Navigating Challenges in Online Cybersecurity Education: Insights from Postgraduate Students and Prospects for a Standardized Framework

SALEM, Maher, SAMARA, Khalid and AL-TAMIMI, Abdel-Karim <http://orcid.org/0000-0003-2459-0298>

Navigating Challenges in Online Cybersecurity Education: Insights from Postgraduate Students and Prospects for a Standardized Framework

MAHER SALEM*

King's College London, Informatics, London, UK, maher.salem@kcl.ac.uk

KHALID SAMARA

Oryx Universal College, School of Business & Leadership, Doha, Qatar, khalid.s@oryx.edu.qa

AL-TAMIMI, ABDEL-KARIM

Sheffield Hallam University, School of Computing and Digital Technologies, Sheffield, UK, a.al-tamimi@shu.ac.uk

Yarmouk University, Department of Computer Engineering, Irbid, Jordan, altamimi@yu.edu.jo

This study focuses on the challenges encountered in online cybersecurity education. It adopts an exploratory research design using a mixed-methods approach to investigate the perceptions and experiences of postgraduate students enrolled in an online cybersecurity program. The collection of data is structured into two distinct phases. In the initial phase, qualitative insights are gathered through workshops with students and industry experts, followed by administering a questionnaire to delve deeper into students' perceptions and challenges. Thematic analysis of the responses reveals significant interest in online cybersecurity programs but also highlights issues such as ineffective communication and poor engagement. The findings highlight the necessity for a standardized framework to improve communication, engagement, and overall effectiveness in virtual learning environments. By empowering instructors to design more interactive courses and leveraging technology efficiently, the framework aims to improve student motivation, satisfaction, and learning outcomes. Moreover, it serves as a valuable resource for institutions, fostering collaboration and innovation in cybersecurity education. Implementing this framework will create a more conducive learning environment, directly enhancing student preparation for success in the dynamic field of cybersecurity.

CCS CONCEPTS • Social and professional topics. Professional topics. Computing education. Computing education programs.

Additional Keywords and Phrases: Cybersecurity Education, Distance Learning, Student Perceptions, Online Learning Challenges, Technology-supported learning environments

ACM Reference Format:

First Author's Name, Initials, and Last Name, Second Author's Name, Initials, and Last Name, and Third Author's Name, Initials, and Last Name. 2018. The Title of the Paper: ACM Conference Proceedings Manuscript Submission Template: This is the subtitle of the paper, this document both explains and embodies the submission format for authors using Word. In Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY. ACM, New York, NY, USA, 10 pages. NOTE: This block will be automatically generated when manuscripts are processed after acceptance.

1 INTRODUCTION

Cybersecurity has emerged as a critical discipline, intricately woven into the fabric of modern technology, serving as a formidable defense against the ever-evolving landscape of cyber threats, including sophisticated malware, advanced persistent threats, and anomalous activities. Recognizing the paramount importance of cybersecurity, organizations have made substantial investments in comprehensive training and awareness programs, aimed at fortifying the knowledge and threat awareness of their employees and clientele (Aldawood & Skinner, 2019).

The journey to acquiring cybersecurity skills encompasses a diverse array of pathways, ranging from dedicated training programs and the pursuit of industry-recognized professional certifications to self-guided learning and hands-on practical experience. However, it is widely acknowledged that the foundational theoretical and practical knowledge required in this field is primarily acquired through formal higher education programs, which provide a structured and comprehensive curriculum in cybersecurity principles, technologies, and best practices (Fantinelli, Cortini , Fiore, lervese, & Galanti , 2024).

Higher education institutions, acknowledged for their expertise in offering flexible learning opportunities, have embraced various modalities such as distance, hybrid, and online learning. These approaches accommodate not only to local students but also reach international learners, reflecting the ongoing demand for education that accommodates work commitments, familial responsibilities, and social obligations (Palvia, et al., 2018). Within the expansive landscape of higher education, cybersecurity courses become essential, enhancing both undergraduate and postgraduate programs. Usually located within departments like engineering, computer science, and business and management, these courses focus intensively on information security (Shoemaker, Kohnke, & Sigler, 2018), (Baskakova, Belash, & Shaposhnikov, 2021).

The popularity of cybersecurity programs, however, is met with several challenges. Despite the available pathways, several challenges persist in cybersecurity education and training, including a lack of intrinsic motivation among learners, technological barriers that hinder effective learning experiences, and difficulties in fostering meaningful learner-instructor interactions—particularly in student-centric environments that prioritize active engagement and self-directed learning. (Baburajan, Noushad, Faisal, & Awawdeh, 2022). The effectiveness of cybersecurity education is further underscored by the realization that students' exposure to cybersecurity issues profoundly depends on the instructional methodologies employed in their degree programs. Consequently, the development of robust problem-solving skills often lags, posing challenges when graduates confront real-world cybersecurity scenarios. Compounding this, the cybersecurity industry deals with a persistent shortage of skilled professionals, attributing this deficiency to the insufficient number of individuals possessing the requisite expertise and experience for cybersecurity roles (Kreider, & Almalag, 2019), (Legg, 2021).

In response to these multifaceted challenges, this paper goes beyond analysis and critique; it endeavors to contribute to the advancement of cybersecurity education by proposing a comprehensive framework tailored to the needs of higher education. The framework aims to address dimensions of cybersecurity education, including pedagogical strategies, technological integration, fostering effective learner-instructor engagement, and aligning curriculum content with real-world industry demands. By defining a robust framework, this study seeks to offer actionable insights and recommendations to enhance the delivery and effectiveness of cybersecurity education programs in higher education. Conducted in two phases, the study employs a mixed-methods qualitative approach, with workshops involving industry experts and a subsequent questionnaire, offering an exploration of post-graduate students' experiences in a full-time online cybersecurity program. This holistic approach serves as the foundation for the proposed framework, positioning it as a valuable contribution to the ongoing discourse on optimizing cybersecurity education in higher learning environments.

In the following sections, the paper proceeds to comprehensively review the literature on online learning, explaining existing barriers. Subsequent sections detail the methodology, data collection and analysis methods, present findings, and

engage in insightful discussions. The study concludes by highlighting its limitations and emphasizing its contributions to the substantive field, laying the groundwork for a refined understanding of and potential enhancements to the delivery of cybersecurity education in higher education. This proposed framework serves not only as a guide for educators and institutions but also as a blueprint for future research endeavors aimed at continually refining and evolving cybersecurity education in response to the dynamic landscape of digital threats and industry needs.

2 LITERATURE REVIEW

2.1 Online Learning

Online learning has become an essential method of instruction for most higher education institutions (Lomellini, Lowenthal, Snelson, & Trespalacios, 2022), (Deeley, 2018). There is also considerable literature that has examined different methods for highlighting the benefits of deploying online learning in higher education (Castro & Tumibay , 2019), (Dumford & Miller, 2018), (Sun & Chen, 2016). Stephani et al., (Stephani, Alvin, & Riatun, 2023) investigated the motivations behind students preferring online learning amid the challenges in communication and time management. Using a qualitative approach, their study identified four key motivations namely flexibility, learning, interaction, and expression. The conclusion underscored the crucial role of motivation in shaping student behaviors and satisfaction, offering practical implications for tailored activity design. The study also highlighted the benefits of online learning and proposed an explorative framework for understanding motivations.

Lomellini et al., (Lomellini, Lowenthal, Snelson, & Trespalacios, 2022) examined the role of leaders in higher education online learning in promoting accessibility and inclusivity, focusing on disabled students. Through interviews with nine leaders, the study highlighted varying perceptions and challenges, highlighting the need for buy-in from senior leadership. Despite limitations, the study underlined the crucial role of online learning leaders in addressing accessibility challenges and advocated for a deeper understanding of leadership perspectives to enhance inclusive online education, particularly for disabled students.

Naeem and Bosman made a significant contribution to student engagement by investigating the effectiveness of various on-campus learning activities on first-year students' engagement (Naeem & Bosman, 2023). The authors employed an online pedagogic framework in a programming module, emphasizing virtual labs as a means to evaluate student engagement. Consequently, the positive feedback received endorsed the use of virtual labs in online learning, establishing a positive engagement metric. Expanding on this, Indumathi et al., (Indumathi, Evangelista, & Wang, 2023) presented a generalized concept comparing students' performance in online versus face-to-face settings, with a focus on a specific degree program in civil engineering. In their evaluation study, remote labs emerged as an excellent platform for both online and on-campus learning. As a result, enhanced motivation, contribution, and academic success, ultimately confirming the positive impact of online learning on student performance. Further contributing to this narrative, Ebojoh and Xu's study evaluated the effectiveness of assessments and delivery methods in online learning over a three-month period (Xu & Ebojoh, 2007). While satisfaction with assessment tools was predominant, significant concerns surfaced regarding communication, course delivery and design. Consequently, the research highlights the need for substantial improvements in design delivery, suggesting interactive technologies such as discussion forums and video conferencing for enhancing program effectiveness.

A study by Yang et al., explored the growing trends for inclusivity in online learning and the challenges associated with applying universal design (UD) principles (Yang, et al., 2024). Through a systematic analysis of relevant studies, they identified trends, strategies, impacts, and challenges of integrating UD into online education. Their study highlighted the

importance of aligning course goals with UD principles and suggested professional development and collaborative efforts among instructors to overcome implementation challenges. Ultimately, the study underscored the broader benefits of UD strategies for serving diverse student populations effectively. However, its application in online education presents notable challenges for instructors, compounded by various barriers. Moreover, evidence-based strategies for integrating UD into online learning remain unclear (Griful-Freixenet, Struyven, Vantieghem , & Gheyssens, 2020).

Brooks et al., explored the transition to online learning prompted by the COVID-19 pandemic, with a particular focus on computer science instructors in a Midwestern university (Brooks, , Hardin, Scianna, Berland, & Legault, 2021). The study tackled the complexities encountered and the actions taken during this transition, highlighting the importance of documenting experiences and lessons learned. The main conclusion of the study highlights the continued challenges with scheduling across diverse time zones, suggesting the need for additional research into the challenges and effective strategies when transitioning reluctantly to online teaching. The results also offer important insights and teaching recommendations, guiding current decision-making in education, and suggesting further investigation in diverse educational settings (Castro & Tumibay , 2019).

Brown et al., investigated university students' perceptions of online learning during the 2020/21 academic year, which was marked by the Covid-19 pandemic and subsequent lockdowns (Brown, et al., 2023). The research included 13 focus groups and a subsequent survey with 759 participants across higher education institutions in Wales. Thematic analysis of the focus group discussions identified eight key themes, encompassing positive experiences, learning facilitators and barriers, community loss, university-related disappointments, workload, assessment, and health/well-being. The survey revealed overall satisfaction with online learning quality but highlighted challenges such as community absence, well-being concerns, loneliness, and isolation. The insights from both focus groups and the survey inform valuable recommendations for teaching practices, institutional strategies, and considerations for student health and well-being.

A study by Gama et al., explored how an online hackathon was used as a method to boost student participation in a distributed applications course during Emergency Remote Teaching (ERT) (Gama, Zimmerle, & Rossi, 2021). By using an online platform for real-time collaboration, this approach successfully tackled issues linked to decreased engagement. Although there might be some participant bias, students shared positive results, expressing higher motivation and improved learning.

In a study focusing on cybersecurity in the online learning approach, Prasad et al., explored students' perceptions and engagement during a 12-week online Python programming course with a focus on cybersecurity (Prasad, Balse, & Warriem, 2023). The concept of "transactional distance," which reflects the psychological and communication gap resulting from spatial separation, is examined. The study's findings revealed that mitigating the perceived distance between learners and instructors significantly enhances students' sense of belonging and satisfaction in online programming courses. These insightful conclusions hold profound implications for instructors and researchers striving to improve cybersecurity education in online and distance learning contexts, informing strategies to foster more engaging, supportive, and effective virtual learning environments.

