Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #46313

An Experience Report on Using a Cyberlearning Environment for Cybersecurity Courses

Dr. Ingrid Buckley, Florida Gulf Coast University

Dr. Ingrid Buckley is an Associate Professor in the Software Engineering and Computing Department at Florida Gulf Coast University. She earned her Ph.D. in Computer Science from Florida Atlantic University. Dr. Buckley's research interests focus on software engineering education, fault-tolerant software design, software quality, and cybersecurity education. She has received funding from the National Science Foundation and the Cyber Florida Capacity Building Program. Additionally, Dr. Buckley has authored and co-authored several peer-reviewed conference and journal papers, contributing to research in pedagogy.

Bogdan Carbunar, Florida International University

Bogdan Carbunar is an Associate Professor in the Knight Foundation School of Computing and Information Sciences at FIU, and directs the Cyber Security and Privacy Research (CaSPR) Lab, where he develops secure and usable systems. His research interests are at the intersection of security, privacy, and distributed systems, where he derives novel insights through the use of machine learning, applied cryptography, and user studies. He holds a PhD in computer science from Purdue University

Dr. Juan P Sotomayor, Florida International University

Dr. Juan P. Sotomayor received his Ph.D. in Computer Science from Florida International University, where he also completed his Master's degree. His research interests include software testing, model-driven software development, and computer science education. His work explores innovative testing strategies and the utilization of open-source tools to enhance the reliability and efficiency of microservices. He also contributed to the development and maintenance of the Software Engineering and Programming Cyberlearning Environment (SEP-CyLE). He is currently a full-time instructor at Keiser University - Pembroke Pines. He is a member of ACM and IEEE Computer Society.

Dr. Peter J Clarke, Florida International University

Peter J. Clarke received his B.Sc. degree in Computer Science and Mathematics from the University of the West Indies (Cave Hill) in 1987, his M.S. degree from SUNY Binghamton University in 1996, and his Ph.D. in Computer Science from Clemson University in 2003. His research interests are software engineering, software testing, model-driven software development, and computer science education. He is an associate professor in the Knight Foundation School of Computing and Information Sciences at Florida International University. He is a member of the ACM (SIGSOFT, SIGCSE, and SIGAPP), IEEE Computer Society, and the Association for Software Testing (AST).

An Experience Report on Using a Cyberlearning Environment for Cybersecurity Courses

Abstract

The increasing cyber threats to online systems have resulted in the need for a more inclusive approach to educating the broader population on preventative measures to reduce the impact of these threats. It is estimated that the cybercrime cost to the world will be $10.5 trillion annually by 2025. No longer can cybersecurity courses be specialized courses in university curricula, but some of these courses need to become core courses for all students. These courses should not only be tailored for university and college students but also be required to thread the curricula, starting in elementary schools.

This paper describes our experiences conducting a collaborative cybersecurity project to increase access to undergraduate cybersecurity education. The project was funded by the NSF and Cyber Florida. The project was a collaboration between two Florida public universities. One university is a large urban Hispanic-Serving Institution. We describe how the Software Engineering and Programming Cyberlearning Environment (SEP-CyLE), in conjunction with other cybersecurity systems, was used to develop basic cybersecurity materials, labs, and activities for undergraduate students and instructors. SEP-CyLE motivates students to learn in an interactive environment where they can provide feedback to their peers while employing three learning and engagement strategies (LESs). These LESs include collaborative learning, gamification, and social interaction.

We present the objectives of the project, describe how the objectives were met, briefly describe SEP-CyLE, and provide data showing students' interactions with SEP-CyLE. The data retrieved from SEP-CyLE provides insight into how the learning environment was used, students' performance on the learning objects, and the impact of the LESs on students' overall performance in an introductory cybersecurity course.

Keywords: Cybersecurity Education, Cyberlearning Environment, Learning and Engagement Strategies, Learning Objects.

1 Introduction

The ubiquitous nature of information and communication technology (ICT) in the 21st century has resulted in an upsurge in cyberattacks. This upsurge is expected to increase in frequency and severity every year. Cybersecurity attacks are a growing problem for private sector businesses and government agencies that rely on or use software and computer technology to perform their core responsibilities. However, most software and computer technologies are vulnerable to a variety of cyberattacks if they are misused, misconfigured, or accessed by unauthorized entities. Various users utilize these software and computer technologies daily to perform their work but are not well-trained or educated to avoid inevitable common cyberattacks. Cybersecurity Ventures [1] estimated that the worldwide cybercrime costs will hit about $10.5 trillion yearly by 2025. Cybint [2] reported that about 95% of all data breaches occurred because of human error. Human error

includes clicking on dangerous links or falling prey to phishing scams, using weak passwords, data mishandling, failure to update software, and misconfiguration. IBM [3] reported that the global average data breach cost is about $4.88 million in 2024, which is a 10% increase compared to 2023. Because the human factor in driving and supporting cybercrimes is exceptionally high due to human ignorance or negligence, these weaknesses and deficiencies can be addressed through education, training, and awareness.

