STUDENT PERCEPTIONS OF EXPERIENTIAL-BASED LEARNING EXERCISES IN CYBERSECURITY EDUCATION

by

JOSHUA LEE BRUNTY

B.A., Marshall University, 2005

M.S., Marshall University, 2009

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2023

Student perceptions of experiential-based learning exercises in cybersecurity education

Josh Brunty, *Middle Georgia State University, joshua.brunty@mga.edu*

Abstract

The shortage of qualified cybersecurity professionals is a growing concern in the information technology industry, and the rapid growth of the field exacerbates this shortage. Employers express concern over the shortage of hands-on, practical skills and problem-solving abilities among recent graduates, leading to the "cybersecurity skills gap." A study was conducted to examine how students perceive cyber competitions and Capture the Flag (CTF) learning environments as effective tools for learning cybersecurity concepts. A mixed-methods study investigated the effects of age, gender, job experience, and years of experience on these perceptions. The results showed that job experience has a significant effect on the perception of CTF exercises, while age, gender, and CTF experience were not significant. The qualitative analysis revealed factors that hinder students from participating in cybersecurity learning exercises. These findings provide valuable insights into how to improve student involvement and address the cybersecurity skills gap through effective programs and initiatives.
Keywords: cybersecurity, education, experiential learning, capture the flag (CTF), cyber skills gap

Introduction

The cybersecurity industry has experienced rapid and phenomenal growth in recent years, with a projected increase of 35% by 2031 (US Bureau of Labor Statistics, 2022). As of October 2022, there are currently 714,000 open cybersecurity job positions in the US (Cyberseek, 2022). US News and World Report (2022) also ranked cybersecurity as the top job of its 100 Best Jobs list in the United States in 2022. As a result, cybersecurity professionals in both public and private sectors are in need of specialized, hands-on education and training in order to effectively fill these positions (Stines, 2020).

Problem Statement

The shortage of qualified cybersecurity professionals is exacerbated by the rapid growth of the industry, as there aren't enough workers to meet its demands (Reagin & Gentry, 2018). The criticality of this shortage in professionals also raises another concern regarding cybersecurity education itself. Employers are expressing growing concern over the shortage of hands-on, practical skills and problem-solving and communication abilities among recent cybersecurity graduates (Ramezan, 2023). While many cybersecurity college and university classroom settings provide the tools, software, and resources necessary for students, they may not prepare them for post-college, career-based scenarios such as: cyber-attack mitigation, offensive and defensive security countermeasures, and adversarial thinking (NIST, 2018). Moreover, students often struggle to translate the theoretical knowledge that is learned in the college classroom into real-world solutions applicable in the workforce. This is what has become known in the industry as the cybersecurity skills gap (Vogel, 2016). Improving skills through the introduction of learning opportunities through hands-on, interactive experiential scenarios like cyber competitions may more adequately prepare students for the cybersecurity workforce upon graduation. An integral aspect of these competition communities is the chance for students to apply their knowledge in real-world settings and reflect on that learning in both academic and workplace contexts (Stylianos, 2020). As such, learning using hands-on experiential exercises is a valuable tool and catalyst to be utilized in these efforts (NIST, 2018).

However, the overall effectiveness of these competition environments as a valuable learning tool and students' perceptions of them need to be further studied (Stylianos, 2020).

Purpose of the Study

The purpose of this mixed-methods study was to examine students' perceptions of cyber competition and Capture the Flag (CTF) learning environments as an effective tool for learning cybersecurity concepts. This study examined independent variables such as age, gender, the relevant job experience, years of experience (cyber competitions/cyber ranges) and sought to determine whether these variables have a positive or negative effect on the perceptions of cybersecurity experiential-based learning exercises such as CTFs, cyber ranges, and collegiate cyber tournaments.