As discussed in this section, existing research unequivocally acknowledges the efficacy of online learning modalities; however, a consensus emerges on the pressing need for substantive enhancements (Ferrer, Ringer, Saville, Parris, & Kashi, 2022). While the above studies focused on aspects relating to cybersecurity in education and how they have been used to promote the academic success of students, relatively little work has been undertaken to evaluate online cybersecurity programs – as a whole – and the online tasks undertaken within the context of real-life pedagogical activities in the higher education setting. Therefore, despite these efforts, there has been a relative paucity of research dedicated to examining the pedagogical elements underpinning online cybersecurity teaching and learning strategies in higher education. In addition,

many such studies fail to account for the various actors (instructor-student and student-student) engaged in online cybersecurity programs, along with the interactions and online learning pedagogy aimed at supporting them (Salem, Samara, Pray, & Hussein, 2024). Thus, this study attempts to fill this gap and provide a more encompassing framework and critically examine those multifaceted dimensions of online cybersecurity programs, placing particular emphasis on the pedagogy of online cybersecurity programs in higher education, thus making a valuable contribution to the field.

2.2 Cybersecurity Education Frameworks

As the online learning approaches demonstrate their feasibility, higher education institutions are increasingly incorporating them to deliver cybersecurity courses for both undergraduate and postgraduate students (Nolte, Affia, & Matulevičius, 2022) and (Ali , Lundqvist, Watterson, & Baghaei, 2020). In light of these challenges and the recognized need for improvements, a growing body of research has begun to explore the imperative of developing a comprehensive cybersecurity framework tailored specifically for higher education institutions (Salem, Samara, Pray, & Hussein, 2024).

A research study led by Goupil et al., addressed the severe global shortage of over 3 million skilled cybersecurity professionals by correlating job advertisements with academic curricula (Goupil, et al., 2022). Identifying significant gaps in key skill categories, the study highlights the dynamic nature of these shortages and advocates for periodic reassessment using automated analysis tools. The findings underline the necessity of a comprehensive cybersecurity education approach, encompassing both technical and managerial aspects. This study contributes valuable insights to the literature, emphasizing the ongoing evolution of cybersecurity skill landscapes.

Another study by Dragoni et al., (Dragoni, Lafuente, Massacci, & Schlichtkrull, 2021) addresses the question of whether European universities adequately prepare students in building security in higher education. A comprehensive review of over 100 M.Sc. programs in the field of cybersecurity across 28 countries reveals that the current educational landscape lacks the necessary emphasis on developing pertinent skills related to cybersecurity. Moreover, it aims to assist decision-makers, such as program leaders and policymakers, in recognizing and prioritizing skills essential for industry and government needs. This finding highlights a significant gap in cybersecurity education programs and underscores the need for further investigation and improvements in curriculum design (Salem, Samara, Pray, & Hussein, 2024).

A study by Kreider and Almalag addressed the persistent cybersecurity skills gap by proposing a comprehensive framework that goes beyond traditional curricular evaluations (Kreider, & Almalag, 2019). In contrast to existing models, the proposed framework considers program capacity and the student pipeline, providing a holistic perspective for higher education institutions. Despite limitations in the quantitative approach and the literature review's brevity, the framework makes a unique contribution to understanding and mitigating the involved challenges of the cybersecurity skills gap. The proposed work provided further research on validating the framework, conducting a comprehensive literature review, and operationalizing identified dimensions for enhanced applicability.

On the other hand, Crick et al., provided a focused examination of cybersecurity education through a case study approach, concentrating on general computer science students in the UK (Crick, Davenport, Irons, & Prickett, 2019). It addresses critical questions regarding curriculum content, teaching approaches, and the impact of national accreditation. The findings underscored the positive influence of accreditation on universities and pointed out the need for international collaboration within the computer science academic community. By presenting a comparative analysis with the US, the study offered insights for ongoing research, curriculum development, and the advancement of effective cybersecurity education practices.

Other researchers focused on designing a cybersecurity awareness framework such as the one proposed by Khader et al., (Khader, Karam, & Fares, 2021). Their research addresses a notable gap by introducing a tailored Cybersecurity

Awareness Framework (CAFA) for academic institutions. The conceptual framework is designed to systematically improve the integration, delivery, and assessment of cybersecurity knowledge across various university disciplines, fostering comprehensive awareness among graduates. It provides a flexible blueprint for institutions to formulate policies and procedures, ensuring the effective promotion of cybersecurity awareness within academic settings. In addition, it supports the establishment of entities like the Cybersecurity Awareness Center (CAC) and office of Information and Communication Technology Support (ICTS), aiding operational efficiency and adaptability.

González-Manzano and Fuentes (González-Manzano & de Fuentes, 2019) addressed the challenge of designing effective online cybersecurity courses by providing recommendations based on the analysis of 35 free courses using NIST's NICE (Alsmadi & Easttom, 2020) reference framework. The analysis reveals gaps in existing training programs, suggesting areas for improvement and the creation of new courses. The paper introduced an open-source framework for analyzing students' performance in EdX MOOCs to support further research. The conclusion underscored the demand for cybersecurity professionals, the importance of addressing identified gaps, and the potential for developing new courses.

A similar study conducted by Hajny et al., addressed the need for effective cybersecurity education and training by proposing practical tools and strategies for higher education institutions to design comprehensive cybersecurity curricula (Hajny, et al., 2021). The study involved the analysis of 89 existing global study programs, incorporating recommendations from renowned institutions within and outside the EU. The authors presented a comprehensive survey along with a dynamic web application, "Education Map," to offer insights into the current state of cybersecurity education. The SPARTA Cybersecurity Skills Framework is introduced as a crucial link between work roles and required expertise, aiding in the development of curricula aligned with job market demands. The paper's approach, which integrates global program analysis, renowned recommendations, and a practical framework, demonstrates a holistic strategy for higher education institutions. The inclusion of the SPARTA Cybersecurity Skills Framework is particularly noteworthy, serving as a valuable bridge between industry work roles and required expertise. However, it's essential to explore areas where the proposed framework or approach might fall short or face practical challenges in implementation.

However, despite these insightful studies, a more profound understanding of the effectiveness of online studies in the cybersecurity program's context remains vague for researchers. Consequently, our study aims to bridge this gap by considering all the aforementioned factors in the evaluation of an online cybersecurity program and by proposing a practical framework for online cybersecurity in higher education.

2.3 Double Diamond Model

In the journey of designing an effective online cybersecurity programme, understanding the concerns and preferences of learners and domain experts is paramount. To design an effective online cybersecurity program, the research team employed the double diamond methodology, which was introduced by the design council (Council Design, 2024) as shown in figure 1, a user-centric approach that emphasizes rigorous discovery, definition, development, and delivery phases. This section, describes the detailed process undertaken in the initial phase of the Double Diamond Model, focusing on discovery and definition. The Double Diamond Model has been extensively utilized in various higher education research projects, emphasizing its effectiveness in guiding design processes and fostering multidisciplinary collaboration. Ojasalo et al. (2022) applied the model to a service design project in higher education, where it facilitated the creation of a new pricing model for the mobile game industry. The four phases—discover, define, develop, and deliver—helped students achieve practical insights and iterate effectively.

Abensur et al. (2023) extended the application of the Double Diamond Model to bioengineering, utilizing it to overcome infrastructure limitations faced by an inkjet bioprinter research team. Their findings emphasize the model's ability to

support multidisciplinary collaboration and user-centred design, crucial for tackling complex challenges in health research. However, the authors highlight the model's complexity and subjectivity, suggesting the need for additional guidelines to optimize its use.

Similarly, Luojus et al. (2015) employed the Double Diamond Model in the WeLive project to guide the creation of digital services through collaboration between students, companies, and public stakeholders. The model was found to be flexible and effective in this context due to its user-centred approach. Wang et al. (2023) also found the model useful in the design of a project-based teaching platform, particularly in identifying stakeholder needs and developing key service concepts.

Mitchell et al. (2020) applied the Double Diamond Model in a user experience design (UXD) pedagogy, focusing on designing digital touch communications. The four phases provided a framework for students to explore innovative digital touch concepts. While the model was effective in promoting divergent and convergent thinking, the study highlighted limitations in the students' engagement with the sensory and experiential dimensions of touch. The authors called for additional tools to enhance the exploration of touch's social meanings and nuances in the design process.

Overall, the Double Diamond Model serves as a robust framework for teaching in the cybersecurity context due to its structured yet flexible approach to problem-solving and curriculum development. By emphasizing the iterative phases of discovery, definition, development, and delivery, this model aligns seamlessly with the dynamic nature of cybersecurity—a field that necessitates continuous adaptation to emerging threats and technological advancements. Its user-centric focus underscores the importance of understanding the needs and preferences of learners and industry stakeholders, allowing educators to tailor the curriculum to foster relevant skill sets. The model's iterative nature facilitates continuous improvement in course design and delivery, encouraging regular feedback from students and experts, which is essential for maintaining educational effectiveness. Furthermore, the Double Diamond Model promotes multidisciplinary collaboration, integrating diverse perspectives into the curriculum, thereby enriching the learning experience and preparing students to work in interdisciplinary teams. By engaging in hands-on projects, students apply theoretical concepts to practical scenarios, fostering critical thinking and problem-solving skills essential in the field. Finally, the model provides a structured framework for reflection and evaluation, enabling ongoing enhancements that align with industry standards and learner needs. In summary, the Double Diamond Model not only supports pedagogical processes but also enhances the alignment of educational outcomes with the competencies required in cybersecurity, fostering an enriching learning environment that prepares students to navigate its complexities effectively.

3 METHODOLOGY

3.1 Methodology Overview

In the initial discovery phase, the team sought to gather comprehensive insights into the needs, concerns, and preferences of key stakeholders – learners and industry experts. A multimodal data collection strategy was implemented spanning two phases. This dual-pronged strategy is aimed at capturing relevant insights into the learners' experiences and expectations within the online cybersecurity learning domain.

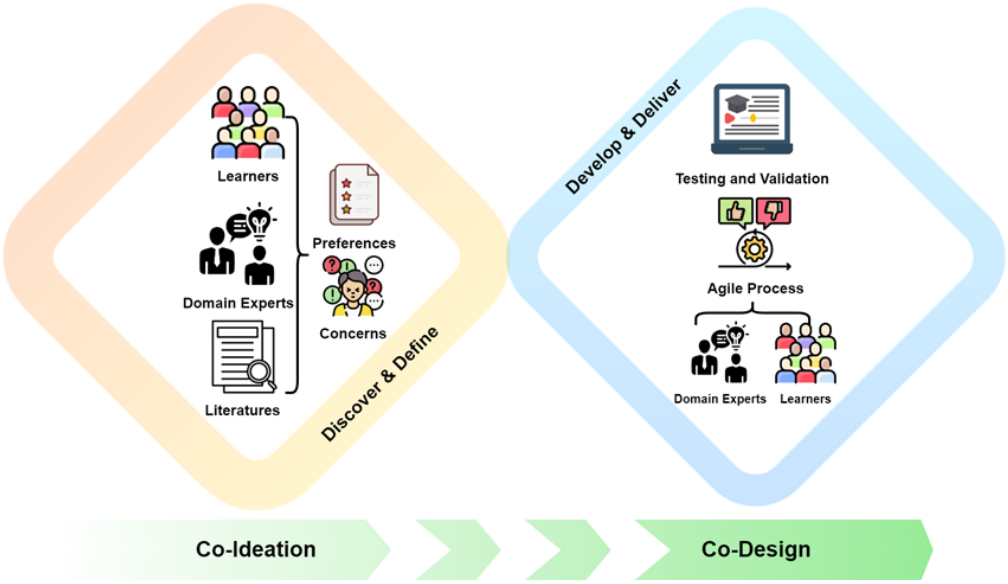

Figure 1. Double Diamond Model for Co-Designing a Cybersecurity Online Programme

3.1.1Phase 1: Workshop Engagement

The initial phase of our research involved a focused workshop designed to elicit in-depth reflections on online learning experiences from a cohort of postgraduate cybersecurity students. Through facilitated discussions, participants were encouraged to articulate their challenges, satisfactions, and suggestions, providing valuable insights into the key factors influencing online learning effectiveness. To enhance the richness of the discussions and contextualize the students' perspectives within a broader industry context, two seasoned cybersecurity experts were invited to participate in the workshop. Their contributions offered valuable insights into industry best practices and expectations, enriching the dialogue and ensuring that the workshop's findings were grounded in real-world experience. The workshop agenda included the following key topics:

- **Online Learning Challenges:** Participants discussed common challenges faced in online learning environments, such as technical difficulties, time management issues, and lack of face-to-face interaction.
- **Effective Online Learning Strategies:** Students shared their strategies for successful online learning, including time management techniques, study habits, and engagement with course materials.
- **Feedback and Suggestions:** Participants provided feedback on their online learning experiences and offered suggestions for improvement, such as increased opportunities for collaboration and personalized support.
- **Industry Perspectives:** The industry experts shared their insights on the skills and competencies required for success in the cybersecurity field, highlighting the importance of continuous learning and adaptation to emerging threats.