The reality is that businesses and government systems are constantly under attack by malicious entities globally, and the consequences and cost of addressing these breaches are expensive. To tackle this pervasive problem, the goal is to reduce cybersecurity breaches by educating the workforce on how to avoid aiding or participating in cybersecurity attacks. We present a collaborative educational initiative to educate undergraduate software engineering students in a software engineering degree program. The collaboration is between two Florida Universities with grant support from the Cyber Florida [4] and the National Science Foundation [5]. They provide cybersecurity education and training to undergraduate students and support faculty members using the Software Engineering and Programming Cyberlearning Environment (SEP-CyLE) [6, 7, 8], an instance of STEM-CyLE[a], to teach cybersecurity concepts.

The main goals of the Cyber Florida project are to create new cybersecurity learning materials and develop faculty expertise to significantly increase the number of students who are exposed to cybersecurity attacks and defensive techniques and tools to protect ICT. The project's first objective is to create new cybersecurity digital learning objects, referred to simply as learning objects (LOs), and tool tutorials to be hosted in SEP-CyLE that improve the students (i) conceptual understanding of cybersecurity concepts and (ii) practical skills in applying cybersecurity techniques to real applications. The second objective is to conduct a workshop for Florida college faculty to develop faculty expertise in cybersecurity and form a learning community that can contribute learning materials to a cyberlearning platform to support pedagogy.

We conducted a cybersecurity study in the spring of 2019 and 2020 with 76 software engineering undergraduate students. The students learned various cybersecurity topics and tools using SEP-CyLE. We evaluated the students' proficiency based on the total time they spent engaging with the material, their performance on assessments, the virtual points they earned as a team, their feedback, their perception of SEP-CyLE, and the quality of the material and instruction. Overall, the results show that in both years, students spent the most time learning the LO content; however, on average, the students spent twice the amount of time on the LO recorded assessment when compared to the LO practice assessment. The overall combined average assessment scores for both groups is approximately 85.18%. There was a slight decrease in average performance from 2019 to 2020, but the distribution of scores was broader in 2020. Similarly, for each year, only 30% of the teams employed a strategy to earn the maximum virtual points to earn first, second, and third place status in the course. Overall, students shared that they found cybersecurity material helpful but experienced technical challenges when using SEP-CyLE.

The remainder of the paper is structured as follows. Section 2 provides related work about various cybersecurity educational approaches and initiatives. Section 3 presents an introduction to the SEP-CyLE learning content and Learning and Engagement Strategies (LESs) used in the environment.

[a]https://stem-cyle.cis.fiu.edu/

Section 4 summarizes the cybersecurity workshop held for faculty members. Section 5 describes the study conducted with students and the results obtained. Section 6 concludes the paper.

2 Related Work

Software and technology are used in every domain, including education, health care, financial systems, government agencies, and education systems. Humans cannot avoid using software or technology in their daily lives. With human error playing a key part in 95% of cybersecurity breaches, most cybercrimes exploit weaknesses and ignorance limitations in software, technology, and humans. As a result, cybersecurity principles and concepts span a wide cross-section of domains, sectors, and devices. Cybersecurity topics and training include education around phishing attacks, removable media, passwords and authentication, physical security, mobile device security, viruses, malware, data security, cryptography, network security, Cloud Security, Social Media Use, Privacy, and Internet and Email Use, Social Engineering, among other specialized topics [9]. Below, we present some cybersecurity training studies on different cybersecurity topics or delivery format and their impact.

Buckley et al.[10] used buggy code that was transformed into flowchart format to teach undergraduate students how bad programming habits or confusing code can lead to vulnerabilities and defects that are exploitable. A total of sixty-five (65) students completed this project - twenty-nine (29) juniors and thirty-six (36) seniors. All students completed a pretest and posttest, evaluating code and identifying bugs. In the end, the seniors and juniors obtained the same posttest score, roughly 72%, even though the juniors had lower pretest scores at the beginning of the project. This project showed that students are more focused on quickly writing code or reusing code that will compile and do what they want. However, most students were not careful in inspecting the code for logic errors, ensuring it is bug-free, and following best practices to reduce vulnerabilities and bugs that can be exploited and lead to unnecessary cybersecurity breaches in the future.

Prümmer et al. [11] conducted an extensive study by reviewing 142 articles on cybersecurity training initiatives to educate a wide cross-section of participants. The cybersecurity training topics ranged from general cybersecurity education to more specific topics such as phishing, insider threat, WIFI safety, malware protection, and password safety. The studies include various training methods, delivery methods, platforms, approaches, and creative techniques such as extreme gaming. Overall, the cybersecurity training yielded positive results. However, the authors found that many aspects of the cybersecurity training and design process were unclear and ad-hoc, and restructuring was required to increase the effect. The authors noted that the outcome measures for the effectiveness of cybersecurity training in the studies did not consider cybersecurity behavior and only focused on other factors, such as attitudes and intentions, which impacted the effectiveness of cybersecurity training. As a result, a participant might have a positive attitude and the right intention towards cybersecurity but not always follow through with secure behavior to mitigate and avoid a cybersecurity threat or potential attack.

