Issues in Information Systems
Volume 24, Issue 2, pp. 33-45, 2023

DOI: https://doi.org/10.48009/2_iis_2023_104

The changing landscape in cybersecurity education, the impact of COVID-19, and the promise of online education programs

Cassie Longhart, *Purdue Global, cassie.longhart@purdueglobal.edu*
Jacob Mack, *Purdue Global, Jacob.mack@purdueglobal.edu*

Abstract

Over the past few years, the use of technology has increased significantly causing more demand for cybersecurity professionals. During the pandemic universities, companies, and schools transitioned to online courses, seminars, and meetings. This research will demonstrate the perception students and faculty have toward the success of online learning in a cybersecurity program at Purdue Global. This study will be non-experimental and uses quantitative data collected through a survey. This study will help provide an understanding of how students and faculty feel about the current cybersecurity courses, and how the online courses compare to that of a traditional course through literature review. According to Krieder & Almalag (2019), despite the government and NICE framework efforts, there is still a gap between the professional needs and those who are qualified for these positions. The literature focuses on program implementation and less on the quality of outcomes. Therefore, this study will bring value to how well online courses affect outcomes, satisfaction, and job readiness.

Keywords: cybersecurity, COVID-19, online education, asynchronous

Introduction

As online cybersecurity education continues to become a more common learning modality across the U.S. and those with the National Security Agency (NSA) Center of Excellence (CAE) designation continue to rise, it is important to understand better how students receiving the education and faculty providing the education perceive the overall quality of their respective cybersecurity programs. COVID changed the educational, training, and professional testing landscape significantly and contributed to alterations to general cybersecurity behaviors. Since Purdue Global is an online Institution and is CAE designated, it is beneficial to understand how these cohorts perceive the usefulness and educational quality of their respective programs.

This research study evaluated the perception of students and faculty on the quality of the cybersecurity education program at Purdue Global. Currently Purdue Global has several online cybersecurity options for students to enroll in. The study allowed the researchers to have a better understanding of course satisfaction with non-traditional courses compared to traditional courses through previous research. In addition, this quantitative non-experimental study provides the opportunity to understand what has changed with education perspectives before the pandemic and during the pandemic. The pandemic has especially altered cybersecurity practices and educational efforts. This study sought to uncover key attitudes and sentiments regarding the online education delivery of cybersecurity programs at a non-profit, public University, Purdue Global.

Literature Review

The literature review was conducted using Google Scholar and ProQuest search engines. The following keywords were used to retrieve relevant research over the past ten years:

- Online cybersecurity education
- CAE-accredited schools
- Online cybersecurity universities versus traditional universities
- COVID and online cybersecurity education
- Student perceptions of online cybersecurity programs
- Faculty perception of online cybersecurity programs
- Effectiveness of online cybersecurity programs in higher education
- Satisfaction with online cybersecurity degree programs

Each search yielded different results that included about 30,000 articles. Most of the literature focused on COVID's effects on education and cybersecurity. The literature was narrowed down to those directly related to cybersecurity behaviors and perception of online versus traditional cybersecurity educational programs before and during the pandemic. Only articles from 2014 and later were chosen to ensure accurate, valid, and current knowledge related to the most recent research. Only 18 articles were retained for the research. These articles represented the best evidence to support the purpose of this study.

The review of recent literature points to overall satisfaction with online education and job readiness. According to Chitkushev et al. (2014), students' satisfaction with the online course strongly correlated with the student's satisfaction with their instructors. The research also indicated the workforce is equally satisfied with students' knowledge and skills. While at the same time, the demand for cybersecurity professionals continues to rise. Therefore, the study will demonstrate the difference between the student's perception and the faculty's perception of course satisfaction.

Cybersecurity Behaviors Before the Pandemic and During the Pandemic

Before the COVID-19 pandemic, cybersecurity behaviors differed from those noted during the pandemic. The primary focus in cybersecurity before the pandemic was geared more toward security, whereas the pandemic brought new cybersecurity challenges, including privacy and fraud. Here the researchers define security as the transactional processes that keep digital systems secure overall and privacy as the state of data within a digital system. According to Kumar et al. (2022), before COVID-19, technical security, security attributes, game-theory attacks, and software vulnerabilities were highlighted compared to ransomware attacks, supply chain disruptions, and digital banking during the pandemic.