The decision to involve two experts in this research was informed by several factors. First, the experts possessed a deep and specialized understanding of cybersecurity and online learning, ensuring that their insights were highly valuable and relevant to the research objectives. Second, the exploratory nature of the workshop and the qualitative focus of the research

made a smaller sample size appropriate. Third, while we would have ideally interviewed more experts, practical constraints such as time limitations and the availability of suitable candidates prevented us from expanding the sample.

Furthermore, during the workshop, we observed a phenomenon known as data saturation, where additional participants were unlikely to provide significantly new or different insights. This indicated that the two experts we interviewed were sufficient to capture the key themes and perspectives relevant to our research.

To enhance the validity and reliability of our findings, we also employed methodological triangulation by combining expert interviews with other data sources, such as the questionnaire. This approach helped to strengthen the credibility of our research and provided a more comprehensive understanding of online learning effectiveness in cybersecurity education.

3.1.2Phase 2: Questionnaire Design

Building upon the qualitative narratives extracted from the workshop sessions, the second phase involved the systematic construction of a comprehensive questionnaire. This instrument incorporated a blend of closed and open-ended questions, strategically formulated to elicit multifaceted feedback from the participants.

The questionnaire was carefully crafted to probe into various dimensions of online cybersecurity education, including pedagogical approaches, technological infrastructure, assessment methodologies, and learner support mechanisms. By delving into these dimensions, prevalent concerns and preferences emerged organically, providing valuable insights for subsequent phases of the design process.

3.1.3Implications for Programme Design

The qualitative data collected from both phases of data collection served as foundational inputs, furnishing the design team with a rich number of perspectives and experiences. These insights were instrumental in setting the contours of the emerging framework, guiding subsequent design decisions towards greater alignment with learners' needs and industry imperatives. The findings from the discovery phase highlighted the crucial need to develop an online cybersecurity program that strikes a balance between strong academic rigour and close alignment with the real-world demands and realities of the cybersecurity industry. The detailed insights into learners' concerns and preferences will guide the following stages of the design process, enabling the development of a learning environment that is both pedagogically sound and technologically advanced.

Leveraging an agile methodology, the future development phase will involve rapid prototyping and iterative refinement of the online cybersecurity program. Multidisciplinary teams, comprising instructional designers, subject matter experts, and technologists, will collaborate to generate and evaluate potential solutions addressing the defined problem statement.

Central to this phase will be the integration of continuous feedback loops with learners and industry experts. Prototype versions of the program will be regularly deployed and tested with representative user groups, enabling the team to gather real-time insights and dynamically incorporate user feedback. This approach will ensure that the evolving program design remains closely aligned with end-user needs and preferences.

As the development cycle progresses, the most promising solutions will be identified, refined, and integrated into a cohesive final program design. Rigorous quality assurance processes, including comprehensive testing and validation by subject matter experts, will further enhance the program's robustness and relevance. The delivery phase will conclude in the launch of the online cybersecurity program, carefully tailored to address the identified needs and concerns of learners and industry stakeholders. Mechanisms for ongoing program evaluation and continuous improvement will also be established, ensuring the long-term success and relevance of the offering in the rapidly evolving cybersecurity landscape.

3.2 Sample and Procedure

In this investigation, the selection of subjects is purposive rather than random driven by the study's objective of gaining an understanding of complicated issues surrounding students 'experiences and viewpoints, with a central emphasis on amplifying the voices of the students. The sampling process was carefully designed to recruit students who had completed a full-time online degree program in cybersecurity at a higher educational institution. Primarily, the university selected for this study is in London, United Kingdom, which provides a full-time postgraduate online program in cybersecurity, from which the students were selected for participation in this study. Moreover, the sample also encompassed industry experts working in the field of cybersecurity, facilitating the exploration of broader perspectives and opinions on the implementation of online cybersecurity programs as justified in section 3.1.1.

3.3 Instrument and Data Collection

During Phase 1 of data collection, this study employed open-ended questions to draw insights from students' perspectives toward online learning. The workshop was attended by 54 students alongside 2 industry experts specialized in Cybersecurity. The moderation was led by a primary researcher with considerable experience in facilitating workshops within educational contexts, while a secondary researcher undertook the role of observer, recording qualitative data notes.

In the second phase of the data collection, additional observations and perspectives were acquired through the administration of a questionnaire featuring both closed and open-ended questions. Insights gathered from Phase 1, particularly the 'Post Workshop feedback,' informed the refinement and design of the questionnaire. Participants were encouraged to provide explanations for their responses, with a focus on aspects of their online learning experiences deemed most relevant. The questionnaire was created utilizing Qualtrics Software and distributed using Prolific Platform, yielding substantive data with responses obtained from 127 participants.

The following table summaries the demographic data of the population and shows how this questionnaire was carried out considering equity, inclusivity and diversity.

Table1: Demographic Data of the population

Data	Description
Current/Completed Educational Level	Doctorate degree (PhD/other) Graduate degree (MA/MSc/MPhil/other) Technical/community college Undergraduate degree (BA/BSc/other)
Employment Sector	Education & Training Government & Public Administration Science, Technology, Engineering & Mathematics Transportation, Distribution & Logistics
Industry	College University and Adult Education Computer and Electronics Manufacturing Information Services and Data Processing Scientific or Technical Services Software and Telecommunications
Age / Gender	[20 – 30] ~ 50% [31 – 40] ~ 30% [above 40] ~ 20% 60 % Male 40 % Female
Country of residence	Australia, Chile, France, Germany, Greece, Ireland, Italy, Mexico, Netherlands, Poland, Portugal, South Africa, Spain, United Arab Emirates, United Kingdon, and the United States

The primary objective of the questionnaire was to tap into the participants' individual knowledge and perspectives concerning the effectiveness of online cybersecurity programs. Specifically, the goals were to complement and validate the findings derived from Phase 1's workshop, thereby facilitating iterative refinement and enhancement of the framework through successive assessments and comparisons of responses.

3.4 Analysis

In this study, thematic analysis was employed to ascertain the effectiveness of online cybersecurity programs by systematically categorizing emergent concepts, utilizing various coded data sets assembled subsequent to data collection. The primary unit of analysis comprised statements or textual excerpts. The initial phase of analysis aimed to generate and enrich the array of codes and emergent themes. These codes predominantly reflected substantive elements drawn from the participants' language and were subsequently utilized to develop overarching categories and subcategories. Subsequently, phase two involved discovering connections between the identified categories and their respective subcategories. Through several iterative cycles, the final phase entailed identifying categories that stood out above the others.

Qualtrics Software served as the platform for coding data, facilitating the seamless transfer of transcripts generated from Phases 1 and 2 for further analysis. Leveraging this software optimized the efficiency of the iterative qualitative research process, allowing for enhanced comparison of various concepts and categories prior to the identification of overarching themes. Additionally, alongside software-assisted coding, manual analysis was also conducted during the initial stages to foster a deeper familiarity with emerging themes and to address potential limitations of the tool, particularly concerning the interpretations of the data.

4 FINDINGS AND DISCUSSIONS

The workshop was thoroughly documented and subsequently transcribed precisely. Following transcription, all recorded discussions and noted responses underwent a thorough analysis, with each response systematically assigned a conceptual label. These labelled responses were then organized into distinct categories and properties, allowing for a structured representation of the data and facilitating comprehensive thematic exploration.

4.1 Phase 1: Workshop Findings

The data from the workshop was obtained through recording and note-taking. The primary focus of the workshop was to facilitate engagement between students and experts, enabling the collection of feedback and reflections on key indicators. Participants were encouraged to articulate their opinions, drawing from their experiences within the online program, with a range of options provided for each indicator. Subsequently, participants exercised discernment in selecting the most significant option reflective of their firsthand encounters in the online cybersecurity program. These identified indicators were also integrated into the questionnaire design, owing to their essential relevance to the online cybersecurity program.

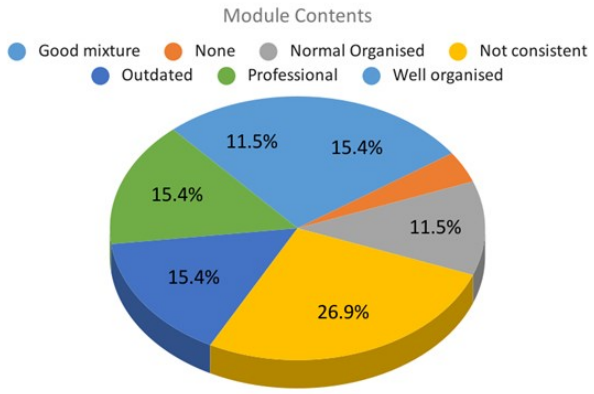

Figure 2: Distribution of Student Feedback on Module Content in Cybersecurity Program

The distribution indicates that most students find the module content organized and professional, with nearly 60% of respondents rating it as either "Well Organised," "Professional," or "Good Mixture." However, around 11.5% feel the content is outdated, which may suggest a need for some content updates. The feedback highlights an overall positive reception with some room for improvement, particularly concerning content consistency and keeping up-to-date with current trends in the field. The qualitative analysis of the reflections provided by cyber security students on the program contents highlights several key themes. While the majority of participants expressed concerns about the consistency and organization of the module contents, it is notable that a subset of students perceived the material positively, citing its professionalism and organization. This divergence in opinions underscores the complexity of designing online cybersecurity programs that effectively cater to diverse learning preferences and expectations. Moreover, the presence of varying perceptions suggests a need for targeted interventions to address the identified challenges and enhance overall program satisfaction.

Furthermore, the prominence of concerns related to consistency and outdated content reflects broader issues within online cybersecurity education, such as curriculum alignment with rapidly evolving industry standards. Addressing these concerns necessitates a dynamic and responsive approach to curriculum development, ensuring that content remains relevant and up-to-date. Additionally, the recognition of well-organized and professional aspects of the modules indicates areas of strength that can be leveraged to inform future program enhancements.

While a majority of participants found the practical labs to be clear and easy to follow, indicating effective instructional design, a subset of students perceived the labs as challenging or unclear. This discrepancy suggests a need for further examination of the instructional materials and delivery methods to ensure that they cater to the diverse learning needs and abilities of students. Additionally, the presence of differing perceptions underscores the importance of soliciting ongoing feedback and implementing iterative improvements to enhance the overall learning experience.

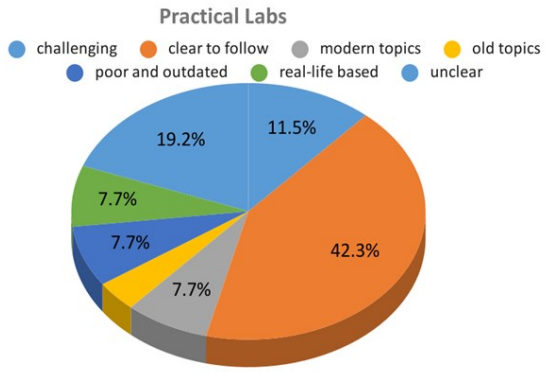

Figure 3: Distribution of Student Feedback on Practical Labs in Cybersecurity Program

Furthermore, the distribution of responses regarding the relevance of the practical labs to modern topics versus old topics highlights the importance of curriculum alignment with industry trends and advancements. The inclusion of real-life based labs is particularly commendable, as it enhances the practical relevance and applicability of the learning experience. However, the presence of feedback indicating poor and outdated labs underscores the need for continuous evaluation and updating of instructional materials to maintain alignment with current industry standards and practices.