Loffler et al. [12] reported positive feedback, especially when employing game-based or simulation-based cybersecurity training techniques. They used a virtual prototype to simulate an escape room game addressing various cybersecurity challenges. In the escape room game setup, participants form a team to solve puzzles with the help of clues and strategies to escape from a confined area within a predefined timespan. Escape room challenges involve activities that require teamwork,

critical thinking, and problem-solving.

Abawajy [13] provided phishing cybersecurity training using video-based, text-based, and gaming-based formats. He found that participants rated video-based training as their favorite, followed by text-based training. While only 5% of participants selected game-based training as their favorite, overall, 60% of participants stated that they enjoyed the experience of undergoing game-based training in Cybersecurity even though it was not their first preference. The participants in this training were a general group; this could mean that most participants were mature learners, as opposed to younger learners who typically enjoy and are more enthusiastic about gaming.

Most cybersecurity breaches occur because victims fail to take basic but well-known steps in response to cybersecurity attacks and threats, and this causes a significant knowing-doing gap [14]. Workman et al. [14] conducted a study with 320 undergraduate computer science students at one university to address the knowing-doing gap. They used various modes of instruction, including class instruction, labs, gamified simulations, live activities such as hackathons and capture the flag competitions, and a combination of live activities and gamified simulations to teach Cybersecurity. The students were exposed to a misconfigured firewall that allowed too many access rights and permissions, as well as a server-side request forgery (SSRF) attack, and using tools to identify vulnerabilities attacks and take the appropriate corrective actions. Their study showed that Cybersecurity gamified simulations increased practical performance over classroom and lab instruction. Additionally, when live activities, such as capture-the-flag and hackathons, were added to classroom and lab instructions, it added a small benefit to the learning outcome. However, when live activities were combined with gamified simulations, that combination yielded the most significant gains in the student's applied learning performance.

3 Software Engineering and Programming Cyberlearning Environment (SEP-CyLE)

In this section, we describe the cyberlearning environment (SEP-CyLE) [6, 7, 8] used to collect the data for the study presented in the paper. The description includes the structure of SEP-CyLE, how active learning approaches (Learning and Engagement Strategies) are embedded, and the data collected.

3.1 Structure

SEP-CyLE is a platform developed to provide vetted learning content to students and faculty through learning objects (LOs)[15] and tutorials. The learning content is provided to students using three learning and engagement strategies (LESs), *collaborative learning*, *gamification*, and *social interaction*. The structure of SEP-CyLE contains many of the components that are in other learning management systems (LMSs), such as Canvas [16]. These components include user management, course management, discussion boards/forums, a learning content creator, and data analytics. What makes SEP-CyLE different from other LMSs is that it embeds the LESs previously mentioned into many of the components students use in their classes. Additional details of the LESs will be provided in the next subsection. SEP-CyLE does not provide a grade book and currently cannot be connected to other third-party learning applications. Additional details on the structure of SEP-CyLE may be found in [7, 8].

3.2 Learning Content

Smith [15] defines an LO as *any grouping of materials that is structured in a meaningful way and is tied to an educational objective*. Each LO in SEP-CyLE consists of a learning objective,

content on a specific topic, practice assessment, recorded assessment, and a list of references. The materials or learning content in an LO may consist of different media, including text, pictures, movies, and animations. SEP-CyLE currently has 40 LOs in areas such as the introduction to programming (CS1), cybersecurity (CSY), software engineering (SWE), software testing (SWT), and programming IDEs (IDE). The development of each LO is guided by the learning objective, which has the *ABCD* structure [17], where *Audience* - the targeted learner, *Behavior* - what the learner is expected to do, *Condition* - setting or circumstance under which the behavior occurs, and *Degree* - the acceptable standard of performance of the behavior.

The learning objectives for four of the cybersecurity LOs in SEP-CyLE used in the study presented in Section 5 are shown below.

> *Introduction to Security* : CSY-001 - Given no prior knowledge of security concepts, undergraduates will be able to identify core security concepts with 80% accuracy.
>
> *Introduction to Cybersecurity* : CSY-002 - Given no prior knowledge of cybersecurity concepts, undergraduates will be able to identify core security concepts with 80% accuracy.
>
> *Introduction to Cryptography* : CSY-BC-001 - Given no prior knowledge of cryptography, undergraduates will be able to describe symmetric key cryptography, including the basic concepts of stream and block ciphers, with 80% accuracy.
>
> *Introduction to Zenmap* : CSY-STH-002 - Given knowledge from the Introduction to Nmap Learning Object, undergraduates will be able to identify and use the Zenmap tool to complete a full scan on scanme.nmap.org with complete accuracy.

3.3 Learning and Engagement Strategies

The learning and engagement strategies (LESs) in SEP-CyLE include collaborative learning, gamification, and social interaction [18]. *Collaborative learning* is where two or more people work in groups mutually searching for understanding, solutions, meanings, or creating a product [19]. *Gamification* uses game design elements and game mechanics to improve user experience and engagement with a system, which may be applied to an educational context [20]. *Social interaction* is an approach that enhances knowledge acquisition through social activities, such as students establishing meaningful dialogue within student groups and with teachers [21, 22]. Unlike the collaborative learning defined by Smith et al., [19], a lightweight version of collaborative learning is implemented in SEP-CyLE, where team members encourage each other to complete LOs to gain extra virtual points, as described in the next subsection.

