Cybersecurity-related Curriculum for Diverse Postgraduate Cohorts: A Case Study

Eliana Stavrou, Irene Polycarpou
Computing Department, Applied Cybersecurity Research Laboratory
University of Central Lancashire Cyprus
Larnaca, Cyprus
estavrou@uclan.ac.uk , ipolycarpou@uclan.ac.uk

ABSTRACT

Cyber threats have highly increased over the last decade, including ransomware, identity stealing, etc. Ensuring the security of cyberspace is imperative and should constitute a top priority for society to promote its growth and support its sustainability. Educational organizations, worldwide, have recognized the need to educate people on cybersecurity. This need has driven educational organizations to design postgraduate cybersecurity curriculums to educate and train recent graduates and IT professionals. Having a diverse audience, with different experiences and backgrounds with regards to knowledge and practical skills, can greatly challenge the design and delivery of a cybersecurity curriculum. Moreover, the fact that blended environments are promoted, where a curriculum is delivered to both face-to-face and distance learning students, can challenge the curriculum design and delivery even further. This paper presents a case study, critically discussing the challenges in the design and delivery of an ethical hacking curriculum targeting diverse postgraduate cohorts in conventional and distance learning. Moreover, the utilized practices that have successfully addressed the challenges are discussed. The aim of this work is to assist curriculum planners and developers to deliver an enhanced teaching and learning cybersecurity environment.

Keywords: Cybersecurity curriculum, cybersecurity education, curriculum design, curriculum development, diverse postgraduate cohort, penetration testing.

1. INTRODUCTION

Cyber threats such as ransomware and identity stealing have highly increased the last few years, impacting individuals and organizations. Society has recognized the importance of cyberspace to promote its growth and support its sustainability, thus, the necessity to protect it. Cybersecurity deals with the protection of cyberspace [1] and requires both knowledge on fundamental principles and practical skills in the area [2] [3]. Educational organizations, worldwide, have identified the need to educate people on fundamental principles in cybersecurity and to build relevant practical skills. This need challenges educational organizations that would like to offer courses on cybersecurity as a number of aspects [4] [5] need to be considered to establish an appropriate teaching and learning (T&L) cybersecurity environment and promote an enhanced student experience.

A driving factor for the development of a successful T&L cybersecurity environment is the design of the respective course curriculum and its delivery [6]. The need to cultivate the future generation of skilled cybersecurity professionals, has driven educational organizations to design postgraduate cybersecurity curriculums to educate recent graduates and IT professionals. Designing and delivering such curriculums can be challenging as there are various factors that can either assist or hinder this task. To deal with this challenge, one should not consider the curriculum design in isolation from the delivery but rather in tandem [7]. This will provide to the curriculum designer a wider view of the issues [8] that need to be considered, potentially decreasing tensions that typically exist between curriculum design and delivery [9].

Another key factor that plays an important role in the development of an enhanced T&L cybersecurity environment is the supported student cohort diversity. In the case of postgraduate cohorts, the diversity degree of the group can challenge even more the curriculum design and delivery. Postgraduate cohorts may include professionals and/or recent graduated students, having different experiences and backgrounds with regards to knowledge and practical skills. Moreover, the globalization of the market has pushed educational organizations to offer their courses through distance learning and/or conventional class delivery [10] [11]. A course may be delivered to both online and face-to-face students. Such a requirement, to establish a blended educational environment, can put extra challenges to the curriculum design and delivery as the objective should be for all students (online and face-to-face) to receive a similar learning experience.

This work critically discusses the challenges in the design and delivery of an ethical hacking curriculum targeting diverse postgraduate cohorts in conventional and distance learning. Moreover, the practices that have been utilized to successfully address the identified challenges are presented. The findings aim to assist curriculum planners and developers to achieve a superior T&L cybersecurity environment in diverse postgraduate cohorts. Section 2 presents related work. Section 3 presents the design and delivery efforts of the cybersecurity curriculum, discussing the challenges faced. Section 4 provides good practices recommendations. Section 5 summarizes with conclusions.

