Issues in Information Systems
Volume 24, Issue 1, pp. 101-112, 2023

DOI: https://doi.org/10.48009/1_iis_2023_109

The influence of traditional cybersecurity training on user attitudes towards VR cybersecurity training

Rhonda Chicone, *Purdue University Global, rchicone@purdueglobal.edu*
Shaila Rana, *Purdue University Global, shaila.rana@purdueglobal.edu*

Abstract

Effective cybersecurity training methods are needed as a primary defense against cyber threats. Traditional cybersecurity training methods have many issues and may not always translate into positive learning outcomes. Virtual Reality (VR) cybersecurity training methods may mitigate the pitfalls found in traditional cybersecurity training methods. This study utilizes the Technology Adoption Model (TAM) to explore user attitudes toward VR cybersecurity training modules. Moreover, the influence undergoing traditional cybersecurity training has on user attitudes is explored. A survey method is utilized to determine if the engagement and entertainment levels of traditional cybersecurity training methods influence on the perceived ease of use and usefulness of VR training platforms. There were 82 participants in this study. This study aimed to explore the perceived ease of use and usefulness of VR cybersecurity training modules. The results of this study demonstrate a statistically significant relationship between rated entertainment and engagement levels of traditional cybersecurity training methods and perceived ease of use and usefulness of VR training platforms. This study provides important insight for organizations and decision-makers seeking effective cybersecurity training methods.

Keywords: traditional cybersecurity training, cybersecurity training, VR cybersecurity training, TAM, ease of use

Introduction

Effective cybersecurity training methods are required to defend against the plethora of security threats and vulnerabilities that threaten organizations and individuals. Positive learner outcomes are essential for cybersecurity training. Consequently, this study explores the potential acceptance of VR cybersecurity training platforms by observing the relationship between the influence traditional cybersecurity training has on user attitudes towards VR cybersecurity training methods. This study utilized the Technology Adoption Model (TAM) and measured perceived ease of use and usefulness of VR cybersecurity training methods.

Moreover, this study observes the impact of rated levels of engagement and entertainment of traditional cybersecurity training methods has on perceived usefulness and ease of use of VR training methods. A statistically significant relationship was found between entertainment and engagement levels of traditional cybersecurity training methods and perceived ease of use and usefulness of VR training methods. Consequently, this study provides insights into the potential acceptance and use of VR cybersecurity training platforms and the importance of engagement and entertainment levels for cybersecurity training. Overall, this study demonstrates the potential acceptance and importance VR cybersecurity training platforms can have for effective cybersecurity training methods.

Background

Traditional cybersecurity training programs have become ineffective in changing people's security behavior (Sabillon, Serra-Ruiz, & Cavaller, 2019). Cyber defenses and prevention techniques are only effective if used effectively and disseminated effectively (Nagarajan et al., 2012). Research demonstrates that users fail to block or report cyber threats within their organization's environment (Sabillon, Serra-Ruiz, & Cavaller, 2019). Cybersecurity training is one of the most effective defenses to protect people and organizations from the continuing threats of cyberattacks. Part of these ineffective training platforms is the lack of quality in delivery and content. However, effective cybersecurity training is essential. Unfortunately, traditional cybersecurity training methods are less effective in changing user security behaviors. Consequently, new approaches to cybersecurity training are essential to prepare users and organizations against the continuing evolution and proliferation of cyber threats. VR cybersecurity training methods may provide an effective way in which to deliver cybersecurity training due to its interactive nature, content, and delivery methods. Research demonstrates that gaming and other interactive and engaging methods support positive learning outcomes (Nagarajan et al., 2012). Cybersecurity training is indispensable and requires hands-on activities to support understanding cyberattacks, which continue to evolve at an unprecedented rate (Beuran et al., 2017).

Interactive methods to train the cybersecurity workforce and address the barriers to entry into the cybersecurity industry are crucial. Gamification of cybersecurity training can address the weaknesses of traditional cybersecurity training and make it more accessible to learners (Fouché & Mangle, 2015). Gamification utilizes interactive methods to support effective cybersecurity training. All in all, this demonstrates the importance of incorporating interactive and engaging methods for cybersecurity training and awareness. The cybersecurity workforce and users that need to be trained in cybersecurity awareness fundamentals lack interactive and effective ways of training. Additionally, this training is essential regardless of age, gender, industry, and profession. Consequently, the aforementioned highlights the importance of utilizing effective methods for disseminating crucial security-related information. Frameworks for creating effective training also create positive outcomes for training activities regarding usability (Beuran et al., 2018). Effective training will yield a higher likelihood of users practicing secure behaviors and possibly entering the cybersecurity workforce.