Before COVID-19, there was less remote learning or work compared to after COVID-19 arrived. With the pandemic, new challenges associated with digital work, distance learning, and social media usage have come to the forefront of cybersecurity. One of the significant changes included the education platform and e-learning. According to Georgescu (2021), education moved to digital e-learning, social media, and video conferencing during the pandemic, thus raising the risk of cybersecurity. During the pandemic, social media platforms were used more often for educational applications, personal use, and professional meetings. According to Georgescu (2021), Zoom conferencing and Google Classroom significantly increased usage during the pandemic.

Since 2020, digital technology has been used in greater capacity and more diverse areas than ever. Cybersecurity has become more critical with the increase in how technology is utilized, from online

education, training, virtual meetings, social networking, etc... According to Deutron et al. (2022), scams, cyber-crimes, and overall security issues have spiked significantly. This has caused problems across all arenas in the technology world that have cost significant money to fix. The lessons learned from the pandemic have shown the need for cybersecurity education.

Overall Perception of Cybersecurity Education Online versus Traditional Courses

The need for proper knowledge and educational training increases as cybersecurity risk increases. Cybersecurity has always been a significant concern. The pandemic highlighted cybersecurity risks worldwide, making cybersecurity academic courses better understood. Distance learning is becoming more preferred than traditional courses within the latter-mentioned context. Researchers have gauged the perception of students using online, hybrid, and traditional courses. In a recent study conducted by Morales-Romero et al. (2022), about 73.8% of students felt the virtual classroom improved communication and exchange of information between students, and 71.4% of students felt the virtual classroom made them more efficient. During the pandemic, online asynchronous learning became the new norm, the online learning environment allowed adults to obtain an education while working. According to Goerke (2018), research conducted on two courses showed that students had positive perceptions of both traditional and online learning environments and instructor engagement. This demonstrates that the online course room provides a comparable positive and engaging learning environment to the conventional classroom.

Student's Expectations of Cybersecurity Training

In addition to understanding the perception perceived from online courses compared to traditional classes, it is crucial to understand the student's expectations for the learning environment and their understanding of cybersecurity. In a recent study conducted by English & Maguire in 2023, a survey was conducted to understand students' knowledge of cybersecurity demonstrated students had a good idea of what cybersecurity meant, but felt the education was more theoretical and had a stronger desire for real-world application. Providing real-life scenarios for the student greatly benefits preparedness for the workforce. These applications also show applications, understanding, and knowledge of cybersecurity practices. According to A recent study conducted by Affia, et al.in 2022, hackathons provide students with hands-on learning environments with real-world applications that promote teamwork, collaboration, and participation in cybersecurity education. While cybersecurity risk grows, it has been proven that understanding the different education models, theories, and how they relate to the individual learner. According to researchers, creating an educational environment that encourages active involvement successfully engages learners. In another study conducted by Ros et al. in 2020, a game developed using the eleven main themes in cybersecurity was tested to understand the behavior of students who chose to play the game compared to those who did not choose to play and the successful completion. In this study, the students who decided to play the game had a higher success rate than those who did not choose to play. The study also found that confidence, engagement, and usefulness contributed to students' perception of a thriving learning environment.

When developing an online course, it is equally important to understand what students expect to receive from their education to increase successful knowledge and skills related to cybersecurity. In addition to course outcomes, course engagement has been another perception of recent University students. According to Kurucay and Inan (2017), a survey measuring students' satisfaction, learning, and achievement in an online undergraduate program demonstrated students who worked in a group with other students had higher achievement than that compared to working independently. Active engagement, participation, and collaboration show student satisfaction and higher achievements. Instructor engagement, knowledge, and cooperation also ranked high with student satisfaction with online learning platforms. According to

Chitkushev et al. (2014), students overall performance decreased when the student was less satisfied with the course instructor. In a synchronous learning environment, the course instructors engage with students through discussion or live presentations, proving higher performance among students. According to Robles-Gomez et al. (2020), in the distance education of cybersecurity, the learning process for students has changed, causing a focus on keeping students happy to increase retention rates.

