2018

The Role of CAE-CDE in Cybersecurity Education for Workforce Development

Maurice Dawson
Ping Wang, *Robert Morris University*
Kenneth Williams, *American Public University System*

The Role of CAE-CDE in Cybersecurity Education for Workforce Development

20

Maurice Dawson, Ping Wang, and Kenneth Williams

Abstract

With a fast-growing demand for properly trained cybersecurity professionals to defend our cyber space and information systems, effective cybersecurity education programs and courses with consistent and reliable quality control and evaluation are necessary to prepare qualified workforce for the cybersecurity industry. The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program jointly sponsored by the US National Security Agency (NSA) and Department of Homeland Security (DHS) is a rigorous certification and national standard for maintaining quality of cybersecurity education. This paper explains the CAE-CDE program criteria and requirements and discusses the important role of the designation in cybersecurity education and workforce development. This paper illustrates the educational value and impact of the CAE-CDE program with case studies of three different institutions: (1) University of Missouri—St. Louis, which has obtained the CAE-CDE and Security Policy Development and Compliance Focus Area designations; (2) American Public University System, which has just completed the application for CAE-CDE; and (3) Robert Morris University, which is in the process of applying for the CAE-CDE designation.

Keywords

Cybersecurity education · Workforce development · Centers of Academic Excellence (CAE) · Cyber Defense Education (CDE) · Designation

M. Dawson
University of Missouri—St. Louis, MO, USA

P. Wang (✉)
Robert Morris University, Moon, PA, USA
e-mail: wangp@rmu.edu

K. Williams
American Public University, Charles Town, WV, USA

20.1 Introduction

Cybersecurity has been a fast-growing career field and an important area with increasing demand and opportunities for higher education. Information security analyst is only one of the cybersecurity career titles. According to U.S. Department of Labor Bureau of Labor Statistics (BLS), employment of information security analysts is projected to grow 18% from 2014 to 2024, much faster than the average growth rates of 7% for all occupations and 12% for all computer related occupations [1].

The latest cybersecurity workforce framework published by the National Initiative for Cybersecurity Education (NICE) recognizes the growing need for an integrated cybersecurity workforce with technical and non-technical roles for organizations to address their cybersecurity challenges and implement their missions and business processes connected to cyberspace. The NICE Cybersecurity Workforce Framework (NCWF) emphasizes that "academic institutions are a critical part of preparing and educating the cybersecurity workforce" [2]. A recent study shows that top U.S. universities were failing at cybersecurity education with a lack of cybersecurity requirements for graduates and a slow change in curriculum and courses [3]. However, it is encouraging to see more and more 2-year and 4-year academic institutions have started to offer cybersecurity degree programs and courses across the country. Quality assurance is needed for cybersecurity-related degree programs to meet high cybersecurity academic standards in order to prepare the graduates for the growing number of cybersecurity positions [4].

The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program jointly sponsored by the US National Security Agency (NSA) and Department of Homeland Security (DHS) is a national quality standard for certifying and maintaining high quality of cybersecurity education with rigorous and consistent requirements for program evaluation and close alignment to specific

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 738,
https://doi.org/10.1007/978-3-319-77028-4_20

cybersecurity knowledge units. Out of over 5300 colleges and universities in the U.S., only about 200 of them have achieved the CAE-CDE designation status. Attendance at a CAE school will give students confidence in learning, and a degree from a CAE school will give employers confidence in hiring [4].

This paper will describe the background for CAE-CDE program, highlight the important application and designation criteria, and use the case study methodology to present three different cases of academic institutions with different CAE status: University of Missouri—St. Louis (UMSL), American Public University System (APUS), and Robert Morris University (RMU). The goal of the study is to illustrate the important role of the CAE designation and the application process in the cybersecurity education and workforce preparation at these institutions.