Effectively training a cybersecurity workforce requires educational interventions (Sharevski, Trowbridge, & Westbrook, 2018). These educational interventions and methods to train individuals are necessary to respond to emerging and evolving cybersecurity threats. Topics and threats within the cybersecurity field evolve quickly. Moreover, best practices also evolve quickly to respond to these changing threats. Thus, it is essential that there be novel educational interventions in cybersecurity curriculums to address the ineffectiveness of traditional cybersecurity training methods and respond to emerging threats. Hands-on experimentation has been demonstrated to yield positive learning outcomes to support experiential learning and address trending knowledge within the cybersecurity industry (Sharevski, Trowbridge, & Westbrook, 2018). VR cybersecurity training formats, by nature, are experiential, immersive, and hands-on, creating an interactive user experience. Visual designs also support positive learning outcomes and hands-on learning (Sharevski, Trowbridge, & Westbrook, 2018). Overall, this demonstrates that VR cybersecurity training platforms should be further explored in order to support positive learning outcomes and respond to emerging cybersecurity threats.

Higher education institutions require enhancements to cyber education to include interactive experiences, or hands-on "experiential" training (Glantz et al., 2021). These enhancements require interactive learning tools that keep up with the changes in the cybersecurity industry, including the security threats associated with Internet of Things (IoT) devices and Cyber Physical System (CPS) applications (Glantz et al., 2021).

Ultimately, this demonstrates the importance of incorporating and exploring cybersecurity training platforms that provide immersive, engaging, and interactive experiences to support learning outcomes. Additionally, the need for enhancements to cyber education may be alleviated through VR training platforms, which provide hands-on and immersive learning experiences (Chowdhury & Gkioulos, 2021). Overall, VR cybersecurity training formats yield positive learning outcomes and support learners in understanding complicated cybersecurity concepts (Giaretti, 2022).

Contribution

This study aims to fill a gap in literature and studies addressing the influence traditional cybersecurity training has on the potential adoption of VR cybersecurity training platforms. VR cybersecurity training modules may support positive learner outcomes, especially when creating a hands-on and immersive learning experience that allows learners to grasp complex concepts. Moreover, VR cybersecurity training may address the weaknesses found in traditional cybersecurity training, such as the lack of an interactive experience and the inability to address evolving cyber threats. Moreover, traditional cybersecurity training is found to be ineffective in changing user security behaviors (Sabillon, Serra-Ruiz, & Cavaller, 2019). Most individuals must undergo some form of cybersecurity training and awareness due to the proliferation of computing devices in work and personal lives.

Thus, this study aims to understand the relationship between undergoing traditional cybersecurity training and the perceived usefulness and ease of use of VR training. Understanding how traditional training influences or affects user attitudes toward the potential adoption of VR training platforms provide important insights for organizations. A positive relationship between the more traditional training a user undergoes and higher perceived levels of usefulness and ease of use of VR training may allow organizations to develop games and implement these VR training platforms to support positive learning outcomes. This study aims to fill a gap in literature that explores the potential adoption of VR technologies within the cybersecurity training industry.

Furthermore, this study aims to provide organizations and decision-makers with a deeper understanding of how traditional cybersecurity training influences perceived levels of ease of use and usefulness of VR training technologies. All in all, this study demonstrates that undergoing traditional cybersecurity training can impact perceived ease of use of VR training technologies, meaning users may find VR platforms to be easier to use if they have undergone some type of traditional cybersecurity training. Organizations can benefit from this knowledge and utilize it to develop and implement VR cybersecurity training modules to address the ineffectiveness of traditional training formats.