Research Questions

Consistent with the purposes of the study the following research questions were formulated:

- **RQ1:** Do the independent variables (i.e., age, gender, job experience, CTF experience) individually influence the dependent variable (i.e., perception of experiential learning exercises)?
- **RQ2:** Does a combination of the independent variables have the same effect on the dependent variable as they would individually (i.e., does gender combined with experience in cyber competitions have the same effect as gender alone)?
- **RQ3:** Are there other unknown perceptions of cyber competitions that hinder students from either not participating or hindering participating in these experiential cybersecurity learning exercises?

Research Objectives

The findings of this study reveal whether the independent variables (i.e., age, gender, job experience, CTF experience) individually influence the dependent variable (i.e., perception of experiential learning exercises). Additionally, the study measures whether the independent variables have the same effect on the dependent variable as they would individually (i.e., does gender combined with experience in cyber competitions have the same effect on overall perception as gender alone). Lastly, qualitative responses from participants sought to discover other unknown perceptions of cyber competitions that hinder students from either not participating or hindering participating in these experiential cybersecurity learning exercises.

Review of The Literature

The Use of Experiential Learning in Cybersecurity

Experiential learning is defined as "gaining knowledge from experience" or "learning through doing" (Jewer, 2015). This approach to active learning encourages participants to comprehend the experience fully and actively by directly participating in relevant context (Lewis, 1994). The process of experiential education starts with providing the learner with an experience, followed by reflection to cultivate skills, attitudes, new ways of thinking, and competencies (Aaltola, 2019). Kolb and Kolb (2005) categorize experiential learning as a four-phase cycle, including (1) hands-on experience, (2) reflective observation, (3) abstract conceptualization, and (4) active experimentation (Kolb, 2005).

In recent years, the study of experiential learning in higher education has gained significant attention as a means to improve educational outcomes (Kolb, 2005). In response, colleges and universities have rapidly developed practical and innovative hands-on degree, certificate, and credentialing programs in technology and cybersecurity to equip students for high-demand careers in these fields. However, instructors in these

programs often face the challenge of devising both engaging and realistic training exercises to teach cybersecurity skills and shrink the cybersecurity skills gap that is prevalent in the industry (Jewer, 2015).

The Cybersecurity Skills Gap

College and University-level classroom settings for cybersecurity often provide students with a multitude of exposure to hardware, tools, software, and other expensive resources. However, they may not be adequately prepared for post-college real-world and career scenarios in areas such as cyber-attack mitigation, offensive and defensive security measures, and adversarial thinking (NIST, 2018). Students often struggle to translate the theoretical knowledge that is learned in higher education classrooms into real-world solutions. This is what has become known as the cybersecurity skills gap (Vogel, 2016). Instructors in these programs frequently encounter the challenge of designing exercises that are both educational and practical in nature, in order to impart cybersecurity skills and mitigate the perceived skills gap (Jewer, 2015).

Cybersecurity competitions and challenges are gaining popularity as a method of identifying talented individuals in the cybersecurity field and reducing the responsibility of institutions and educators to create such exercises. These events are often sponsored and supported by various industry organizations and governments as a means of attracting and identifying top talent. Competitions may be organized and executed by means of a physical infrastructure, multi-user simulation, or through a virtual "cyber range" type of environment (Topham, 2016). Stylianos & Magkos (2020) explain the importance and appeal of hands-on Capture the Flag (CTF) style competitions both in professional and academic cybersecurity settings. Their research concluded that the lack of funding for large-scale training(s) to increase security awareness therefore leads entities such as higher education institutions and organizations to build and/or host CTF-based competitions in lieu of traditional lecture-based curriculum.

Many training programs and conventional academic courses lack adaptability and primarily target experienced users. As a result, they may fail to address the educational needs of beginners and individuals without an IT background (Stylianos, 2020). Their qualitative research of college student participants concluded that the learning process was significantly enhanced through the introduction and incorporation of CTF-style competitions. This enhancement of the learning process through the introduction of CTFs integrated elements of interactivity which, in turn, improve the learning experience among these students. Competitions like the National Collegiate Cyber Defense Competition program and the National Cyber League provide ample learning resources along with the competition experience, which enhances cybersecurity training (Topham, 2016). However, as Topham et. al. noted that "cybersecurity competitions provide little opportunity to find and develop new talent. Training must be provided before students have the ability to be at the competitive level required by these competitions, though, some competition developers do provide learning materials" (Topham, 2016, p. 70).

