Inter-Curricular Cybersecurity ABET Assessment Perspectives

Suzanna Schmeelk[1], Denise Dragos[2], Joan E. DeBello[3]

St. John's University, Queens, New York, United States of America[1, 2, 3]

Abstract

The field of cybersecurity has been rapidly developing over the past few years primarily from the quickly changing legal requirements for maintaining privacy and security of assets and their internal sensitive data. To address the changes within the computing field, the Accreditation Board for Engineering (ABET) proposed preliminary cybersecurity accreditation criteria a few years ago. After ABET introduced the preliminary criteria, less than 10 universities have both applied and become ABET Cybersecurity accredited. This research explores ABET Cybersecurity Assessment perspectives from multiple courses in the Bachelor of Science program at St. John's University in Queens, New York. Specifically, this research first examines current published trends on ABET accreditation. We, then, examine how different ABET assessment criteria are assessed with respect to three core cybersecurity courses in our program: Network Security, Digital Forensics, and Secure Software Development. These courses were chosen as they introduce three different perspectives of cybersecurity: development, risk management, and forensics. Interestingly, the inter-curricular courses are all inter-related and share assessment topics. Our research explores how the courses share fundamental assessment topics; but, each has stronger relationships to a different perspective within the field. Finally, the paper concludes with both lessons learned, from the ABET assessments, and prospective future cybersecurity assessment research topics.

Keywords: *Accreditation Board for Engineering, ABET, Assessment, Network Security, Secure Software Development, Digital Forensics, Undergraduate Program, New York State*

1. Introduction

Cybersecurity has become fundamental to all information networks and systems. One of the recent drivers for the importance of cybersecurity are regulations and the protection of factors which go into risk assessments such as reputation, life protection, among other concerns. To keep pace with the changing cybersecurity industry needs and research, academic institutions have been developing and expanding curricula to both address the real world changes and to prepare students for entry into the international workforce.

2. Review of Literature

Undergraduate programs are normally accredited by a governing body that oversees the curriculum and resulting data of programs within institutions. Given the popularity of many engineering, computing and more recently cybersecurity programs, specialized accreditations are highly sought after to strengthen the program simultaneously creating a competitive advantage over programs that are not specifically accredited with top accreditors such as the Accreditation Board for Engineering and Technology (ABET) that focuses on specific outcomes to see if a program has met fundamental and foundational goals necessary for the program to be successful and for graduates to succeed [2, 7, 8].

2.1 ABET Accreditation

ABET created an accreditation criteria for cybersecurity programs that would offer flexibility to the institution as well as extensive guidance by the CSEC 2017 and expert input. In its first year of accreditation, only a small group of selected cybersecurity programs were accredited as pilots [9].

If a program is accredited, it is periodically renewed as long as it is maintaining its educational quality standards. Because the accreditation is highly sought after and highly valued in academia, the process is very time consuming and often rigorous.

Many of the ABET criteria that were finalized as part of its standards were guidelines that were created based on recommendations from key and prominent figures in computer science, engineering and technology who served as members of the ACM, SIGCSE and other prominent organizations [11].

With help from professional organizations such as the Computing Sciences Accreditation Board (CSAB), IEEE Computer Society and the Association of Computing Machinery (ACM), ABET's criteria for the cybersecurity curriculum was developed and this will help to maintain that each program that receives accreditation will continue to develop and meet continuous improvement measures based on assessment that is provided to its constituents which include students, family, academic institutions, government agencies and the public community [6].

Because of its popularity, both within the US and internationally, many universities and colleges are offering more courses and programs designed to meet the needs of careers that are geared towards qualified cybersecurity professionals. The cybersecurity programs that are accredited by ABET will be complimentary to programs that already are part of the ABET accreditation such as computer science, information technology and information systems [5].

2.2 Assessment

A few papers have discussed ABET assessment criteria. Nitta and Eiselt [3] discussed an assessment where the questions mapped to the 2019 ABET Computing Accreditation Commission (CAC) Student Outcomes (SO). Sanderson [4] discussed computer science ABET assessment criteria in the early 2000s. There are limited, if any papers, on the new ABET cybersecurity accreditation assessment criteria.