Lesson Learned

The technology field is ever-changing and continues to grow, including the demand for cybersecurity professionals and education. According to Towhidi & Pridmore (2023), cybersecurity jobs have increased, and there is difficulty finding skilled employees; therefore, designing education courses that provide theoretical applications aligned with industry needs is complex. A significant gap is associated with skills, knowledge, and understanding of the technology industry. According to Ukwandu et al. (2021), with the rapid growth of machine-to-machine, human-to-machine, artificial intelligence, smart devices, network, and cloud technologies, cybersecurity attacks grow significantly, increasing the demand for a shift in education and programs that support cybersecurity and data science that will lead to better ethics and practices in cybersecurity skills. In addition to better practices, researchers have shown that hands-on applications provide better learning outcomes. According to Sitnikova et al. (2018), hands-on applications such as case studies gradually improve students' skills and understanding of course material and prove that the main dissatisfaction among students related to other students' participation. Thus, proving that students prefer to interact and communicate with other students and the instructor.

In addition, communication and teamwork apply to the learning environment as much as to the workforce. Collaboration improves success in cybersecurity education regardless of hands-on application or theoretical context. According to Wang & Sbeit (2017), teamwork or collaboration in education includes activities in small groups to promote problem-solving, completion of a task, or creation of a product. Synchronous work in the online learning environment allows students to collaborate, communicate, exchange ideas, and improve critical thinking.

Another lesson learned was the number of courses, certificates, or degrees available in cybersecurity. A literature review conducted by Kreider & Almalag in 2019 showed that the most significant gap in cybersecurity higher education was associated with insufficient cybersecurity programs offered, program capacity demand through online options and faculty recruitment, and student flow in programs compared to the need. Even though the demand for cybersecurity education and the need for creating more educational opportunities have increased, is there a concern with recent graduates? In a study by Clair & Girard (2020), overall, supervisors were satisfied with recent graduates and felt they showed appropriate knowledge; skill sets met performance, were willing to learn, and were technically savvy. The research available on recent graduates' satisfaction in the workforce could have been improved; therefore, more research is needed to understand better.

Methodology

This non-experimental quantitative study evaluated the IT/Cybersecurity faculty and students' perception of Purdue Global's educational program. This study provides a better understanding of how faculty and students feel about the education received from the IT/Cybersecurity program at PG through a review of current literature and a survey collected from the faculty and staff. The outcome will provide the school's program data related to growth opportunities and success areas based on feedback from the faculty and students. The study was conducted using a Likert scale survey created using Microsoft Forms. Microsoft Forms allowed the researcher the ability to create the Likert scale questions that could be emailed to

participants and results received electronically to one central location. This quantitative survey included 9 questions containing 1-5 (1- Strongly Disagree, 2- Somewhat Disagree, 3- Neither Agree nor Disagree, 4- Somewhat Agree, 5- Strongly Agree) Likert scales, and 1 question for participant status of student or faculty as seen in Table 2. The data collected was cleaned to remove unqualified participants and analyzed using R coding and Excel to calculate the percentages, median scores, and standard deviation.

Participants

Before interacting with participants, the researchers submitted a full research proposal including survey questions to the IRB board and gained full IRB approval in accordance with the DHHS Regulation for the Protection of Human Subjects (45 CFR 46).

Participants were recruited using the school directory for faculty and students' emails. The survey was sent to faculty members through the University Center for Teaching and Learning (CTL) department. The Assistant Dean of Students (ADOS) Office emailed the survey to the students on behalf of the researchers. The participants were informed of the project, risks associated with the study, and their participation in the study is voluntary, per IRB approval. Participants included current IT/Cybersecurity faculty and students in the undergraduate and graduate programs. If participants did not meet the criteria, they were excluded from participation. According to Wang & Sbeit (2017), social constructivist philosophy states that learning is a social process in which individuals take responsibility for their learning while respecting the contributions of other peers and group members. Therefore, the survey helped provide a better understanding of how students and faculty perceive the learning experience at PG.

Data Collection

Data was collected from a survey that was sent to 1838 students and 37 faculty (n = 1875). The participants were recruited using the CTL faculty email directory and the ADOS active student directory. The link to the survey was emailed by CTL and ADOS. The participant received the informed consent form along with the survey. The informed consent included the background of the study, who is conducting the study, how the information will be used, and contact information to cancel participation. The participants were able to access the survey through an online browser or mobile device. Data were cleaned and analyzed using R coding and Excel. The data analysis provided the needed information to answer the following questions:

1. Does PG's IT/Cybersecurity program provide preparation for cybersecurity positions?
2. Does the National Security Agency Center for Academic Excellence (NSA-CAE) provide necessary standards for student success?
3. Are the hands-On virtual labs preferred over written assignments in training students?
4. Is the online curriculum better at preparing students than the traditional curriculum?
5. Does Purdue Global equally prepare students for cybersecurity roles compared to the traditional course?

