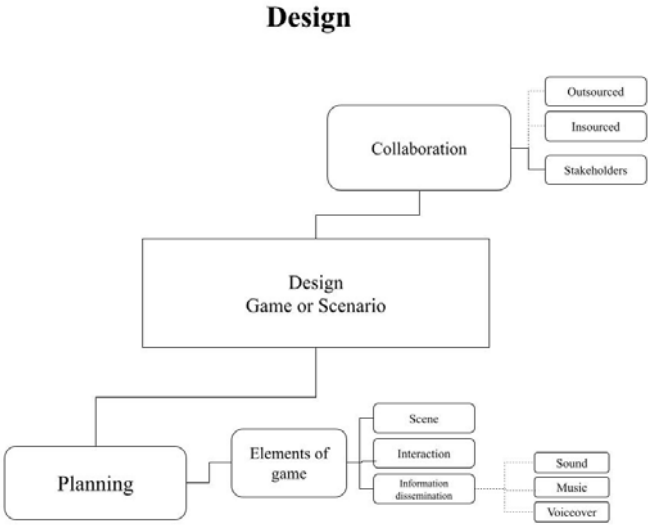

Fig. 4 Design stage

D. Stage IV: Development

Stage four focuses on the development of the training module. This includes selecting the software for software development and developing the game or scenario. If 360-degree photographs are decided upon by the training organizer, this is the stage in which the photography would occur. The selection of hardware must happen in this stage or before developing an appropriate training module. Development of the training module that embodies the requirements and design by the training organizer(s) may be insourced or outsourced depending on the resources, budget, and preferences of the training organizer(s). How development is done is dependent upon the earlier stages and overall design of the game.

Fig. 5 VR simulation example of a common office environment

E. Stage V: Testing

Testing the VR training module is essential and sets the ontology proposed in this paper apart from other cybersecurity training frameworks. VR training modules can have adverse effects if testing is not done adequately. Simulation sickness is a consequence of development errors and insufficient testing. Furthermore, if the VR module is required to be more interactive, hand, eye, and head coordination must be tested beforehand. Additionally, depending upon the VR simulation or game's hardware, graphics needed to be tested. Graphics should be appropriate not only for the equipment hosting the VR training but also for the learner. Consequently, the testing stage needs to be thorough and rigorous compared to other cybersecurity training development platforms. Poor graphics and simulation sickness will cause a negative experience for the learner and may not yield effective learner outcomes. Thus, the testing stage is vital and should be a specific step or stage in creating VR training modules.

F. Stage VI: Administer Training

The sixth stage is to administer the training module to learners. After sufficient testing, this is conducted to ensure that the VR training module fulfills the requirements and design of the training organizer(s) and avoids adverse outcomes (i.e., simulation sickness).

G. Stage VII: Evaluate and Revise

Surveys, observations, quizzes, and interviews may be conducted to measure the VR training module's efficacy. Learner feedback will help revise the training module that supports cybersecurity training requirements. On the sample of feedback received from learners, the sample can be divided into groups to measure the effectiveness between learner groups. Thus, this can give a unique perspective on the efficacy of the VR training module.

IV. Conclusion

The ontology is divided into seven distinct phases, building on the four phases included in the CyTrONE framework. The way in which this ontology is distinct from other cybersecurity training frameworks, such as NICE and CyTrONE, is due to the highly interactive and immersive nature of VR simulations and games. In general, VR simulations have been demonstrated to provide an interactive and engaging platform that supports active learning [2]. Compared to other training platforms, VR simulations have been demonstrated to be more effective [14]. Therefore, the proposed ontology of this paper aims to support the creation of VR cybersecurity training programs by addressing the unique nature of VR simulations. The proposed methodology builds upon the author's previous research determining the need to study the efficacy of VR cybersecurity training compared to traditional methods [13]. This ontology is a work in progress and has not yet been quantitatively studied. Future work aims to address how this framework quantitatively differs from other cybersecurity training frameworks.

References

[1] 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.

[2] 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).

[3] Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology (JCIT), 21(3), 26-39.

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

[5] Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020, September). CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. In Proceedings of the International Conference on Advanced Visual Interfaces (pp. 1-8).

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

[7] Oltramari, A., Henshel, D. S., Cains, M., & Hoffman, B. (2015). Towards a Human Factors Ontology for Cyber Security. *Stids*, *2015*, 26-33.

[8] Kim, E., & Beuran, R. (2018). On designing a cybersecurity educational program for higher education. *Proceedings of the 10th International Conference on Education Technology and Computers*, 195–200. https://doi.org/10.1145/3290511.3290524

[9] Beuran, R., Pham, C., Tang, D., Chinen, K. I., Tan, Y., & Shinoda, Y. (2017). Cytrone: An integrated cybersecurity training framework. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017) (pp. 157-166). SCITEPRESS – Science and Technology Publications

[10] Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training?. International Journal of Serious Games, 3(1), 53-61.

[11] Boopathi, K., Sreejith, S., & Bithin, A. (2015). Learning cyber security through gamification. Indian Journal of Science and Technology, 8(7), 642-649.

[12] Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018, February). Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 68-73).

[13] 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*, *15*(1), 10-17.

[14] 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.