Methodology

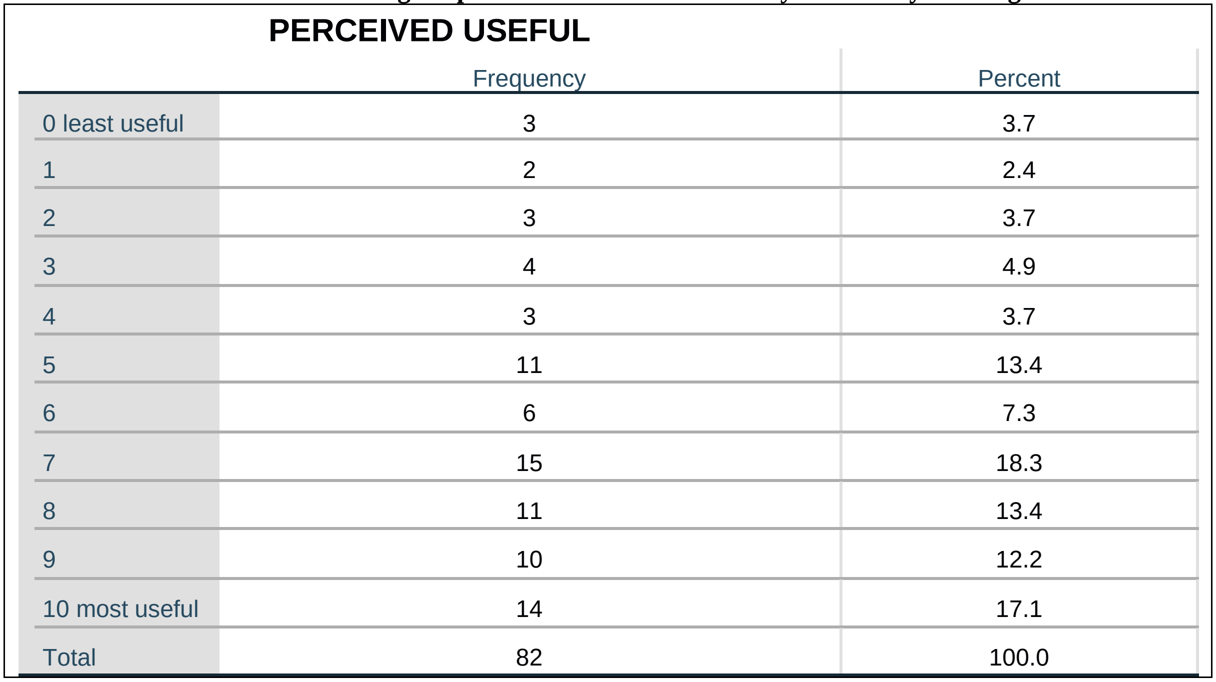
This study utilizes a survey based on the Technology Adoption Model (TAM) to assess user attitudes toward VR cybersecurity training modules. This survey was hosted by SurveyMonkey and consisted of twelve questions. Respondents are asked if they have undergone any form of traditional cybersecurity training and respond in a yes or no format. Moreover, the survey asks participants what form of cybersecurity training they have undergone. Participants are asked to rate VR cybersecurity technologies' potential usefulness and ease of use on a scale from 0-10 and their potential interest levels in undergoing VR cybersecurity training on a scale from 0-10. The questions respondents are asked to measure user attitudes toward a new technology. This study utilizes TAM to analyze whether undergoing traditional cybersecurity training affects user attitudes toward VR cybersecurity training platforms. In general, TAM is used to predict human behavior towards a new technology (Marangunić & Granić, 2015). The variables from TAM were utilized for this study, as TAM has a proven survey instrument. This study also underwent a pilot study to study the efficacy of this survey instrument. This study utilizes paid survey responses and targets individuals that are employed full-time, as they are most likely to have undergone some form of traditional cybersecurity training. This study aims to explore the influence that undergoing traditional cybersecurity training has on user attitudes towards perceived ease of use and usefulness of VR cybersecurity training modules. Overall, this study hypothesizes that the more traditional cybersecurity training a user undergoes, the more likely VR cybersecurity training will be perceived to be easy to use and useful.

Results

Descriptive Analysis

Participants were asked to rate how useful do you think VR cybersecurity training will be for you on a scale from 0-10 with 0 being the least useful and 10 being the most useful. Table 1 shows that, on a scale of 1-10, with 0 being the least useful and 10 being the most useful, most of the population voted that VR training would be very useful for them, whereas, only three people said that it would not be useful for them at all.