2. RELATED WORK

There are various cybersecurity curriculum design guidelines that are proposed by different organizations, working groups and individuals. The Emerging Security Challenges Working

Group (ESCW) has proposed a reference curriculum design framework that offers guidance in identifying key cybersecurity areas and recommends learning objectives and key sources [12]. The Joint Task Force on Cybersecurity Education (JTF) is a collaboration between major international computing societies, including ACM, IEEE, AIS SIGSEC and IFIP WG 11.0. JTF has developed a comprehensive curricular guidance in cybersecurity education, identifying a wide range of knowledge areas and specific topics that should be taught [13] [14]. ISACA has developed two model curriculums providing a basic framework of the education required to develop the skills needed to work as an Information Security Management [15] or an Information Systems Audit and Control [16] professional. The UK government accredits cybersecurity training providers offering relevant courses against the nominated area(s) of the Institute of Information Security Professionals (IISP) Information Security Skills Framework [17]. An indicative topic coverage is listed in the respective certification scheme [18] that can assist the development of relevant cybersecurity curriculums. Curriculum guidelines offer information to a varying degree, focusing mostly on the topics that need to be covered and the skills that can be developed. This information is only part of the equation to develop a successful curriculum. When designing and documenting a new cybersecurity curriculum, educational organizations should analyze: a) the national policies and procedures that will drive the level of detail that is required, b) the curriculum objectives, c) their resources, and d) the target audience and its diversity. The analysis will allow organizations to a) adapt the proposed guidelines to their needs, b) extend them to cover aspects that are not included in the respective guidelines, and c) develop an effective T&L cybersecurity environment that will meet their needs.

There are many learning style models proposed in the literature [19]. To consider specific learning styles in a cybersecurity context, it is important to first identify what kind of learning elements are utilized in this discipline. This information will assist to promote the learning elements in a way to fit across different learning styles. Typically, there are four key learning elements that characterize the presentation of cybersecurity content/activities: a) Pictures/schemas (e.g. that explain security processes such as cryptography), b) Hands on/lab activities (e.g. to train on specific security techniques and tools), c) Listening (e.g. to be able to comprehend concepts but also to learn to communicate effectively with potential clients and identify their security needs. For example, in the context of risk assessments.), and d) Presenting/Reporting (e.g. communicate concepts and security evaluation results to a client, both orally and written). Neil Fleming's VAK/VARK model [20] proposes four sensory modalities (visual, auditory, read/write and kinesthetic) that seem to cover well the learning elements that are typically utilized in a cybersecurity context. Therefore, this model can be considered when specifying the teaching strategies to deliver a cybersecurity module and maintain a balanced approach with regards to supporting diverse learning styles.

3. ETHICAL HACKING CURRICULUM DESIGN & DELIVERY

This section presents the challenges and the T&L strategies utilized to address them when designing a curriculum for an Ethical Hacking course, considering diverse postgraduate cohorts. It should also be noted that the curriculum has been designed, developed and delivered by the same person.

3.1 Curriculum Design: Challenges & Solutions

The overall aim of the Ethical Hacking course was to examine a systematic approach to evaluate the security level of systems, to identify and document vulnerabilities and propose measures to enhance their security. This was one of the core courses to obtain a postgraduate Cybersecurity degree. To specify the curriculum design, Biggs' model [21] was utilized. Biggs' model articulates the idea of constructive alignment between the three key areas of the curriculum: the intended learning outcomes, what the student does to learn and how the student is assessed. This model was selected as it was expected to assist the planner to setup an enhanced T&L environment.

An appropriate template was utilized to document the curriculum design. The template was already specified by the academic institution. Initially, the course's outcomes were specified, focusing on acquiring skills and knowledge on the key steps of the systematic approach that is typically utilized in a penetration testing setup (plan-design-execute-analyze-report). Then the summative assessment methods have been selected to test the learning outcomes. These included delivering a report, critically discussing results from a penetration test that the students would have to carry out, and a written examination. The rationale of selecting as coursework a penetration testing report was that the report is a main element of the ethical hacking process that is provided to a client, if the test is conducted in a real setup. To write the report, one has to be knowledgeable of all key aspects of the penetration testing process, demonstrate practical skills and be able to critically discuss the results in the context of the client. All these skills are directly mapped to the course's learning outcomes. The written exam was selected to assess if the students acquired the key knowledge that is relevant to each learning outcome. Finally, the core T&L content/activities have been specified, including selecting the relevant formative assessments. Bloom's taxonomy of learning was utilized to focus on the main teaching content that should be taught.

