# Synergy of Accreditations and CAE Designation

Thomas Augustine
*Computer Science & Engineering*
*University of Colorado Denver*
Denver, CO, USA
thomas.augustine@ucdenver.edu

Haadi Jafarian
*Computer Science & Engineering*
*University of Colorado Denver*
Denver, CO, USA
haadi.jafarian@ucdenver.edu

Ilkyeun Ra
*Computer Science & Engineering*
*University of Colorado Denver*
Denver, CO, USA
ilkyeun.ra@ucdenver.edu

***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 and enhancing our international ABET (computer science) and AACSB (business) accreditations. 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 an active outreach to other programs. All of these benefits work in concert with the ABET and AACSB accreditations, which explicitly require an internationally recognized curriculum that is taught by experts in their field and regularly assessed.**

***Keywords—CAE, ABET, AACSB, accreditation, cybersecurity***

## I. 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 with and without research focuses. With increased reliance on electronic information sharing, cybersecurity careers have come to the forefront. The U.S. Bureau of Statistics projects a 32 percent growth of Information Security Analysts jobs over the next decade, further noting a current shortfall of thousands of well-trained experts [1]. There are many ways that a person might gain skills in cybersecurity, including numerous certificates sponsored by international organizations, Bachelor's and Master's degrees, and more focused academic certificates. With these opportunities, academic institutions are adding cybersecurity programs with the intent of gaining students while ensuring their programs remain rigorous and respected [2].

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 or AACSB, which set strict standards for curriculum and assessment. Students, employers and other academic institutions depend on these accreditations to demonstrate the strength of academic programs. As such, these 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 and AACSB accredited 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.

## II. 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 a more diverse set of employees, including 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 typical duties of a system administrator. 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 focusing on analysis and higher-level mathematics. 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 courses. This technical requirement encourages the inclusion of traditional

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

technical computer science and data analysis as an integral part of cybersecurity [3]. The non-technical foundation (or possibly better stated as less mathematical analysis) now focuses not only on information systems, but in incorporating a broader understanding of how people use these systems.

Many computer science departments and business schools 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 accreditation. Since many programs have successfully navigated the requirements for ABET or AACSB 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 program.

### *A. Potential CAE Benefits*

Since the CAE designation requires a well-established cybersecurity program and potentially requires hundreds of hours to map the curriculum to standards and write the application, Institutions must first see the benefit outweighing the workload required. A few members of our Computer Science department focused on networking and technical cybersecurity concepts and were familiar with the CAE program, but the rest of our faculty had to be convinced first that the field of cybersecurity fit into a traditional computer science discipline and that applying for the CAE was the best use of our resources.

We started by researching the direct and indirect benefits of CAE designation. We found two direct benefits. First, institutions must be a designated CAE in order to apply to be a principal investigator for the National Science Foundation and Department of Homeland Security sponsored Cyber Corps program. This program provides large dollar amount scholarships and stipends to undergraduate and graduate students willing to take a job with Federal or State governments after graduation. In addition to scholarships and stipends, students earn great opportunities for paid internships at some of the Nation's top cybersecurity organizations [4].

As a second benefit, many cybersecurity-related grant proposals ask the applicant to describe their related previous academic and research experience. CAE designation gives National recognition for well-established cybersecurity programs. When choosing among various cybersecurity-related proposals, agencies will often give higher priority to CAE designated programs as it demonstrates that the entire University supports the cybersecurity efforts.

Though not yet a designated CAE, we found additional benefits of building a strong cybersecurity program. Students were motivated by having multiple opportunities to apply their computer science skills in a perceived "hot" topic and many chose to continue their education with a Master's degree or certificate to further their work in cybersecurity. Additionally, in the past few years as we have demonstrated to employers that our students have a strong cybersecurity background, they have offered dozens of internship and post-graduation job opportunities. Students have attributed these opportunities for more challenging work assignments and greater pay to their cybersecurity skills.

After explaining these benefits and describing more than 60 areas of specialization that are addressed in the CAE curriculum mapping, we had multiple faculty members determining how they could use these course mappings to inject cybersecurity principles in their courses and research. Additionally, noting great student and employer interest in both technical and analytical skills, the Business School became very interested in advertising their cybersecurity efforts, ultimately helping with the CAE Designation effort.

### *B. 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 [5]. 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 [6].

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. [7] 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 providing some resources for inclusion or development of cybersecurity areas of study. The ACM and IEEE Computer Society jointly published a computing curriculum or computer science programs in 2013 and cybersecurity programs in 2017 [6]. 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 56 specialties including those that are more computer science-related areas and those that are traditionally more business or information technology-oriented. Each of these lists knowledge, skills and abilities as well as means to assess each [8]. ABET evaluates a program's knowledge, skills and abilities as well as the documented assessment of each, so the NICE framework is a good start for the ABET requirement to incorporate cybersecurity into the curriculum [6].