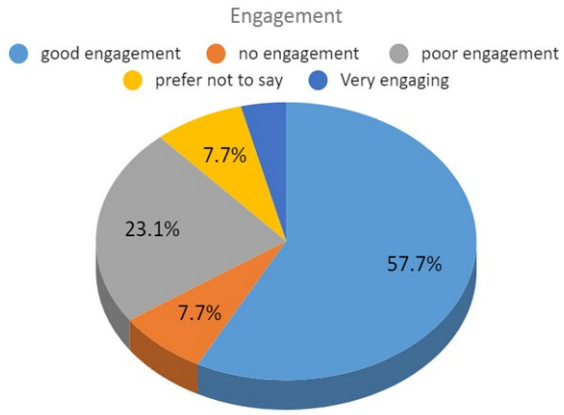

Figure 4: Distribution of Student Feedback on Engagement in Cybersecurity Program

A majority of students, 57.7%, reported good engagement, indicating that more than half of the participants feel meaningfully involved and actively engaged in the learning process. This strong positive response suggests that the course design and delivery are effective at capturing student attention and encouraging participation.

However, 23.1% of students reported poor engagement, suggesting that nearly a quarter of the students struggle to connect with the course material. This may indicate issues such as teaching methods not resonating with some learners, or possibly a lack of engaging activities that draw students into the learning process.

A small percentage of students (7.7%) found the course to have no engagement, indicating a more severe disconnect where a few students may feel completely unengaged in the program. Additionally, 7.7% of respondents preferred not to comment on their level of engagement, which could suggest uncertainty or mixed feelings about their experience, underscores the

complexity of assessing and addressing engagement issues, and highlighting the importance of creating a safe and supportive environment for student feedback.

Interestingly, the acknowledgment of "very engaging" experiences by some participants suggests areas of strength that can be leveraged to inform pedagogical approaches and enhance overall program engagement.

These differences suggest a need for further investigation into factors influencing student engagement, such as teaching methodologies, course materials, and interactive elements.

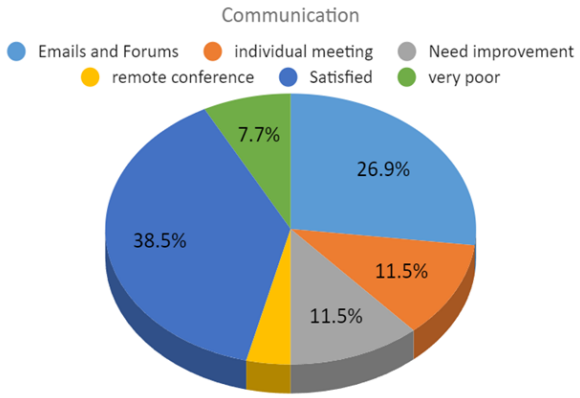

Figure 5: Distribution of Student Feedback on Communication in Cybersecurity Program

Figure 5 illustrates the distribution of responses to a survey question regarding preferred communication methods among a cohort of postgraduate students enrolled in cybersecurity programs. The data reveals a clear preference for digital communication channels, with emails and forums emerging as the most popular options, accounting for 38.5% and 11.5% of satisfied responses, respectively. This preference can be attributed to the accessibility and flexibility of digital communication, which allows students to engage in asynchronous learning and access information from various devices. However, a significant portion of respondents (11.5%) expressed dissatisfaction with communication methods, suggesting that while digital channels offer convenience, they may not fully meet the needs of all students. To address these issues, institutions may consider strategies such as improved technical support, enhanced communication platforms, regular check-ins, and clear guidelines. By implementing these measures, institutions can enhance communication effectiveness and improve the overall learning experience for postgraduate students in online programs.

Figure 6 illustrates the perceived impact of upskilling initiatives on a group of individuals. It categorizes respondents based on their self-reported skill development. The data reveals that a majority of respondents (75.6%) experienced positive outcomes, with improvements in practical skills (30.8%), research skills (26.9%), and soft skills (19.2%).

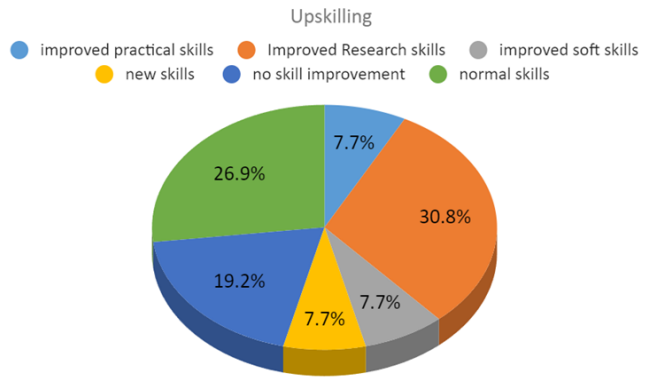

Figure 6: Distribution of Student Feedback on Upskilling in Cybersecurity Program

However, a smaller percentage (7.7%) reported no skill improvement or normal skills, suggesting that the effectiveness of upskilling programs can vary. To maximize the impact of upskilling initiatives, organizations should carefully assess employee needs and select programs that align with their goals. Ongoing evaluation and feedback are also essential to ensure that upskilling initiatives are meeting their intended objectives.

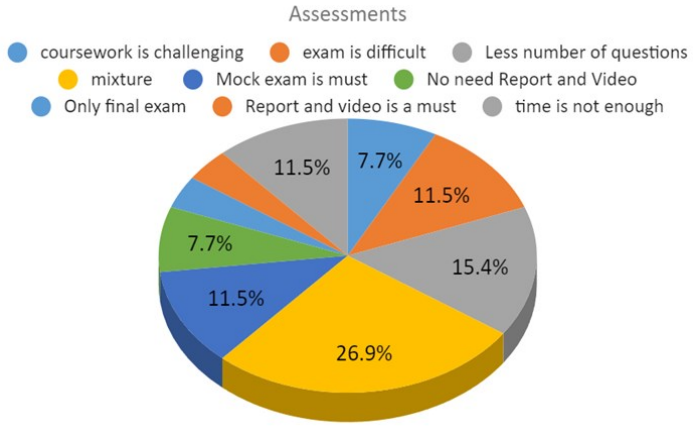

Figure 7: Distribution of Student Feedback on Assessments in Cybersecurity Program

However, figure 7 illustrates the responses of postgraduate students to a survey about their assessment experiences. The largest percentage of students (26.9%) found coursework challenging, followed by 15.4% who considered exams difficult. A significant portion (11.5%) expressed a need for fewer questions in assessments. Other challenges included the requirement for a mock exam (11.5%), the need to submit reports and videos (11.5%), and insufficient time for assessments (7.7%). While a small percentage (7.7%) preferred a combination of coursework and exams, the majority (7.7%) expressed satisfaction with the current assessment structure. hese findings highlight the need for educators to consider the challenges faced by postgraduate students and make adjustments to assessments accordingly. By addressing these concerns, institutions can improve the overall student experience and ensure that assessments are fair and effective. In summary, it reveals that postgraduate students in online programs face various challenges with assessments. The most common

concerns are the difficulty of coursework and exams, followed by the need for fewer questions. These findings suggest that the workload and expectations may be perceived as demanding by students. Additionally, the requirement for mock exams, reports, and videos, coupled with insufficient time, can contribute to student stress and frustration.

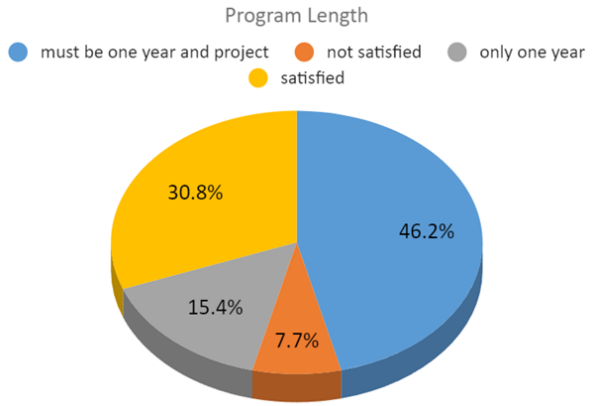

Figure 8: Distribution of Student Feedback on the length of Cybersecurity Program

There is a predominant preference for a one-year program with a project component, with the majority of participants expressing satisfaction with this format (46.2%). This suggests a recognition among students of the value of project-based learning in consolidating theoretical knowledge and fostering practical skills development within a condensed timeframe. Additionally, the presence of responses (30.8%) indicating satisfaction with a one-year program without a project component underscores the importance of flexibility in program structure to accommodate different learning preferences and career aspirations. However, it is noteworthy that a small subset of participants (7.7%) expressed dissatisfaction with the program length, suggesting potential areas for improvement or adjustment to better meet the needs and expectations of students.

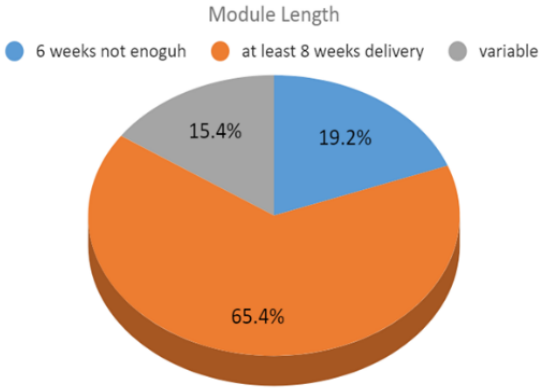

Figure 9: Distribution of Student Feedback on Module Length in Cybersecurity Program

Similarly, there is a predominant preference for longer delivery periods, with the majority of participants expressing a desire for modules lasting at least 8 weeks (65.4%). This preference suggests a recognition among students of the

importance of sufficient time for in-depth exploration of course content, engagement in practical activities, and consolidation of learning. Additionally, the presence of responses (19.2%) indicating dissatisfaction with a 6-week module length underscores the potential limitations of shorter delivery periods in meeting the diverse learning needs and expectations of students. Furthermore, the acknowledgment of variable preferences suggests the importance of flexibility in program design to accommodate different learning styles and academic requirements.

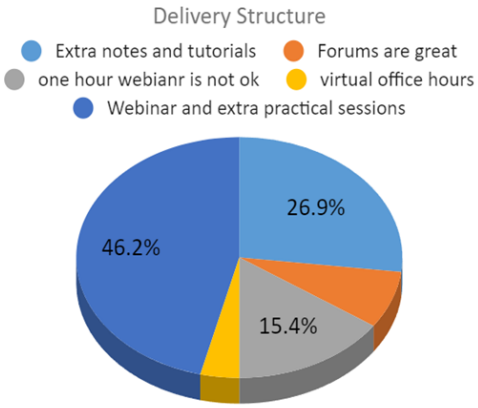

Figure 10: Distribution of Student Feedback on Delivery Structure in Cybersecurity Program

Figure 10 illustrates the responses of postgraduate students to a survey about their preferred delivery structure in an online program. The data reveals a clear preference for a blended approach that combines synchronous and asynchronous learning modalities. Specifically, the majority of students (46.2%) expressed satisfaction with a combination of webinars and extra practical sessions. This suggests that a balance between live lectures and opportunities for hands-on practice is essential for effective online learning. Additionally, a significant percentage of students (26.9%) found forums to be a valuable resource. This indicates that online discussion forums can play a crucial role in facilitating interaction, knowledge sharing, and peer support among students. While one-hour webinars were not sufficient for 15.4% of respondents, this suggests a need for longer or more frequent synchronous sessions to provide adequate opportunities for interaction and clarification. Furthermore, the demand for extra notes and tutorials highlights the importance of supplemental resources to support student learning. Overall, the findings suggest that a well-designed online program should incorporate a blend of synchronous and asynchronous learning modalities, provide opportunities for practical application, and offer supportive resources to enhance the student experience.

The results in figure 11 reveal a strong inclination towards obtaining certification, with the majority of participants indicating that it is recommended (65.4%). This consensus underscores the perceived value of professional certification in enhancing career prospects, validating skills, and demonstrating proficiency to potential employers. Additionally, the presence of responses (26.9%) highly recommending certification highlights its importance as a recognized credential within the field of cyber security.

