Synergy of ABET Accreditation and CAE Designation

Abstract - One of the impediments to applying for the NSA/DHS Center of Academic Excellence in Cyber Defense designation is the fear that it will require a great change to the curriculum or may negatively impact international functional accreditations. This paper provides lessons learned while preparing to apply for this designation while maintaining and enhancing our international ABET (computer science) accreditation. We found synergy between the new cybersecurity requirements for accreditation and CAE designation. Additional benefits of CAE designation include standards which help design, build, market and assess strong, well-defined cybersecurity programs in both computer science and business, each of which caters to a different audience of students and future employers. Finally, the CAE designation requires collaboration inside and outside the University, encouraging a more active outreach to other programs. All of these benefits work in concert with the ABET accreditation which explicitly requires an internationally recognized curriculum that is taught by experts in their field and regularly assessed.

Keywords

CAE, ABET, AACSB, accreditation, cybersecurity

1 INTRODUCTION

The National Security Agency (NSA) and Department of Homeland Security (DHS) supported Center of Academic Excellence in Cyber Defense Designation (CAE) was set up with a goal of increasing the quality of the Nation-wide cyber workforce. Since that time, the program has grown to include over 200 academic institutions with two-year, four-year, and graduate programs and research focuses. With many means of gaining cybersecurity skills and very strong career opportunities, academic institutions are adding cybersecurity programs with the intent of gaining students while ensuring their programs remain rigorous and respected. [1]

Many institutions are looking at the CAE designation to help differentiate their programs. Since the designation includes mapping to learning outcomes and a community of support, this makes starting a program easier than starting from scratch. Most major universities maintain established national or international functional accreditations such as ABET which must take precedence over new programs or designations. Often departments will not take on a new program until they are clear on the benefit, the amount of work, faculty expertise requirements and importantly can ensure no negative impact on their functional accreditations.

The rest of the paper is organized as follows. Section two discusses some of the cybersecurity requirements allowed or required of ABET programs as well as how the CAE designation fully supports this accreditation. Section three discusses our processes and curriculum changes in applying for the CAE while maintaining our ABET accreditation. Section four discusses some of the key lessons learned associated with navigating current accreditations while starting a new cybersecurity program. Finally section five summarizes our findings.

2 FUNCTIONAL ACCREDITATIONS AND CAE

Over the past decade, employers have changed their perceptions of defensive cybersecurity from being the responsibility of system administrators

to becoming an integral function of most organizations including network, mobile device, data science, financial, marketing, personnel and operational security. As such, employers need graduates with a solid basis in cybersecurity fundamentals combined with education in many functional areas.

A decade ago, the CAE designation required a mapping to learning outcomes that followed the old perception of cybersecurity as an extension of system administration. This led many degree programs such as computer or data science to believe that the CAE designation did not align with their expected learning outcomes and curricula. Now, the designation requires a mapping of learning outcomes to the NIST National Initiative for Cyber Education (NICE) framework, updated in 2017, by an entire community of computer science, business, academic and industry professionals. The CAE designation requires either a technical or non-technical foundation in cybersecurity concepts as well as a fairly rigorous choice of functional areas allowing programs to customize their programs. This requirement allows inclusion of traditional technical computer science and data analysis as an integral part of cybersecurity. [2]

Many computer science departments will avoid additional accreditations and designations either because they believe the benefits do not outweigh the amount of work required or because they believe it may have a negative impact on their ABET accreditation. Since many programs have successfully navigated the requirements for ABET along with CAE designations, it is clearly possible to maintain both but is there synergy in maintaining both functional accreditations and CAE designations? Our experience shows that while the CAE designation may require building some additional coursework, the mapping and assessment processes associated with both the accreditation and designation work in concert to produce a better overall computer science program.

