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 #46483

Cybersecurity Students' Choices of Learning Strategies for Covering Major-specific Concepts

Dr. Emre Tokgoz, State University of New York - Farmingdale

Emre Tokgoz is a faculty of Department of Computer Security at SUNY - Farmingdale. His research interests in STEM education include understanding and proposing improvement ideas for advancing undergraduate and graduate students conceptual mathematics, engineering, computing, and cybersecurity knowledge.

Alyssa Xiang

Cybersecurity Students' Choices of Learning Strategies for Covering Major-specific Concepts

[1]Emre Tokgoz, [2]Joel Joseph, [3]Julissa Molina, [4]Tanvir Ahmed, [5]Alyssa Xiang, [6]Sergio Duarte

[1]Emre.Tokgoz@farmingdale.edu; [2]josej18@farmingdale.edu; [3]molij17@farmingdale.edu; [4]ahmet9@farmingdale.edu; [5]xiana21@farmingdale.edu; [6]duarsp@farmingdale.edu

[1-6] Department of Computer Security, State University of New York, Farmingdale, New York, 11375

Cybersecurity degree program offerings started to increase in the United States as internet-based technologies are advancing. These technological and educational advancements and offerings raise critical pedagogical research questions towards identifying which teaching methods can be the most affective on students' cybersecurity conceptual learning and how can such education be improved undergraduate and graduate students' conceptual learning. On the contrary to the importance of such focus on conceptual learning of students, the research conducted on understanding and improving undergraduate and graduate students' best understanding practices are underestimated and hardly any pedagogical research is conducted in this manner; Therefore, in this work, we focus on several factors that play significant roles on cybersecurity students preferred methods or strategies that help them the most during their learning cybersecurity concepts and their ideal learning resources for learning these concepts. Qualitative and quantitative data is collected from 98 students at a university located in the northeastern side of the United States. The data of this Institutional Review Board (i.e. IRB) approved research is collected by the Principal Investigator (P.I.) and five research assistants. The quantitative data analysis shared in this work relied on the statistical analysis of survey data while the qualitative analysis relied on the follow-up interviews conducted by the P.I. The participants received money compensation for participating in interviews to further explain their survey responses. Qualitative and quantitative results indicated the participants' strong interest and high prioritization of learning from professors and self-study. The design of the course materials and the instructor are two of the major factors that are determined to impact their learning the most. The priority of the learning environment among the online, in-class, and hybrid learning options, participants choices depended on their life conditions that relied on having a family, a part time or full-time job, and availability of the coursework in the associated environment

Keywords: Cybersecurity education, cybersecurity learning factors, cybersecurity learning environments, online learning, in-person learning, hybrid learning, professor, social media, self-study.

1. Introduction.

Cybersecurity careers are continuing to increase with the demand rate increasing over time. The analysis presented in the Cybersecurity Workforce Supply and Demand Report by the U.S. Cybersecurity Workforce Data Initiative of the U.S Government (published in May of 2024) shows that the *cybersecurity workforce currently ranges between 164,000 and 3,492,000 workers out of an estimated total of 161,052,000 workers in the United States* [6]. Nationwide, the report by U.S. Bureau of Labor Statistics on Information Security Analyst (ISA) job category indicates a 33% projected percent increase in the employment from 2023 to 2033 while the average growth rate for all occupations is 4%. The expected employment increase from the year 2022 to 2033 is 59,100 jobs [7]. As the number of employment opportunities increases, the university offerings of cybersecurity related programs also increase therefore there is a need for better understanding of good practices that students learn.