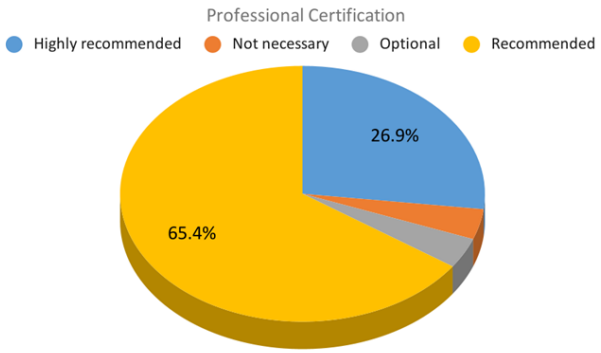

Figure 11: Distribution of Student Feedback on Professional Certifications in Cybersecurity Program

While the overwhelming majority of participants recommend certification, it is noteworthy that a small subset expressed differing opinions, with one participant considering it not necessary and another viewing it as optional. These contrasting perspectives may reflect varying career goals, industry expectations, or individual circumstances. Nonetheless, the prominence of recommendations for certification suggests that it is widely regarded as a valuable asset in the cyber security profession.

4.2 Workshop Findings: Discussion

To enhance the cyber security education program, several recommendations emerge from the qualitative analysis of student reflections. Firstly, addressing concerns about consistency and outdated material is crucial. Updating content to align with industry standards and offering diverse materials can enhance engagement and satisfaction. Additionally, refining instructional materials for practical labs and aligning them with modern topics can improve relevance and applicability.

Moreover, creating a supportive environment for feedback and leveraging engaging pedagogical approaches can enhance overall engagement. Improving communication channels, such as offering flexible options and virtual office hours, can foster better communication effectiveness and address individual needs. Furthermore, incorporating more hands-on activities and workshops can enhance skills development, while offering mock exams and reviewing time allocations can better prepare students for assessments.

Secondly, program flexibility is crucial to accommodate diverse preferences and enhance satisfaction. Offering varied module durations and ensuring alignment with learning objectives can optimize learning outcomes. Moreover, providing flexibility in program length and structure, such as a one-year program with a project component, can facilitate hands-on learning experiences and better meet the needs of students. In terms of delivery structure, expanding communication platforms and tailoring delivery methods to individual preferences can improve engagement and satisfaction. Additionally, professional certification is highly recommended for career advancement, and providing certification preparation support can encourage more students to pursue certification. By implementing these recommendations, cyber security education programs can enhance engagement, satisfaction, and skill development among students, ultimately better preparing them for success in the field.

4.3 Phase 2: Questionnaire

The questionnaire was disseminated utilizing Qualtrics Software and Prolific platform, yielding substantive data from 127 participants who completed the survey. The primary objective of the questionnaire was to leverage the students' individual

knowledge and perspectives regarding efficacy of online cybersecurity programs. Specifically, the aim was to both strengthen and validate the conclusions drawn from Phase 1 workshop.

Consequently, a questionnaire comprising 10 qualitative questions was designed and distributed to the participants. From the 127 individuals approached, 87 respondents provided feedback, a sufficient sample size for our study's purposes.

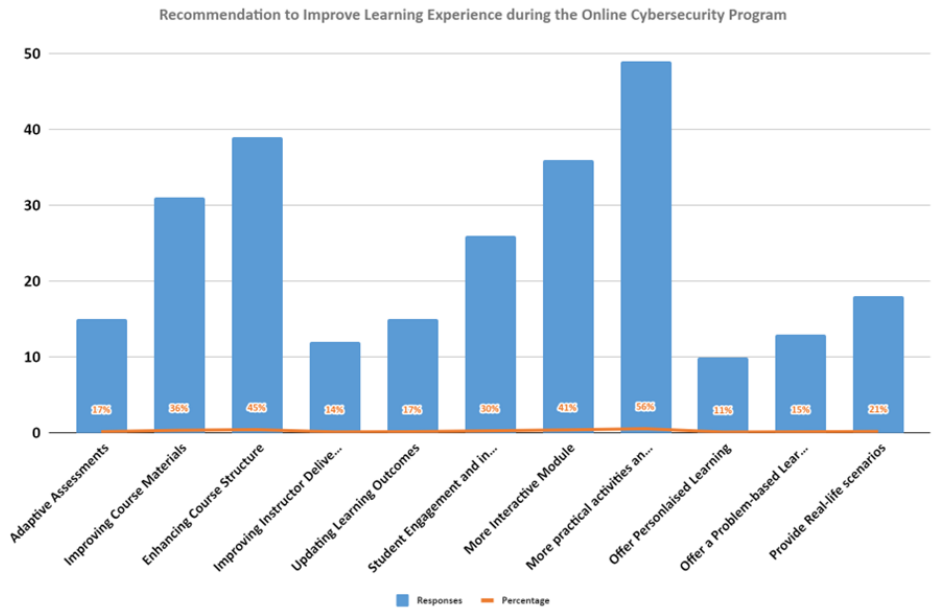

Figure 12: Distribution of Student Feedback on Recommendations for Improving Online Cybersecurity Program

Participants express a strong desire for enhancements in course materials, with 36% indicating a need for improvements. This highlights the importance of ensuring that course content remains relevant, up-to-date, and aligned with industry standards to facilitate effective learning. Additionally, (45%) of participants put emphasis on the need to enhance the course structure, suggesting a demand for greater flexibility and adaptability in program design to cater to diverse learning preferences.

Moreover, participants advocate for more interactive modules (41%) and practical activities (56%), indicating a preference for hands-on learning experiences and problem-based approaches. These findings underscore the significance of incorporating real-life scenarios (21%) and personalized learning opportunities (11%) to engage students and foster deeper understanding. Furthermore, recommendations for increasing student engagement (30%) and improving instructor delivery methods (14%) highlight the importance of fostering a supportive and interactive learning environment.

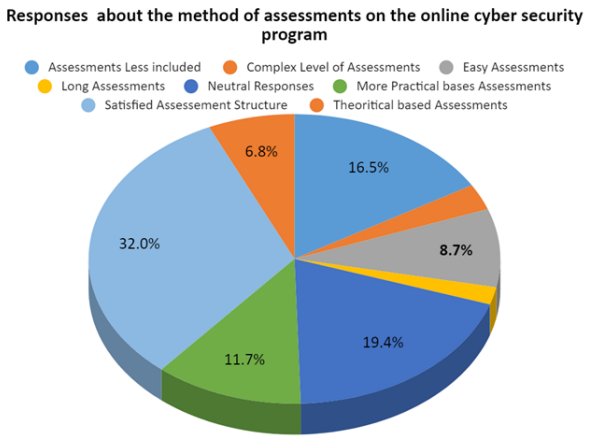

Figure 13: Distribution of Student Feedback on Method of Assessments in the Online Cybersecurity Program

While a considerable portion of participants express satisfaction with the assessment structure (32%), suggesting that it meets their expectations and facilitates their learning process, others indicate a desire for improvements. Some participants feel that assessments are less included (16.5%), implying a perceived inadequacy in the assessment coverage or frequency. Moreover, concerns about the complexity of assessments (3%) and a preference for more practical-based assessments (11.7%) highlight a desire for assessments that align more closely with real-world scenarios and practical skills development. Conversely, some participants find assessments to be easy (9%) or theoretical-based (7%), indicating potential concerns about the depth or relevance of assessment content.

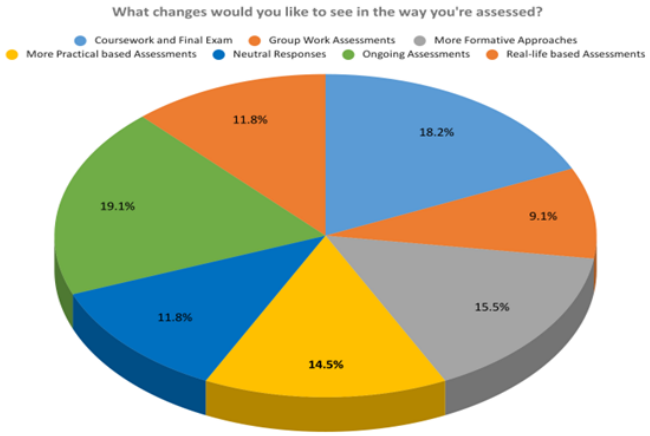

Figure 14: Distribution of Student Feedback on Desired Changes in Assessments within the Online Cybersecurity Program

Participants express a desire for more diversified assessment methods, with 20 responses advocating for improvements in coursework and final exams. This suggests a need for assessments that effectively evaluate both theoretical knowledge and practical skills. Additionally, 10 responses highlight a preference for group work assessments, indicating a desire for collaborative learning experiences that simulate real-world team dynamics.

Moreover, participants highlight the importance of ongoing assessments (21 responses) and more formative approaches (17 responses), suggesting a need for continuous feedback and opportunities for skill development throughout the program. Furthermore, 16 responses advocate for more practical-based assessments, emphasizing the importance of assessments that mirror real-life scenarios and enhance practical skills application. The presence of 13 neutral responses underscores the complexity of assessing individual preferences and highlights the need for flexibility in assessment methods to accommodate diverse learning styles and preferences.

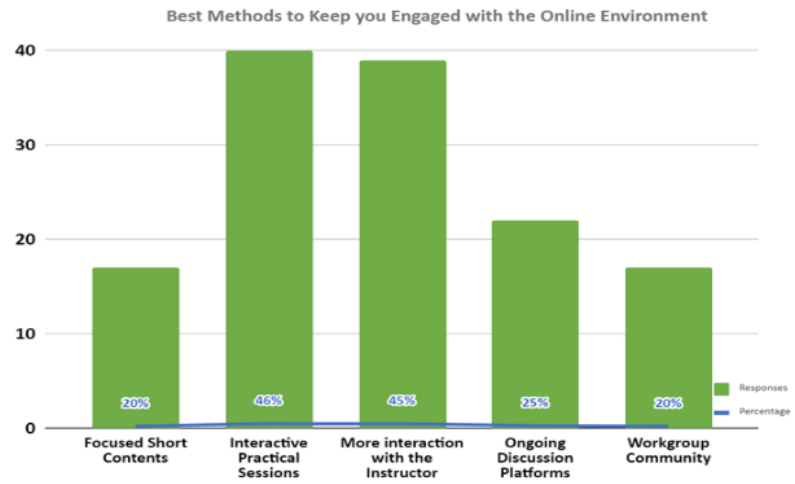

Figure 15: Distribution of Student Feedback on Best Method of Engagement within the Online Cybersecurity Program

Participants overwhelmingly advocate for interactive practical sessions (46%) as a highly effective method for engagement. This underscores the importance of hands-on learning experiences and active participation in enhancing student involvement and comprehension. Additionally, a significant number of responses accentuate the value of more interaction with the instructor (45%), highlighting the crucial role of instructor engagement and support in fostering a conducive learning environment.

Moreover, participants express a preference for ongoing discussion platforms (25%), emphasizing the importance of continuous communication and collaboration among peers to sustain engagement. Similarly, the presence of responses endorsing workgroup communities (20%) underscores the significance of peer interaction and support networks in maintaining motivation and interest. Furthermore, participants highlight the value of focused short contents (20%) in facilitating engagement, emphasizing the importance of concise, relevant content delivery in capturing and retaining student attention.

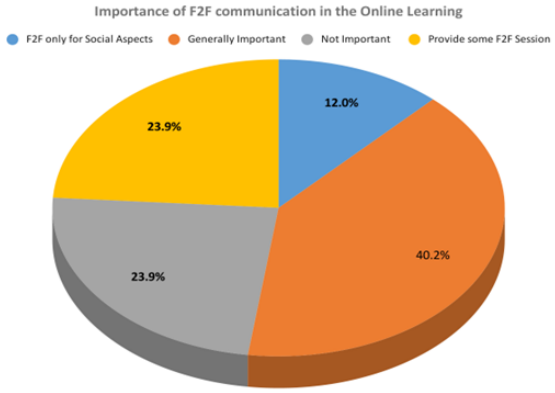

Figure 16: Distribution of Student Feedback on the Impact of F2F Communication in the Online Learning

A significant number of participants (40.2%) emphasize the general importance of traditional face-to-face communication, highlighting its value in facilitating various aspects of the learning experience. However, views diverge regarding the specific contexts in which F2F interaction is deemed essential. For some participants, traditional face-to-face communication is primarily valued for social aspects (12%), underscoring the significance of interpersonal connections and peer interactions in fostering a sense of community and camaraderie.

Furthermore, a notable proportion of participants (23.9%) express the view that traditional face-to-face communication is not important. This perspective may stem from a preference for the flexibility and convenience offered by remote learning modalities, which are perceived as sufficient for achieving their learning objectives. Similarly, results showed some participants prefer F2F sessions (23.9%), suggesting a recognition of the potential benefits of integrating occasional in-person interactions to complement online learning experiences.