3.4 Data Collected

Data is collected based on the activities performed by the students registered for the class in SEP-CyLE. The data that is most important to the students are the virtual points computed based on the allocation of the points by the instructor and the student's completion of tasks. In the course management section on SEP-CyLE, the instructor can set the number of virtual points allocated for each activity. The categories used for virtual points allocations are as follows:

- *Assessment Completion* - student completes the LO assessment with the minimal required percentage set by the instructor.
- *Team Completion* - all team members complete the LO assessment with the minimal required percentage as set by the instructor.

- *First Team Completion* - first team where all team members completed the LO assessment with the minimal required percentage as set by the instructor.
- *Second Team Completion* - second team where all team members completed the LO assessment with the minimal required percentage as set by the instructor.
- *Third Team Completion* - third team where all team members completed the LO assessment with the minimal required percentage as set by the instructor.
- *Course Thread Post* - posting a thread to the class forum. These points are allocated for the first post only.
- *Profile Picture Upload* - uploading a picture to the student's profile.

SEP-CyLE also collects data for each student on the time spent completing various activities assigned by the class instructor. The time is recorded for the LO content, LO practice assessment, and LO recorded assessment. The instructor can generate a report comprising the student's name, email address, assignment (LO) name, recorded assessment score, time spent on the LO, and recorded total virtual points. It is worth noting that the SEP-CyLE database may be queried for additional information on students' detailed activities. These details may include which team placed first on each LO or if all team members completed the LO assignment.

4 CyberSecurity Workshop

We hosted a workshop for instructors in Florida titled the *First Workshop on Critical Cybersecurity Education (WCCE-2018)* [23]. Twenty-nine (29) faculty and students attended the workshop from ten (10) academic institutions, including one (1) institution from outside of Florida. The funding was appropriated to help instructors at Florida colleges teach cybersecurity in their courses. The objectives of the workshop were to:

- Identify the cybersecurity concepts, skills, and toolsets that are considered to be critical for a large cross-section of students;
- Develop learning content for the critical cybersecurity knowledge identified;
- Form a learning community that can contribute additional learning materials to a cyberlearning environment (SEP-CyLE) to support pedagogy.

4.1 Sessions

The workshop consisted of ten (10) sessions over 2 days [23]. These sessions included a keynote talk by *Mr. Benjamin Scribner* Director of Outreach, Cybersecurity Education and Awareness Branch Office of Cybersecurity and Communications, Department of Homeland Security DHS Representative. The workshop started with a session identifying the critical cybersecurity areas for which learning objects (LOs) should be created. The subsequent workshop sessions focused on how to develop cybersecurity learning objects and develop learning objects for the cybersecurity areas identified. Attendees were then introduced to using SEP-CyLE in a learning environment. During the workshop, participants were allowed to present any novel ideas or projects they were doing at their universities in cybersecurity education.

4.2 Evaluation Summary

The participants evaluated each session at the end of each workshop day. Each session was evaluated using a 5-point Likert scale, where 1- Very Dissatisfied, 2- Dissatisfied, 3-Neutral, 4 - Satisfied, 5 - Very Satisfied, and 0 - No Response. Additionally, each session was evaluated based on the following criteria:

Table 1: Average evaluation score for workshop presenters.

Day	Session	Title of Session	Avg. Score
1	1	Keynote Speaker	4.37
	2	Identification of Critical Cybersecurity Areas Organization of Work Team	4.10
	3	Introduction to Learning Objects	4.44
	4	Development of Cybersecurity LOs	4.55
	5	Introduction to Cyberlearning Environment	4.76
		Daily Average	**4.44**
2	1	Upload LOs into SEP-CyLE	4.84
	2	Cybersecurity Project Presentations by Participants (Novel Ideas)	4.89
	3	Cyberlearning Environment in-Class Assignment	4.73
	4	Review Session	4.81
		Daily Average	**4.82**

1. Presenter's knowledge of the subject.
2. Presentation of material.
3. Ability to explain the subject matter.
4. Clarity regarding integrating testing into programming development.
5. Provided adequate time for questions.
6. Satisfactory responses to questions.
7. Overall satisfaction with the presenter.

Table 1 shows the average evaluation score for the 7 criteria listed above for each session, on Day 1 and Day 2 of the workshop, and the total average per day. The total average evaluation scores for all sessions on Day 1 and Day 2 are 4.44 and 4.82, respectively. The total average evaluation score for all sessions on Day 1 and Day 2 combined is 4.32.

On Day 2, the last day of the workshop, all participants were asked to evaluate the organization of the workshop. The overall workshop evaluation was rated based on the categories: (1) Workshop Content, (2) Workshop Design, (3) Facilities/Arrangements and (4) General. Each of the four areas was evaluated using a 5-point Likert scale, where 1- very Dissatisfied, 2- Dissatisfied, 3-Neutral, 4 - Satisfied, 5 - Very Satisfied, and 0 - No Response.

