Enhancing Cognition through Cooperative Learning and Augmented Mentorship

Michael-Brian Ogawa[1], Rita M. Vick[2], Barbara Endicott-Popovsky[1], Ran J. Hinrichs[3], Alejandro D. Ayala[4], Sean Mosier[1], and Martha E. Crosby[1]

[1] University of Hawai'i at Mānoa, Honolulu, HI 96822, USA
{ogawam,bendicot,smosier,crosby}@hawaii.edu

RMVick Consulting[2] USA
pandrvick@gmail.com

[3] Norwich University, Northfield, VT 05663, USA
rhinrich@norwich.edu

[4] University of Washington, USA
aayala@uw.edu

Abstract: With increasing cybercrime, educational institutions are working to create increased opportunities for people to enter the cyber workforce. Some programs are expanding their entry criteria to include those from a wider variety of backgrounds. This two-part study uses augmented cognition approaches to identify how individual differences can influence instructional design for security education. Higher levels of variance and time on task typically led to lower performance. In addition, the design of content (internal and external content) influenced performance and time on task, where external supplemental content led to increased effort and lower outcomes.

Keywords: Security education, augmented cognition, instructional design

1 Introduction

Between 2018 and 2022, the Federal Bureau of Investigation (FBI) reported that cyber-crime increased 380% over the five-year period. They received 3.26 million complaints about cyber-crime, which resulted in a reported loss of $27.6 billion [4]. Of which, $10.3 billion in losses were reported in 2022 alone. These statistics highlight the growing trend in cyber-crime and illustrate that it is continuously growing. Therefore, there is a high need for security professional in the workforce to protect assets of organizations and individuals. There is an approximate need for 1.7 million cyber security professionals in the United States [3]. However, approximately one-third of these positions remain unfilled and is expected to continuously grow based on the rapid growth in cyber-crime [2]. Educational institutions developed cyber security education

programs to account for this need starting primarily with master's program and expanding to certificates and other micro credentials.

1.1 Cybersecurity Education

Approaches to Cyber security education and training includes theoretical models [1, 10] and practical simulation approaches [5, 6]. [1] conducted a meta-analysis of extant literature to identify features that can create learning situations with effective outcomes. These generally included an evaluation of evaluation criteria, conducting a needs assessment, and identifying a match between skill/task and training method. Cognitive modeling in cyber security education was also studied [10], where multiple models such as standalone model (network modeling, pure simulations, hybrid networking emulation), tracing for attacker behavior prediction, and model tracing for automation. They found that these models were more accurate with precise predictions when they were customized to reflect the population's tendencies. Although larger models of education and training like these exist, other studies focused on specific approaches such simulation and game-based mechanics [5, 6]. These approaches typically utilize a directed learning approach focusing on specific objectives followed by task-performance behaviors. These task-performance behaviors may be in the form of educational/serious games within a simulation. Specific approaches tended to improve motivation and learning by melding it with entertainment characteristics. Game-based mechanics such as capture the flag [8], can improve engagement for learners by offering a hands-on cyber challenge that is rooted in real-world scenarios. Many of these scenarios are offered in virtual machine environments to allow learners to attempt real defense and attack scenarios within a safe environment.

In addition to overarching approaches to cyber security education, other studies targeted specific methods of learning computer security concepts [7, 9, 11]. [7] studied the impact of perceptions of risk and secure behaviors. They found that the largest impact on out-of-class secure behaviors came from a combination of mini lectures and active learning tasks. This approach helped to change actual behaviors outside the classroom such as modifying passwords after data breaches. [9] reviewed the different levels of learning using similar constructs with static and animated content. The authors found that static content was generally more effective when paired with more complex concepts such as mathematical content such as encryption. Animated content was generally more useful for practical applications such as visualizing a distributed denial of service attack. [11] researched a specific approach to cyber security education, Present-Test-Practice-Assess (PTPA). This approach used the four major components: 1) Present: target s single set of related concepts, 2) Test: check understanding through an assessment of learning, 3) Practice: opportunities to apply concepts learned and 4) Assess: evaluation of performance on practice tasks. This method of instruction utilized live activities (simulations) to create replicate real-world scenarios. They found that the PTPA was more effective than traditional approaches that added capture the flag activities and hackathons.