Cybersecurity students' efficacy in learning computer security specific concepts and the educational modalities that they are comfortable with learning such concepts are important aspects of their education. There is very limited investment in pedagogical research of cybersecurity students' learning based on their interest of learning modalities, pedagogical strategies of learning the associated concepts, and the psychological factors that impact their learning. Majority of the relevant literature research focuses on either hypothetical discussion on how psychological factors impact cybersecurity education from a cybersecurity perspective rather than factors that impact students' ability to learn relevant concepts in different environments as well as interaction with others or corporate-based cybersecurity behaviors [2,3,4]. There are educational attempts made to offer summer camps and attract high school students through summer camps however these attempts do not include pedagogical research on better understanding of the students [8]. Similarly, a peer mentoring framework for students in an introductory Information Systems course is tested in [9] for students to interact with their peers in an upper-level elective course in cybersecurity that focused on Data Analytics for Cybersecurity concepts. The purpose of the tested framework was to encourage more students to explore cybersecurity careers through peer led cybersecurity discussions. The initial results indicated an increased interest of the students in cybersecurity for the observed course's students in addition to the positive impact of post interactions that both groups had with a clearer interest and understanding of cybersecurity concepts.

Cybersecurity education is expanding throughout the United States, and in the World, with a tremendous growth over the past decade. Hence, understanding and helping students to learn better after determining their best interest in learning environment in this emerging field is necessary to investigate [5]; Therefore, this research is aiming to investigate the cybersecurity students' best interests in the learning environment that help them to learn major-specific concepts and the external factors such as professor, social media, classmates, internships as well as self-study that play a role in their cybersecurity learning. To the best of our knowledge, there is no pedagogical study that aims to understand such considerations that can help cybersecurity educators about undergraduate students' effectiveness in learning during their major-specific learning from a

psychological perspective, and their ideal conceptual learning environment (such as in-class online learning, etc.)

2. Research Methodology

The results presented in this work are outcomes of a research conducted in one of the public universities in the Northeastern region of the United States by a P.I and five research assistants. The data is collected by the research team after attaining Institutional Review Board (IRB) approval to conduct the research. Pre- and post-data collection and evaluation included two informed consent forms, a survey, and video recordings of the interview participants with the transcription of the data. Qualitative and quantitative data is collected from cybersecurity students; The quantitative data is the numerical data attained from 98 students based on the following two research questions as a part of the survey they completed:

1. What method or strategy helps you the most during your learning computer security experiences?

2. What is your ideal learning environment for learning computer security courses?

The quantitative analysis of the data is based on the statistical distributions of the data as well as the statistical analysis of the numerical responses. The qualitative data consists of the data collected from students during scheduled interviews that lasted anywhere between 30-40 minutes to furthermore understand their survey responses. The interviews are recorded and transcribed, and students are compensated with money for their participation in the conducted interviews. The follow-up interviews aimed to cover the details of the participants survey responses with additional follow-up questions to understand the details of the survey responses. The recordings are analyzed to identify the details of responses collectively. Statistical calculations form quantitative results while qualitative results rely on the voice-recorded interviews. This research is currently in progress and a summary of the results will be included in the abstract once it is completed.

3. Quantitative Results

In this section we focus on the quantitative results derived from the collected numerical data. The initial stage of research investigation relied on the normal distribution nature of the data for further implementation of the statistical analysis as well as the statistical distributions of the data that will be explained next. What follows next is the application of Wilcoxon Ranking Sum and the Mann-Whitney U tests as the normality analysis indicates the need for non-parametric analysis. Statistical percentage values will be explained as the last to furthermore explain the quantitative nature of the data. These quantitative results will be interpreted within the context of the results, and they will be integrated into qualitative results in the conclusion section.

3.1 Normality Analysis & Data Distributions

The normal distribution investigation demonstrated in this section relies on prioritization levels of the students based on the following specific choices:

- Professors
- Classmates
- Self-study
- Internships
- Social media

The top two choices of the that they prioritize as the resources of learning is essential for furthering their learning needs. Analyzing the highest prioritization of the students as a learning resource for cybersecurity concepts, an exponential distribution was identified to be the best option with an R-square value of 99.75% as shown in Figure 1 below. The top choice of the students is determined to learn from professors with the second choice being classmates, third choice being self-study, fourth choice being the internships, and the last choice being the social media.