2.1 ABET (CS) and CAE Designation

ABET is the primary internationally accepted accreditation for undergraduate engineering and computing programs. There are currently 375

institutions accredited by the ABET Computing Accreditation Commission [2]. It lays out expected standards for faculty qualifications, curricula and assessment of learning outcomes. Just this year, ABET added a requirement for a focus on cybersecurity throughout the curriculum for all computing program accreditations. While ABET standards describe "what" needs to be addressed, it leaves the "how" to the academic institution. ABET assessors and evaluators require evidence of both curriculum and assessment of those areas it requires. The academic institution must justify how its programs meet these expected outcomes. [4]

To meet new ABET accreditation requirements, computer science and computing programs will require either curriculum development or enhancement of existing courses in the areas of technical cybersecurity. Since there is a shortage of technical cybersecurity and data science faculty, often computer science and computing programs will have to add cybersecurity to their curriculum without support from a cybersecurity expert. Many computer science programs find that most of the classroom-based cybersecurity resources focus on systems administration and information technology aspects leaving out the programming, data science and mathematics analysis concepts expected of an ABET-accredited computer science program. Parrish et al. [5] propose a framework for cybersecurity education that either augments traditional computing programs with cybersecurity content or development of new cybersecurity programs. They recognize that new cybersecurity degree programs generally require different expertise than found in existing computer science programs. They further describe resources which underscore both the difference between and importance of separate programs while and providing some resources for inclusion or development of cybersecurity areas of study. The ACM and IEEE Computer Society joint published a computing curriculum or computer science programs in 2013 and cybersecurity programs in 2017 [4]. The curriculum for computer science does not address cybersecurity, while the curriculum for cybersecurity provides a series of learning outcomes separated by areas of study. ABET has defined standards for a newly accredited degree in cyber operations, yet has not provided guidance for the inclusion of

cybersecurity into the separately accredited computer science program. The CAE designation was created two decades ago and has helped bring together academic, government and industry professionals. As such it is currently the prevailing guideline for creating an academic cybersecurity program or certificate option.

Before applying to become CAE designated, programs must be in existence for at least three years. There are, however, two requirements for designation that can be of great help in implementing a cybersecurity program even if not applying right away. First, a program must map learning outcomes and assessment methods to specific areas defined in the NIST National Initiative for Cyber Education (NICE) framework. It includes a series of seven cybersecurity-related categories and 36 specialties including those that are more computer science related areas and those that are more traditionally business or information technology oriented. Each of these lists knowledge, skills and abilities as well as means to assess each. ABET evaluates a program's knowledge, skills and abilities as well as documented assessment of each, so the NICE framework is a good start for the ABET requirement to incorporate cybersecurity into the curriculum. [4]

In addition to the NICE framework, the CAE designation application provides some guidance on which of the categories and number of specialties required to have a robust cybersecurity program. Additionally, it requires a commitment at the Provost-level and collaboration with departments outside Computer Science as well as interaction with local industry. While these requirements are more detailed than required by ABET, departments could benefit from understanding the methodology and intent of the CAE program. By doing so, they can decide whether to simply meet ABET requirements, or start on a path toward creating a strong, tailored cybersecurity program that meets the needs of the faculty, students and industry.

3 CURRICULUM CHANGES

The Computer Science and Engineering Department at our university offers Bachelor and Masters degrees in Computer Science, focused on programming, low level systems analysis, mathematics, data science, network, operating system and system security. Additionally, we have created new undergraduate and graduate certificates in Cybersecurity that register successful completion on a student's transcript.

3.1 Undergraduate Computer Science

For more than twenty-five years, the Bachelor of Science in Computer Science at our University has been an ABET accredited degree. The new ABET accreditation standards require integration of secure computing with no direction on how to implement, so we chose to better define by addressing the CAE requirements including the NICE curriculum mapping. ABET standards require specific knowledge obtained through programming, database, network and operating systems and mathematics courses all of which are foundational to technical aspects of cybersecurity. Since the new ABET standards require some integration of cybersecurity into the curriculum, we chose to add cybersecurity as a required course while modifying some of our core curricula to add cybersecurity concepts. This way we ensure that cybersecurity concepts are addressed and assessed with each student in the program. We turned to the CAE designation requirements including mapping to NIST NICE guidelines to help determine which aspects of cybersecurity to incorporate. We found many of the NICE areas of specialties helpful in integrating computer science focused cybersecurity knowledge into the existing curriculum. Further, the technical core requirements for the CAE mapping provided an excellent set of knowledge, skills, abilities and assessments useful in building and updating a cybersecurity-focused course. Table 1 describes the foundational and core technical subject areas that we incorporated into both our Bachelor and Masters program.