These studies highlighted the importance of unveiling instructional approaches that best benefit cyber security education. Due to the large gap between total positions and

positions filled, it may be helpful to expand the pool of applicants with individuals from a range of backgrounds. This study aims to distill one of the major approaches to learning, case studies in cyber security education when the participants have a wide range of backgrounds. We focused our efforts on time on task based on individual differences, performance alignment, and how it can influence security education design.

The following questions guided the study:

1. How does students' time on task influence their ability to accomplish assignments?
2. What types of approaches are best aligned with performance?
3. How can student differences influence security education design?

2 Exploratory Analytics

2.1 Setting and Participants

The exploratory study was conducted with students enrolled in a Cybersecurity Education program, CyberEd in a Box. This cybersecurity educational program was designed to build capacity to fill the need for professionals in the cybersecurity workforce. Due to workforce gap and wide range of cybersecurity positions available, this program invites students from any field to enroll, not just computer science. Approximately 20 students are enrolled in the program each year and come from a wide range of academic backgrounds such as Computer Science, Engineering, Information Systems, Business, Management, Marketing, Education, Psychology, and Sociology. The program includes three courses, mentoring and an overarching internship that occurs throughout the program (Fig. 1). Each of the courses includes three major components: 1) tech labs, 2) projects and 3) discussions. Tech labs focus building information technology security skills such as networking, network defense, and ethical hacking. Projects target critical thinking skills in information security and risk management by having students complete case studies to determine appropriate actions in a chief security officer role with a range of security issues such as data breaches and information leakage. Discussions give students the opportunity to build their network by sharing resources with their peers and offering feedback to one another to build the community of practitioners throughout the term. Based on these major areas of each course, the researchers explored the projects portion due to the broad range of critical thinking and learning skills taught.

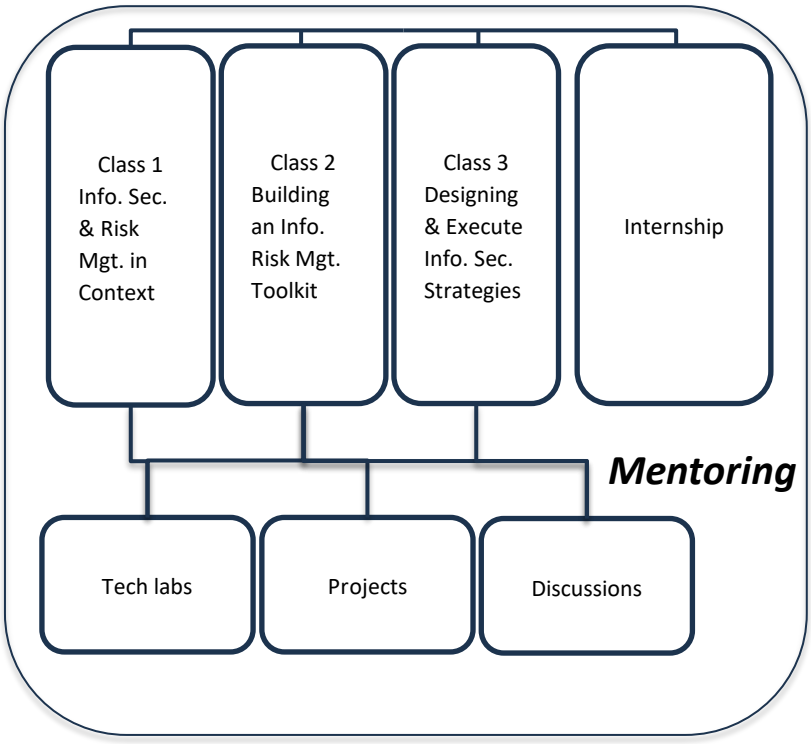

Fig 1. CyberEd in a Box Program structure

The initial study included 17 participants enrolled in class 3. These students came from a wide range of educational backgrounds and were at the ending of their program of study, which allowed them to hone their study skills over the course of the CyberEd in a Box program. Therefore, the final class would limit the initial influence of students getting acclimated to a new program of study.