As the research points out, while hands-on-based competitions in classrooms challenge students to use their cybersecurity skills, many of these are often restricted in their scope and only teach specific aspects of cybersecurity, such as offensive or defensive-based security objectives (Topham, 2016). Additionally, Topham (2016) noted that training is a factor when examining involvement in cybersecurity exercises. Noting that training may come in the form of job experience (on-the-job training) or years of job experience (learning by doing), very little research has been conducted to examine the effect that experience has on the motivation to participate in live-fire cybersecurity exercises. Moreover, the literature also does not address external factors, such as age, gender, or interest, that may reduce the effectiveness or hinder the impact of CTF and cyber range learning exercises in higher education cybersecurity settings.

Factors that Affect Experiential Learning in Higher Ed Cybersecurity

Limited research has been performed on the attitudes that may hinder student participation in higher education cybersecurity learning exercises. Crandall et al. (2019) investigated the views of cybersecurity among high school students to determine what barriers may prevent these students from possibly pursuing a career in the industry. They discovered various attitudes held by the students that could discourage or obstruct their consideration of cybersecurity as a future career. Many of the students described a lack of overall interest in the occupation, mainly due to their distorted views of the cybersecurity work environment or a self-perceived lack of knowledge about the concepts of cybersecurity. Others cited obstacles such as drive/motivation, time, and cost constraints correlated with completing the hands-on training. The authors used a qualitative coding process that identified seven categories, which included: occupational awareness, lack of occupational interest, occupational aspirations, lack of excitement, lack of perceived skill, and resources. The research study also uncovered significant gender disparities in particular attitudes, specifically the categories of excitement and occupational interest, with females being more than twice as likely to hold these views compared to males. However, both genders felt similarly capable of pursuing a career in cybersecurity. Although there were disparities in certain categories, the data showed that both males and females had the same level of perceived self-efficacy (Crandall, 2019).

Kshetri et al. (2022) investigated the impact of gender asymmetry in the field of cybersecurity through the lens of socioeconomic factors. The authors noted that there are barriers faced by women in entering cybersecurity-related careers, which can stem from broader political, legal, and cultural factors, as well as factors specific to the technology and cybersecurity industry. The study also highlighted that stereotypical biases and decision-making practices within organizations have limited women's access to technology-based jobs, including cybersecurity roles. For instance, the industry's emphasis on technical skills over experiential soft skills in its advertisements can lead to the perception among women that cybersecurity is overly specialized and uninteresting (Kshetri, 2022).

An observational study was conducted by Thompson et al. (2018) to examine student misunderstandings regarding cybersecurity. They used thematic analysis to identify patterns in students' cognition and problematic reasoning that transcended different higher education institutions, scenarios, and demographics. The study found that students overgeneralized, conflated concepts, and made incorrect assumptions when working with tabletop cybersecurity scenarios. These misconceptions indicated that students lacked a useful framework to organize their thoughts and had limited comprehension and experience with the complexity of cybersecurity challenges. The authors recommended incorporating adversarial thinking as a framework to help students organize knowledge and gain experience, as well as utilizing experiential learning methods to engage students in complex scenarios (Thompson, 2018).

Methodology

Instrument

Using an exploratory sequential mixed methods design based upon a design used by Betancourt et. al. (2011) and Crandall et. al. (2019), the researcher used a mixed methods approach to examine students' perceptions of cyber range and CTF learning environments as an effective tool for learning cybersecurity concepts. Questions 1-6 collected independent variable demographic data (age, gender, class standing, academic major, job experience, CTF/cyber range experience). Questions 7-12 measured the dependent variable of students' perceptions and utilized a seven-point Likert scale using the following scoring breakdown: *7 = completely agree, 6 = mostly agree, 5 = somewhat agree, 4 = neither agree nor disagree, 3 = somewhat disagree, 2 = mostly disagree, 1 = completely disagree*. These survey questions are listed in Appendix A.