Specifying the main content of the curriculum was challenging as a variety of issues needed to be considered. With regards to the specification of content, it was necessary to incorporate industry needs so that students could gain relevant expertise and knowledge and a competitive market advantage. It was considered that many companies require new hires to possess a university degree and specific cybersecurity-related professional certifications as an evidence of specialized in-depth expertise and proven knowledge. Having this in consideration during the course's curriculum design, the T&L material was aligned to cover information from best practices from leading organizations (e.g. NIST, SANS, ENISA, OWASP) and the curriculum of well-established certification exams such as CEH, OSCP, CREST, etc. As a result, key topics in Ethical Hacking have been selected to be taught.

Another issue that challenged the specification of the T&L strategies was the diverse student cohort that was expected to enroll to the course. The course was expected to be offered to online and face-to-face students. Even though distinct sessions would be delivered to online and face-to-face students, the objective was to specify common T&L methods. The overall idea was to setup a learning environment that would offer a similar experience to all students. This was a great challenge, especially considering that in online courses it is harder to keep the students engaged compared to a face-to-face case. To address this issue, appropriate technologies and tools had to be selected to deliver the curriculum.

The course was designed to be delivered weekly over two sessions. One session was specified to deliver the theoretical part. The second was a practical session were students could apply their knowledge. The first session was specified to have one-hour duration while the second session duration was set to two hours. Both the lecture and practical sessions have been delivered by the tutor to in-class students. With regards to online students, it was decided not to follow the approach of pre-recording sessions. The lecture was decided to run online and then students could work on the lab unattended. The tutor would provide her support through various means such as email, Skype, phone, etc.

With regards to the theoretical part, this was planned to be delivered through lectures, covering information with regards to each step of the penetration testing. Beyond the lectures delivery, a variety of other technologies/tools have been selected to form the learning environment and promote the module's objectives: a) Blackboard. This is a widely used platform to share content, communicate asynchronously (e.g. through forums), deliver assignments, etc., b) Adobe Connect. This is a well-known tool to deliver online sessions and interact synchronously with participants. Online sessions would be recorded and made available to the students, c) Cloud-based virtual laboratories developed to allow the students to practice their technical skills and work on their practical assignments.

3.2 Curriculum Development & Delivery: Challenges & Solutions

It was essential that different aspects of delivery (e.g. technologies/tools utilized) to be considered during the curriculum design. This assisted to select T&L strategies and align the course's learning outcomes with the respective curriculum design. Although delivery aspects have been considered during the curriculum design, it was expected that the effectiveness of the decisions made, and the degree at which the selected strategies facilitate learning, would be demonstrated/evaluated during the course's delivery.

The curriculum delivery itself posted new challenges that had to be overcome throughout the delivery of the course. This was the first delivery of the course. The curriculum was developed and delivered in tandem, something that posed a great challenge to the tutor in terms of preparation time. The fact that a thorough planning was initially performed during the curriculum design, greatly assisted the tutor and directed the material development. Without such a thorough planning, it would be very difficult to prepare a high-quality teaching material and support the curriculum's objectives in such a short timeframe between content development and delivery. Also, due to the research that was performed during the curriculum design, stimulating learning content has been identified from established organizations such as the USA Department of Defence Information Assurance Support Environment (IASE) and the SEED labs hosted at Syracuse University (New York), which have been adopted by the tutor in her delivery. Moreover, content was developed taking into consideration the design objective to align the curriculum with professional certifications. All the aforementioned actions, resulted into establishing an exceptional student experience and delivering a high-quality course, utilizing latest technologies and superior training, aligned with industry needs, while boosting students' preparation with regards to pursuing professional certifications and professional development.