2.2 Project Tasks

The course included five major projects with each project including two to three tasks each based on case study complexity. Data were collected based on initial opening of a case study in the course management system and submission of each assignment. The CyberEd in a Box program is a professional program that assesses assignments on a meets or does not meet professional standards. Thus, data were also collected based on number of submissions to meet the professional standard.

2.3 Analysis

The data were analyzed using a repeated measures design to determine the time on task for each student and how it differed throughout the term. We used an analysis of

variance to determine the individual differences between users and identified different clusters based on metrics such as performance, variance, and time on task. Data were aligned with course content analysis to determine difficulty of task and possible approaches to improve cognition through appropriate mentoring and support.

3 Results

3.1 How does students' time on task influence their ability to accomplish assignments?

As expected, there was a statistically significant difference between participants' time on task based on each component of the case studies with $p<.001$ (Table 1). This finding

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	5852.248	16	365.7655	2.736949	0.000652	1.703315
Within Groups	22718.78	170	133.6399			
Total	28571.03	186				

Table 1. One-Way ANOVA for time on task for case studies

highlights individual differences and the need to further analyze the data to determine a descriptive background for the data set to identify clusters for performance and the challenge of each assigned task. The summary data (Table 2) illustrates a wide range of time on task for students with a minimum of 1.07 days on average per assignment and a maximum of 18.67 days on average per assignment. On average, students spent approximately 7.34 days per assigned task. Over the course of the term, students spent a minimum of 11.84 days on the class projects and had a maximum of 205.39 days. The average time spent on project tasks was 80.79 days.

We clustered the data by total number of resubmissions by individual to determine performance based on time on task. Three groups emerged, 1) those without any resubmissions, 2) those with a single resubmission, and 3) those with two resubmissions. Based on these groupings, students with the least variance and time on task were in either the no resubmission or one resubmission groupings. Six students in this cluster spent on average one to two days on each task and had a variance less than 10. Two of which had one resubmission while the rest of the group did not resubmit any assignments. Ten of the remaining 11 students had a variance in time over 100. Only one student in this group had a variance of 62. The cluster with the variance mainly above 100 included six students with zero resubmissions, one student with one resubmission, and four students with 2 resubmissions. It appears that the higher the variance in time on each task tended to have participants with increased levels of submission to attain a professional level of performance on case studies.

Groups	*Count*	*Sum*	*Average*	*Variance*	*Resubmission*
1	11	132.0029	12.00027	244.9879	0
2	11	18.70464	1.700422	9.141954	0
3	11	76.90679	6.991527	135.2517	0
4	11	14.81988	1.347262	2.273724	1
5	11	72.97556	6.634141	100.5736	0
6	11	205.394	18.67218	199.8102	2
7	11	48.93757	4.44887	101.2293	0
8	11	131.9491	11.99537	291.9185	1
9	11	65.71566	5.974151	140.1004	2
10	11	19.20168	1.745607	1.71381	0
11	11	114.2145	10.38314	121.4065	2
12	11	189.5093	17.22812	609.6	0
13	11	19.67366	1.788514	3.282195	0
14	11	11.84257	1.076597	2.158005	0
15	11	12.53883	1.139894	1.25678	1
16	11	94.91159	8.628326	62.64685	0
17	11	144.0921	13.09928	244.5265	2

Table 2. Summary data for time on task across case studies

To determine task challenge, we created a stacked bar chart to identify patterns in the data (Fig. 2). Assignments 3 and 4 appeared to have the greatest range in assignment completion. We conducted an ANOVA on the time spent per assignment, however, the results were not statistically significant ($p>.05$). The variance for these assignments were the highest of all assignments at 394.56 for assignment 3 and 339.00 for assignment 4. Interestingly, these two assignments were a part of the same case study. This led the researchers to conduct a content analysis on the case studies to identify major differences which could lead to the disparity in time spent to achieve a professional level submission for this project.