To address Research Question #3, the researcher investigated student perceptions of the factors that might prevent them from participating in experiential cybersecurity exercises such as CTFs. This was done through a single open-ended question, Survey Question #13, which asked*: "What do you feel prevents you from participating in experiential cybersecurity exercises such as Capture the Flag (CTF) competitions?"* The question was based on and adapted from an instrument previously used by Crandall, Noteboom, and El-Gayar (2019) in their study of high school students.

Subjects and Procedure

Prior to administering the survey, this researcher sought IRB (Institutional Review Board) approval to use human subjects. After IRB approval, the survey was generated and administered electronically online using Qualtrics XM™ software. The target subjects for this study were focused primarily on approximately 500 currently enrolled undergraduate and graduate college students majoring in a technology-related major field based at a mid-sized Southeastern and a mid-sized Northeastern United States University. Each participant was presented with a consent form that they agreed to prior to their participation in the study. Each participant was assured confidentiality and anonymity. An email with an invitation to participate in the study and a hyperlink to the instrument was sent to the students' university email. The email for the survey invitation was re-sent at the midpoint of the study for a total of a 7-day data collection period.

At the time of this study, a total of 123 surveys had been received. Of those 123 total responses, 17 collected responses were observed as incomplete and were therefore eliminated. This resulted in 106 total surveys (n=106) that were used for data analysis. The gender breakdown of the subjects was as follows: 61.32% male (n=65), 36.79% female (n=39), and 1.89% non-binary/third gender (n=2). In terms of education, 44.34% were graduate students (n=47), 27.36% were seniors (n=29), 11.32% were juniors (n=12), 9.43% were sophomores (n=10), and 7.55% were freshmen (n=8). In terms of job experience in cybersecurity or a related field, 59.43% reported less than 1 year of experience (n=63), 4.72% had 1 year of experience (n=5), 6.60% had 2 years of experience (n=7), 3.77% had 3 years of experience (n=4), 0.94% had 4 years of experience (n=1), and 24.53% had 5 or more years of experience (n=26). Of the total respondents, 65.09% (n=69) reported never having played in a CTF or cybersecurity competition, while 8.49% reported playing in at least one competition (n=9), 5.66% reported playing in 2 (n=6), 3.77% reported playing in 3 (n=4), 3.77% reported playing in 4 (n=4), 1.89% reported playing in 5 (n=2), and 11.32% reported playing in more than 5 (n=12). The minimum and maximum age of respondents was 18 and 72, respectively, with an average age of 29.78 years.

Data Analysis

To answer Research Question 1, the researcher used a one-way univariate analysis of variance (ANOVA), and for Research Question 2 the researcher used a between-subjects ANOVA test on data contained in survey questions. For the first question, the researcher sought to determine the variables from survey questions 1, 2, 5, and 6 (i.e., age, gender, job experience, and CTF experience) and their individual influence on the perception of experiential learning exercises (total mean of survey questions 7-12). For the second research question, the researcher sought to determine if a combination of the independent variables had the same effect on the dependent variable as they would individually (i.e., does gender combined with experience in cyber competitions have the same effect as gender alone). According to Rutherford (2011), a univariate ANOVA is commonly used to determine if there are significant variations between mean scores in different experimental conditions. The purpose of the ANOVA test is to uncover a linear relationship between the dependent variables (such as age, gender, class standing, academic major, job experience, and CTF/cyber range experience) and the predictor variable (perception of cybersecurity exercises). To achieve this, the *F* test must show significance (the p-value should be *equal to or less than* .05).