Another challenge that needed to be addressed during the module's delivery was the diversity of the student cohort. The student cohort should fit the planned curriculum [22]. The curriculum should be designed taking into consideration the characteristics and qualifications of the student cohort. If the enrolled students do not fit well the planned curriculum, this can challenge the curriculum design and delivery. Distance learning students are sitting behind a device and they may disengage easier compared to in-class students. The tutor was well informed in advance of good practices with regards to online (and face-to-face) students. For example, she avoided reading passively from slides, but rather tried to discuss the topics in a natural way. Questions were posted during the lecture, instead at the end, to keep the students' attention. Also, the tutor payed attention to her voice tone to emphasize key points that were formatted in bold. Moreover, the lectures were delivered utilizing content-rich presentations such as text, tables, schemas, YouTube videos and tools' demonstrations. The rationale of the aforementioned content elements was to create an enhanced material and student experience. The aim here was to provide a balanced content, applicable to a variety of learning styles, targeting to maintain the attention of students. Another teaching strategy was to provide real world examples so that students could map and comprehend ethical hacking concepts. Also, the tutor provided extra material (e.g. articles, web links, etc.) through Blackboard to support independent study. With regards to practical assignments, attention to detail was considered to provide clear instructions to online students that executed the lab unattended. All the aforementioned points have not been included in the curriculum design documentation. This was mainly due to the template that has been utilized to document the design. This meant that it was up to the tutor to be aware of best practices with regards to distance learning delivery.

The aforementioned teaching strategies have also been applied during the in-class delivery to keep the students' engaged with the course. Overall, all strategies worked in the in-class setup but some adjustments were needed to align better with the in-class cohort. The diversity of the student cohort with regards to their professional qualifications has been identified to create a tension between the curriculum design and delivery. This was a postgraduate module. IT professionals and recent BSc graduates were expected to join the MSc Cybersecurity and enroll to Ethical Hacking. This meant that they had different experiences and knowledge with regards to practical and transferable skills (e.g. communication, analytical skills, time management, etc.). The professional qualifications of some of the students assisted them to finish fast from laboratory assignments compared to recent graduated students. This created a tension between in-class students, some felt that they needed more challenging material while some others were happy with the existing difficulty level. Since this issue was identified early in the delivery, actions have been taken to tackle this situation. Extra (optional) material was provided to students that finished their laboratory assignment to keep them engaged while other students were still working on the mandatory assignment. In future deliveries, the tutor provided pre-module material to guide independent study of students that felt that they lack some basics. This way they were better prepared and followed assignments easier. Moreover, although the refined details kept the online students happy, part of the in-class cohort felt that the details could have been omitted to challenge their skills further. This issue was addressed by maintaining two versions of in-class assignments. One version included refined details while the other version omitted detailed instructions to challenge the knowledge and skills of students. Students selected the version they felt more comfortable to work with and improve their skills.

The online lectures have been delivered live and at the same time, they have been recorded. To further provide a similar experience to all students, recordings have been offered to all online and in-class students, so they could watch the lectures in case they missed a session or just wanted to view again the delivery. This action was embraced by all students that reported their satisfaction and a superior learning experience.

Utilizing a variety of technologies/tools to deliver the program created an enhanced learning environment but at the same time it burdened both the tutor and the students that needed to be trained to use them. The tutor was well trained on the technologies utilized, therefore, it has been easier to introduce these technologies to the students. If the situation was different, the tutor would have needed to get familiar with many technologies/tools in a short timeframe, this would probably have affected her delivery. Moreover, the tutor provided manuals of the tools utilized and troubleshooting guides. This material was given proactively so that students could easily search for information if they encounter any issue. This approach worked well as problems were quickly tacked by the students themselves, minimizing tutor's intervention. Overall, the decision to integrate various communication and teaching means, seemed to work well with the target audience (diverse postgraduate cohorts).

Quality of teaching plays a key role for a successful delivery. The tutor is essential to be open minded and demonstrate flexibility in teaching. Such an ability is essential to deal with diverse student cohorts where some students may disengage from the current activities. Therefore, the tutor must be able to adjust dynamically his/her delivery to re-engage students. Moreover, it is important to dynamically adjust learning activities and assessments to meet and evaluate the learning outcomes, taking into consideration the needs of the student cohort. Of course, this to happen, needs to be supported by the curriculum that has to demonstrate some flexibility with regards to the T&L strategies and activities. If the curriculum documentation is too specific with regards to aspects such as assessments, etc., and does not provide flexibility to the tutor to adjust, this can hinder the delivery and students' satisfaction. This situation can be dealt with by providing formal feedback to the university and request changes to be made to the curriculum. This confirms that curriculum design, development and evaluation is a continuous work.