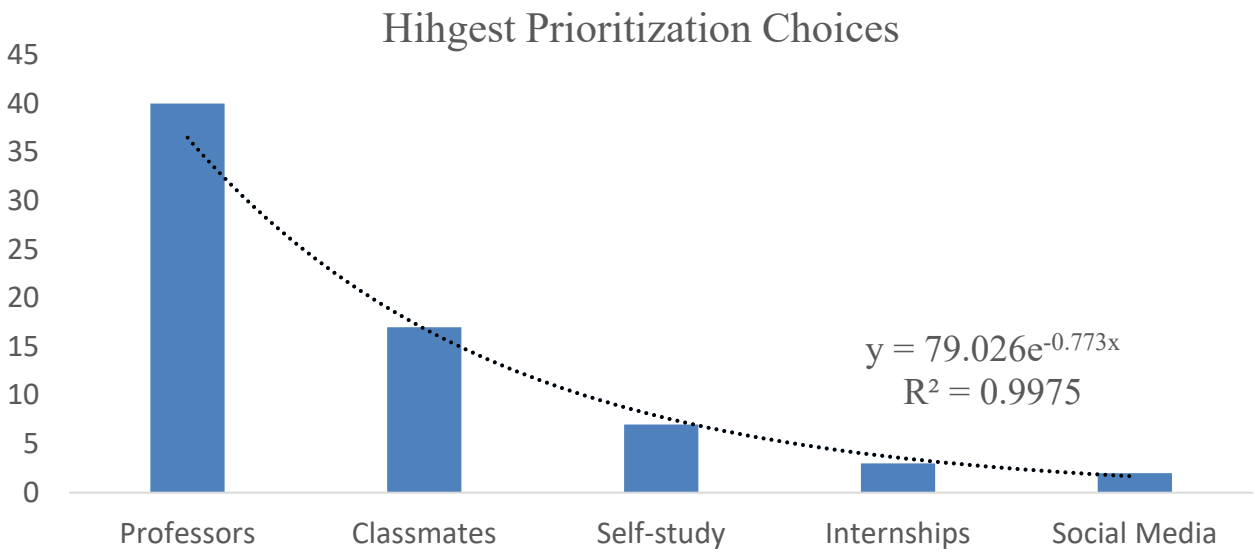

Fig. 1 Top prioritization of the students as a learning resource for cybersecurity concepts

The second-best option learning choice is demonstrated in Figure 2. As it can be seen from this graph, the distribution is skewed towards right with higher priority given to internship and social media while self-study having the highest priority among the participants with a percentage value of 33.33%. Given professors and classmates were selected as a part of the top priority, they had less weight in the distribution with 2.9% and 20.29% respectively. Having an internship for learning experiences purposes received the second highest option with 23.19%.