To address Research Question #3 and gain a deeper understanding of the qualitative perceptions of college students towards cybersecurity experiential exercises, the responses to Survey Question #13 underwent a two-pronged analysis using open coding and natural language processing techniques. The open coding method was utilized to categorize and identify the recurring themes and concepts present in the qualitative responses. The findings of Tesch (1990) and Rossman & Rallis (2012) support this approach as open coding helps to understand themes that are interconnected and may have been overlooked in strictly quantitative analysis. Additionally, the analysis was amplified by applying Qualtrics' TextIQ™, a cutting-edge tool for automating unstructured data analysis, to the qualitative responses (Qualtrics, n.d.). This technology allowed for a more in-depth analysis of the data, uncovering patterns and insights that were not immediately noticeable through manual coding methods.

Results

RQ1: *Do the independent variables (i.e., age, gender, job experience, CTF experience) individually influence the dependent variable (i.e., perception of experiential learning exercises)?*

Overall perception data was collected and is presented in Appendix B. The total mean perception of these results was calculated and compared individually against the variables of age, gender, job experience, and CTF experience.

Age: There was not a significant effect of the independent variable age on the dependent variable of overall perception at the $p < .05$ level *[F(3,102) = .874, p= .457]*.

Gender: There was not a significant effect of the independent variable gender on the dependent variable of overall perception at the $p < .05$ level *[F(1,104) = .375, p= .542]*.

Job Experience: There was a significant effect of the independent variable of job experience on the dependent variable of overall perception at the $p < .05$ level *[F(2,103) = 5.567, p= .005]*.

Post hoc comparisons using the Scheffe test (shown in **Table 1**) indicated that the mean score for those with less than 1 year of experience *(M=6.1905, SD=.61409)* was significantly different from the mean score of those with more than 1-5 years of experience *(M=5.6961, SD=51786),* and those with more than 5 years of experience *(M=5.8141, SD=.79906).*

Table 1: Post hoc Comparisons (Scheffe Test) of job experience on overall CTF perception

					95% Confidence Interval for Mean			
	N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Less than 1 year experience	63	6.1905	.61409	.07737	6.0358	6.3451	4.50	7.00
1-5 years experience	17	5.6961	.51786	.12560	5.4298	5.9623	4.67	6.50
More than 5 years experience	26	5.8141	.79906	.15671	5.4914	6.1369	3.83	7.00
Total	106	6.0189	.67859	.06591	5.8882	6.1496	3.83	7.00

Taken together, these results suggest that job experience does have an effect on the perceptions of CTF exercises. Specifically, our results suggest that when an individual gains additional job experience, their perceptions of the importance of hands-on CTF exercises will increase as well.

CTF Experience: There was not a significant effect of the independent variable CTF experience on the combined dependent variable of overall perception at the $p < .05$ level *[F(3,102) = .874, p= .457]*.

RQ2: *Does a combination of the independent variables have the same effect on the dependent variable as they would individually (i.e., does gender combined with experience in cyber competitions have the same effect as gender alone)?*

A between-subjects ANOVA was conducted (see **Table 2**). Results revealed a *non-significant* main effect of age and job experience *[F(4,93) = .765, p=.551]*, suggesting that the relationship of the overall perception of CTF exercises was not moderated by age and job experience. Additionally, there was a non-significant main effect on the combination of gender and job experience on overall perception *[F(2,93) = .903, p=.409]*.

Table 2: Test of Between-Subjects ANOVA of Combined Age & Job Experience, Gender & Job Experience upon Overall CTF Perception

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	7.565[a]	12	.630	1.438	.163
Intercept	1414.278	1	1414.278	3224.849	<.001
Age	.119	3	.040	.091	.965
Gender	1.206E-5	1	1.206E-5	.000	.996
Job Experience	3.799	2	1.899	4.331	.016
Combined Age & Job Experience	1.341	4	.335	.765	.551
Combined Gender & Job Experience	.792	2	.396	.903	.409
Error	40.786	93	.439		
Total	3888.389	106			
Corrected Total	48.351	105			

[a] R Squared = .156 (Adjusted R Squared = .048)

RQ3: *Are there other unknown perceptions of cyber competitions that hinder students from either not participating or hindering participating in these experiential cybersecurity learning exercises?*

The analysis of the data in the open-coding process produced the following ten categories shown in Table 3: lack of knowledge, time, lack of experience, social anxiety, awareness, lack of education, motivation, career, logistics, and gender. Figure 1 shows the word cloud.