According to the National Security Agency/Central Security Service (NSA) (2023), the National Centers of Academic Excellence in Cybersecurity (NCAE-C) is a program that is managed by NSA and aims to manage a collaboration between cybersecurity programs that establishes standards, competency, professional development, integrated cybersecurity practice and engages solutions to challenges with cybersecurity education.

Data Management

To ensure the anonymity of the survey participants, in using Microsoft Forms, the researchers did not collect IP addresses. In addition, the survey did not collect any demographic information to ensure the survey remains anonymous and to protect the participants' privacy. The data were collected over 2 weeks electronically. Once the data was collected, the data was stored on the researcher's flash drive with encryption. This flash drive will be accessible only by using a strong password known to the researcher. The researchers will be the only person to have access. The data will be kept for 5 years per the IRB requirements. After 5 years, the data will be disposed of by wiping the flash drive since there will be no sensitive information collected.

Statistical Analysis

The data was collected using a quantitative survey. The following Likert scale was used to measure participants' responses, scale 1-5 (1- Strongly Disagree 2-Somewhat Disagree 3-Neith Agree/Nor Disagree 4-Somewhat Agree 5-Strongly Agree). The Likert-based questions were analyzed via R and Excel generating cumulative counts, percentages, and relevant charts to better visualize the data for the five questions listed in the data collection section. The statistical analysis of the data will help the researchers and Purdue Global leadership better understand the perceived value of an online CAE-designated cybersecurity education at the University and how this compares to beliefs about cybersecurity education in general and at traditional campus-based Universities. The mean and percentages of each response were performed between critical responses on the survey to see if there is a relationship between certain beliefs and how respondents generally answered the survey.

Results

This study aimed to provide a better understanding of how faculty and students perceived the effectiveness of the IT/Cybersecurity program at PG. The survey will help determine room for improvement for future advancement within the program. The population size for this survey included 1875 (n = 1875) sent via email by the CTL and ADOS departments sent to faculty and students. The data was collected over 2 weeks and yielded 157 responses where 1 response was discarded due to participant did not meet the criteria. Therefore, the sample size was 156 (n = 156). The sample size was appropriate in determining the overall satisfaction with the online cybersecurity program at PG. The sample size n = 156 included 12 faculty and 145 students' responses. (Table 1)

Table 1: Participants

	Total Responses (n = 156)	Percentage
Faculty	12	8
Student	144	92

Overall, the mean response from participants felt the online learning environment could provide preparation for cybersecurity 4.4 and hands-on virtual labs are superior to written assignments 4.5. While it appeared that participants disagreed that the cybersecurity curriculum did not adequately prepare them for their current roles in the workforce 2.7. The mean response of 3.9 might indicate participants are unsure of CAE accreditations requirements (Table 2).

According to current research, Covid brought new meanings to virtual learning environments. Out of 156 (n = 156) responses, 92 percent of faculty strongly agreed that online institutions could provide adequate preparation for cybersecurity positions compared to 59 percent of students. With the challenges Covid-19 brought, virtual learning became the norm for almost 3 years. According to Georgescu (2021), the pandemic forced education to rely on synchronous and asynchronous e-learning environments. Whereas 58 percent of faculty participants neither agreed nor disagreed that traditional universities better prepared students for cybersecurity roles compared to 55 percent of student responses. (Tables 3 & 4)

Table 2: Means and Standard Deviations for each Question.

	N	Mean	Std. Deviation
1. Online institutions can provide preparation for cybersecurity positions?	156	4.4	0.94
2. Center for Academic Excellence (CAE) Accreditation Provides Necessary Standards for Students?	156	3.9	1.10
3. Hands-on virtual labs are superior to written assignments in training students for cybersecurity roles?	156	4.5	0.89
4. Writing assignments are a necessary augment to hands-on virtual labs?	156	3.2	1.29
5. Traditional universities on average better prepare students than online universities for cybersecurity roles?	156	2.6	0.97
6. Online universities on average better prepare students than traditional universities for cybersecurity roles?	156	3.3	0.92
7. Cybersecurity curriculum, in general, does not adequately prepare students for cybersecurity roles?	156	2.7	1.25
8. Purdue Global is adequate in how it prepares students for cybersecurity roles?	156	3.8	1.04
9. Purdue Global prepares students for cybersecurity roles as well as traditional CAE Universities.	156	3.9	1.01

Prior to the pandemic students already attended online universities to obtain a degree. According to Sitnikova et al (2018), students dislike peer assessments and did better overall in the online learning environment when allowed to demonstrate their skills and knowledge through scaffolded assignments. The analysis represented 66 percent of faculty participants strongly agreed that virtual labs were superior to written assignments, compared to 68 percent of student responses. (Table 3 & 4).