The average overall workshop scores were as follows.

- *Workshop content* - focuses on communication of the workshop objectives and expectations relevant to classes taught and will improve the classes taught. Average score 4.57.
- *Workshop Design* - clarity of workshop objectives, activities stimulated learning, time allocation, and the variety of topics covered. Average score 4.71.
- *Workshop Facilities* - local arrangements, refreshments served, meeting rooms, and transportation to/from the venue. Average score 4.36.

5 Student Study

This section presents the details of the undergraduate cybersecurity study conducted in 2019 and 2020. The details of the study include the method - learning content, classes, and the use of SEP-

CyLE; results obtained during the study; and a discussion of the results, including the limitations of the study. The research questions we investigated during the study are as follows:

RQ1 How engaged were students using the SEP-CyLE in the classroom?
RQ2 How did students perform on the LOs in SEP-CyLE?
RQ3 Did teams use a strategy to maximize points in SEP-CyLE?
RQ4 What were students' perceptions of the LOs in SEP-CyLE?

5.1 Method

Courses Offered: An introductory cybersecurity course called Introduction to Cybersecurity (CIS4930) was developed to teach undergraduates the fundamentals of cybersecurity principles and concepts, as well as cybersecurity tools. The course was offered in Spring 2019 and Spring 2020. The cybersecurity LOs were integrated into the coursework and contributed to students' overall grades. The student learning outcomes for the course are as follows. The students should be able to:

- Describe the fundamental cybersecurity principles, protocols, and standards;
- Identify some of the common problems and solutions in the cybersecurity domain;
- Use cybersecurity tools and operations to implement cybersecurity principles and protocols;
- Analyze cybersecurity breaches and provide appropriate solutions;
- Describe cybersecurity hygiene, ethics, auditing, and management of software systems.

The textbook by Kim et al. [9] and companion hands-on lab environment [24] were used to teach the course in Spring 2019 and Spring 2020.

The first time the course was offered in Spring 2019, students completed 3 exams. However, the instructor changed the number of exams in Spring 2020, where students completed three quizzes and two exams. Table 2 shows a breakdown of grades in Spring 2019 and Spring 2020 in the cybersecurity course.

COVID-19 Impact. During the Spring 2020 semester, the course modality changed from in-person to online delivery because of the COVID-19 pandemic. As a result of this disruption, we transitioned from in-person to online teaching; thus, students were not able to complete the same amount of coursework when compared to Spring 2019 due to technology issues, working in a virtual space instead of in person, stress, illnesses, and other factors. In Spring 2020, students completed four learning objects, which is 50% less when compared to Spring 2019. Additionally, students did 10 assignments, which is 37.5% fewer assignments when compared to the number of assignments completed in Spring 2019.

Assignments in SEP-CyLE. Students worked in teams on SEP-CyLE during the course and were awarded virtual points individually and as part of their team. The allocations of the virtual points are as follows:

- 10 virtual points if they correctly completed all the recorded assessment questions on an LO with a score of 70% or higher.
- 1 virtual point if every member of the team completed the LO with a score of 70% or higher
- 2 virtual points for the first team to complete the LO with all members scoring 70% or higher
- 1 virtual point for the second team to complete the LO with all members scoring 70% or higher
- 1 virtual point if a student posts a comment

Table 2: Grade breakdown in Spring 2019 and Spring 2020.

Course Data & Deliverables	Spring 2019 (% weight)	Spring 2020 (% weight)
Number of students	45	31
Number of teams	11	10
LOs Assigned	8 (8.28%)	4 (6.74%)
Number of Assignments	16 (6.72%)	10 (2.53%)
Number of Handson Cybersecurity Labs	5 (25%)	4 (6.74%)
Quizzes	0 (0%)	3 (20%)
Exams	3 (60%)	2 (64%)
Total	(100%)	(100%)

- 1 virtual point if a student uploads their photo on their profile

5.2 Results

Table 3 presents the study data collected in 2019 and 2020, which includes the number of student comments, total student activity entries on SEP-CyLE, overall course grades, team placements - first, second, and third place, as well as the total, average, maximum, and standard deviation for virtual points earned, time spent on learning objects (LOs).

In 2019 and 2020, students spent 512,284 and 82,682 seconds, respectively, on learning objects. The average time students spent to complete all the assigned learning objects in 2019 and 2020 was 1,526 and 667 seconds, respectively. The standard deviation of the time spent on learning objects is 2,211 and 1,131 seconds. The maximum time students spent to complete the learning objects in 2019 and 2020 was 25,473 and 7,327 seconds, respectively.

The average, maximum, and standard deviation for recorded assessment scores in 2019 were 86.63, 100, and 21.94, respectively. The average, maximum, and standard deviation for virtual points in 2020 were 82.96, 100, and 29.14, respectively.

The total number of student comments posted on SEP-CyLE in 2019 was 35, while no comments were posted in 2020. The total number of student activities on SEP-CyLE in 2019 and 2020 was 743 and 256, respectively. The overall course grade in 2019 and 2020 is 88.33% and 79.71%. The average scores on learning objects on SEP-CyLE in 2019 and 2020 are 87% and 83%, respectively.