Moreover, it needs to be considered that in this case study, the same person was involved with the curriculum design, development and delivery. This has made easier the development and delivery of the curriculum as the person responsible had a view of all aspects involved. However, if the situation was different, potentially the curriculum development and delivery would not have been a straightforward process. This is mainly due to the fact that the current template utilized for documenting the curriculum design does not include clearly all the things that the planner had considered, e.g. alignment with specific certification exams, good practices to consider for delivering online modules, etc. If such cases occur, this means that key information considered by the planner may not be evident to the implementer of the curriculum, leading to difficulties to develop the curriculum and meet the course's objectives. Therefore, it is not only necessary to consider evaluating and updating the curriculum itself, but it is equally important to utilize documentation templates that include key information that will support a successful development and delivery of the respective course. Institutions should make sure to adopt such design templates that can support the work of all the team members involved (e.g. curriculum planner/developer/tutor).

3.3 Quality Assurance

Evaluating the quality of T&L was a continuous task. The course has been delivered for four years and fifty students have attended it. Student questionnaires indicated that there was a high level of student satisfaction. Some students recommended to enhance some of the labs to demonstrate more features of the relevant tools and this will be considered in future deliveries. A number of students were providing their feedback informally throughout the delivery of the module, this greatly assisted the tutor to adjust the T&L strategies to address the issues and keep the students satisfied. Moreover, the institutional quality assurance strategy assisted in providing high-standards learning material. The graded assessment components have been internally and externally verified and moderated. This action contributed in delivering useful assessments that the students found essential to assist them gain knowledge and develop skills that are required in the real world. Moreover, the good practices utilized have been praised by the external examiner of the course.

4. GOOD PRACTICES

This section briefly discusses good practices for the design and delivery of a cybersecurity curriculum targeting diverse postgraduate cohorts.

4.1 Organizational Level

The support of the organization itself in the overall process of the curriculum design and delivery is imperative. The organization should allocate resources to first design the curriculum and then deliver it. This will allow the planner and developer to have enough time to perform the intended tasks and build a superior T&L environment. Moreover, in a cybersecurity context, aspects of delivery should be considered while designing the curriculum. This requires the curriculum planner to have deep knowledge of the subjects to be taught. This knowledge will facilitate thorough planning of the material to be covered. The organization should involve people with the appropriate expertise and knowledge to design the curriculum. Also, where possible, the curriculum planner should also be the one to implement the curriculum, or at least supervise this task. Appropriate documentation is another element that should be promoted by the organization. Curriculum design templates should be selected or developed that will guide people to provide the necessary design details that will help the developers build the T&L environment that was envisioned by the curriculum designer. With regards to distance learning, the organization should fund training of tutors on best practices, so they are able to deliver successfully online content and interact with the students. Finally, the organization should realize that an appropriate budget should be allocated to create a superior T&L environment, enriched with cutting-edge technologies and tools.

4.2 Material Development

The delivered material plays a crucial role in the success of the course and whether the learning objectives are met. In a cybersecurity context, it is important to have a balanced content, using elements that are applicable to a variety of learning styles. Moreover, the material should be aligned with best practices, standards and professional certifications that are required by the local and/or international industry. This will greatly promote students' employability. Superior material that is developed by leading organizations should be reused, if permitted by copyrights. This will benefit the students as they can build advanced knowledge and skills. Assignments with varying challenging levels should be considered to address the case of different knowledge and experiences of the student cohort. With regards to online students, clear instructions with refined details should be given to enhance their experience when working unattended. Industry leaders should be invited to deliver talks and assist in aligning the curriculum with industry needs.

As discussed, teaching the same curriculum to face-to-face and online students is challenging. Informal feedback from the students throughout the course delivery is imperative to address issues that are not working well. This requires the tutor to have an open communication with students to identify issues early in the delivery and seek solutions. This is for the benefit of both the students and the taught curriculum.

5. CONCLUSIONS

Development and design of a cybersecurity curriculum is a continuous work. A variety of challenges exist that need to be taken into consideration to minimize tensions that exist between curriculum design and delivery activities and promote a successful T&L environment. Following, the key points identified through the presented case study are summarized: a) The curriculum design template and provided details [23] play a driving factor for the development and delivery of the respective module. This is especially important in case where the curriculum planner is not the same person that will develop and/or deliver the module, b) In a cybersecurity context, Biggs' and Bloom's models were beneficial to assist in the design and delivery of the curriculum. It also demonstrated that design and delivery aspects need to be considered in tandem in order to minimize any potential tension between design and delivery tasks, c) A blended postgraduate cohort greatly challenges the curriculum design and delivery. Keeping students engaged is one of the key challenges that need to be considered. The dynamics of engaging a blended postgraduate cohort can complicate the curriculum delivery. It is upon the tutor to identify the cohort's disengagement, act promptly at any given time, adjusting teaching/learning strategies and activities and re-engaging students. The tutor's efforts can be supported by utilizing different teaching methods. This can increase the chances to maintain the students' interest.