In addition to the NICE framework, the CAE designation application provides some guidance on 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.

## III. Curriculum Changes

The Computer Science and Engineering Department at our university offers Bachelor's and Master's 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.

### *A. 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 additional 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 I describes the foundational and core technical subject areas that we incorporated into our Bachelor of Science program.

TABLE I. Mapping of NICE Specialization to Undergraduate Computer Science Courses

| NICE Specialization | Computer Science Courses |
|---|---|
| Foundational<br>Cybersecurity Foundations<br>Cybersecurity Principles<br>IT Systems Component | Core Technical<br>Basic Cryptography<br>Basic Networking<br>Basic Scripting and Programming<br>Network Defense<br>Operating System Concepts |

The CAE mapping requires foundational areas, either technical or non-technical core areas and 14 optional areas for undergraduate students. Table II lists those courses we chose to map our undergraduate program 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 II. Mapping of NICE Specialization to Undergraduate Computer Science Courses

| NICE Specialization | Computer Science Courses |
|---|---|
| Foundational (Table I)<br>Core Technical (Table I) | Principles of Cybersecurity<br>Data Structures and Program Design |

| NICE Specialization | Computer Science Courses |
|---|---|
| Optional Areas<br>Algorithms<br>Data Structures<br>Database Management Systems<br>Databases<br>IA Architectures<br>IA Standards<br>Intro to Theory of Computation<br>Linux System Programming<br>Low Level Programming<br>Network Technology and Protocols<br>Operating Systems Hardening<br>Probability and Statistics<br>Vulnerability Analysis<br>Windows System Administration | Database Systems<br>Operating System Concepts<br>Introduction to Computer Networks |

### B. *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 III lists those areas and courses we chose to map to the CAE requirements.

TABLE III. MAPPING OF NICE SPECIALIZATION TO GRADUATE COMPUTER SCIENCE COURSES

| NICE Specialization | Computer Science Courses |
|---|---|
| Foundational (Table I)<br>Core Technical (Table I)<br>Optional Areas<br>Operating Systems Theory<br>Network Technology and Protocols<br>Vulnerability Analysis<br>Secure Programming Practices<br>Intrusion Detection / Prevention Systems<br>IA Architectures<br>Cybersecurity EthicsOperating Systems Hardening<br>Probability and Statistics<br>Vulnerability Analysis<br>Windows System Administration | Cybersecurity Programming and Analysis<br>Cyber and Infrastructure Defense<br>Computer Networks (Graduate)<br>Operating Systems (Graduate)<br>Cyber-related Thesis or Project |

### C. *AACSB (Business) and CAE Designation*

One of the premier business degree accreditations is AACSB, with 831 business schools accredited worldwide [9]. This accrediting body has also put out a new standard. Like the ABET accreditation, AACSB requires defining and assessing a set of core knowledge, skills and abilities. This accreditation focuses on business and accounting degrees, so unlike ABET, does not address separate requirements for information systems or information technology degrees. The new AACSB standard did address a new area for "Technology Agility" which requires integrating current and emerging technologies as well as ethical use and security of privacy and key data. [3]

As there are many business degree options available, business schools and departments are distinguishing themselves by adding additional degree and certificate options to their curricula. Cybersecurity has become a logical extension of Management Information Systems degrees. Business programs have similar challenges associated with starting or enhancing a cybersecurity program to make it respected and relevant while ensuring that prerequisite knowledge is obtained primarily through business courses. Again, business programs looking to offer a respected cybersecurity track will benefit from choosing business-specific categories and specializations from the NIST NICE framework as part of the CAE process.

Our Business School offers three opportunities for post-bachelor students to take cybersecurity-related programs. While they are not immediately ready to submit their programs for CAE designation, members of the business faculty do recognize the possible benefits of designation and see great benefit in working with other programs to help build a strong University reputation for its cybersecurity programs. We have agreed to regular cybersecurity-related forums among University departments interested in incorporating cybersecurity principles into their programs. We have also designated forums with University faculty, students and employers to help shape cybersecurity studies. Tables IV, V, and VI show the Business School cybersecurity-related programs and define some possible NICE specializations that might map to their programs.