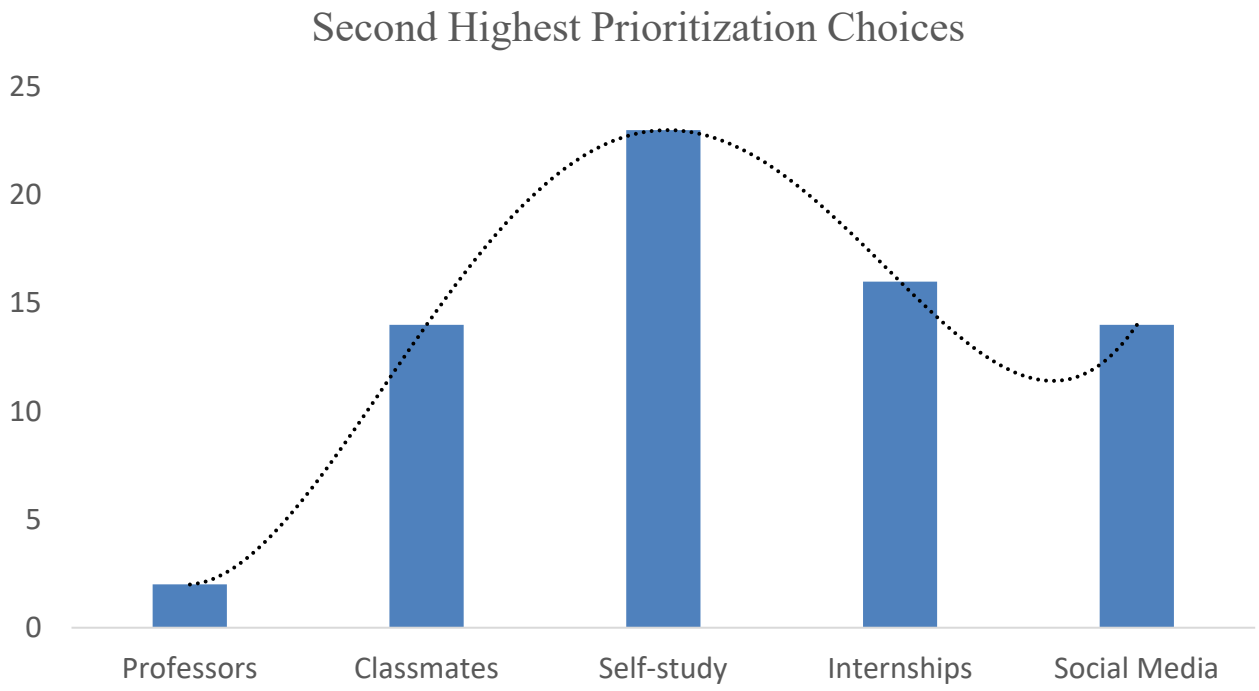

Fig. 2 Secondary level choices of cybersecurity students learning source prioritization.

Figure 3 illustrates the following three choices (i.e. 3rd through 5th) of the students. These choices demonstrated in the figure do not have a specific statistical distribution nature therefore they are shown together. The main take-aways from this figure are the following:

- Third best option is determined to be the internships with 34.78%
- Fourt best option is determined to be the social media with 42.03%
- Fifth best option is determined to be the self-study with 31.88%

These numerical results rely on categorical evaluation of the participants; Each one of the above-mentioned options totaled to 100% based on the prioritization choices of the students. Table 1 demonstrates the quantitative percentages distribution of the participants that also demonstrates the priority levels of their choices in percentages.

	1st Priority	2nd Priority	3rd Priority	4th Priority	5th Priority
Professor	57.97%	2.90%	18.84%	17.39%	2.90%
Classmates	24.64%	20.29%	21.74%	11.59%	21.74%
Self-study	10.14%	33.33%	13.04%	11.59%	31.88%
Internships	4.35%	23.19%	34.78%	17.39%	20.29%
Social media	2.90%	20.29%	11.59%	42.03%	23.19%

Table 1. Percentage distribution of the external factors based on the priority levels of the cybersecurity students