Table 1 Mapping of NICE Specialization to Undergraduate Computer Science Courses	
NICE Specialization	**Computer Science Courses**
Foundational Cybersecurity Foundations Cybersecurity Principles IT Systems Component	**Core Technical** Basic Cryptography Basic Networking Basic Scripting and Programming Network Defense Operating System Concepts

Table 2 lists the 14 optional areas we chose to map our undergraduate program to in preparation for CAE designation. Computer Science faculty were pleasantly surprised that more than 80% of CAE mapping guidance was already covered in one or more courses required by the ABET accreditation. This helped faculty to understand that cybersecurity enhances but does not replace traditional computer science principals, and allowed us to gain greater faculty support for the inclusion of cybersecurity into the curriculum.

Table 2 Mapping of NICE Specialization to Undergraduate Computer Science Courses	
NICE Specialization	**Computer Science Courses**
Foundational (Table 1) **Core Technical (Table 1)** **Optional** Algorithms Data Structures Database Management Systems Databases IA Architectures IA Standards Intro to Theory of Computation	Principles of Cybersecurity Data Structures and Program Design Database Systems Operating System Concepts Introduction to Computer Networks

Linux System Programming Low Level Programming Network Technology and Protocols Operating Systems Hardening Probability and Statistics Vulnerability Analysis Windows System Administration	

3.2 Graduate Computer Science Certificate

ABET does not accredit graduate programs in Computer Science, so there is greater flexibility in defining programs. Again, we used the CAE designation requirements to help build a graduate certificate in cyber security and defense that provides graduates with strong enough knowledge and skills to be valuable to local employers. Our industry leaders requested a strong focus on cybersecurity programming and low-level systems analysis, so we incorporated specific NICE specializations into existing and new courses. The CAE requires graduate program coverage of foundational, and core technical areas as well as seven optional areas and a Thesis or capstone experience. Table 3 lists those areas and courses we chose to map to the CAE requirements.

Table 3
Mapping of NICE Specialization to Graduate Computer Science Courses

NICE Specialization	**Computer Science Courses**
Foundational (Table 1)	Cybersecurity Programming and Analysis
Core Technical (Table 1)	Cyber and Infrastructure Defense
Optional	Computer Networks (Graduate)
Operating Systems Theory	Operating Systems (Graduate)
Network Technology and Protocols	Cyber-related Thesis or Project
Vulnerability Analysis	
Secure Programming Practices	
Intrusion Detection/Prevention Systems	
IA Architectures	

Cybersecurity Ethics	

4 LESSONS LEARNED

Through the process of creating cybersecurity courses and later defining a program which could be CAE designated, we had a number of lessons learned that other academic institutions might find useful.

4.1 Map to CAE when creating cybersecurity courses

The NICE guidelines prescribed by the CAE provide a set of knowledge, skills, abilities as well as means for assessments of cybersecurity-related concepts. Rather than simply choosing a cybersecurity textbook and hoping that it addresses the aspects of cybersecurity, a course developer can use the CAE designation requirements to build a course that is mapped to internationally accepted guidelines. This mapping lists very specific knowledge, skills and abilities which help course developers better understand prerequisite knowledge as well as which topics lend themselves to hands-on, lab-based skills.

Additionally, though application for the CAE designation requires a program to be in existence for at least three years, building a course to meet a set of requirements is far easier than retrofitting. The CAE requires a mapping to more than one course, so building the fundamental course to these standards allows the course designer to properly align prerequisite subjects, and advise inclusion of additional subject matter in other courses.