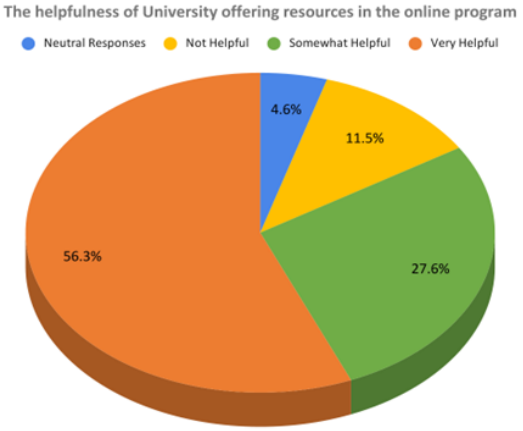

Figure 17: Distribution of Student Feedback on Helpfulness of University Resources in the Online Cybersecurity Program

A significant majority of respondents (56.3%) express that their universities have been very helpful in offering resources to support remote learning, indicating a high level of satisfaction with the support provided. Conversely, a smaller but

notable proportion of participants (11.5%) report that their universities have not been helpful, suggesting dissatisfaction with the available resources or support mechanisms.

Furthermore, a considerable number of respondents (27.6%) perceive their universities as somewhat helpful in offering resources for remote learning. While these participants acknowledge the efforts made by their universities to provide support, they may also identify areas where additional assistance or resources could further enhance the remote learning experience. Additionally, a few respondents (4.6%) provide neutral responses, indicating a lack of strong sentiment regarding the level of assistance received from their universities.

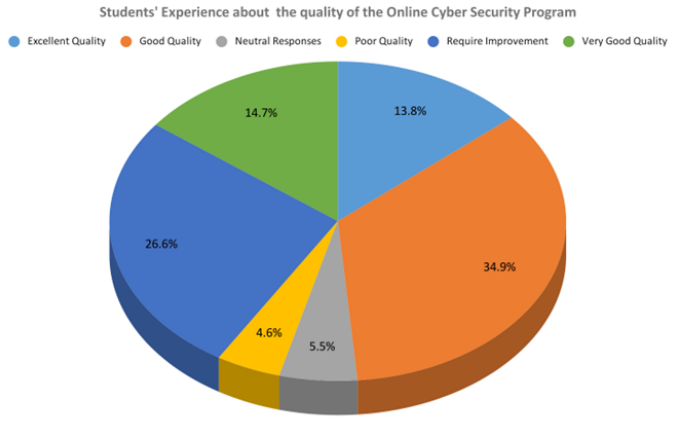

Figure 18: Distribution of Student Feedback on Their Experience about the Quality of the Online Cybersecurity Program

A notable proportion of respondents (34.9%) regard the program as of good quality, indicating a generally positive experience with the offered curriculum, instruction, and resources. Similarly, a significant number of participants (26.6%) express a need for improvement in the program's quality, suggesting areas where enhancements could enhance the overall learning experience.

Moreover, a substantial percentage of respondents (13.8%) perceive the program as exhibiting excellent quality, underscoring a high level of satisfaction with various aspects of the program, including content relevance, instructional delivery, and learning outcomes. Conversely, a smaller but noteworthy subset of participants (4.6%) consider the program to be of poor quality, indicating dissatisfaction with certain aspects of the program or its implementation. Additionally, a few respondents (5.5%) provide neutral responses, indicating a lack of strong sentiment regarding the quality of the program.

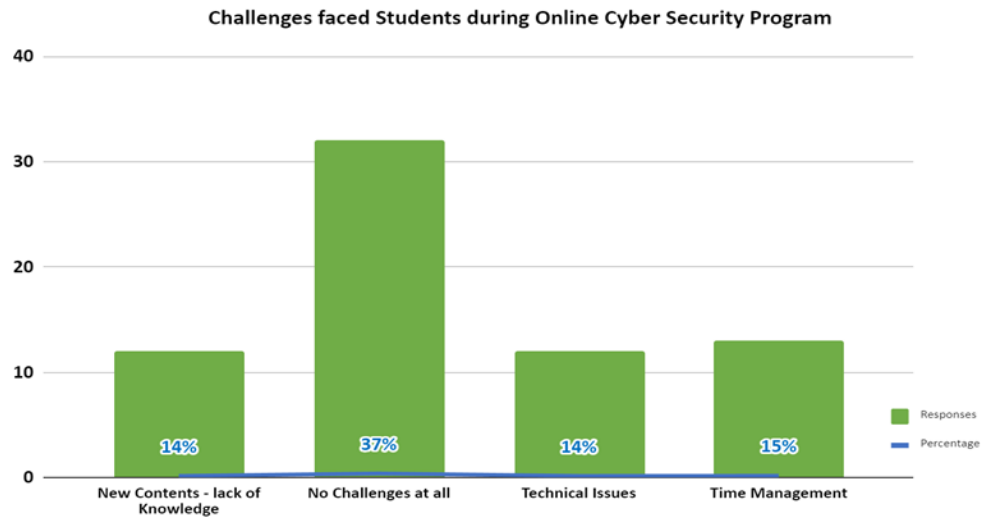

Figure 19: Distribution of Student Feedback on Challenges Faced During the Online Cybersecurity Program

A significant proportion of respondents (37%) report encountering no challenges at all, suggesting a smooth and seamless experience with the program. Conversely, several participants (15%) identify time management as a key challenge, indicating difficulties in balancing program requirements with other commitments.

Moreover, a notable subset of respondents (14%) cites technical issues as a challenge, highlighting the impact of technological barriers on their learning experience. These challenges may include internet connectivity issues, software compatibility issues, or difficulty navigating online platforms. Additionally, a similar percentage of participants (14%) express facing challenges related to new content and lack of knowledge, indicating difficulties in comprehending unfamiliar concepts or keeping pace with the program's curriculum. Despite these challenges, participants employ various strategies to overcome them, such as seeking assistance from instructors or peers, dedicating specific time slots for studying or leveraging online resources for additional support.

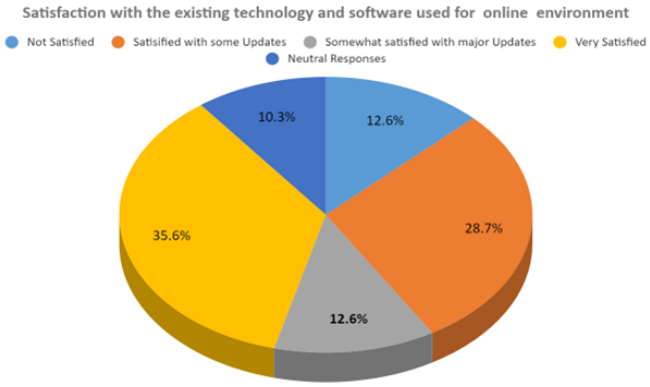

Figure 20: Distribution of Student Feedback on their Satisfaction with the Technology and Software used in the Online Cybersecurity Program

A significant portion of respondents (35.6%) express being very satisfied with the existing technology and software, indicating a high level of contentment with the tools and platforms employed for their online learning experience. Similarly, a substantial number of participants (28.7%) report being satisfied with some updates to the technology and software, suggesting a favorable perception of recent improvements made to enhance the educational environment.

Conversely, a smaller yet noteworthy subset of respondents (12.6%) indicates not being satisfied with the existing technology and software, highlighting areas where enhancements or adjustments may be needed to address shortcomings or meet user expectations. Additionally, a comparable percentage of participants (12.6%) express being somewhat satisfied with major updates, indicating a mixed sentiment regarding recent changes to the technology and software infrastructure. Finally, a small percentage of respondents (10.3%) provided neutral responses, suggesting a lack of strong sentiment regarding their satisfaction with the technology and software utilized in their online educational environment.

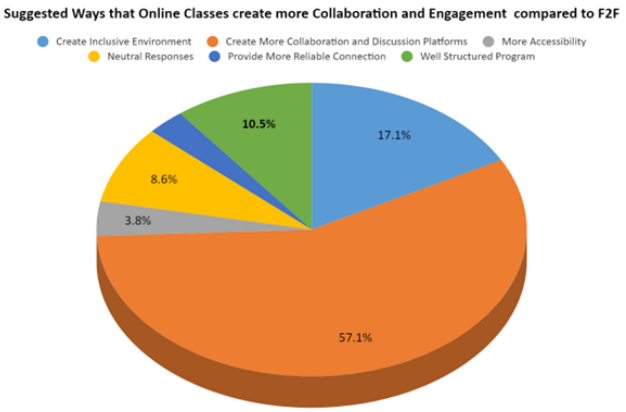

Figure 21: Distribution of Student Feedback on Suggestions to Create more Collaboration and Engagement in the Online Cybersecurity Program

A significant majority (57.1%) emphasize that online classes create more collaboration and discussion platforms, indicating that digital environments facilitate increased interaction and exchange of ideas among peers. This suggests that features such as virtual discussion boards, group chats, and online forums enable students to engage more actively in collaborative learning activities, regardless of physical distance.

Furthermore, a notable subset of respondents (17.1%) mention that online classes create an inclusive environment, suggesting that digital platforms provide opportunities for participation from a diverse range of individuals. This inclusivity can result from features like asynchronous communication tools, which allow students to contribute at their own pace and provide input irrespective of geographical or temporal constraints. Additionally, a smaller proportion of participants (10.5%) mention the importance of a well-structured program in enhancing collaboration and engagement, indicating that clear organization and delivery of course materials can facilitate meaningful interactions and foster a sense of community within online learning environments.

4.4 Questionnaire Findings Discussion

In conclusion, the findings highlight the multifaceted nature of students' experiences and perceptions within the Online Cyber Security Program. While there is a general satisfaction with certain aspects of the program, such as course materials and instructor engagement, there are also areas identified for improvement, particularly in enhancing course structure and assessment methods. The importance of interactive and practical-based learning experiences is emphasized, suggesting a preference for hands-on activities and real-world applications to deepen understanding and engagement. Additionally, the significance of ongoing support and communication from universities is highlighted, indicating the pivotal role of institutional resources in facilitating remote learning success.

Based on these findings several recommendations can be proposed to enhance the Online Cyber Security Program. Firstly, there should be a concerted effort to update and diversify course materials to ensure relevance and alignment with industry standards. Moreover, incorporating more interactive and practical-based assessments can provide students with opportunities to apply theoretical knowledge in practical scenarios. Additionally, fostering a collaborative and inclusive learning environment through ongoing discussions and community-building activities can further enhance student engagement and satisfaction. Furthermore, universities should continue to invest in technological infrastructure and support services to address technical challenges and ensure seamless remote learning experiences for all students. By implementing these recommendations, the Online Cyber Security Program can continue to evolve and adapt to meet the ongoing needs and expectations of students in the digital age.

5 PEDAGOGICAL FRAMEWORK FOR ONLINE CYBERSECURITY LEARNING

The themes and core categories that emerged from all phases of the data analysis generated a pedagogical framework for online cybersecurity learning.

Figure 22: Overview of the Proposed Pedagogical Framework of Online Cybersecurity in Higher Education

The nine dimensions are defined in Table 2. The framework consists of the core dimensions of online learning that were identified in this study and emerged largely from the participants' responses to specific challenges they experienced during the online program. We constructed these categories into 9 dimensions: (1) Assessments, (2) Engagement, (3) Practical Labs, (4) Module Contents, (5) Upskilling, (6) Delivery Structure, (7) Module Length, (8) Program Length, (9) Professional Certifications, and each of the dimensions are systemically interrelated. Central to the pedagogical framework for online cybersecurity learning are the participants, technology, and services. The technology competencies of instructors are an essential component of the framework. For example, if instructors cannot utilize technology effectively, they will not be able to demonstrate expert behavior for learners or assist those encountering challenges with the technology. Furthermore, the visual behavioral indicators in an online environment are not as evident as they are in face-to-face learning environments. Consequently, these elements are fundamental to recognizing the learners and their interaction with the online learning program.