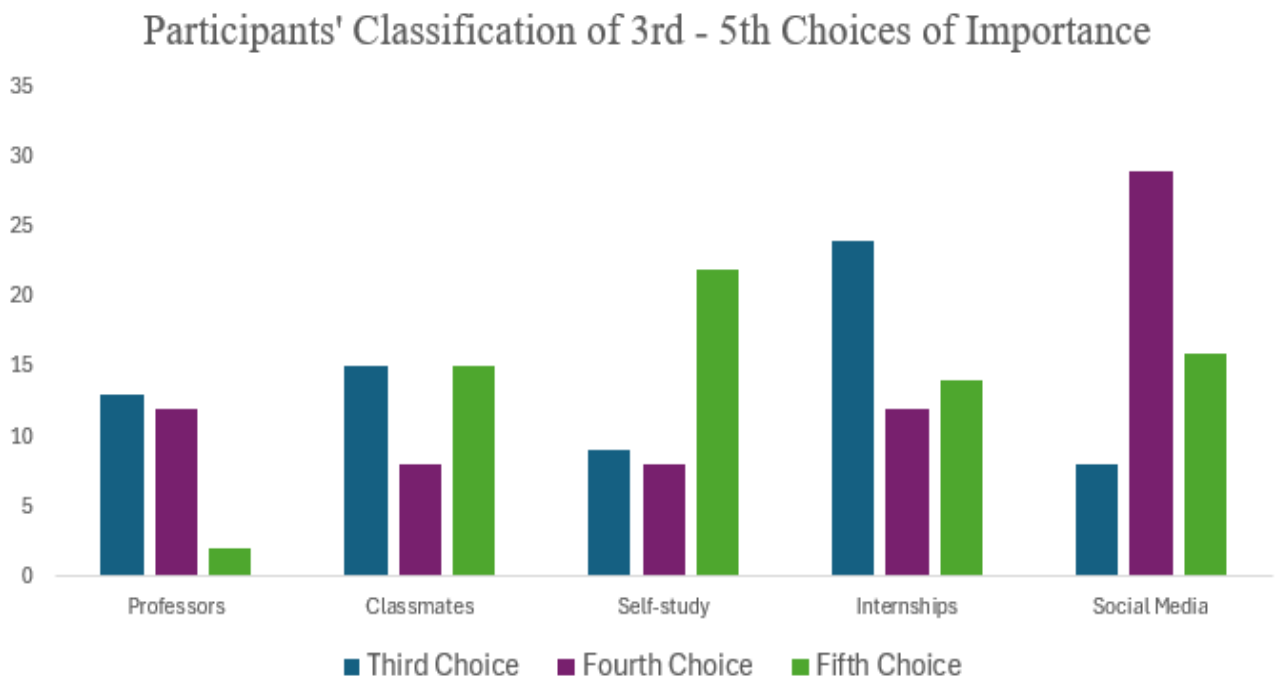

Fig. 3 Cybersecurity students' third, fourth, and fifth levels of choices as learning resources of cybersecurity concepts.

3.2 Mann-Whitney U and Kruskal-Wallis Tests

In this section we focus on identifying the statistical results of cybersecurity students in learning resource preferences from a paired grouping perspective depending on their prioritization. Noting the non-normal nature of the data, we use non-parametric statistical Mann-Whitney U test for identifying the impact of the two groups on each other using the survey questionnaire grouping. We used the pairing of five columns with columns values consisting of the total number of prioritizations that the students had for all five categories. Assuming a α=0.05 confidence level for the statistical significance, each paired column's Mann-Whitney U test suggested to accept the null hypothesis for all coupled five prioritization levels of the students indicating that the prioritizations levels of the students do not have significant differences with each other.

Next, we apply Kruskal-Wallis test by taking all five categories into account together and apply the test due to the non-normal distribution and small data set nature. The main aim is to determine if we have a significant difference between the five categories to accept or reject the ranking of these groups. We identified the p-value to be greater than 0.05 therefore we accept the fact that there is no significant difference in ranking when all the five groups are chosen that confirms the results of Mann-Whitney U test for all five categories collective analysis.

4. Learning Environment Choices

Understanding learning environment choices of cybersecurity students is a major interest of any cybersecurity department to be able to design the corresponding curriculum and coursework offerings. The offering environment/modalities are not always stable and there are certain factors that play roles in the decision-making process of cybersecurity programs for such offerings. Given the importance of understanding students' interested student environments, we asked the research participants about their learning environment preference. As shown in Figure 4 below, in-person meeting is the most popular option due to its 58.33% percentage share while hybrid course offerings received the second place with 27.08%, and online meeting option received 14.58%. The online meeting option is the asynchronous meeting option by the participants.