20.2 Background

The national CAE-CDE program evolved from the initial national CAE in Information Assurance Education (CAE-IAE) program started by NSA in 1998 with DHS joining as a co-sponsor in 2004, and the CAE in IA Research special designation was added in 2008 to encourage doctoral level research in cybersecurity [5]. In 2010, the CAE2Y component was created to provide the CAE designation opportunity for 2-year institutions, technical schools, and government training centers. Hence, the current CAE-CD program includes these designations: CAE2Y for 2-year institutions, and CAE-CDE for 4-year institutions, and CAE-R for doctoral universities or Department of Defense schools. All regionally accredited 2-year, 4-year and graduate level institutions in the United States are eligible to apply for the appropriate CAE designation. The designation is granted to schools which have demonstrated compliance with rigorous CAE criteria and curricula mapping to a required core set of cyber defense knowledge units (KUs) with optional Focus Areas [5].

20.2.1 Application Requirements

Eligible applicants should submit their CAE applications online, and new applicants should complete a checklist for readiness check to determine if optional application assistance, such as program and curriculum development assistance or application mentoring, is needed. An official Letter of Intent and Endorsement signed by the applicant institution's Provost or higher is a mandatory requirement to be included in online application. This letter should express institutional commitment and support for the CAE program, identify the institution's CAE point of contact, and provide information on regional accreditation and list accomplishments in the cyber defense field [6].

20.2.2 Criteria for Measurement

All applications will be reviewed and assessed by qualified independent cyber professionals and subject matter experts from CAE schools, government, and industry. New applications will be assessed by three reviewers, and applications for re-designations will be reviewed by two reviewers. Initial designation is valid for five academic years, and re-application is required for retaining the designation. The following are the latest criteria for assessing CAE applications for the 2018 cycle [6].

20.2.2.1 Cyber Academic Curriculum Path

This is to demonstrate a relevant and mature cyber curriculum program in place for at least 3 years with mappings to KUs and NCWF and student enrollment and completion data.

20.2.2.2 Student Skill Development and Assessment

This is to show student development activities and assessment in cyber defense, including syllabi, assignments, hands-on labs, competitions, and guest lectures from cybersecurity practitioners.

20.2.2.3 "Center" for Cyber Education

This is to an officially established physical or virtual center to serve as a guidance and resource center with an external advisory board for the institution's cyber curriculum and practice.

20.2.2.4 Cyber Faculty Qualifications and Courses Taught

This is to show the faculty in charge of the cyber defense program, relevant faculty publications, presentations, and faculty support student cyber activities and clubs.

20.2.2.5 Multidisciplinary Practice in Cyber Defense

This is to demonstrate that Cybersecurity is integrated additional degree programs and courses in the same institution.

20.2.2.6 Institutional Security Plan

This is to show the institution's security plans, responsible party, and its implementation of cybersecurity practices.

20.2.2.7 Cyber Outreach and Collaboration

The institution must demonstrate activities to extend cyber defense practices beyond the institution, including faculty and curriculum sharing with community schools, credit transfer agreement, participation in the CAE community, and outreach activities and industry collaboration.

20.3 Case Study: UMSL

20.3.1 School Profile, Demographics, Mission

The University of Missouri—Saint Louis (UMSL) is the largest public research university in eastern Missouri. It provides excellent learning experiences and leadership opportunities to a diverse student body whose influence on the region upon graduation is immense. UMSL is spread across 470 acres in suburban St. Louis County. UMSL's College of Business Administration is accredited by Association to Advance Collegiate Schools of Business (AACSB) International. UMSL is the region's first and only NSA/DHS designated CAE-CDE. UMSL is the only institution within the eight states that border Missouri to hold any of the 17 available focus areas.

20.3.2 Cyber Programs and Data

The cybersecurity program at UMSL is a multidisciplinary effort between the Department of Mathematics and Computer Science in the College of Arts and Sciences and the Department of Information Systems in the College of Business Administration. This collaborative approach allows students to explore the many avenues of information security and adapts to the evolving nature of the field. UMSL has created an undergraduate certificate, graduate certificate, undergraduate minor, and graduate track in cyber security. The programs were created to address the shortfall of 3800+ jobs in the Saint Louis Metropolitan Region [7]. Table 20.1 below displays the courses for the cybersecurity certificate programs in the Information Systems Department which require students take at least one computer science course.