In 2019, there were 11 teams in the Introduction to Cybersecurity course. Teams 1, 6, and 7 consistently earned virtual points for teamwork. Team 1 earned first place on three LO assignments - Introduction to Cybersecurity, Introduction to Security, Introduction to Passwords, and PGP: Pretty Good Privacy learning objects. Team 6 and 7 earned second place on two LO assignments - Introduction to Cybersecurity and Introduction to Security learning objectives, while team 5 earned third place on these LOs.

In 2020, there were 10 teams in the cybersecurity course. Similarly, three teams - teams 5, 7, and 8, consistently earned virtual points for teamwork. Team 7 earned first place in Introduction to Cybersecurity and Introduction to Cryptography learning objects. Team 5 earned first place on the Introduction to Zenmap tutorial. Team 8 earned first place on the Introduction to Passwords

Table 3: Team performance in Spring 2019 and Spring 2020.

Teams Data	Spring 2019	Spring 2020
Number of 1st Place Teams	4	4
Number of 2nd Place Teams	2	2
Number of 3rd Place Teams	2	1
Total Virtual Points	7,126	2,380
Total Student Comments Posted	35	0
Average Virtual Points on LOs	158.36	76.77
Maximum Virtual Points on LOs	249	125
Std. Deviation Virtual Points on LOs	64.86	45
Average Time Spent (seconds) on LOs	1,526	667
Std. Deviation Time Spent (seconds) on LOs	2,211	1,131
Maximum Time Spent (seconds) on LOs	25,473	7,327
Total Time Spent (seconds) on LOs	512,284	82,682
Total Student Activity Entries	743	256
Average Assessment Scores on LOs	86.63%	82.96%
Maximum Assessment Scores on LOs	100%	100%
Std. Deviation of Assessment Scores on LOs	21.94	29.14
Overall Course Grade	88.33%	79.71%

learning object, while Team 7 earned third.

In 2019, students posted various comments on SEP-CyLE to earn points and rate their experience using SEP-CyLE. We include three positive and three negative comments posted by students on SEP-CyLE. Their feedback is listed below:

Positive Student Comment 1: Some students felt that the LO assignments were useful for learning the material in class, as described in the following comment.

"This assignment was straightforward and fairly easy to complete. I did learn some useful information from it, particularly in regard to PGP. I was completely unfamiliar with it; being able to easily encrypt and decrypt e-mails seems very useful."

Positive Student Comment 2: Some students stated that it helped them when topics were repeated, as this reinforced previous topics covered in the class, as described in the following comment.

"This assignment had the same requirements as a previous one for Introduction to Cybersecurity. It was not particularly difficult and was a helpful review for several important concepts discussed in class."

Positive Student Comment 3: As described in the following comments, some students appreciated that relatable examples were used to explain key concepts covered in the class.

"Some of the content was general knowledge, but there were some excellent points for review from

our Software Security class. It was also good that the LO content provided examples related to the key concepts."

Negative Student Comment 1: Some students had issues submitting their recorded assessments on SEP-CyLE and indicated that some correct answers were marked as incorrect, as described in the following comment.

" I learned a lot throughout the LO's; the only problems I came across were that sometimes I would have a problem submitting the LO and that some of the answers were marked as incorrect when the correct answer had been provided."

Negative Student Comment 2: Some students complained that some recorded assessments contradicted information given in LOs and included questions that were not taught, as described in the following comment.

"The content given was fine overall, but the quizzes sometimes contradicted it or had things simply not covered."

Negative Student Comment 3: Some students complained that LO content was not being displayed correctly in the SEP-CyLE environment, as described in the following comment.

" Good information that was easy to absorb. There are significant issues with how SEP-CyLE is delivering content."

5.3 Discussion

We present a discussion of the results obtained in 2019 and 2020 to answer the research questions in our study below.

RQ1. How engaged were students using the SEP-CyLE in the classroom? The data in Table 3 shows the amount of time students spent on different sections of an LO on SEP-CyLE. Each learning object (LO) is comprised of three units: information about a given topic (LO content), a practice assessment, and a recorded assessment. In 2019, the average time students spent on content, practice assessment, and recorded assessment was 1,026.34 seconds, 123.58 seconds, and 375.93 seconds, respectively; this indicates that students spent 1.9 more time (185.5% more time) working on the recorded assessment than on the practice assessment. In 2020, the average time students spent on content, practice assessment, and recorded assessment was 361.02 seconds, 79.3 seconds, and 226.47 seconds, respectively; this indicates that students spent more than two times the time (204.9% more time) working on the recorded assessment compared to the practice assessment.

The overall results show that in both years, students spent the most time learning the content, but they spent more time on the recorded assessment and less time on the practice assessment. In general, students spend more time on the recorded assessment than the practice assessment because the recorded assessment decides their final grade for the LO. Moreover, the students got three attempts to retake the recorded assessment in 2019 and two attempts to retake the recorded assessment in 2020; their final grade is the average of all attempts, hence why most of their efforts went into learning the content and working on the recorded assessment.