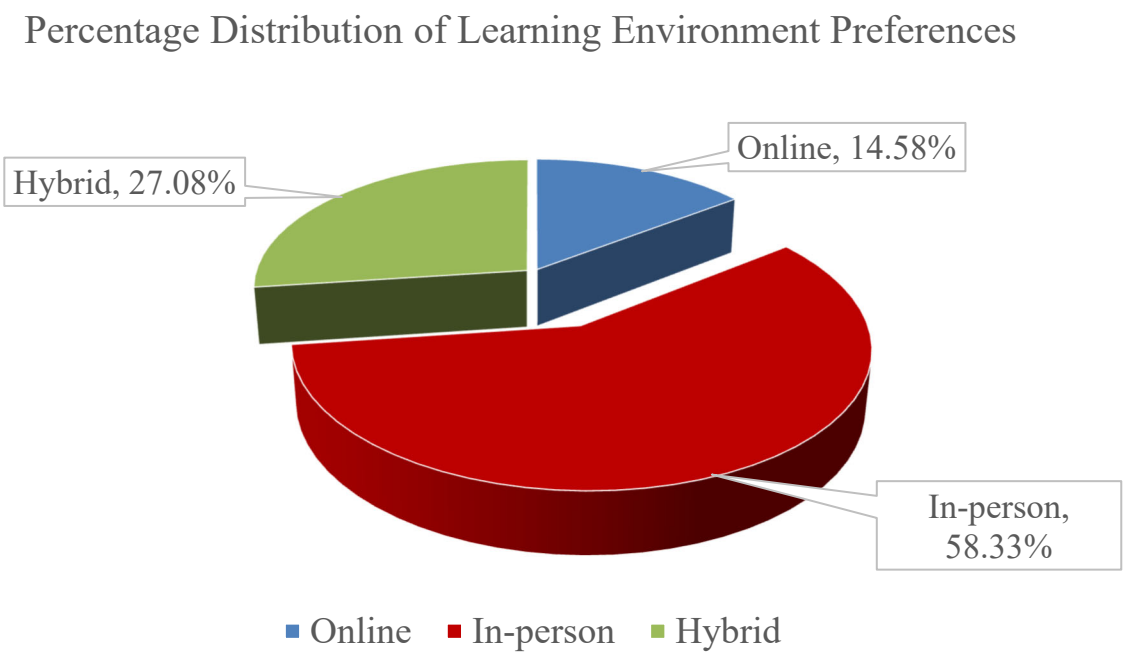

Fig. 4 Percentage distribution of cybersecurity majors' learning environment choices depending on online, hybrid, and in-person meeting options.

5. Qualitative Results

In this section we evaluate the qualitative results attained from the interviews conducted with the research participants to furthermore understand their responses to the survey questions. Examples of statements provided by the participants will be displayed for the readers to have a better understanding of the explanations of the participants. The results shared in this section are particularly important for the conclusions drawn from this research as a complementary support to the quantitative results attained. The top two choices of the learners in the qualitative assessment were the professors and self-study, therefore our focus is mainly on these two choices without excluding the importance of the other choices.

Students' perception of the professor and information shared by the professor was the key outcome of the results for both online and in-class education. All students particularly indicated the importance of the examples shared by the professor in the classroom and how knowledge of the professor makes a significant difference in their motivation and understanding. One of the participants outlined the importance of professor during the interview as follows:

Interviewer. *What matter or strategy helps you the most during your learning computer security experiences? Can you please also explain your choices?*

RP 2. *Sure, I'd say number one would definitely be the professors. They're the ones who really guide me through learning everything. Since I'm a junior and don't have a ton of hands-on experience in cybersecurity yet, my professors play a huge role. They bring so much real-life experience to the table, and they're always explaining what's happening in the industry right now, what's changing, and what the future looks like. Their detailed explanations really help me understand things thoroughly.*

Number two would be my classmates. When you work on group projects or even just have friends in class, it makes learning so much more engaging. You can bounce ideas off each other, discuss what you're learning, and support each other, which is super helpful.

And number three would be internships. For me, I have a lot of theoretical knowledge, but internships are where you really get to apply that knowledge in a hands-on way. That's something I'm still working on, but I think it's key. Internships give you the practical experience you need to become a well-rounded candidate for real-world jobs.

So yeah, I'd rank professors first, classmates second, and internships third. Those are the factors that have made the biggest difference in my learning so far.

Interviewer. *Alright. And how about Self-study on social media?*

RP 2. *Social media can be useful, but honestly, it's not always the best way to learn. For example, there are a lot of influencers out there sharing advice like, this is what you need to do for a career in cybersecurity, but the problem is we often don't fully engage with it. A lot of the time, we just watch these videos while lying in bed or eating, and we're not really paying attention. We might even save the video thinking we'll go back to it later, but most of the time, we never do.*

Now, self-study is definitely important. It's what you rely on when you don't have strong influences around you—like if your classmates or professors aren't available to help or if you don't have access to internships. Self-study is what pushes you to learn on your own and stay disciplined.