Table 3: Coded categories with total count & percentage

Answer	**%**	**Count**
Lack of Knowledge	25.18%	35
Time	17.27%	24
Lack of Experience	15.83%	22
Social Anxiety	10.79%	15
Awareness	9.35%	13
Lack of Education	7.19%	10
Unknown	5.76%	8
Motivation	3.60%	5
Career	2.16%	3
Logistics	2.16%	3
Gender	0.72%	1
Total	100%	139

Figure 1: The word cloud

Lack of Knowledge. The grouping "lack of knowledge" refers to the student's perception of insufficient prior knowledge to successfully participate in a cybersecurity exercise. In the research, 32 responses (23.9%) expressed this concern. The source of this lack of knowledge may be linked to other categories identified in the research, such as lack of education or lack of experience. Sample responses: "I would not know where to start or what to do", "My lack of knowledge in cybersecurity", A general feeling like I don't know enough or that the information necessary doesn't stick with me well enough."

Time. This category identifies any students who reported time constraints as a limiting factor in participating. There were 23 coded responses (16.55%) that made mention of time as a factor. Sample responses: "Busy schedule", "I also work full time and I am raising children, so my time is very limited", "Class load and work has impacted my ability to participate in experimental cybersecurity exercises."

Lack of Experience. This category refers to the student's perception of insufficient prior experience to successfully participate in a cybersecurity exercise. 21 responses (15.11%) addressed experience as a concern. This category may also be linked to lack of knowledge as well. Sample *responses: "I am new to cybersecurity and have no experience in it right now", "I would say my experience level", "Experience in the field."*

Social Anxiety In this section, the focus is on remarks that pertain to anxiety or social anxiety. Social Anxiety Disorder (SAD), commonly referred to as social phobia, is an anxiety disorder that causes an individual to experience intense anxiety and fear in social situations, causing significant distress and hindering their ability to engage in everyday activities (Stein, 2001). Out of the total instances coded, 15 (10.79%) students mentioned the words "social anxiety" or "anxiety." Sample responses: "Just how intimidating it seems. I feel like if I don't know what I'm doing I'll get made fun of for it. I just feel like I don't know enough about cybersecurity stuff", "The reason I haven't participated in Capture the Flags is because of the imposter syndrome", "Not wishing to be seen as the weakest member of a team or participant."

Awareness. Awareness refers to the student simply not knowing that such competitions existed. There were 13 (9.35%) coded responses that were related to lack of awareness. Sample responses: "I am not aware of such competitions", "I didn't know what it was until now", "I do not know when they are going on, how to sign up, etc."

Lack of Education. There were 10 coded instances (7.19%) that were correlated to lack of education. Many students in this group also simultaneously reported a lack of skill and knowledge as well. Sample responses: "I just haven't learned enough yet because I am only in my sophomore year and I am scared to be

embarrassed in front of upperclassman", "What I feel prevents me from participating is that I understand that what I learn in the classroom will not completely translate to the competition."

Motivation. There were 5 coded responses (3.60%) where motivation was reported to be a factor in participation. Sample responses: "Lack of competitive drive", "Not enough encouragement", "Laziness on my part."

Career. There were 3 coded responses (2.16%) relating to career factors as a limitation to playing CTFs. Sample responses: "A change in career interest", "Time is primary, alignment with my career is secondary."

Logistics. Logistics refers to any logistic issues such as scheduling conflicts, or never being able to participate due to logistical reasons. There were 3 coded instances (2.16%) related to logistics. Sample Responses: "Nothing other than scheduling conflicts", "I've never had the opportunity to participate."