RQ2. How did students perform on the LOs in SEP-CyLE?. Overall, the students completed 50% more learning objects in 2019 when compared to 2020. Students in spring 2019 overall course

grade was 9.76% higher than students overall course grade in 2020; this shows a notable difference in performance between the two groups. Student grades were higher in 2020 because they did not experience any significant displacement during the course. As a result, students in 2019 spent much more time on learning objects on average, with more variation in the time spent because there were more students in the course, and all learning objects were completed.

The overall recorded assessment scores indicate a slight decrease in average performance from 2019 to 2020, but more importantly, it highlights that the distribution of scores was broader in 2020, indicating more varied performances among students. The disparity in student performance and activity on SEP-CyLE was due to two factors in 2020: (1) fewer students enrolled in the course, and (2) they did not complete all the assigned learning objectives because of the disruption and stress caused by COVID-19. In 2019, students performed better on LOs and course material, as shown in 3. The results highlighted in course grades and LO scores show that the COVID-19 pandemic significantly impacted students, which reduced their average performance in 2020.

RQ3. Did teams use a strategy to maximize points in SEP-CyLE? In 2019, the data for team performance shows that Team 1 was the first-place team overall; they formulated a strategy to earn as many virtual points as possible in the course. The data shows that the top 3 teams assimilated and understood the cybersecurity principles taught in Introduction to Cybersecurity and Introduction to Security compared to other LOs completed. In 2020, there were 10 teams in the cybersecurity course. Similarly, in 2020, Team 7 came first overall; they displayed good team synergy and devised a strategy to consistently earn points as a team, as the data shows that they earned first and second place on multiple LOs. Overall, the 3 top teams performed well on the Introduction to Zenmap tutorial and Introduction to Passwords, indicating that students understood the principles taught in those learning objects compared to other LOs they completed.

In 2019 and 2020, the maximum overall time spent on LOs shows that there were instances of students (teams) spending a significant amount of time working on learning objects, indicating that they worked hard to obtain high scores and more virtual points. The data shows that the high-performing teams performed well on the Introduction to Passwords learning object in 2019 and 2020, respectively.

RQ4. What were students' perceptions of the LOs in SEP-CyLE? The positive and negative student comments shared gave helpful feedback to address student needs. Many students shared that they benefited from the information and examples taught in the learning objects and tutorials. They expressed that the LOs provided a good review of the topics covered in the lectures. Other students said they had issues with incorrect recorded assessment answers and experienced technical difficulties using the SEP-CyLE environment. In 2020, students did not post comments or complete reviews about the four learning objects they completed on SEP-CyLE. We assume that the COVID-19 pandemic provoked this, the disruption in modality, and the overall stress students experienced, so they did not take the extra time to post comments or leave a review to earn additional points.

To address the negative student comments, we took several corrective actions. We created a user manual to show students step-by-step how to navigate SEP-CyLE. We conducted comprehensive reviews of the LOs and quizzes. We corrected the LOs and quizzes that had incorrect answers. The corrected LOs and quizzes were later imported into Canvas LMS [16] at Florida Gulf Coast

University, and students in successive years completed them as homework material. However, they were not part of a study when administered on Canvas LMS; the LOs and quizzes were still valuable in courses that introduced cybersecurity principles. Additionally, should we obtain funding in the future, we plan to enhance the material in the LOs to include different learning styles, for example, (1) auditory - some students prefer to listen, (2) Visual - using diagrams and videos appeal to some students, and (3) Verbal - some students prefer to read. These changes would create a learning environment that is more inclusive and appeals to a wider variety of student learning styles.

6 Conclusion

In this paper, we present an overview of a cybersecurity educational project using the Software Engineering and Programming Cyberlearning Environment (SEP-CyLE) to teach cybersecurity to software engineering undergraduate students. The cybersecurity educational project was supported by a grant from the Florida Center for Cybersecurity, and SEP-CyLE was created as part of an NSF project. In this project, we hosted a cybersecurity workshop to provide professional development to Florida college instructors by introducing them to SEP-CyLE, educating them about cybersecurity, and how they could easily integrate cybersecurity learning objects (LOs) in their courses. The workshop attendees gave positive feedback and ratings of 4.32/5 for presenters, SEP-CyLE, and topics covered at the workshop. In sum, the project's goals and objectives were met based on the outcome of the study, workshop, and development of cybersecurity LOs.

In 2019 and 2020, we conducted a study using SEP-CyLE and cybersecurity LOs to help 76 undergraduates learn cybersecurity principles. The students completed various learning objects covering multiple cybersecurity topics and tools using SEP-CyLE. Overall, the study's results highlight that students assimilated what they learned on SEP-CyLE; their combined average for both groups on the SEP-CyLE LO assignments was approximately 85.18%. Students in both groups performed well on the LO recorded assessments and earned virtual points as a team despite the disruption of the COVID-19 pandemic. In our future work, we plan to conduct a longitudinal study using the LOs on SEP-CyLE over several semesters and perform a corresponding comparative analysis of student performance in cybersecurity education.