According to Affia et al. (2022), students benefit from interventions that support teamwork and collaboration, which promotes participation and interest in the course. Finally, 42 percent of faculty participants in the study either strongly agreed or somewhat agreed that PG prepares their students for current cybersecurity roles as well as the traditional CAE universities. Whereas 34 percent of student participants either strongly agreed or somewhat agreed PG prepares them for current cybersecurity roles.

Overall, the results demonstrate that participants are confident in the online curriculum and PG's cybersecurity program's ability to accurately train and prepare students for current roles compared to other CAE-accredited universities. As noted in Table 3 responses left blank accounted for less than 2 percent of n = 156.

Table 3: Percent of Faculty Responses

	N	1	2	3	4	5	Blanks	Total
1. Online institutions can provide preparation for cybersecurity positions?	12	0	0	0	8	92	0	100
2. Center for Academic Excellence (CAE) Accreditation Provides Necessary Standards for Students?	12	0	9	0	25	50	16	100
3. Hands-on virtual labs are superior to written assignments in training students for cybersecurity roles?	12	0	9	16	9	66	0	100
4. Writing assignments are a necessary augment to hands-on virtual labs?	12	0	0	9	66	16	9	100
5. Traditional universities on average better prepare students than online universities for cybersecurity roles?	12	9	24	58	9	0	0	100
6. Online universities on average better prepare students than traditional universities for cybersecurity roles?	12	0	0	75	25	0	0	100
7. Cybersecurity curriculum, in general, does not adequately prepare students for cybersecurity roles?	12	41	25	9	25	0	0	100
8. Purdue Global is adequate in how it prepares students for cybersecurity roles?	12	0	25	9	25	41	0	100
9. Purdue Global prepares students for cybersecurity roles as well as traditional CAE Universities.	12	0	0	16	42	42	0	100

Table 4: Percent of Student Responses

	N	1	2	3	4	5	Blanks	Total
1. Online institutions can provide preparation for cybersecurity positions?	144	3	1	9	28	59	0	100
2. Center for Academic Excellence (CAE) Accreditation Provides Necessary Standards for Students?	144	3	4	24	36	33	0	100
3. Hands-on virtual labs are superior to written assignments in training students for cybersecurity roles?	144	3	1	5	23	68	0	100
4. Writing assignments are a necessary augment to hands-on virtual labs?	144	13	17	22	33	15	<1	100
5. Traditional universities on average better prepare students than online universities for cybersecurity roles?	144	17	17	55	7	3	1	100
6. Online universities on average better prepare students than traditional universities for cybersecurity roles?	144	4	7	57	17	15	0	100
7. Cybersecurity curriculum, in general, does not adequately prepare students for cybersecurity roles?	144	18	24	32	14	11	1	100
8. Purdue Global is adequate in how it prepares students for cybersecurity roles?	144	3	8	14	51	23	<1	100
9. Purdue Global prepares students for cybersecurity roles as well as traditional CAE Universities.	144	1	5	26	34	34	<1	100

RQ1: *Does PG's IT/Cybersecurity program provide preparation for cybersecurity positions?*

After the final analysis of the faculty and student responses, 41 percent of faculty strongly agreed that PG adequately prepared students for cybersecurity. Whereas 51 percent of students somewhat agreed PG provided them with preparation for cybersecurity positions. Figure 1 also demonstrates that while most faculty and students feel the institution adequately prepares the student for active cybersecurity roles, there are still about 36 percent overall who disagree.

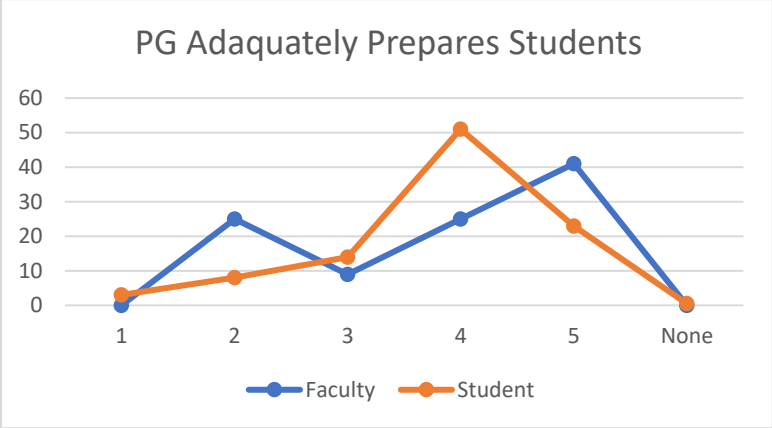

Figure 1: Cybersecurity Preparation

RQ 2: *Does the National Security Agency Center for Academic Excellence (NSA-CAE) provide necessary standards for student success?*