All of the projects included an introduction page (Fig 3.), lecture videos page, case study page and submission page. The introduction page included the learning objectives, workflow details and resources (internal and external). The lecture videos page included each of the videos to support the case study, while the case study page detailed the case and the guidelines for the project. The case study for assignments 3 and 4 included external sites that needed to be utilized to solve the case. Based on a content analysis of all of the case studies, this one in particular included a greater dependency on the use of information external to the course management system. Students needed to search an external site to identify and utilize pertinent information that was not directly discussed in the case study video. Therefore, it appears that requiring the use of external content may have influenced the time spent for individual students on

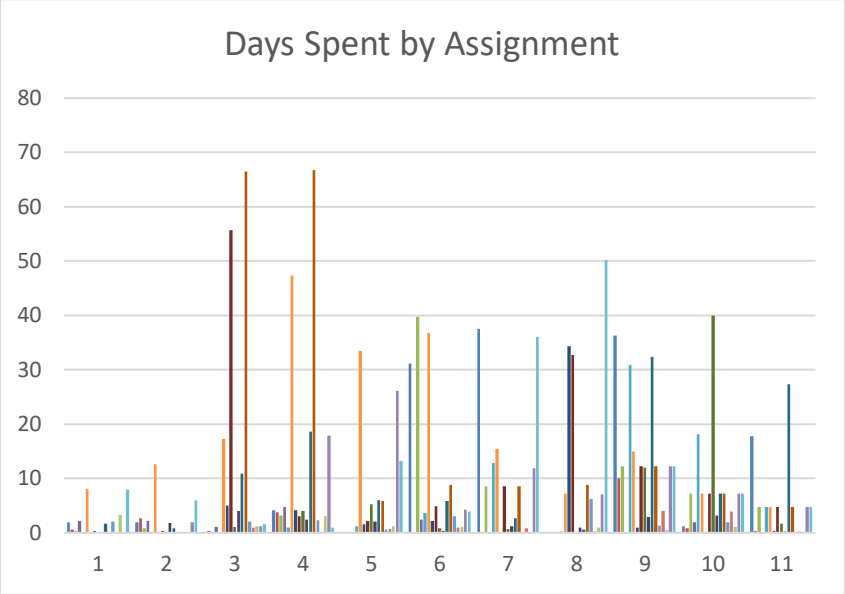

Fig. 2. Average days spent on each case study task

Reading/Resources Assigned - Focus Points

Assigned Resources	Description/Context	Focus Points tied to objectives
Short Lecture: **The Models of this Program: The Decision-Making Model for Capstone**	*Dr. Endicott-Popovsky reviews the thinking models of this program, adding one for decision-making, a managerial model.*	• Explain the program models from Course 1 to Course 3 and derive a personal philosophy on the general application of models in cybersecurity strategy. • Synthesize your thinking about decision-making in the cybersecurity field.
Case Study: Breach of HIPAA Protected Information?	*In this first more complex case, analyze the context of a possible HIPAA breach by studying the case presentation. Video lecture has also been included.* *Come to a decision on whether a HIPAA breach has occurred, and what the resolution should be.*	• Apply case analysis skills to a case involving a possible HIPAA breach. • Practice risk assessment and documentation. • Identify at least three essential questions that framed your approach to the case. • Engage in peer review of others' resolutions. • Compare and contrast your own resolution to the one given by the practitioner.
HIPAA: HHS.gov Health Information Privacy site	This site provides a search for specific HIPAA questions. For example, you can search for "breach notification requirements" to find notification rules that apply to this case.	• Apply case analysis skills to a case involving a possible HIPAA breach. ◦ Conduct strategic research of applicable regulations and requirements.