TABLE IV. BUSINESS SCHOOL GRADUATE CERTIFICATE IN CYBERSECURITY AND INFORMATION ASSURANCE

| NICE Specialization | Computer Science Courses |
|---|---|
| Core Non-technical<br>Cyber Threats<br>Cybersecurity Planning and Management<br>Policy, Legal Ethics andCompliance<br>Security Program Management<br>Security Risk Analysis<br><br>Optional Areas<br>Basic Cyber Operations<br>Cloud Computing<br>Cyber Crime<br>Cybersecurity Ethics<br>Digital Forensics<br>IA Compliance | Information systems security and privacy<br>Cloud computing<br>Ethical hacking<br>IT risk management<br>Digital forensic analysis |

TABLE V. BUSINESS SCHOOL GRADUATE CERTIFICATE IN RISK MANAGEMENT AND INSURANCE

| NICE Specialization | Computer Science Courses |
|---|---|
| Fraud Prevention and Management<br>IA Compliance<br>IA Standards | Principles of risk and insurance<br>Practical enterprise risk management<br>Strategic risk management<br>Corporate risk management<br>Cyber risk management<br>Cyber warfare |

TABLE VI. BUSINESS SCHOOL MS INFORMATION SYSTEMS WITH CYBERSECURITY AND INFORMATION ASSURANCE SPECIALIZATION

| NICE Specialization | Computer Science Courses |
|---|---|
| Basic Cyber Operations<br>Cybersecurity Ethics<br>IA Compliance<br>IA Standards<br>Intrusion Detection & Prevention<br>Lifecycle Security<br>Penetration Testing<br>Privacy | Securing and protecting enterprise<br>IT risk management<br>Ethical hacking<br>Intrusion detection and incident response |

## IV. 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.

### A. *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 a cybersecurity fundamentals course to these standards allows the course designer to properly align prerequisite subjects, and advise the inclusion of additional subject matter in other courses.

### B. *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.

### C. *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 computer science and business programs built 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 complementary to creating robust, business or information systems focused cybersecurity programs [10].

### D. CAE is a multi-year process

In order to apply for a CAE designation, an institution must have an active cyber security curriculum matching the NICE mapping for at least 3 years. Further, an institution must demonstrate at least one year of student program completion. Most programs require a few school years to complete the courses listed in the mapping, so this designation leaves little time for major changes in course objectives and outcomes [11]. Additionally, the support of many initiatives tends to fade after changes in faculty, program managers and leadership. We found in order to keep the required support, we regularly communicated positive results to our cybersecurity curriculum changes, support of our ABET accreditation and student satisfaction rather than strictly focusing on an end goal of CAE designation. In this case the process and curriculum changes were more important than the formal designation will further add to those benefits.

### E. CAE Application Team

Most initiatives require a champion. While it is typical for a single individual to initially advocate CAE application, we found it important to form a formal committee with both junior and senior faculty members. While one advocate may be able to create and offer one or two cybersecurity-related courses, a greater committee is needed to build a program which includes all stakeholders. Often the junior faculty have the greatest willingness to add new concepts like cybersecurity to the curriculum, however more senior faculty are needed to help push initiatives through implementation and gain public support from the Administration.

Once we formed our team and agreed on roles and timelines, we found that working with currently designated CAE Universities and appointed mentors to be of great value. Of course, there is value in asking another organization how they successfully navigated the process through approval and designation. Perhaps of even greater value, though was in demonstrating that universities with perceived “top” or rigorous computer science and business programs saw the benefits of seeking CAE designation. Like our program, these universities have been ABET and AACSB accredited for decades and have extensive undergraduate, graduate, Ph.D. and research programs. Discussions with these university program advocates helped our faculty and administration understand that CAE designation helps better define ABET accreditations, gain student interest and bolster cybersecurity-related research proposals.

## V. 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 programs 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. The CAE designation process provides structure and means to build a strong cybersecurity program, but requires a great deal of effort over a number of years. We have found great benefit to the University, our accreditation programs and to students in following the CAE designation process and working with CAE designated programs.

## References

[1] Bureau of Labor Statistics, "Occupational Outlook Handbook," [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm. [Accessed Oct 12 2019].

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

[3] ABET, "ABET Computing Accreditation Commision Version 2.0," 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. [Accessed 07 Feb 2019].

[4] US Office of Management and Budget, "Cybercorps Scholarship for Service," [Online]. Available: https://www.sfs.opm.gov/. [Accessed 12 Oct 2019].

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

[6] 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.

[7] 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.

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

[9] AACSB, "AACSB Accredited Business Schools," [Online]. Available: https://www.aacsb.edu/accreditation/accredited-schools. [Accessed 07 Feb 2019].

[10] S. Yang and B. Wen, "Towards 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. 1-18, 2017