4.2 CAE helps to formalize ABET accreditations requirements

As noted, the new requirements for ABET accreditation call for an integration of cybersecurity principles into the curriculum but stops short of defining what is acceptable. ABET gives great latitude to the experts assigned to evaluate the programs. These experts are typically tenured faculty with twenty or more years in academia who may or may not specialize in cybersecurity or data science. Explanations of sufficiency in cybersecurity curriculum are bolstered by national or international community consensus

provided through NICE guidelines and CAE designation, as these are the most established, internationally accepted cybersecurity education community guidelines.

4.3 CAE encourages cross-collaboration and University level support

There are seven criteria required for CAE designation. Among them are a mapping of curriculum to standards, faculty engagement, collaboration outside a single department and outside the University and importantly Provost-level endorsement.

Like many Universities, we identified cybersecurity as one of the key areas of interest among students and employers. Both our Computer Science and Business programs started to fill that community need about five years ago. This focus included hiring cybersecurity and risk analysis focused faculty and creating individual courses. As student and employer interest grew, each department separately created undergraduate and graduate certificate programs.

While both business and computer science had strong cybersecurity programs, we had yet to work together until preparing to apply for the CAE which required University level collaboration. Once we started sharing our curricula and meeting with industry, we recognized that instead of competing for students, we could market the CAE description of technical and non-technical cybersecurity. The technical description deals with traditional computer science topics like programming, cryptography, mathematics-based data science, networks and operating systems. The non-technical description deals with personnel security, data privacy and risk analysis. These descriptions and collaboration allowed us to build and market both programs to different audiences rather than competing for attendance. The result of working together has been an increased university-wide interest in cybersecurity which has benefitted enrollment and outreach in both computer science and business cybersecurity programs. Though cybersecurity is less prescribed in the AACSB business accreditation than in the ABET accreditation, many business departments have also identified the CAE as

being complimentary to creating robust, business or information systems focused cybersecurity programs [7].

5 SUMMARY

The CAE designation process helped our Computer Science and Business programs design, build and market strong cybersecurity programs. Its requirement to map course curriculum to the cyber community approved NIST NICE guidelines allowed a structured approach to defining and assessing knowledge, skills and abilities both for technical computer science and more business-centered areas of study. This approach allowed a well-defined set of learning outcomes and assessments, which fit well into both the ABET and AACSB accreditation requirements, and gained great support among the faculty of both departments. Ultimately the CAE requirement for collaboration within and outside the University encouraged our computer science and business to market the differences in their programs, increasing student and employer interest in both programs. Since the CAE designation process requires endorsement by University Provost, there was great visibility of our cybersecurity programs allowing greater collaboration throughout the campus and with local industry.

REFERENCES

[1] NSA/DHS, "CAE Designated Institutions," [Online]. Available: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm. [Accessed 07 Feb 2019].

[2] ABET, "ABET Computing Accreditation Commision Version 2.0," Nov 2018. [Online]. Available: https://www.abet.org/wp-content/uploads/2018/02/C001-18-19-CAC-Criteria-Version-2.0-updated-02-12-18.pdf.

[3] ABET, "ABET Accredited Programs," [Online]. Available: http://main.abet.org/aps/accreditedprogramsearch.aspx. [Accessed 07 Feb 2019].

[4] M. J. Oudshoorn, S. Thomas, K. R. Rajendra and A. Parrish, "Understanding the New ABET Computer Science Criteria," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18).*, New York, NY, 2018.

[5] A. Parrish, J. Impagliazzo, K. R. Rajendra, H. Santos, M. Rizwan, A. Josang, T. Pereira and E. Stavrou, "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)*, New York, NY, 2018.

[6] NIST, "NIST SP 800-181," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf. [Accessed 07 Feb 2019].

[7] S. Yang and B. Wen, "Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States", *Journal of Education for Business*, vol 92, no 1, pp 1-8, 2017.