The pedagogical framework for online cybersecurity learning supports an iterative process of planning, designing, evaluating, and implementing online learning which is conducive to both learner and instructor environments. Engagement is a key dimension of the framework which allows for supporting a dynamic online learning environment that is multi-dimensional with attention to behavioral and cognitive types of engagements (Redmond, Abawi, Brown, Henderson, & Heffernan, 2018). Students who exhibit a deeper level of cognitive learning and are more self-regulated can integrate their ideas from various sources and present new information. Such individual-level understanding of engagement can help higher education institutions construct a more comprehensive interpretation of learner behaviors for improving student engagement.

Upskilling is an essential area for cybersecurity, and students are constantly in need of acquiring new technical skills and knowledge in the field. The appropriate mix of traditional instruction and extracurricular learning intervention is needed, such as live webinars, guest lecturers, reflectional exercises, and online quizzes, which can be solutions to acquiring new and essential skills. Furthermore, the IT security industry continuously experiences rapid change which means it demands learners to acquire new skills in the field. As such, the framework places emphasis on different forms of professional development including industry certifications that support mastery of career and industry-oriented skills.

The type of assessment methods are important indicators in measuring students' learning to better prepare instructors to support and obtain insights into learners' current ideas and gaps. Essentially, the influence of assessment methods on students' learning also depends on the student's learning attainment "deep level learning strategies'' (essays and e-portfolios) and ''knowledge-based factual recall'' (exams and quizzes) (Scouller, 1998). The framework highlights that learners can acquire a better understanding of the body of knowledge if they engage in different forms of assessments that present different types of cognitive challenges (portfolios, oral presentations, MCQs). In addition, information communication technology facilitates a dialogic approach to assessment and feedback and thus is an important medium in which the subject matter related to formative and summative assessments can be reinforced (Deeley, 2018).

The module content is an important feature of the context of instructor-learner interaction. It influences the delivery structure of the cybersecurity online program and provides an essential medium for learners to engage in the subject. Similarly, effective module content contributes to various forms of interactions and instructional approaches which can promote the ability of students to act as independent learners in an asynchronous online learning environment. Critically, the focus of the module content environment is essential as the goal of the online program is to support learners to become more self-regulated. Furthermore, the interrelationships between teacher, student, and content in an online environment is facilitated within the framework to support a student-driven independent online learning environment. Therefore, central to student independent learning, is creating an online environment to nurture effective inquiry-based (Al Mamun & Lawrie, 2023). As such, our framework proposes that such an environment can be facilitated by encompassing interactive technology interfaces, for instance, using simulation-based learning to assist in scaffolding mechanisms for problem-based learning.

The delivery structure of an online cybersecurity program can restrict the desired learning objectives if a lack of preparation is made to the structure and design of the online learning environment. A cybersecurity online learning process needs to be articulated and structured within its context. Student satisfaction is determined by the level of structure in the program such as clearly defined objectives, assignments, and deadlines, in order to increase student satisfaction (Ferguson & DeFelice, 2010). Specifically, the online environment must reflect the specific characteristics of the discipline or subject matter (Park, 2011). The learning management system (LMS) must be designed to engage both learners and faculty, as well as customized in a way that allows learners to experience high-quality interactive learning. These include provisions for effective communication channels (e.g., discussion boards, blogs, live chats), content format and learning evaluation tools to support interactive learning (Park, 2011). Moreover, such tools provide opportunities for using LMS that are consistent with constructivist approaches to learning for student-centered knowledge construction rather than just basic transmission of knowledge (Lonn & Teasley, 2009).

The duration or module length of the online cybersecurity program is another essential element of the framework. The facilitation and intensity of the module duration may influence learners to participate differently in the online learning process depending on their prior background experience and the learners (traditional and non-traditional learners) ability to adjust to a new learning environment. In the case of this study, students undertook a block teaching delivery of the online cybersecurity program. Thus, the pace of block modules can place different demands on learners. Instructors need to adjust

the learning environment to allow learners to absorb and reflect on the subject materials. In addition, the volume of content needs to be filtered to its fundamental elements so that learners can successfully achieve the learning objectives.

Independent and self-regulated learning environments are equally essential for such fast-paced programs. Notably, instructors should provide tools and methods to facilitate an environment that can foster and encourage independent learning. Critical thinking needs to be achieved at this level with greater innovative approaches and to empower students to become more accountable for their own learning. Furthermore, in order to engage in fast-paced modules, the learner's time-management behaviors are important characteristics for their own progress monitoring. In doing so, instructors can establish a supportive learning environment maximizing student attention and learning so that they can control procrastination and manage their study schedule.

The proposed framework emphasizes the importance of the length of an online program and considers it to be, to a large extent, greatly dependent on the type of teaching strategy. Specifically, the length of an online program can have a pedagogical effect on students, especially in block-intensive length programs in comparison to semesterised teaching formats. The framework recommends more emphasis on student interaction and engagement to keep the intensive course learners focused (Ferguson & DeFelice, 2010). Most importantly, the teaching strategies of the online instructor must include different forms of communication, particularly in shortened-length programs, where learners must remain constantly focused on the task. These strategies can include live chat rooms, online discussions, and the use of recorded podcasts, that would provide opportunities for increased interaction. Furthermore, such feedback and ongoing support is essential to motivation and hence to student satisfaction (Ferguson & DeFelice, 2010).

Table2: The framework core dimensions of Cybersecurity online learning

Dimensions	Descriptions
Engagement	• Design online instruction that is conducive to high-level student-instructor engagement • Communication methods to support online learning activities and services • Students interact with the content, instructor, and working with peers (Student-Student interaction) • Design online strategies for feedback, online discussions, and collaboration, simulations (theory application), videos, discussion spaces, and learning resources • Collaborative learning: discussion forums and online spaces for feedback (threaded discussions) • Adopt self-regulated strategies to plan, monitor, and evaluate student level of cognition
Practical lab	• Setting up real-life scenarios • Practical activities in the online learning platforms (e.g., simulations, videos, virtual laboratories) • Practical lab activities help and enable learners to be more engaged and draw their attention to the online program

Module length	• Students focus • Case discussions • Time-management • Content adjustment • Self-regulated learning • Consideration for both traditional and non-traditional learners • Use of online forums and synchronous chat sessions • Formative assessment submission and feedback
Program length	• Refine the instruction style with more focus on student interaction • Apply an engaging teaching strategy • Discussions and debate activities • Probing questions in online forums • Frequent communication via online forums, live chat rooms, online announcements, discussion spaces, recorded podcasts
Delivery structure	• Interactive Learning Management Systems • Customized learning environment • Alignment with the discipline or subject matter to achieve the desired learning objectives • Facilitate communication channels • Content format and interactive learning
Module content	• Instructor-learner interaction • Student-independent online driven learning environment (self-regulated) • Scaffolding learning environment • Guided-learning • Interactive simulations/technology integration • Problem-based learning
Upskilling	• Live webinars, guest lecturers, reflectional exercises, and online quizzes, as solutions to acquire new technical skills
Professional certifications	• Exit Certification Assessments • Industry Certificates that support mastery of career-oriented skills (e.g., Certified Ethical Hacker, CompTIA security) • Professional Certificate, Advanced Certificate, Professional Licensure • Professional Development
Assessments	• A mixed assessment approach to learning formative and summative • Assess various levels of cognitive skills and intellectual abilities • Online quizzes • Oral presentations • Essay versus Exams/e-portfolios • Technology-mediated communication • Formative Feedback

A broad stream of research has examined the advantages of cybersecurity programs in higher education, focusing primarily on curriculum design and revision (Hajny et al., 2021; Knapp, Maurer, & Plachkinova, 2017). Other studies have predominantly addressed specific issues such as enhancing awareness of cyber-attacks (Erendor & Yildirim, 2022; Davidson & Hasledalen, 2014), aligning curricula with industry requirements (Towhidi & Pridmore, 2023), and investigating specific topics or the absence thereof within existing cybersecurity courses (Cabaj et al., 2018). Additionally, other significant research contributions have centered on cybersecurity hackathons and competitions as pedagogical tools

in educational settings (Affia, Nolte, & Matulevičius, 2022; Bashir et al., 2015; Cheung et al., 2012). Building on this foundation, we broadened our study by exploring student-shared experiences and responses to cybersecurity online learning within higher education settings, leading to the development of a comprehensive pedagogical online cybersecurity framework. Consequently, this study fills a significant gap in the literature concerning the absence of a comprehensive framework within higher education that establishes a pedagogical link between instruction and online learning spaces in cybersecurity programs. The presented framework combines pedagogical methods to support the complexities of course organisation, design, and structure of online cybersecurity programs for higher education settings.

The framework draws parallels between the instruction of an online cybersecurity program and broader individual-level behaviors, with a specific emphasis on student-student and instructor-student interactions. Such interaction is deemed crucial for fostering active learning and engagement, and for gaining a deeper understanding of the scope and quality of online cybersecurity programs (Salem, Samara, Pray, & Hussein, 2024). Furthermore, the significance of the framework in this study lies in its recognition of the evolving nature of cybersecurity online programs, advocating for a flexible approach that emphasizes the continuous adaptation of online programs for ongoing improvement (Vesin et al., 2022). Thus, it offers a tool to aid educators in the development and refinement of their courses to facilitate a more comprehensive, holistic, and systematically integrated approach to cybersecurity online programs.

Specifically, the framework serves as a resource for academics to reflect on and enhance students' critical thinking abilities, equipping them to solve complex, hands-on tasks that address both current and future challenges in online cybersecurity. In addressing these challenges, the framework highlights the importance of fostering close collaboration between academia and industry (Exter et al., 2018). Therefore, academics are expected to leverage their new understanding of the online cybersecurity framework to enhance current programs and guide the development of new ones. For example, analyzing the interactions between postgraduate students, and academics as well as how industry professionals engage with students, is vital, as these dynamics play a crucial role in shaping the identity of online cybersecurity programs, an area that is underrepresented in many online cybersecurity courses within higher education (Salem, Samara, Pray, & Hussein, 2024). This connection enables higher education institutions and external stakeholders to engage more effectively, allowing students to confront real-world cybersecurity problems as part of their learning process, particularly those transitioning from traditional online course formats to more interactive and dynamic online learning environments. Such collaboration will significantly contribute to the sustainability and longevity of future online cybersecurity programs in higher education.

6 CONCLUSION

Based on the findings from the exploratory research design employed in this study, it is evident that online cybersecurity programs in higher education are attracting significant attention, especially among full-time postgraduate students. However, the study also revealed themes related to ineffective communication and poor learning engagement, highlighting persistent challenges faced by students enrolled in online cybersecurity programs. These challenges, including issues with technology-supported learning environments and interpersonal dynamics among learners and instructors, underscore the importance of further investigation and potential interventions to enhance the effectiveness of online learning experiences in cybersecurity education.

The seamless integration of data collection methods, including both qualitative insights gathered from a workshop attended by a cohort of postgraduate cybersecurity students and industry experts, as well as quantitative data obtained through a questionnaire with closed and open-ended questions, provided a comprehensive understanding of students' perceptions and experiences in online cybersecurity programs. Thematic analysis revealed valuable insights into the

strengths and weaknesses of current online learning models, shedding light on areas for improvement and potential strategies to address challenges faced by students in virtual learning environments.

As higher education institutions continue to adapt to the surging demand for distance learning, addressing these challenges will be essential to ensure the quality and success of online cybersecurity programs. Future research endeavors should focus on implementing strategies to improve communication, increase student motivation, and foster active engagement in online learning environments, ultimately contributing to the advancement of cybersecurity education in the digital age.

ACKNOWLEDGMENTS

For the purpose of open access, the authors have applied a Creative Commons Attribution (CC BY) license to any Author Accepted Manuscript version of this paper arising from this submission. This work has been partially funded by Enterprise and Engagement grant /King's College London.