Table 1: Ratings of perceived usefulness of VR cybersecurity training



PERCEIVED USEFUL

	Frequency	Percent
0 least useful	3	3.7
1	2	2.4
2	3	3.7
3	4	4.9
4	3	3.7
5	11	13.4
6	6	7.3
7	15	18.3
8	11	13.4
9	10	12.2
10 most useful	14	17.1
Total	82	100.0

Figure 1 demonstrates that the majority of population, said that VR training would be very useful for them, whereas, only three people said that it would not be useful for them at all.

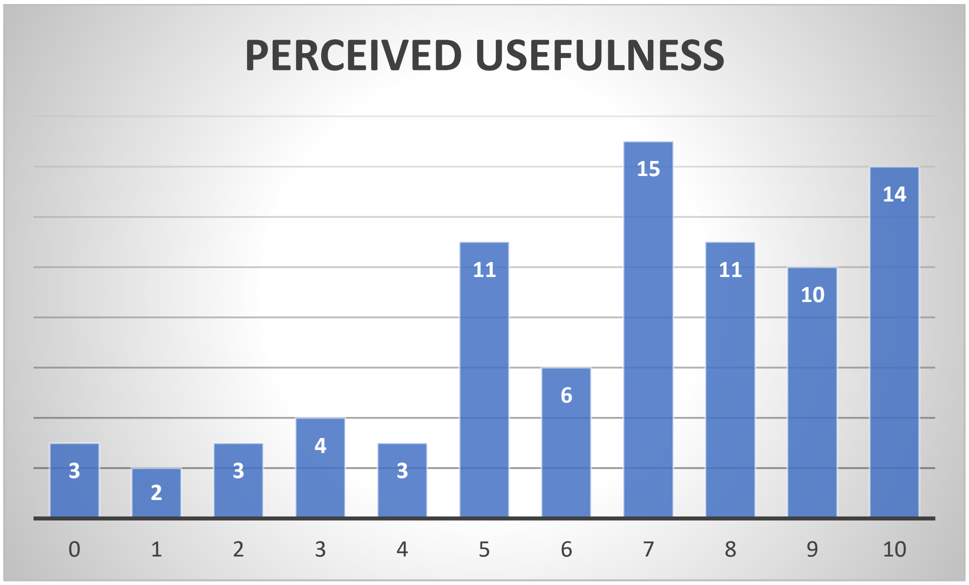
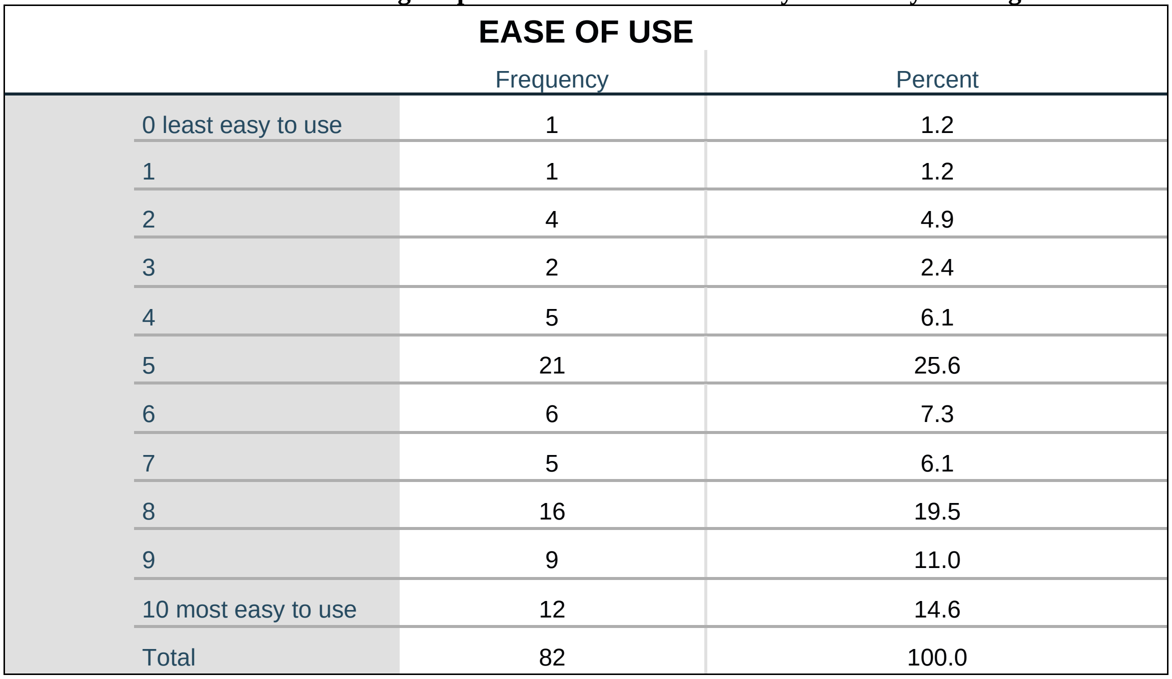