3. Cybersecurity and Digital Forensics Curriculum

As the St. John's University website states, students who graduate with a BS in Cybersecurity from St. John's University at the Collins College of Professional Studies, will attain meaningful positions toward successful careers in cybersecurity or a related field, will advance their professional development through self-directed learning and or graduate study, will practice cybersecurity professionally and with specific regard to ethical and societal responsibilities. Additionally, it is noted that students who major in cybersecurity at St. John's University will be able to analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions; design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline; communicate effectively in a variety of professional contexts; recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles; function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline; and apply security principles and practices to maintain operations in the presence of risks and threats [1].

A sample 4 year cybersecurity major plan consisting of 120 credits [1] is as follows, (available here).

Year 1

Fall Semester (15 credits)	Spring Semester (15 credits)
Foreign language elective	CUS1116 Programming Fundamentals II
CUS1115 Programming Fundamentals 1	Foreign language elective
DNY1000C Discover NY	ENG1100C Literature in a Global Context
MTH1009 Calculus I	MTH1022 Discrete Mathematics
FYW1000C First Year Writing	CSS1005 Fundamentals of Cyber Security

Year 2

Fall Semester (15 credits)	Spring Semester (15 credits)
CUS1126 Introduction to Data Structures	CUS1165 Database Management Systems
SCI1000C Scientific Inquiry	NET1011 Introduction to Networks
CSS1006 Management of Information Security	HIS1000C Emergence of a Global Society
MTH1013 Probability & Statistics I	MTH1014 Probability and Statistics II
PHI1000C Philosophy of the Human Person	THE1000C Perspectives on Christianity

Year 3

Fall Semester (15 credits)	Spring Semester (15 credits)
CSS1021 Cyberlaw and Ethics	NET1015 Routers and Router Concepts
DFR1001 Intro to Digital Forensics	CSS1011 Network Security
Free elective	Free elective
ECO1001 Principles of Economics I	ECO1002 Principles of Economics II
THE1040 Moral Theology	PHI1020 Ethics

Year 4

Fall Semester (15 credits)	Spring Semester (15 credits)
PHI3000C Metaphysics	CSS elective*
CSS1032 Cyber Threats and Detection	SPE1000C Public Speaking for College Students
CSS1035 Secure Software	THE any elective
CSS elective*	Free elective
Free elective	Free elective

4. Curriculum Assessments

Our university chose six main Student Outcomes (SOs). Our SOs involve the following topics: (1) compute complex problems, (2) design, implement, and evaluate solutions, (3) communicate effectively, (4) recognize professional responsibilities, (5) functional effectively in a team, and (6) apply security principles and practices. This paper focuses on the shared and unique assessments across the three following courses: Introduction to Digital Forensics, Network Security, and Secure Software Development.

4.1 Shared Relationships between Courses

Digital Forensics, Network Security and Secure Software Development share commonalities in that students need to be able to function effectively in a team and recognize professional responsibilities in all of these subfields. Furthermore, from a cybersecurity perspective, both Digital Forensics and

Network Security need to share SOs for communication. Lastly, all the courses need students to be able to apply security principles and best practices.

Network security and Secure Software Development share some relationships especially when it comes to designing, implementing and evaluating solutions. The actual software development and deployment of network security risk mitigation techniques are closely related at the undergraduate perspective. As Digital Forensics is currently a specialization within our Cyber Secure System degree, we are not yet focusing undergraduate study on the development of new digital forensics tools.

4.2 Unique Relationships among Courses

We found that Digital Forensics needed to be the focus of our assessment for students being able to compute complex problems. Digital Forensics typically involves cyber-investigations, which in many cases involve complex malware or breach problems. From a cyber secure system perspective, many large and complex problems involve data mining, which is traditionally an entirely separate course.