That said, I think self-study works best when combined with other factors like professors, classmates, and internships. Those three things provide the structure, guidance, and experience you need to succeed in cybersecurity. So, while self-study is important, it's not enough on its own to make you a perfect candidate for the job—you need a mix of everything.

The following explanations by another participant relied on self-study being the top choice due to the reason of difficulty in understanding some of the professors:

RP 1. *Internships at the bottom and self-study probably at the top. Professors, then social media and classmates.*

Interviewer. *And for the top reason, what motivates you to choose that?*

RP 1. *...If I take self-study. Just like I've found that a lot of the professors not all of them, but it's I don't always get the best understanding of the content from the professor, and I will have to go home and look up, you know. A clearer explanation of what the professor was teaching and that varies. It's not every professor you know. Some are better than others…*

Interviewer. *In terms of the self-study, what resources do you use?*

RP 1. *YouTube like forums, online communities, researching the same topic, news articles, things like that. So, self-study and social media resources are kind of overlap in a sense.*
Interviewer. *And internships when you put it there. Does it help with anything?*
RP 1. *I've never done an internship.*

Interviewer. *And classmates, do you get to work with them when you're in the online environment?*
RP 1. *Not really, no.*

Asynchronous online meeting option was chosen by the working professionals in the cybersecurity programs while in-class meetings are mainly preferred by the students who had either internships, part-time work, or no-work. Students who were motivated to participate and learn in the classroom indicated their attempts to design their schedule accordingly.

The interview transcriptions of the participants had similar key phrases and words to the above presented transcription of the two participants' responses. Professors and self-efforts are determined to be the major factors while social media is determined to be not a highly trustable source of developing brand-new knowledge. The participants particularly indicated the need for reliable resource need for furthering the knowledge by using social media resources. Similarly, learning from classmates are identified to be not necessarily a reliable resource however important for being interactive and learning. The participants who completed internships related to information technology indicated the importance of the internship while others who don't have such experience didn't consider it to be a resource of learning experience necessarily.

6. Conclusions & Future Works

In this work, we focused on learners' interest of cybersecurity learning environments and the factors that play significant roles in their understanding of cybersecurity concepts. The following are the key takeaways from the qualitative and quantitative research results:

- The top choice of external factors that impact cybersecurity students was learning from Professors by 57.97% of the research participants while 24.64% of the research participants' top choice was learning from classmates. 10.14% of the participants chose self-study as their highest priority while 4.35% of the participants chose internship as the best learning option, and the last choice being social media is favored by 2.9% of the participants as the top choice.
- The second most important external factor was learning through self-study with a distribution of 33.33% while 23.19% of the research participants' secondary choice was learning during internships. Learning from classmates and social media both received 20.29% popularity of the participants as the secondary choice while 2.9% of the participants chose professors as the second most important option.
- In-class learning of cybersecurity concepts was favored by 58.33% percentage of the research participants while hybrid course offerings received the second place with 27.08%, and online (asynchronous) meeting option received 14.58%.
- Factors such as family and work are determined to be the significant elements of participants' choices of learning environments. Those who are motivated to enroll in class learning environments attempted to their best for such attempts depending on the circumstances of their ever-changing semester-based conditions for adapting changes.

Figure 5 is a summary of the external factors that play roles in students learning cybersecurity concepts. As indicated by the "1st choice", the highest priority is dedicated Professors with their information sharing in the classroom. Interactive learning and real-life examples and experiences are mentioned to be two of the critical elements of learning during the interviews.