Gender. There was 1 (0.72%) coded response where gender was a reported factor. Sample responses: "Most of the Women in Cyber members refuse to participate in cyber competitions because they do not have much knowledge regarding cyber security or forensics, and they are afraid they will do poorly. I avoided them at first because of this but have utilized them as a great learning experience and encourage everyone to do the same."

None. A total of 8 (5.76%) coded responses either left this section blank or included a statement that was unable to be coded by the researcher.

Discussion

The results of the survey suggest that job experience has a significant effect on the perception of cyber competition experiential learning exercises. The results showed that individuals with more job experience tend to have a higher perception of the importance of hands-on CTF exercises. However, the independent variables of age, gender, and CTF experience were not found to have a significant effect on the overall perception of these exercises. Additionally, the combination of age, gender, and job experience was not found to have a moderating effect on the perception of cyber competition exercises. The results of the qualitative analysis showed that the participants cited factors such as lack of knowledge, time, lack of experience, social anxiety, lack of awareness, lack of education, motivation, career, logistics, and gender as factors that influence their perception and participation in cyber competitions.

Implications of Findings

The findings from the study suggest the following implications:

1. Age and gender do not have a significant effect on the overall perception of experiential learning exercises in cybersecurity (RQ1).
2. Job experience, however, has a significant impact on the overall perception of such exercises. Specifically, those with more job experience have a higher perception of the importance of hands-on CTF exercises (RQ1).
3. The combination of age and job experience, as well as the combination of gender and job experience, do not have a significant impact on the overall perception of CTF exercises (RQ2).

The data analysis of the open-ended responses, however, uncovered unknown perceptions (RQ3) that can hinder students from participating in cybersecurity experiential learning exercises, such as lack of knowledge, time, lack of experience, social anxiety, lack of education, lack of motivation, career concerns, logistics, and gender. These findings of unknown perceptions provide deeper insights into how to improve

the participation and engagement of students in cybersecurity experiential learning exercises and can help inform the development of effective programs and initiatives to increase student involvement in this field.

Conclusion

In summary, this study aimed to examine the perception of cybersecurity students towards Capture the Flag (CTF) learning environments as an effective tool for learning cybersecurity concepts. The results showed that job experience had a significant impact on the perception of CTF exercises. The data analysis of open-ended responses revealed that the factors of "lack of knowledge", "time", "experience", "social anxiety", "education", "motivation", "career concerns", "logistics" and "gender" can influence participation and engagement in cybersecurity experiential learning exercises. These findings provide valuable insights into ways to improve student involvement and can inform the development of effective programs in the field.

References

Aaltola, K., & Taitto, P. (2019). Utilising experiential and organizational learning theories to improve human performance in cyber training. *Information & Security*, *43*, 123–133. https://doi.org/10.11610/isij.4311

Crandall, K. S., Noteboom, C., & El-Gayar, O (2019). High school students' perceptions of cybersecurity: An Explanatory case study. *Issues in Information Systems, 20*(3).

Cyberseek Cybersecurity Supply/Demand Heat Map. (n.d.). Retrieved October 11, 2022 from https://www.cyberseek.org/heatmap.html.

Jewer, J., & Evermann, J. (2015). Enhancing learning outcomes through experiential learning: Using open-source systems to teach enterprise systems and business process management. *Journal of Information Systems Education, 26*(3), 187–201.

Kolb, A. & Kolb, D. (2005). Learning styles and learning spaces: Enhancing experiential learning in higher education. *Academy of Management Learning & Education*, 4(2), 193-212.

Kshetri, N. and Chhetri, M. (2022). Gender asymmetry in cybersecurity: Socioeconomic causes and consequences. *Computer,* 55(2), pp. 72-77. doi: 10.1109/MC.2021.3127992.

Lewis, L. & Williams, S. (1994). Experiential learning: Past and present. *New Directions for Adult and Continuing Education, 62,* 5-16.