Figure 1: Graph of distribution of ratings of perceived usefulness of VR cybersecurity training

Participants were asked to rate the ease of use of VR simulations for cybersecurity training on a scale from 0-10 with 0 being the least easy to use and 10 being most easy to use. Table 2 shows that around 25% of population find it moderately easy to use, 14.6% find it most easy to use whereas a small number of population (1.2%) find it most difficult to use.

Table 2: Ratings of perceived usefulness of VR cybersecurity training



EASE OF USE

	Frequency	Percent
0 least easy to use	1	1.2
1	1	1.2
2	4	4.9
3	2	2.4
4	5	6.1
5	21	25.6
6	6	7.3
7	5	6.1
8	16	19.5
9	9	11.0
10 most easy to use	12	14.6
Total	82	100.0

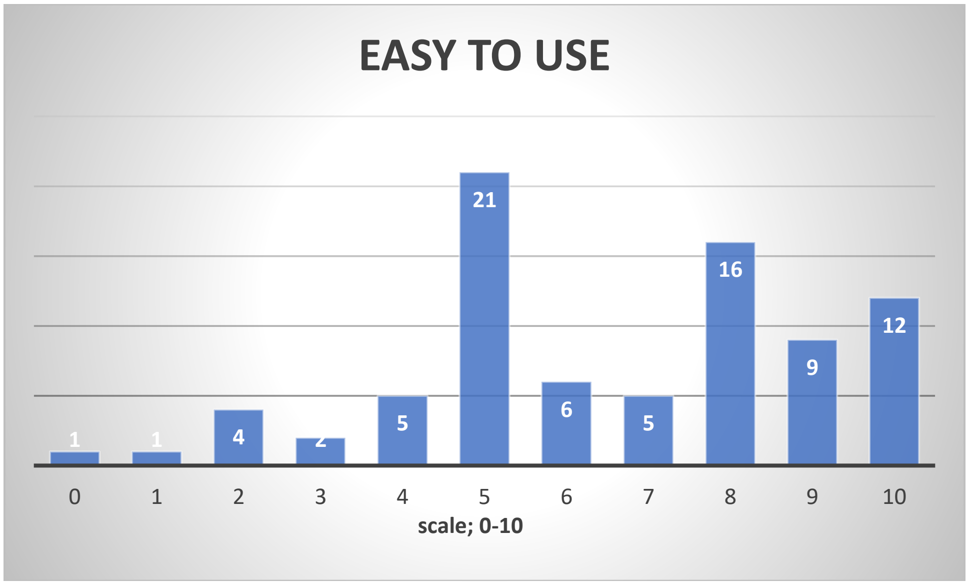


Figure 2: Graph of distribution of ratings of perceived ease of use of VR cybersecurity training

Respondents were asked to rate the ease of use of VR simulations for cybersecurity training on a scale from 0-10 with 0 being the least easy to use and 10 being most easy to use. Figure 2 shows that 21 people find it moderately easy to use, 16 finds it most easy to use whereas a small number of population (1) finds it most difficult to use.

Inferential Analysis

The variable "Ease of Use" and "Perceived Engagement" have statistically significant coefficients, as their p-values are less than 0.05. This means that changes in these variables are significantly associated with changes in the dependent variable. The variable "Perceived Usefulness" does not appear to have a statistically significant relationship with the dependent variable, as its p-value is greater than 0.05.