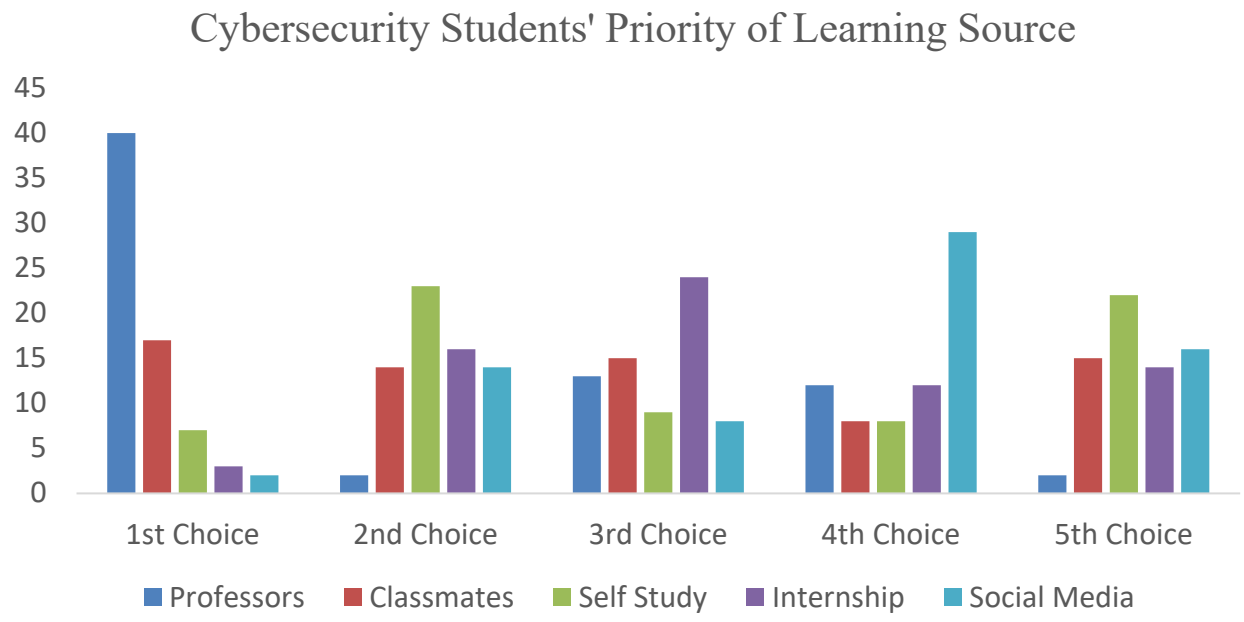

Fig. 5 A summary of the cybersecurity students conceptual learning prioritization based on the five categories of professors, classmates, self-study, internship, and social media.

We invite other researchers and educators to participate in the efforts made for such educational considerations and even applying National Science Foundation grants together with the P.I. of this research to further improve and enhance the educational needs of the cybersecurity students.

References

1. Taylor-Jackson, J., McAlaney, J., Foster, J. L., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating psychology into cyber security education: a pedagogical approach. In *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24* (pp. 207-217). Springer International Publishing.
2. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.
3. AL-Nuaimi, M. N. (2024). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review. *Global Knowledge, Memory and Communication*, *73*(1/2), 1-23.
4. Mukherjee, M., Le, N. T., Chow, Y. W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information*, *15*(2), 117.
5. Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024, March). A Critical Review of Cybersecurity Education in the United States. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1* (pp. 241-247).
6. Cybersecurity Workforce Supply and Demand Final Report, May 2024 file:///C:/Users/HP/Downloads/ncses-cwdi-supply-demand-report%20(1).pdf
7. U.S. Bureau of Labor Statistics, Information Security Analyst, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
8. Hammad, E., Wang, Y., Nelson, J. K., Manley, H. A., & Scarmardo, C. (2024). Towards Models for Cybersecurity Summer Research Institutes for Undergraduate Engagement and Education.
9. Janeja, V. P., Seaman, C., Kephart, K., Gangopadhyay, A., & Everhart, A. (2016, September). Cybersecurity workforce development: A peer mentoring approach. In *2016 IEEE conference on intelligence and security informatics (ISI)* (pp. 267-272). IEEE.