5. Lessons Learned and Future Research

We have learned a great deal from undertaking the ABET cybersecurity accreditation. Furthermore, there are many future research topics which have evolved out of accreditation and assessments.

5.1 Lessons Learned

We have learned many lessons from undertaking the ABET cybersecurity accreditation and assessment development. FIrst, the division must support the process and the dean must also offer the support in order to have the support of the university. Because it is a rigorous process, the support is essential for the faculty throughout the process who are committed to the assessment and data collection process that is essential in the ABET process.

Second, one important element is to consider in advance is the actual student data collection. Student data can either be collected manually or digitally. The manual collection of data may require that the student work is actually digitized. Depending on the collection methodology, pages may be unmarked or stapled together causing difficulty for digitization. Also, many courses employ a Learning Management System (LMS). Depending on which course tasks are employed for assessment, it can be difficult to collect all the student data out of the LMS. Therefore, think carefully in advance on how the actual data will be further collected and categorized.

Third, having an external visiting professor, an external ABET expert and an additional consultant help with the ABET process was a huge benefit for the full time faculty as they helped the process go smoother by alleviating some of the paperwork and offered guidance. The external consultants also helped with the readiness report and the self study report. These were essential to the process and valuable resources to the faculty.

5.2 Future Research

There are many paths for future research. First, we can explore assessments in other courses within our Cyber Security Systems program which are currently employing ABET assessments. Second, we can report on our self-study reflections of our program. Third, we can report on our continual improvement metrics. Such metrics may involve changing our course prerequisites, adding additional courses to our curriculum, changing assessment tasks, among others.

6. Conclusions

The ABET cybersecurity assessment process has been very insightful. First, it motivates faculty to deeply reflect on their courses from the point-of-view of student outcomes. Second, it provides motivation for faculty to communicate and plan topics within each course. Third, it provides motivation for faculty to communicate with students to learn about their difficulties. Overall, it is a very large time commitment; however, the students' learning is the focus.

References

[1] St. John's University (2020) Cyber Security Systems, Bachelor of Science. Retrieved from: https://www.stjohns.edu/academics/programs/cyber-security-systems-bachelor-science

[2] ABET (2018) ABET Approves Accreditation Criteria for Undergraduate Cybersecurity Programs.Retrieved:https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs

[3] Christopher Nitta and Kurt Eiselt. 2020. Using the CS2013 Exam for ABET Student Outcome Assessment. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). Association for Computing Machinery, New York, NY, USA, 1305.

[4] Donald B. Sanderson. 2009. Revising an assessment plan to conform to the new ABET-CAC guidelines. In Proceedings of the 40th ACM technical symposium on Computer science education (SIGCSE '09). Association for Computing Machinery, New York, NY, USA, 352–356.

[5] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018 Companion). Association for Computing Machinery, New York, NY, USA, 36–54.

[6] Greenlaw, Raymond, Andrew Phillips, and Allen Parrish. "Is it time for ABET cybersecurity criteria?." ACM Inroads 5.3 (2014): 44-48.

[7] Conklin, Wm Arthur, Raymond E. Cline, and Tiffany Roosa. "Re-engineering cybersecurity education in the US: an analysis of the critical factors." 2014 47th Hawaii International Conference on System Sciences. IEEE, 2014.

[8] Rajendra K. Raj., and Allen Parrish. "Toward standards in undergraduate cybersecurity education in 2018." Computer 51.2 (2018): 72-75.

[9] Rajendra K. Raj, Vijay Anand, David Gibson, Siddharth Kaza, and Andrew Phillips. 2019. Cybersecurity Program Accreditation: Benefits and Challenges. In Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19). Association for Computing Machinery, New York, NY, USA, 173–174.

[10] Weinstein, Mark D. "Cybersecurity Program Receives Prestigious ABET Accreditation." (2019).

[11] McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K., & Impagliazzo, J. (2014, March). Toward curricular guidelines for cybersecurity. In Proceedings of the 45th ACM technical symposium on Computer science education (pp. 81-82).