For every one-unit increase in "Ease of Use" and "Perceived Engagement," the dependent variable is expected to increase by 0.286 and 0.482, respectively. The intercept value of 0.762 suggests that when all independent variables are zero, the dependent variable is expected to be 0.762.

Table 3: Correlation between usefulness and ease of use

Correlations		
	USEFUL	EASE OF USE
USEFUL	1	
EASE OF USE	.747**	1
** Correlation is significant at the 0.01 level (2-tailed).		

ANOVA tests (Table 4) indicates that the regression model is statistically significant, as the F-statistic has a very small p-value (8.24387E-20). The coefficient of determination (R-squared) is 0.69, indicating that approximately 69% of the variability in the dependent variable can be explained by the independent variables.

Table 4: Demonstration of statistical significance between the traditional cybersecurity training's engagement and entertainment values and respondent's perceived ease of use and usefulness of VR training

Variables	P Value
Entertainment of traditional cybersecurity training and perceived usefulness of VR cybersecurity training	0.001
Entertainment of traditional cybersecurity training and perceived ease of use of VR cybersecurity training	0.002
Engagement of traditional cybersecurity training and perceived usefulness of VR cybersecurity training	0.028
Engagement of traditional cybersecurity training and perceived ease of use of VR cybersecurity training	0.040

Table 5 shows the results of a t-test that was conducted to determine whether there was a statistically significant relationship between rated entertainment levels of traditional cybersecurity training and perceived ease of use of VR cybersecurity training. The t-test yielded a t-statistic of 2.90 with 349 degrees of freedom (t(349) = 2.90, p = .001). The null hypothesis was rejected based on the p-value, which is less than the predetermined alpha level of .05. It can be concluded that there is a significant relationship between rated entertainment levels of traditional cybersecurity and perceived ease of use of VR training modules.

Table 5: t-Test two-sample assuming unequal variances results for the rated level of entertainment of traditional cybersecurity training and perceived ease of use of VR cybersecurity training

	Entertainment	*Ease of Use*
Mean	5.928176796	6.77348066
Variance	9.033701657	6.35395948
Observations	181	181
Hypothesized Mean Difference	0	
df	349	
t Stat	-2.899117626	
P(T<=t) one-tail	0.001989464	
t Critical one-tail	1.649231411	
P(T<=t) two-tail	0.003978929	
t Critical two-tail	1.966784557	

.

A t-test (Table 6) was conducted to determine whether there was a statistically significant relationship between rated entertainment levels of traditional cybersecurity training and perceived usefulness of VR cybersecurity training. The t-test yielded a statistic of 3.01 with 357 degrees of freedom (t(357) = 3.01, p = .001). The null hypothesis was rejected based on the p-value, which is less than the predetermined alpha level of .05. Thus, it can be concluded that there is a statistically significant relationship between rated entertainment levels of traditional cybersecurity methods and perceived usefulness of VR training platforms.

Table 6: t-Test two-sample assuming unequal variances results for the rated level of entertainment of traditional cybersecurity training and perceived usefulness of VR cybersecurity training.

	Entertainment	*Usefulness*
Mean	5.928176796	6.83977901
Variance	9.033701657	7.6019644
Observations	181	181
Hypothesized Mean Difference	0	
df	357	
t Stat	-3.006938599	
P(T<=t) one-tail	0.001412945	
t Critical one-tail	1.649133053	
P(T<=t) two-tail	0.00282589	
t Critical two-tail	1.966631204	

A t-test was conducted to observe if there was a significant relationship between rated engagement levels of traditional cybersecurity training and perceived ease of use of VR training methods and is shown in Table 7. The t-test yielded a statistic of 1.76 with 356 degrees of freedom (t(356 = 1.76, p = .04). Based on the p-value, which is less than the predetermined alpha level of .05, the null hypothesis was rejected. Consequently, it can be concluded that there is a statistically significant relationship between rated engagement levels of traditional cybersecurity training methods and perceived ease of use of VR training methods.