Fig. 3. Sample resources section of introduction page

this assignment. This preliminary finding led us to continue this line of research deeper in a subsequent study.

4 External and Internal Content Study

4.1 Background

Since the cyber security education program, we analyzed targeted participants from a wide range of majors, we conducted the follow-up study with a large-enrollment computer science course for non-majors that is a prerequisite for many fields, such as education, business, kinesiology, etc. It is a 101-level course focused on general computer science topics and productivity. The course we examined was a 6-week asynchronous summer session, which has two lecture topics per week that students are quizzed on. In addition, students do lab work utilizing productivity software. One of the units was focused on computer security, where the students were to watch the lecture video which was under 30 minutes. This video linked out to other videos in the lecture, and students were instructed to pause the lecture video and view the external video, and then return. After watching the video, students would take a quiz on the lecture topics, which included the external video topics. To prevent cheating, the quiz questions were taken as a random draw from a larger question pool.

4.2 What types of approaches are best aligned with performance?

We collected user page view data to determine how long each student spent on each question, along with the student scores on the quizzes. We also performed an item analysis on the question to see how difficult it was for students, and how well a question discriminated between the top and bottom scores.
We then categorized the content of the lecture material and corresponding questions into recent history, types of criminals, general aspects of security, and typical attacks. Our latter three topics were chosen based on being the topics emphasized in computer security textbooks. Our first category, recent history, was chosen because this can have a strong impact in changing student opinions and practices when they can see how it relates to their lives. We first wanted to see if there was a difference between the performance or time spent on the questions in different content sections. A one-way ANOVA analysis was performed on the performance of different content categories and on the time spent on questions between content areas. The results for the performance are seen in the table below, and showed they were nearing a trend in the difference between content areas with $p=0.11$ (Tables 3 and 4). The one-way ANOVA for the time spent showed no significant difference in time spent on questions between content areas.

Even though there was no significant difference between the time spent on questions between content areas, we noticed that there was a large amount of time spent on specific questions of the "recent history" category. Based on the descriptive statistics, we

Groups	*Count*	*Sum*	*Average*	*Variance*
Recent history	12	10.19874	0.849895	0.028213
Criminal types	4	3.847118	0.961779	0.002502
Aspects of security	3	3	1	0
Typical attacks	6	5.859307	0.976551	0.001567

Table 3. Summary data for performance between categories

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.103987	3	0.034662	2.235038	0.113986	3.072467
Within Groups	0.32568	21	0.015509			
Total	0.429667	24				

Table 4. One-way ANOVA on performance between content categories

could see that the "recent history" category had the lowest performance, but the most amount of time spent. We conducted a one-way ANOVA and found a statistically significant difference between the performance on each question. An examination of the item difficulty and item discrimination value showed that the questions with the worst performance and highest discrimination were based on external video questions (Table 5).

As a result, we reviewed questions in this section and identified certain questions that required students to review content from an external video linked in the lecture video, compared to other questions that could be answered solely on the lecture video. We performed a one-way ANOVA (Tables 6 and 7) and found a statistical significance difference between external and internal questions ($P<0.004$), with external questions only receiving 76% correct, and internal content receiving 94% correct.

We performed the same analyses to examine the time spent on each question, and the time spent on each question in internal and external content. The one-way ANOVA showed a statistically significant difference between time spent on each of the questions in the recent history category ($P=0.00$) and a statistically significant difference in time spent on each question between internal and external content to the lecture ($P=0.00$), seen in Tables 8 and 9. The difference here was quite large, with external content taking more than six times as long as internal content.

We performed the same analyses to examine the time spent on each question, and the time spent on each question in internal and external content. The one-way ANOVA showed a statistically significant difference between time spent on each of the questions in the recent history category ($P=0.00$) and a statistically significant difference in time spent on each question between internal and external content to the

lecture (P=0.00), seen in Tables 8 and 9. The difference here was quite large, with external content taking more than six times as long as internal content.