The NSA-CAE is designed to create and manage cybersecurity programs by establishing standards, competency development, providing professional development, integrating practice, and actively engaging the community (National Security Agency/Central Security Service, 2023). The analysis in Figure 2 shows that 50 percent of faculty strongly believed the NSA-CAE provides the necessary standards for the success of students. In addition, about 12 percent of faculty participants did not answer, and about 12 percent disagreed. Whereas 24 percent of students neither agreed nor disagreed and 36 percent somewhat agreed.

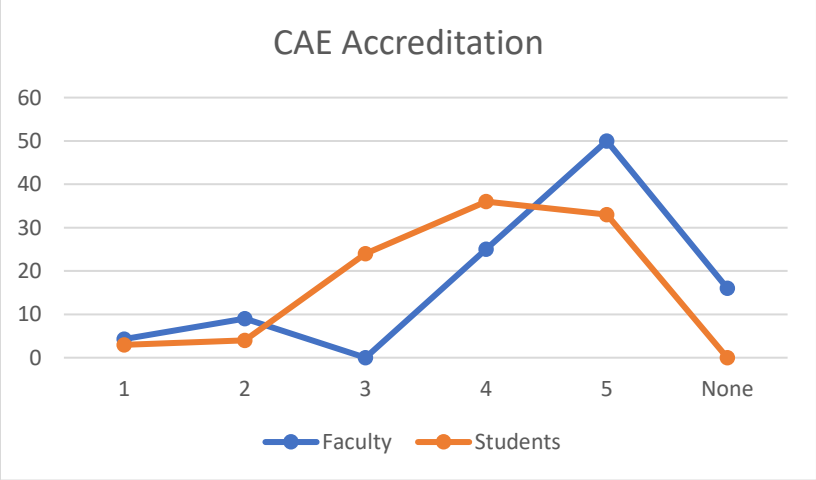

Figure 2: CAE Standards

RQ 3: *Are the hands-On virtual labs preferred over written assignments in training students?*

When it comes to hands-on activities compared to written assignments, it depends on the type of learner the student is. Keeping the interest of students helps promote less dropout rates and participation. A recent study conducted by Robles-Gomez et al. in 2020 concluded that virtual simulations are critical to the threats in the digital era. This study also showed that student attitudes and the usefulness of the lab influenced their participation in virtual labs. Figure 3 demonstrates that 66 percent of Faculty and 68 percent of students strongly prefer hands-on virtual labs compared to written assignments.

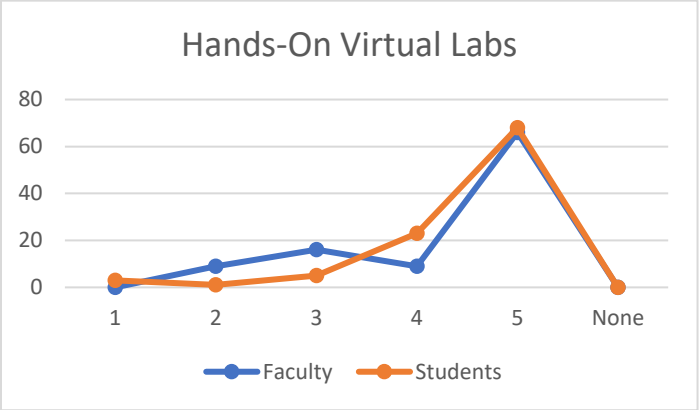

Figure 3: Virtual Labs

RQ 4: *Is the online curriculum better at preparing students than the traditional curriculum?*