REFERENCES

Baburajan, P., Noushad, S., Faisal, T., & Awawdeh, M. (2022). Online Teaching and Learning: Effectiveness and Challenges. *2022 Advances in Science and Engineering Technology International Conferences (ASET)* (pp. 1-6). Dubai: IEEE. doi:https://doi.org/10.1109/ASET53988.2022.9734851

Fantinelli, S., Cortini , M., Fiore, T., lervese, S., & Galanti , T. (2024). Bridging the Gap between Theoretical Learning and Practical Application: A Qualitative Study in the Italian Educational Context. *Educ. Sci. 2024, 14*(2), 198. doi:https://doi.org/10.3390/educsci14020198

Ferrer, J., Ringer, A., Saville, K., Parris, M., & Kashi, K. (2022). Students' motivation and engagement in higher education: the importance of attitude to online learning. *Higher Education, 83*(2), 317–338. doi:https://doi.org/10.1007/s10734-020-00657-5

González-Manzano, L., & de Fuentes, J. (2019). Design recommendations for online cybersecurity courses. *Computers & Security, 80*(1), 238-256. doi:https://doi.org/10.1016/j.cose.2018.09.009

Legg, J. (2021, October 21). *Confronting The Shortage Of Cybersecurity Professionals*. Retrieved from Forbes.com: https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/21/confronting-the-shortage-of-cybersecurity-professionals/?sh=216ae14578b9

Sun, A., & Chen, X. (2016). Online Education and Its Effective Practice:A Research Review. *Journal of Information Technology Education: Research, 15*, 157-190. doi:https://doi.org/10.28945/3502

Al Mamun, M., & Lawrie, G. (2023). Student-content interactions: Exploring behavioural engagement with self-regulated inquiry-based online learning modules. *Smart Learning Environments, 10*(1), 1.

Aldawood, H., & Skinner, G. (2019). An academic review of current industrial and commercial cyber security social engineering solutions. *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy* (pp. 110-115). Kuala Lumpur, Malaysia: ACM. doi:https://doi.org/10.1145/3309074.3309083

Ali , A., Lundqvist, K., Watterson, C., & Baghaei, N. (2020). Teaching Cyber-Security for Distance Learners: A Reflective Study. *2020 IEEE Frontiers in Education Conference (FIE)* (pp. 1-7). Uppsala, Sweden: IEEE. doi:https://doi.org/10.1109/FIE44824.2020.9274062

Alsmadi, I., & Easttom, C. (2020). *The NICE cyber security framework*. USA: Springer International Publishing. doi:https://doi.org/10.1007/978-3-030-02360-7

Baskakova, D., Belash, O., & Shaposhnikov, S. (2021). Assessment of Online Learning Effectiveness by Students of Engineering and IT Degree Programs. *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 783-787). Yaroslavl, Russian Federation: IEEE. doi:https://doi.org/10.1109/ITQMIS53292.2021.9642752

Brooks, , A., Hardin, C., Scianna, J., Berland, M., & Legault, L. (2021). Approaches to transitioning computer science classes from offline to online. *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education* (pp. 81-87). Virtual Event,: ACM. doi:https://doi.org/10.1145/3430665.3456366

Brown, M., Hoon, A., Edwards, M., Shabu, S., Okoronkwo, I., & Newton, P. (2023). A pragmatic evaluation of university student experience of remote digital learning during the COVID-19 pandemic, focusing on lessons learned for future practice. *Plos one, 18*(5), 1-23. doi:https://doi.org/10.1371/journal.pone.0283742

Castro, M., & Tumibay , G. (2019). A literature review: efficacy of online learning courses for higher education institution using meta-analysis. *Education and Information Technologies, 26*(2), 1367–1385. doi:https://doi.org/10.1007/s10639-019-10027-z

Council Design. (2024, April 01). *The Double Diamond.* Retrieved from Design Council: https://www.designcouncil.org.uk/our-resources/the-double-diamond/

Crick, T., Davenport, J., Irons, A., & Prickett, T. (2019). A UK case study on cybersecurity education and accreditation. *IEEE Frontiers in Education Conference (FIE)* (pp. 1-9). Covington, KY, USA: IEEE. doi:https://doi.org/10.1109/FIE43999.2019.9028407

Deeley, S. (2018). Using technology to facilitate effective assessment for learning and feedback in higher education. *Assessment & evaluation in higher education, 43*(3), 439-448.

Dragoni, N., Lafuente, A., Massacci, F., & Schlichtkrull, A. (2021). Are we preparing students to build security in? A survey of European cybersecurity in higher education programs. *IEEE Security and Privacy, 19*(1), 81-88. doi:https://doi.org/10.1109/MSEC.2020.3037446

Dumford, A., & Miller, A. (2018). Online learning in higher education: exploring advantages and disadvantages for engagement. *Journal of Computing in Higher Education, 30*(3), 452–465. doi:https://doi.org/10.1007/s12528-018-9179-z

Ferguson, J., & DeFelice, A. (2010). Length of online course and student satisfaction, perceived learning, and academic performance. *The International Review of Research in Open and Distributed Learning, 11*(2), 73–84. doi:https://doi.org/10.19173/irrodl.v11i2.772

Gama, K., Zimmerle, C., & Rossi, P. (2021). Online hackathons as an engaging tool to promote group work in emergency remote learning. *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education* (pp. 345-351). Virtual Event: ACM. doi:https://doi.org/10.1145/3430665.3456312

Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022). Towards understanding the skill gap in cybersecurity. *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education* (pp. 477-483). Dublin: ACM. doi:https://doi.org/10.1145/3502718.3524807

Griful-Freixenet, J., Struyven, K., Vantieghem , W., & Gheyssens, E. (2020). Exploring the interrelationship between Universal Design for Learning (UDL) and Differentiated Instruction (DI): A systematic review. *Educational Research Review*, 100306. doi:https://doi.org/10.1016/j.edurev.2019.100306

Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, tools and good practices for cybersecurity curricula. *IEEE Access, 9*, 94723-94747. doi:https://doi.org/10.1109/ACCESS.2021.3093952

Indumathi, , V., Evangelista, A., & Wang, S. (2023). Evaluation of Civil Engineering students' performance comparing online versus on-campus delivery mode. *IEEE Global Engineering Education Conference (EDUCON)* (pp. 1-6). Kuwait: IEEE. doi:https://doi.org/10.1109/EDUCON54358.2023.10125235

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information, 12*(10), 1-20. doi:https://doi.org/10.3390/info12100417

Kreider, , C., & Almalag, M. (2019). A Framework for Cybersecurity Gap Analysis in Higher Education. *SAIS 2019 PROCEEDINGS* (pp. 1-6). -: AIS eLibrary. Retrieved from https://aisel.aisnet.org/sais2019/6

Lomellini, A., Lowenthal, P., Snelson, C., & Trespalacios, J. (2022). Higher education leaders' perspectives of accessible and inclusive online learning. *Distance Education, 43*(4), 574-595. doi:https://doi.org/10.1080/01587919.2022.2141608

Lonn, S., & Teasley, S. (2009). Saving time or innovating practice: Investigating perceptions and uses of Learning Management Systems. *Computers & Education, 53*(3), 686-694. doi:https://doi.org/10.1016/j.compedu.2009.04.008

Naeem, U., & Bosman, L. (2023). Learner Engagement Analytics in a Hybrid Learning Environment. *2023 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1-7). Kuwait: IEEE. doi:https://doi.org/10.1109/EDUCON54358.2023.10125108

Nolte, A., Affia, A.-a., & Matulevičius, R. (2022). Integrating hackathons into an online cybersecurity course. *In Proceedings of the ACM/IEEE 44th International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET '22)* (pp. 134–145). Pittsburgh Pennsylvania: ACM. doi:https://doi.org/10.1145/3510456.3514151

Palvia, S., Aeron, P., Gupta, P., Mahapatra, D., Parida, R., Rosner, R., & Sindhi, S. (2018). Online education: Worldwide status, challenges, trends, and implications. *Journal of Global Information Technology Management, 21*(4), 233-241. doi:10.1080/1097198X.2018.1542262

Park, J. (2011). Design education online: Learning delivery and evaluation. *International Journal of Art & Design Education, 30*(2), 176-187.

Prasad, P., Balse, R., & Warriem, J. (2023). Understanding Students' Experiences in an Online Programming Course from a Transactional Distance Perspective. *Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education* (pp. 96-102). Turku: ACM. doi:https://doi.org/10.1145/3587102.3588850

Redmond, P., Abawi, L., Brown, A., Henderson, R., & Heffernan, A. (2018). An online engagement framework for higher education. *Online Learning Journal*, *22*(1), 183-204.

Salem, M., Samara, K., Pray, J., & Hussein, M. (2024). Evaluating the Effectiveness of Online Cybersecurity Program in Higher Education. *IEEE Global Engineering Education Conference 2024. IEEE Education Society.* Greece: IEEE.

Scouller, K. (1998). The influence of assessment method on students' learning approaches: Multiple choice question examination versus assignment essay. *Higher education, 35*(4), 453-472.

Shoemaker, D., Kohnke, A., & Sigler, K. (2018). *A guide to the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework (2.0).* New York: Auerbach Publications. doi:https://doi.org/10.1201/9781315368207

Stephani, N., Alvin, S., & Riatun. (2023). Exploring college students' motivations for choosing online learning program. *Cogent Education, 10*(2), 1-13. doi:https://doi.org/10.1080/2331186X.2023.2266206

Xu, H., & Ebojoh, O. (2007). Effectiveness of online learning program: a case study of A higher education institution. *Issues in Information Systems - Scholarship and Professional Work - Business, 8*(1), 160-166. Retrieved from https://digitalcommons.butler.edu/cob_papers/81

Yang, M., Shams Ud Duha, M., Kirsch, B., Glaser, N., Crompton, H., & Luo, T. (2024). Universal design in online education: A systematic review. *Distance Education, 45*(1), 23-59. doi:10.1080/01587919.2024.2303494

Cabaj, K., Domingos, D., Kotulski, Z. and Respício, A., (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, 75, pp.24-35. Doi:https://doi.org/10.1016/j.cose.2018.01.015

Davidson P, Hasledalen K. (2014) Cyber threats to online education: A Delphi study. *InICMLG2014 Proceedings of the 2nd International Conference on Management, Leadership and Governance: ICMLG 2014* Mar 1 (p. 68).

Erendor, M.E. and Yildirim, M., 2022. Cybersecurity awareness in online education: A case study analysis. *IEEE Access*, 10, pp.52319-52335. doi: 10.1109/ACCESS.2022.3171829

Exter, M., Caskurlu, S. and Fernandez, T., (2018). Comparing computing professionals' perceptions of importance of skills and knowledge on the job and coverage in undergraduate experiences. *ACM Transactions on Computing Education (TOCE)*, 18(4), pp.1-29. https://doi.org/10.1145/3218430

Towhidi, G. and Pridmore, J., (2023). Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education*, 34(1), pp.70-83. https://aisel.aisnet.org/jise/vol34/iss1/6/

Vesin, B., Mangaroska, K., Akhuseyinoglu, K. and Giannakos, M., (2022). Adaptive assessment and content recommendation in online programming courses: On the use of elo-rating. *ACM Transactions on Computing Education (TOCE)*, 22(3), pp.1-27. https://doi.org/10.1145/3511886

Knapp, K.J., Maurer, C. and Plachkinova, M., (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education*, 28(2), p.101.

Cheung, R., Cohen, J., Lo, H., Elia, F. & Carillo Marquez, V. (2012). Effectiveness of Cybersecurity Competitions. *Proc. Int'l Conference on Security & Managemen*t

Bashir M., Lambert A., Wee J. M. C., Guo B. (2015). An examination of the vocational and psychological characteristics of cybersecurity competition participants. *Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education* (3GSE).

Ojasalo, J., Kumar, S. N., & Harviainen, T. (2022). Combining industry development and research in higher education: A case study. *In INTED, International Technology, Education and Development Conference* (pp. 10302-10308).

Abensur, S. I., et al. (2023). Double diamond approach helping multidisciplinary health research team to mitigate infrastructure limitations. *Engineering Research Express*, 5(4), 045046. DOI 10.1088/2631-8695/acff3b

S. Luojus, S. Kauppinen, J. Lahti (2015). Integrating teaching and R&D in higher education - the welive project. *ICERI2015 Proceedings*, pp. 5497-5507.

Wang, X., et al. (2023). Digital Transformation of Education: Design of a "Project-Based Teaching" Service Platform to Promote the Integration of Production and Education. *Sustainability*, 15(16), 12658. https://doi.org/10.3390/su151612658

Mitchell, V., Wilson, G. T., Leder Mackley, K., Jewitt, C., Golmohammadi, L., Atkinson, D., & Price, S., "Digital touch: towards a novel user-experience design pedagogy," *Design and Technology Education: An International Journal*, 25(1), 59-79, 2020.