SUMMARY - Score

Groups	*Count*	*Sum*	*Average*	*Variance*	*Discrim*
According to the Heartbleed video, a set of open source tools is a common implementation between S.S.L and T.L.S.	23	20	87%	0.118577	0.5
According to the Heartbleed video, how long has Heartbleed been around?	24	12	50%	0.26087	1
According to the Heartbleed video, Open S.S.L runs on _____ percent of the Internet.	17	12	71%	0.220588	1
According to the Heartbleed video, what is in the root of Heartbleed?	25	20	80%	0.166667	.83
According to the Phishing video, what information do they want from you?	16	15	94%	0.0625	.25
A computer on a public university network gets attacked more than 2,000 times a day.	17	17	100%	0	0
According to Google, how many new malicious websites are found every day?	12	11	92%	0.083333	.33
In 2008, how many computer viruses were in circulation?	22	20	91%	0.08658	.33
People who attack public networks look for _____ on computers.	17	12	71%	0.220588	1
Which mobile device has a recorded number of 744,000 viruses?	21	20	95%	0.047619	.2
Which of the following networks is constantly being attacked by hackers?	22	22	100%	0	0
You only need to change your passwords to be safe from Heartbleed.	23	23	100%	0	0

Table 5. Item difficulty and discrimination value of recent history questions

Groups	*Count*	*Sum*	*Average*	*Variance*
AveExt	25	19	76%	0.07037
AveInt	23	21.69048	94%	0.012716

Table 6. Summary data for performance between external and internal content

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.401452	1	0.401452	9.380484	0.003658	4.051749
Within Groups	1.968638	46	0.042796			

Total	2.37009	47

Table 7. One-way ANOVA on performance between external and internal content

Groups	*Count*	*Sum*	*Average*	*Variance*
AveExternal	25	1920.3	76.812	824.9162
AveInternal	23	296.4881	12.89079	10.1804

Table 8. Summary data for time spent per question between internal and external quiz Content

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	48945.93	1	48945.93	112.4522	0.00	4.051749
Within Groups	20021.96	46	435.2599			
Total	68967.89	47				

Table 9. One-way ANOVA on time spent per question between internal and external quiz content

4.3 How can student differences influence security education design?

Examining the results, questions based on content contained within the video required less time to answer and resulted in higher scores for students. Conversely, questions based on content contained in external videos required more time and resulted in lower scores and a higher item discrimination value. While the external videos were integrated to provide additional animated content to increase student engagement with the material, this seems to have been detrimental to student learning. This may have occurred because of the increased cognitive load in having students perform additional tasks.

Alternatively, this may have occurred because students were spending time looking up answers in the lecture and external videos. Using page view statistics, we can see some indications of answer-seeking behavior. There were 32 unique views, with only half watching the video in its entirety. Other views spiked at locations we could trace back to answers in the video. This might also indicate that some students may not have watched the external videos prior to starting the quiz or had to go back to check the answers. This would explain the significantly greater time spent on these questions. The item discrimination could also be explained by students who did not watch the external videos at all, as some students already did not watch the internal lecture videos. For example, 35 people took the quiz but page view statistics on the video show that at most only 32 students clicked on the lecture video. Given that watching the external video required more work, even less students may have reviewed the external video.

5 Discussion

5.1 Conclusions and Future Directions

The initial study focused on exploratory analytics from the CyberEd in a Box program that included students from a range of educational backgrounds. The individual differences between students led the research team to identify clusters of students based on performance, time on task, and resubmission rate. These major groupings highlighted the optimal approaches to studying in this environment, spending a consistent amount of time on task for each of the projects. This group spent on average 7.34 days per assignment with a variance under 10 meeting the professional requirements in the first or second submission. The high level of variance in the two-resubmission group led us to our follow-up study to examine the course content and potential underlying reasons for the lower performance.