The courses all have a hands-on component which enables students to gain more technical depth in varied programming languages, forensic tools, static code analyzers, and offensive security applications. The courses are developed to address the future of national and international cybersecurity [8]. The UMSL program heavily uses Open Source Software (OSS) as it serves as a means for students to understand low-level coding and to inspect source code for security [9]. Additionally, the labs become reusable learning objects. To enhance student learning, a physical and virtual lab environment was created with both Linux and Windows systems in which the student is given a dedicated Kali Linux virtual machine that allows them to practice offensive security operations in a controlled environment. The lab activities allow students to obtain hands-on experience in offensive and defensive security.

20.3.3 CAE Status and Accomplishments

The cybersecurity program at UMSL received $493,650 from two NSA grants within the last year. This funding will help develop lab infrastructures, enhance equipment and further advance cyber security curricula. Through two Non-Governmental Organizations (NGOs), faculty and students have also received grants of about $35,000 from John Ogonowski and Doug Bereuter Farmer-to-Farmer Program (F2F). The CAE designation also helped a faculty member to secure a 2-year Fulbright Scholar Cybersecurity Specialist Grant valued at about $20,000. Industry partners have provided more than $150,000 to the Information Systems program UMSL in the form of gifts, equipment, internships, and more.

20.4 Case Study: APUS

20.4.1 Profile, Demographics, and Mission

American Public University System (APUS) has completed preparation for submission as a Center of Academic Excellence (CAE) in Cyber Security Defense (CDE). APUS

Table 20.1 UMSL cybersecurity certificate programs

Undergraduate program	Graduate program
INFSYS 3848 Introduction to Information Security	INFSYS 6828 Principles of Information Security
INFSYS 3842 Data Networks and Security	INFSYS 6836 Management of Data Networks and Security
INFSYS 3858 Advanced Security and Information Systems	INFSYS 6858 Advanced Cybersecurity Concepts
INFSYS 3868 Secure Software Development	INFSYS 6868 Software Assurance
INFSYS 3878 Information Security Risk Management and Business Continuity	INFSYS 6878 Management of Information Security
CMP SCI 4700 Computer Forensics	CMP SCI 4700 Computer Forensics

is accredited by the Higher Learning Commission (HLC) and offers online degree and certificate programs through American Military University (AMU) and American Public University (APU). APUS is an online institution of higher learning serving the needs of military, public service and civilian communities through American Military University (AMU) and American Public University (APU). APUS is a subsidiary of American Public Education, Inc. (APEI)—the parent company that also owns Hondros College of Nursing (HCN) which serves students primarily through five Ohio campuses in Cincinnati, Cleveland, Columbus, Dayton and Toledo. Together, these institutions serve more than 85,000 adult learners worldwide and offer more than 200 degree and certificate programs in fields ranging from cybersecurity, homeland security, military studies, intelligence, criminal justice to technology, business administration, public health, nursing and liberal arts [10]. APUS was founded in 1991 as AMU. Since then, approximately 75,000 alumni have graduated from either AMU or APU. As of September 30, 2017, APUS has a student population of over 81,000. APUS student enrollment by degree level consists of 59% Bachelor's, 16% Associate, 16% Master's and 9% Certificate programs. Demographically, APUS student population includes 88% working adults with an average student age of 33 and an average class size of 9 students, and a gender ratio 64% male versus 36% female in over 200 degree and certificate programs [10].

20.4.2 APUS Cybersecurity Programs

At APUS Cybersecurity is taught as a program within the School of Science Technology Engineering and Math. Students may choose to earn cybersecurity education through certificates, Bachelor's or Master's programs. The cybersecurity undergraduate certificate examines the digital forensics tools, techniques, and methods used by cyber analysts to detect cybercrime, cyber terrorism, cyber war, cyberstalking, and cyberbullying. The Bachelor of Science in Cybersecurity provides students with both theory and know-how required to strategically assess, plan, design, and implement effective cybersecurity defenses in the public and private sectors. This Master of Science in Cybersecurity Studies takes a broad, multi-disciplinary approach to preventing and responding to large-scale cyber threats and cyber-attacks. The first half of this program provides students with a foundation in network security, cybersecurity, cybercrime, and digital forensics. The second half of this program focuses on the issues, policies, practices, and perspectives of various sectors, critical infrastructures, agencies, and disciplines, such as national security, intelligence, criminal justice, and emergency management [11].