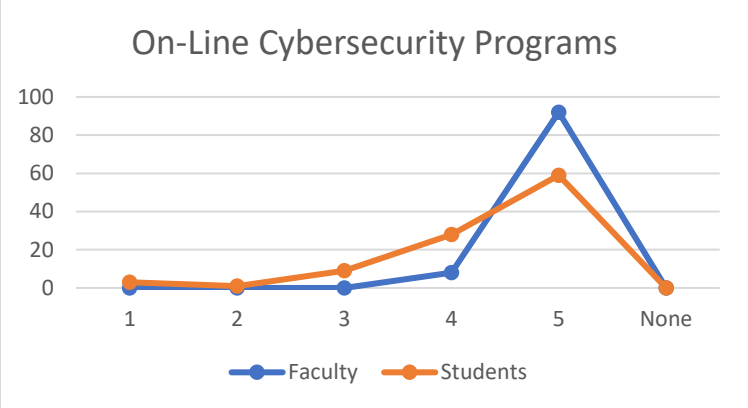

Figure 4: Online Curriculum vs. Traditional Curriculum

Cybersecurity attracts students from all backgrounds. A recent study conducted in 2018 by Sitnikova, et al. showed that many students feel that students preferred the online learning environment over the traditional environment due to the time spent in the course, and difficulty but quality of content despite conflict among group members and lack of participation. In Figure 4, 92 percent of faculty participants strongly agreed that online learning environments better prepared students than traditional courses. While only 59 percent of student participants strongly agreed, it appears that participants feel comfortable with the online learning environment.

RQ 5: *Does Purdue Global equally prepare students for cybersecurity roles compared to the traditional course?*

Figure 5 demonstrates that 34 percent of students and 42 percent of faculty somewhat agree that PG adequately prepares students for cybersecurity roles. Whereas 34 percent of students and 41 percent of faculty strongly agree. While it appears that many of the students and faculty agree PG adequately prepares students in the cybersecurity program, there are still those who do not agree.

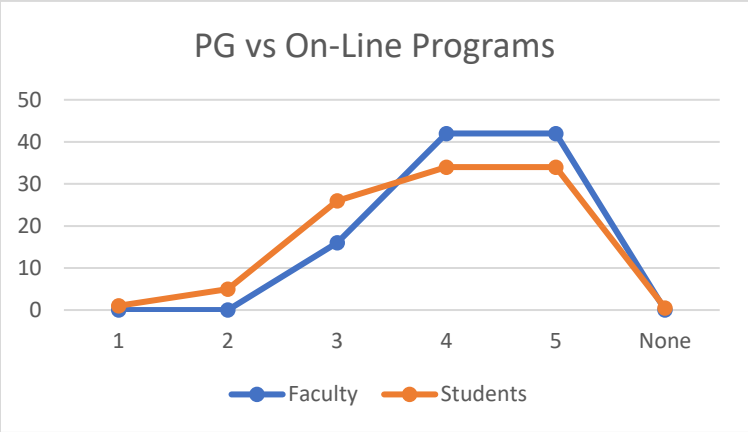

Figure 5: PG and Cybersecurity Preparedness

Discussion, Limitations, and Future Research

Today distance learning is more popular than ten years ago. Since COVID schools, companies, and organizations have proven asynchronous and synchronous learning is comparable to traditional classroom settings. Recent studies found that students tend to do better in an asynchronous environment when they have a positive attitude, timely communication, and feel the content is useful. The NSA-CAE accreditation requires core values that apply to ethical values, sharing, and leading by example. Purdue Global is CAE Cyber Defense accredited. This study aimed to gauge the quality of the cybersecurity program at PG against the perception of current faculty and students of the cybersecurity program.

The study also evaluated current literature comparing traditional universities, online universities, and virtual labs. This study demonstrates students and faculty participants feel comfortable with PG's ability to prepare students for current roles in cybersecurity. In addition, hands-on labs are preferred over written assignments. PG offers the ability for students to engage in asynchronous and synchronous assignments in the online classroom. Students are required to participate in live lectures, complete simulations, and complete written assignments.

The limitations of this study included the sample size being limited to PG faculty and students enrolled in the cybersecurity program, limited research for higher education cybersecurity research, and limited answers for each question. Future research should include increasing the sample size to include traditional and online CAE universities, to prove the validity behind quality cybersecurity online programs compared to traditional university programs. In addition, we recommend more hands-on simulation activities compared to written assignments to gauge competencies such as hack-a-thons. Additional questions concerning the quality of the content and possible overall course completion rates could help understand

the curriculum of these cybersecurity programs. In addition, a comparison of course outcomes from traditional universities and online universities before COVID and post-COVID could help validate the effects of COVID on educational institutions.