Our follow-up external and internal content study sought to examine the impact of techniques to reduce variance in time spent with the material and determine its influence on performance. While external videos were implemented to enhance attention, engagement, and learning, the scores and time spent seem to indicate otherwise. While examining the data and potential roadblocks to their learning, we have found that this might have instead made the barrier to entry too high for some, and they did not engage with the content. As a result, we would recommend embedding case study videos or external data within the main course content, since students who are not majoring in computer science may be less willing to view external content than computer science majors. Interestingly, this finding mirrored information in our first study's data set, many students did not click on the external resources provided for many of the case studies.

These complementary studies highlighted the need for further research in computer security education using augmented cognition-based approaches. With the increase in demand for security professionals and computer security programs broadening their entry point to include non-technical individuals, it is vital to consider individual differences amongst students. We would like to conduct further research on embedded learning scenarios to immerse students in their educational experience and optimize their learning. These future studies could be conducted on a range of learning objectives including technical skills, conceptual knowledge, and applied scenarios. Increasing the technical skillset of those enrolled in security programs may take place in simulation-based environments. Many of which include a detailed breakdown of time and click data based on capture-the-flag events. These types of data could be analyzed to determine potential changes to the system to improve long-term learning. Analysis of conceptual learning can take place using a wide range of tools such as quizzes/tests and assignments. Both offer the possibility of utilizing augmented cognition approaches to improve instructional design techniques for assessments and learning material. We are also interested in application of learning through embedded scenarios. Immersive virtual worlds could give students the opportunity to be immersed in learning environments that could be utilized as "live case studies." These worlds may be rich in data and opportunities to augment student development. Computer security education

continues to evolve in programmatic opportunities for a wide range of individuals and in its approaches in the learning sciences.

6 Acknowledgements

This material is based on work that was partially supported by Grant No. 1662487 from the National Science Foundation (NSF) and by Grant No. H98230-22-1-0329 from the National Security Agency (NSA), National Centers of Academic Excellence in Cybersecurity.

References

1. Arthur, W., Bennett, W., Edens, P., & Bell, T. (2003). Effectiveness of training in organizations: A meta-analysis of design and evaluation features. *Journal of Applied Psychology*, 88(2), 234-245. [models 2]
2. Cobaj, K., Domingos, D., Kotulski, Z., Resp ício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master program. *Computers & Security*. 75, 24-35.
3. CyberSeek (2023). Cybersecurity supply/demand heat map. Retrieved from https://www.cyberseek.org/heatmap.html.
4. Federal Bureau of Investigation (2023). Federal Bureau of Investigation Internet Crime Report (2022). Retrieved from https://www.ic3.gov/.
5. Jalali, M., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game. *Journal of Strategic Information Systems* 28(1), 66-82. [gamification]
6. Jin, G., Tu, M., Kim, T., Heffron, J., & White, J. (2018). Game based cybersecurity training for high school students. *Proceedings of ACM SIGCSE*, Baltimore, MD, 68-73. [gamification]
7. Ogawa, M.B., Auernheimer, B., Endicott-Popovsky, B., Hinrichs, R., & Crosby. M.E. (2023). Privacy and Security Perceptions in Augmented Cognition Applications in Foundations of Augmented Cognition 17th International Conference, AC Proceedings, Schmorrow, D., Fidopiastis, C. (eds.), Proceedings Volume 17, Springer Lecture Notes in Artificial Intelligence.
8. Svabensky, V., Celeda, P., Vykopal, J., & Brisakova, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*. *102* 1-14.
9. Taylor, M., Baskett, M., Allen, M., Francis, H., & Kifayat, K. (2018). Animation as an aid to support the teaching of cyber security concepts. *Innovations in Education & Teaching International*, *55*(5), 532–542.
10. Veksler, V., Buckler, N., Hoffman, B., Cassenti, D., & Sugrim, S. (2018). Simulations in cybersecurity: A review of cognitive modeling of network attackers, defenders, and users. *Frontiers in Psychology*. 9, 1-12. [models]
11. Workman, M. D., Luevanos, J. A., & Mai, B. (2022). A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model. *IEEE Transactions on Education*, *65*(1), 40–45.