20.4.3 CAE Status and Accomplishments

APUS started the process to achieve the status as a Center of Academic Excellence in Cyber Defense (CD) Education (CAE-CDE) in mid-2017 with a self-assessment of readiness. The assessment of the APUS readiness for the CAE-CDE designation resulted in the assignment of a mentor to assist in the completion of the application [6]. Following the result of the self-assessment and assignment of a mentor, a core group of subject matter experts (SME) supported by other members of the APUS staff was convened. This core group was managed by the APUS Provost and consisted of SMEs from the Cybersecurity program along with support from the APUS accreditation group and other department including career services, academics, and other schools throughout APUS. Weekly meetings were held with various members of the core group, including both virtual and face-to-face sessions.

The first significant session of the core group consisted of a face-to-face 2-day conference with SMEs and the assigned mentor. During this session, selection of the cybersecurity path was finalized, resulting in the selection of 12 courses from the Bachelor of Science in cybersecurity program. These 12 selected courses formed the core courses used to meet the requirements of the CAE-CDE mandatory core and optional Knowledge Units (KUs). Along with the selection of the core courses for CAE-CDE program, the group selected seven optional Knowledge Units resulting in a total of 22 KUs to measure the readiness for the APUS CAE-CDE designation. Subsequent meetings with the matrix team followed over a 6-month period to complete the CAE-CDE application. Meetings were also held with members of the NSA CAE-CDE office to include two face-to-face sessions to seek feedback and clarification on the application process. Shortly after the availability of the submission portal in September 2017, the submission process began and reached completion as determined by the mentor. The mentor's determination initiated the process of an independent pre-assessment of the APUS application that was returned with a report of no deficiencies for the mapping of the core courses to the 22 KUs and criteria. Following a final review from the APUS leadership, the final submission of the application will occur to meet the deadline of 15 January 2018.

20.4.4 Impact of CAE-CDE Application

The application of the APUS CAE-CDE application is long lasting in its impact on the programs, course, institution, and its students. The cybersecurity program saw changes to the core courses; allowing students to follow a direct path that will result in the achievement of a robust cybersecurity education, ranging from knowledge in software to database

security and statistics. All students selecting the cybersecurity program are required to follow this CAE-CDE path. Courses within the CAE-CDE path were also examined to ensure the robustness of the CAE-CDE criteria.

Courses from other schools within APUS were also assessed and selected for submission of the CAE-CDE application. The selected courses resulted in a greater appreciation for the importance of cybersecurity across the APUS; initiating a call for additional cross discipline courses that further increase awareness of cybersecurity threats.

Students within APUS were also impacted by the application for CAE-CDE. As noted above all students selecting the BA in cybersecurity are now expected to complete the path; resulting in a robust cybersecurity education and an enhance career opportunity. Students completing the path can share the news of their completion with potential employers; resulting in an edge over other applicants without equal level of education.

20.5 Case Study: RMU

20.5.1 Profile, Demographics, and Mission

Robert Morris University (RMU), founded in 1921, is a selective private non-profit national university located in the Greater Pittsburgh region in western Pennsylvania. RMU has a total enrollment of 4384 undergraduate and 815 graduate students. RMU is accredited by the Middle States Commission on Higher Education and serves a diverse student population of men and women, working professional, military and veteran students, minorities, and international students. RMU provides a professionally focused education with an emphasis on engaged learning.