Conflicts of Interest

The authors have no conflict of interest.

References

Affia, A., Notle, A., & Matulevicius, R. (2022). Integrating hackathons into an online cybersecurity course. *Association for Computing Machinery. P. 134-145.* https://doi.org/10.1145/3510456.3514151

Chitkushev, L., Vodenska, I., & Zlateva, T. (2014). Digital learning impact factors: student satisfaction and performance in online courses. *International Journal of Information and Education Technology.* 4(4). https://DOI:10.7763/IJIET.2014.V4.429

Clair, N. & Girard, J. (2020). Are cybersecurity professionals satisfied with recent cybersecurity graduates. *Journal of The Colloquium for Information Systems Security Education* 7(1). https://cisse.info/journal/index.php/cisse/article/view/103/103

Deutrom, J., Katos, V., & Ali, R. (2022). Loneliness, life satisfaction, problematic internet use and security behaviors: Re-examining the relationships when working from home during COVID-19. *Behavior & Information Technology.* 41(14) p. 3161-3175. https://doi.org/10.1080/0144929X.2021.1973107

English, R. & Maguire, J. (2023). Exploring student perceptions and expectations of cyber security. *Proceedings of the 7th Conference on Computing Education Practice.* p.25-28. https://doi.org/10.1145/3573260.3573267

Georgescu, T. (2021). A study on how the pandemic changed the cybersecurity landscape. *Informatica Economica.* 25(1). https://10.24818/issn14531305/25.1.2021.04

Goerke, L. F. (2018). Student Satisfaction in Traditional, Online, and Hybrid Continuing Education Course: A Case Study. https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/ep_0001_goerke_student_satisfaction_education.pdf

Kreider, C. & Almalag, M. (2019). A framework for cybersecurity gap analysis in higher education. *Association for Information Systems.* https://aisel.aisnet.org/sais2019/6

Kumar, R., Sharma, S., Vachhani, C., & Yadav, N. (2022). What changed in the cyber-security after COVID-19. *National Library of Medicine.* https://doi.org/10.1016%2Fj.cose.2022.102821

Kurucay, M. & Inan, F. (2017). Examining the effects of learner-learner interactions on satisfaction and learning in an online undergraduate course. *Computers & Education.* 115. p. 20-37. https://doi.org/10.1016/j.compedu.2017.06.010

Morales-Romero, G., Quispe-Andia, A., Leon-Valarde, C., Aybar-Bellido, I., Auqui-Ramos, E., Quispe-Guia, S., & Palacios-Huaraca, C. (2022). Asynchronous learning: evaluation of virtual classroom metrics according to the perception of university students. *Indonesian Journal of Electrical Engineering and Science.* 28(2). P 1058-1066. https://DOI:10.11591/ijeecs.v28.i2.pp1058-1066

National Security Agency/Central Security Service. (2023). National centers of academic excellence in cybersecurity. https://www.nsa.gov/Academics/Centers-of-Academic excellence/

Robles-Gomez, A., Tobarra, L., Pastor-Vargas, R., Hernandez, R., & Cano, J. (2020) Emulating and evaluating virtual remote laboratories for cybersecurity. *Sensors.* 20(11). https://doi.org/10.3390/s20113011

Ros, S., Gonzalez, S., Robles, A., Tobarra, L., Caminero, A., & Cano, J. (2020). analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course. *IEEE Access.* 8, p 97718-97728 https://doi:10.1109/ACCESS.2020.2996361

Sitnikova, E., Saberi, M., Joiner, K., Townsend, D., & Robertson, E. (2018). Lessons learned: understanding online engagement satisfaction in a large postgraduate information assurance principles (IAP) course. *Australasian Association for Engineering Education.* http://18aaee.s3.amazonaws.com/proceedings/AAEE18_Sitnikova_68.pdf

Towhidi, G. & Pridmore, J. (2023). Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education.* 34(1), p 70-83. https://jise.org/Volume34/n1/JISE2023v34n1pp70-83.html

Ukwandu, E., Okafor, E., Ikerionwu, C., Olebara, C., & Ugwu, C. (2021). cyber-security in the emerging world of 'smart everything'. https://arxiv.org/ftp/arxiv/papers/2109/2109.05821.pdf

Wang, P. & Sbeit, R. (2017). A constructive team project model for online cybersecurity education. *Issues in Information Systems.* 18(3), p 19-28. https://doi.org/10.48009/3_iis_2017_19-28