Table 7: t-Test two-sample assuming unequal variances results for the rated level of engagement of traditional cybersecurity training and perceived ease of use of VR cybersecurity training

	Engagement	*Ease of use*
Mean	6.281767956	6.77348066
Variance	7.781276857	6.35395948
Observations	181	181
Hypothesized Mean Difference	0	
df	356	
t Stat	-1.759540153	
P(T<=t) one-tail	0.039672354	
t Critical one-tail	1.649145105	
P(T<=t) two-tail	0.079344709	
t Critical two-tail	1.966649995	

.A final t-test was (Table 8) conducted to observe a relationship between rated engagement levels of traditional cybersecurity training methods and perceived usefulness of VR training methods. The t-test yielded a statistic of 1.91 with 360 degrees of freedom (t(360) = 1.91, p = .03). Based on the p-value, which is less than the predetermined alpha level of .05, the null hypothesis was rejected. Therefore, this demonstrates a statistically significant relationship between rated engagement levels of traditional cybersecurity training methods and perceived usefulness of VR training methods.

Table 8: t-Test two-sample assuming unequal variances results for the rated level of engagement of traditional cybersecurity training and perceived usefulness of VR cybersecurity training.

	Engagement	*Usefulness*
Mean	6.281767956	6.83977901
Variance	7.781276857	7.6019644
Observations	181	181
Hypothesized Mean Difference	0	
df	360	
t Stat	-1.914071518	
P(T<=t) one-tail	0.028201806	
t Critical one-tail	1.649097298	
P(T<=t) two-tail	0.056403612	
t Critical two-tail	1.96657546	

Ultimately, a statistically significant relationship was found between respondents’ rated engagement of traditional cybersecurity training and perceived ease of use and usefulness of VR cybersecurity training. Moreover, a statistical relationship was found between respondents’ rated entertainment of traditional cybersecurity training and perceived ease of use and usefulness of VR cybersecurity training.

Discussion

Experience with traditional training may positively impact the perceived levels of ease of use of VR cybersecurity training formats. Respondents who have had experience with traditional training may find it easier to adopt VR cybersecurity training formats. This may be because there is some familiarity with the learning process of cybersecurity training. Thus, this relationship could potentially lead to a more seamless learning experience and improved ease of use of VR cybersecurity training formats. The perceived usefulness of VR cybersecurity training formats may vary depending on users who have undergone traditional cybersecurity training.

Undergoing some form of traditional training may provide some advantages in familiarity with the material, but more research needs to be conducted. This suggests that the efficacy of VR cybersecurity training formats will depend on the specific training format and its desired learning outcomes. Ultimately, it is difficult to make a broad generalization on the impact traditional training has on the perceived levels of VR cybersecurity training formats without additional information about the training program and learning objectives.

The findings demonstrate that engagement and entertainment levels of traditional cybersecurity training methods can play a significant role in perceived ease of use and usefulness of VR cybersecurity training. Moreover, VR training modules are inherently engaging and immersive experiences that could support user outcomes. Consequently, this statistically significant relationship demonstrates that traditional cybersecurity training methods can influence interest and perceived ease of use and usefulness of VR cybersecurity training platforms.

Implications for Practice

Understanding the relationship between undergoing traditional cybersecurity training and perceived ease of use of VR cybersecurity training technologies can support its adoption and implementation. The relationship between traditional cybersecurity training and perceived ease of use of VR cybersecurity training modules suggests that users who must undergo traditional cybersecurity training can benefit from the use of VR cybersecurity training platforms. This is due to the relationship between users who have undergone traditional cybersecurity training and its positive impact on perceived ease of use of VR training.

As many professionals, regardless of industry and profession, must undergo some form of cybersecurity training and awareness, this study can be helpful for organizations looking to adopt VR training to support learner outcomes. All in all, experience with traditional training may positively impact the perceived ease of use of VR cybersecurity training. Consequently, participants with previous experience with traditional training methods may find it easier to adopt and utilize VR training, leading to a more seamless learner experience and less of a learning curve, due to the perceived ease of use.

The statistically significant relationship found between rated entertainment and engagement levels of traditional cybersecurity training and perceived ease of use and usefulness of VR cybersecurity training platforms can be useful for decision-makers. Organizations that utilize traditional cybersecurity training methods may find that adopting engaging and entertaining training methods can support positive learning outcomes. Moreover, users that undergo traditional cybersecurity training may find ease of use and usefulness of VR cybersecurity training platforms. Overall, this study demonstrates the importance of the variables of engagement and entertainment levels in traditional training and the influence that it can play on perceived ease of use and usefulness of VR training methods.