20.5.2 RMU Cyber Programs

Housed in RMU's School of Communications and Information Systems (SCIS), the Department of Computer and Information Systems (CIS) offers four B.S. degrees in Cyber Forensics and Information Security (BS-CFIS), Computer Information Systems (BS-CIS), Information Sciences (BS-IS), and Data Analytics (BS-DTAN). The BS-CFIS, BS-CIS, and BS-IS degree programs are all accredited by the Computing Accreditation Commission of ABET [12]. The key cybersecurity courses for the BS-CFIS and other programs include Computer and Network Security, Intro to Computer Forensics, Digital Evidence Analysis, IT Security, Control/Assurance, and Mobile Forensics.

The department also offers five M.S. degrees in Cyber Security and Information Assurance, Information Systems Management, Internet Information Systems, Information Technology Project Management, and Data Analytics, as well as one doctoral degree in Information Systems and Communications. In addition to its degree programs, CIS offers undergraduate and graduate certificate programs in Information Systems, Mobile Forensics and Security, and Enterprise Systems. Most CIS degree and certificate programs are offered in both traditional and online formats.

20.5.3 CAE Status and Accomplishments

RMU is in the process of preparing to submit the application for a CAE-CDE designation. RMU has submitted a New Applicant Inventory to NSA. Based on the review of the New Applicant Inventory submitted, RMU was assessed to be within 1 year of applying for the CAE designation. Hence, RMU was referred to the mentoring program with designated mentor as part of the Application Assistance Program (APP) funded by the National Science Foundation. RMU has confirmed its participation in the APP program with a designated Mentee Point of Contact to apply for the CAE-CDE designation. The application submission is projected to be completed within 1 year. RMU leadership is very supportive of this pursuit, and faculty and students are looking forward to enhanced cybersecurity programs and courses through the CAE-CDE application and designation.

20.6 Conclusions

This paper explains the rigorous quality control criteria and important role of the NSA/DHS CAE-CDE designation in cybersecurity education and workforce development. Three case studies of different institutions with different CAE status are presented to illustrate the importance of the CAE designation in enhancing cybersecurity education at these institutions. Updates to the CAE designation and application status for the two applicant schools with more specific data and accomplishments will be presented and discussed in future research reports.

References

1. U. S. Department of Labor, Occupational outlook handbook. (2015), https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6
2. NICE (National Initiative for Cybersecurity Education), NICE cybersecurity workforce framework (SP800-181). (2017), https://csrc.nist.gov/publications/detail/sp/800-181/final
3. S.K. White, Top U.S. universities failing at cybersecurity education. CIO. (2016), https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html

4. NICCS (National Initiative for Cybersecurity Careers and Studies), National Centers of Academic Excellence (CAE). (2017), https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae
5. NSA (National Seucrity Agency), National Centers of Academic Excellence in Cyber Defense. (2016), https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/
6. NIETP (National IA Education & Training Programs), CAE-CDE criteria for measurement 2018. (2018), https://www.iad.gov/NIETP/CAERequirements.cfm
7. CyberSeek, Cybersecurity supply/demand heat map. (n.d.), http://cyberseek.org/heatmap.html. Accessed 15 Dec 2017
8. M. Dawson, M. Omar, J. Abramson, D. Bessette, The future of national and international security on the internet, in *Information Security in Diverse Computing Environments*, ed. By A. Kayem, C. Meinel, (IGI Global, Hershey, 2014), pp. 149–178. https://doi.org/10.4018/978-1-4666-6158-5.ch009
9. M. Dawson, I. Al Saeed, J. Wright, F. Onyegbula, Open source software to enhance the STEM learning environment, in *Handbook of Research on Education and Technology in a Changing Society*, ed. By V. Wang, (IGI Global, Hershey, 2014), pp. 569–580. https://doi.org/10.4018/978-1-4666-6046-5.ch042
10. APEI (American Public Education, Inc.), (n.d.), http://www.americanpubliceducation.com/phoenix.zhtml?c=214618&p=irol-homelanding
11. AMU (American Military University), (n.d.), http://www.amu.apus.edu/
12. ABET, ABET Accredited Program Search, (n.d.), http://main.abet.org/aps/Accreditedprogramsearch.aspx