6. REFERENCES

[1] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Accessed 5 August 2020]

[2] J. Rantapelkonen and M. Salminen, The fog of cyber defence, Juvenes Print Oy, 2013.

[3] J. Leclair, Protecting our future, volume 2: Educating a cybersecurity workforce, Hudson Whitman/ Excelsior College Press., 2015.

[4] A. McGettrick, L. N. Cassel, M. J. Dark, E. K Hawthorne, J. Impagliazzo, "Toward Curricular Guidelines for Cybersecurity", SIGCSE '14: Proceedings of the 45th ACM technical symposium on Computer science education, 2014.

[5] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira and E. Stavrou, "Global Perspectives on Cybersecurity Education for 2030:A Case for a Meta-discipline," in 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE Companion '18), 2018.

[6] L. Taylor and J. Parsons, "Improving Student Engagement. Current Issues in Education," 2011. [Online]. Available: https://cie.asu.edu/ojs/index.php/cieatasu/article/download/745/162 . [Accessed 5 August 2020]

[7] UWA - University of Western Australia, Centre for the Advancement of teaching and learning, "Curriculum Development – Key elements and relationships in curriculum," [Online]. Available: https://www.academia.edu/36086759/CI_General_Curriculum_Development_UWA_1_ . [Accessed 5 August 2020]

[8] S. Marble, S. Finley and C. Ferguson, "Understanding Teachers' Perspectives on Teaching and Learning," 2000. [Online]. Available:

http://www.sedl.org/pubs/teaching07/UnderstandTeachersPerspectives.pdf. [Accessed 5 August 2020]

[9] M. S. B., “Challenges of Curriculum implementation in Learning Institutions,” 2010. [Online]. Available: https://sitwe.wordpress.com/2010/12/03/challenges-of-curriculum-implementation-in-learning-institutions/. [Accessed 5 August 2020]

[10] M. Cleveland-Innes and D. Garrison, “An Introduction to Distance Education: Understanding Teaching and Learning in a New Era,” Taylor & Francis, 2010, p. 165.

[11] D. Garrison and N. Vaughan, Blended Learning in Higher Education: Framework, Principles, and Guidelines, Wiley, 2007.

[12] NATO, “Cybersecurity - A Generic Reference Curriculum,” 2016.

[13] Joint Task Force on Cybersecurity Education (JTF), “Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity,” 2017.

[14] M. Bishop, D. Burley, S. Buck, J. J. Ekstrom, L. Futcher, D. Gibson, E. K. Hawthorne, S. Kaza, Y. Levy, H. Mattord and A. Parrish, “Cybersecurity Curricular Guidelines,” in Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology, 2017.

[15] ISACA, “ISACA Model Curriculum for Information Security Management,” 2012.

[16] ISACA, “ISACA Model Curriculum for IS Audit and Control,” 2012.

[17] IISP, “IISP Information Security Skills Framework,” 2010.

[18] GCHQ, “GCHQ Certification of Cyber Security Training Courses,” 2016.

[19] F. Coffield, D. Moseley, E. Hall and K. Ecclestone, Learning styles and pedagogy in post-16 learning: a systematic and critical review, Learning & Skills Research Centre, 2004.

[20] W. L. Leite, M. Svinicki and Y. Shi, “Attempted validation of the scores of the VARK: learning styles inventory with multitrait–multimethod confirmatory factor analysis models,” Educational and Psychological Measurement, vol. 70, no. 2, pp. 323-339, 2010.

[21] J. Biggs and C. Tang, Teaching for Quality Learning at University, McGraw-Hill and Open University Press, 2011.

[22] A. Kelly, The Curriculum: Theory and Practice, SAGE, 2009.

[23] R. DeSantis, “Creating a consistent curriculum design,” 2015. [Online]. Available: https://www.moodlerooms.com/2015/09/22/creating-consistent-curriculum-design/. [Accessed 5 August 2020]