The impact of traditional training on the perceived usefulness of VR cybersecurity training modules is not yet clear. Prior traditional training may affect perceived levels of usefulness; however, more research needs to be done on this topic to understand the relationship. Furthermore, additional information surrounding the training program and learning objectives can support further studies and research on the impact of undergoing traditional cybersecurity training methods on perceived usefulness of VR training platforms. Overall, this study suggests that users may find VR cybersecurity training modules to be easier to use, depending on whether or not they have undergone traditional cybersecurity training methods. Alternatively, the relationship between undergoing traditional training methods and perceived usefulness of VR modules for training is still not clear.

Limitations

A larger sample is needed for a more comprehensive understanding of the relationship between undergoing traditional cybersecurity training and perceived ease of use and usefulness of VR training modules. Moreover, the population sampled in this survey consists primarily of respondents in North America. Thus, a more global population will provide a more holistic view of the relationship that traditional cybersecurity training has on perceived ease of use and usefulness of VR cybersecurity training modules. Cybersecurity training is not restricted to North Americans alone; consequently, a larger and more globally dispersed sample will provide a better understanding of the aforementioned relationship.

Conclusion

This study measured user attitudes toward VR cybersecurity training methods and demonstrated their potential for adoption in the cybersecurity training industry. In general, the statistically significant relationship between rated levels of engagement and entertainment in traditional cybersecurity training methods and perceived usefulness and ease of use of VR training platforms demonstrates its potential acceptance. Moreover, this study demonstrates the importance of creating engaging and entertaining methods for disseminating cybersecurity training.

Cybersecurity training is essential to protect against the growing attacks that threaten users, organizations, and national security. Therefore, this study aims to provide insight to assist decision-makers and organizations in disseminating cybersecurity training in an impactful way that supports positive learning outcomes. VR cybersecurity training methods may support positive learning outcomes and remediate the pitfalls found with traditional cybersecurity training methods. Thus, this study aimed to determine if there was an impact on undergoing traditional cybersecurity training and user attitudes toward VR training platforms.

Overall, this study determined that engagement and entertainment levels had a statistical relationship with perceived ease of use and usefulness of VR training methods. Consequently, this further highlights the potential adoption and acceptance of VR training methods within the cybersecurity training industry.

References

Bernsland, M., Moshfegh, A., Lindén, K., Bajin, S., Quintero, L., Solsona Belenguer, J., & Rostami, A. (2022, June). CS: NO–an Extended Reality Experience for Cyber Security Education. In ACM International Conference on Interactive Media Experiences (pp. 287-292).

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

Beuran, R., Tang, D., Pham, C., Chinen, K. I., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. Computers & Security, 78, 43-59.

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361.

Fouché, S., & Mangle, A. H. (2015, July). Code hunt as platform for gamification of cybersecurity training. In *Proceedings of the 1st International Workshop on Code Hunt Workshop on Educational Software Engineering* (pp. 9-11).

Giaretta, A. (2022). Security and Privacy in Virtual Reality--A Literature Survey. arXiv preprint arXiv:2205.00208.

Glantz, E. J., Bartolacci, M. R., Nasereddin, M., Fusco, D. J., Peca, J. C., & Kachmar, D. (2021, April). Wireless Cybersecurity Education: A Focus on Curriculum. In *2021 Wireless Telecommunications Symposium (WTS)* (pp. 1-5). IEEE.

Marangunić, N., & Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal access in the information society*, *14*(1), 81-95.

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.

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.

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). An effective cybersecurity training model to support an organizational awareness program: The cybersecurity awareness training model (catram). a case study in canada. In *Research Anthology on Artificial Intelligence Applications in Security* (pp. 174-188). IGI Global.

Sharevski, F., Trowbridge, A., & Westbrook, J. (2018, March). Novel approach for cybersecurity workforce development: A course in secure design. In *2018 IEEE integrated STEM education conference (ISEC)* (pp. 175-180). IEEE.