Acknowledgment

The authors would like to thank the reviewers for their thoughtful and helpful comments. Partial support for this work was provided by Cyber Florida, the National Science Foundation's (NSF) Improving Undergraduate STEM Education (IUSE) program under Award Numbers DUE-1562773 (Florida Gulf Coast University), DUE-1525112, DGE-2114911, and CNS-2246004 (Florida International University). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Cyber Florida or the NSF.

References

[1] Steve Morgan. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Nov. 2020. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ [Online] (Accessed Dec. 2024).

[2] Cayley Wetzig. 5 Alarming Cybersecurity Facts and Statistics, Nov. 2022. https://thrivedx.com/resources/article/cyber-security-facts-statistics?referrer=cybint [Online] (Accessed Dec. 2024).

[3] IBM. Cost of a Data Breach Report 2024, Jul. 2022. https://www.ibm.com/reports/data-breach [Online] (Accessed Dec. 2024).

[4] Cyber Florida. Cyber Florida at the University of South Florida, Dec. 2024. https://cyberflorida.org/ [Online] (Accessed Dec. 2024).

[5] NSF. National Science Foundation, Dec. 2024. https://www.nsf.gov/ [Online] (Accessed Dec. 2024).

[6] Raymond Chang-lau and Peter J. Clarke. Software engineering and programming cyberlearning environment (SEP-CyLE), July 2018. https://stem-cyle.cis.fiu.edu/instances.

[7] Ingrid A. Buckley and Peter J. Clarke. An approach to teaching software testing supported by two different online content delivery methods. In *Proceedings of the 16th LACCEI International Multi-Conference for Engineering, Education, and Technology*, 2018.

[8] Leila Zahedi, Jasmine Batten, Monique Ross, Geoff Potvin, Stephanie Damas, Peter Clarke, and Debra Davis. Gamification in education: A mixed-methods study of gender on computer science students' academic performance and identity development. *Journal of Computing in Higher Education*, 33:441–474, 2021.

[9] David Kim and Michael G Solomon. *Fundamentals of Information Systems Security*. Jones & Bartlett Learning, 3rd edition, 2016.

[10] Ingrid A. Buckley, Janusz Zalewski, and Peter J. Clarke. Introducing a cybersecurity mindset into software engineering undergraduate courses. *International Journal of Advanced Computer Science and Applications*, 9(6), 2018.

[11] Julia Prümmer, Tommy van Steen, and Bibi van den Berg. A systematic review of current cybersecurity training methods. *Computers & Security*, 136:103585, 2024.

[12] Emanuel Löffler, Bettina Schneider, Trupti Zanwar, and Petra Maria Asprion. Cysecescape 2.0-a virtual escape room to raise cybersecurity awareness. *International Journal of Serious Games*, 8(1):59–70, Mar. 2021.

[13] Jemal Abawajy. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237–248, 2014.

[14] Michael D. Workman, J. Anthony Luévanos, and Bin Mai. A study of cybersecurity education using a present-test-practice-assess model. *IEEE Transactions on Education*, 65(1):40–45, 2022.

[15] Rachel S. Smith. Guidelines for authors of learning objects. The New Media Consortium, 2004.

[16] Inc Instructure. Canvas. Online, March 2025. https://www.instructure.com/canvas/about [Online] (Accessed Mar. 2025).

[17] Aytac Gogus. *Learning Objectives*, pages 1950–1954. Springer US, Boston, MA, 2012.

[18] Peter J. Clarke, Debra L. Davis, Ingrid A. Buckley, Geoff Potvin, Mandayam Thirunarayanan, and Edward L. Jones. Combining learning and engagement strategies in a software testing learning environment. *ACM Trans. Comput. Educ.*, 22(2), November 2021.

[19] Barbara Leigh Smith and Jean T. MacGregor. What is Collaborative Learning? In A.S. Goodsell, M.R. Maher, and V. Tinto, editors, *Collaborative Learning: A Sourcebook for Higher Education.* National Center on Postsecondary Teaching, Learning, and Assessment, University Park, Pa., 1992.

[20] Sebastian Deterding, Dan Dixon, Rilla Khaled, and Lennart Nacke. From game design elements to gamefulness: Defining "gamification". In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, MindTrek '11, page 9–15, New York, NY, USA, 2011. Association for Computing Machinery.

[21] Beth Hurst, Randall Wallace, and Sarah B. Nixon. The impact of social interaction on student learning. *Reading Horizons*, 52(4):375–398, 2013. `https://scholarworks.wmich.edu/reading_horizons/vol52/iss4/5` (Accessed August 2018).

[22] Kamaruzaman Jusoff and Siti Akmar Abu Samah. *Social Interaction Learning Styles*, pages 3101–3104. Springer US, Boston, MA, 2012.

[23] Ingrid A. Buckley, Bogdan Carbunar, and Peter J. Clarke. First Workshop on Critical Cybersecurity Education (WCCE-2018), February 2018. https://stem-cyle.cis.fiu.edu/events/wcce-2018/ (Accessed April 2025).

[24] David Kim and Michael G Solomon. Cloud lab access for fundamentals of information systems security, 2018.