NIST- National Institute of Standards and Technology (2018). The cyber range: A guide. NIST Special Publication, US Department of Commerce, Gaithersburg, MD. Retrieved October 11, 2022 from https://www.nist.gov/document/cyber-range-guide.

Qualtrics (n.d). *You can't possibly read all of your customers' survey responses. Text iQ™ can.* Retrieved January 29, 2023 from https://www.qualtrics.com/iq/text-iq/.

Ramezan, C. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. *Journal of Information Systems Education, 34*(1), 94–105.

Reagin, M. J., & Gentry, M. V. (2018). Enterprise cybersecurity. *Frontiers of Health Services Management, 35*(1), 13–22. https://doi.org/10.1097/HAP.0000000000000037.

Rossman, G., & Rallis, S. (2012). *Learning in the field: An introduction to qualitative research (3rd ed.)*. Thousand Oaks, CA: Sage.

Rutherford, A. (2011). *ANOVA and ANCOVA: a GLM approach (2nd ed.)*. Wiley.

Stein, M., Murray B.; Gorman, MD, Jack M. (2001). Unmasking social anxiety disorder. *Journal of Psychiatry & Neuroscience. 3*(26) (3): 185–9. http://www.collectionscanada.gc.ca/eppp-archive/100/201/300/cdn_medical_association/jpn/vol-26/issue-3/pdf/pg185.pdf.

Stines, A (2020). Faculty perceptions of open educational resources in cyber curriculum: A pilot study. *Masters Theses & Doctoral Dissertations*, 345. https://scholar.dsu.edu/theses/345.

Stylianos K., & Magkos E. (2020). Adapting CTF challenges into virtual cybersecurity learning environments. *Information & Computer Security, 29*(1), 105–132. https://doi.org/10.1108/ICS-04-2019-0050.

Tesch, R. (1990). *Qualitative research: Analysis types and software tools.* New York: Falmer.

Thompson, J., Herman, G., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D., and Patsourakos, K. (2018). Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice 1*(5). https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/5.

Topham, L., Kifayat, K., Younis, Y. A., Qi Shi, & Askwith, B. (2016). Cyber security teaching and learning laboratories: A survey. *Information & Security*, *35*(1), 51–80. https://doi.org/10.11610/isij.3503.

US Bureau of Labor Statistics (n.d.). Occupational Outlook Handbook: Information Security Analysts. Retrieved October 11, 2022 from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

US News and World Report (2022). *100 Best Jobs.* Retrieved October 11, 2022 from https://money.usnews.com/careers/best-jobs/rankings/the-100-best-jobs.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal, 4*(2), 32–46.

Appendix A

Instrument

Demographic Questions (Categorical)

1) Age (18-25, 26-35, 36-44, 45 or older)
2) Gender (Male, Female, Non-Binary/3rd Gender, Prefer Not to Say)
3) Class-Standing (Freshmen, Sophomore, Junior, Senior, Graduate Student)
4) Academic Major (nominal)
5) Job Experience (Less than 1 year, 1-5 years, More than 5 years)
6) Experiential Learning Experience (how many Capture the Flag- CTF or cybersecurity competitions have you participated in?) (0-5 scale)

Perception Questions

7) I believe that active learning (or learning by doing) is essential to cybersecurity education.
8) I believe that continuous self-assessment is essential to cybersecurity education.
9) I believe that my lack of knowledge limits my participation in cybersecurity competitions and exercises.
10) I believe that doubt in my own skills and talents (i.e., imposter syndrome) influences my lack of participation in cybersecurity exercises and competitions.
11) I believe that participating in experiential learning exercises such as Capture the Flag (CTF) and cyber competitions (i.e., Collegiate Cyber Defense Competition-CCDC and National Cyber League) is essential to my education.
12) I believe that I can apply what I learn in experiential-based cybersecurity competitions and exercises.

Qualitative Question

13) (Open-Ended)- What would or does prevent you from participating in experiential cybersecurity exercises such as Capture the Flag (CTFs)?