https://doi.org/10.48009/3_iis_2019_1-10

Issues in Information Systems
Volume 20, Issue 3, pp. 1-10, 2019

REFLECTIONS ON SECURITY COURSES IN CIS CURRICULUM AFTER ATTENDING A CAE WORKSHOP

Lisa Z. Bain, Rhode Island College, lbain@ric.edu
Suzanne Mello-Stark, Rhode Island College, smellostark@ric.edu

ABSTRACT

Computer Information Systems (CIS) curriculum includes security courses along with many others that focus on the main disciplines in the Information Technology industry. In general, no one course is given more focus than the others unless institutions have dedicated programs that support the needs of local businesses or organizations. The National Security Agency (NSA) and the Department of Homeland Security (DHS) sponsor a special type of designation in the area of cybersecurity called the Center for Academic Excellence in Cyber Defense (CAE-CD). After attending a CAE workshop, faculty are educated in the process of attaining this designation along with the necessary resources. This designation includes detailed coverage of Knowledge Units (KUs) in security courses as well as program requirements focused on outreach and collaboration. Faculty can expect at least a two-year time commitment dedicated to the CAE process along with significant administrative support, but there are many benefits to students, faculty and the institution. However, faculty should also take many other considerations into account before pursuing the CAE. With the breadth of Information System (IS) programs, choices must be made as to which disciplines, if any, should be the focus. Other approaches, like minors or concentrations, could also provide benefits to students. Therefore, it is recommended that faculty thoroughly analyze the student body of their respective institutions and the local job market before selecting a framework for developing security curriculum in IS programs.

Keywords: Security, Cybersecurity, Center for Academic Excellence (CAE) and CIS Curriculum

INTRODUCTION

This reflection paper discusses the current state of Computer Information Systems (CIS) curricula at one medium-sized, public institution and ponders the potential issues with pursuing the CAE-CD designation. The benefits of having this designation are obvious to institutions, students and the surrounding community. However, many institutions face limited resources as well as the need to cover an increasing number of disciplines in their programs. The following sections highlight some of surrounding issues in this area, a recap of a CAE workshop, and several resulting reflections.

The Computer and Information Technology industry includes a wide variety of technical disciplines and provides an amazing amount of career opportunities. The college programs supporting these are primarily in the areas of Computer Science, Information Systems and Information Technology. The curricula for Computer Science programs seem to vary slightly by institution but tend to be relatively standardized thanks to work sponsored by ACM for bachelor programs and K-12 (ACM, 2019). There is also an Advanced Placement (AP) Computer Science course provided by the College Board (College Board, 2019). The curricula for Information Systems programs not only vary by institution, but also by name. There is a recommended curriculum for Information Systems programs but it has not been updated since 2010 (ACM, 2019). The most common names for Information Systems programs are Computer Information Systems, Information Sciences and Technology, Information Technology, Management Information Systems and Information Systems (Bain, Bhatnagar & Chapman, 2017). Regardless of the name, the standardization of courses does not appear to be as consistent as the Computer Science curriculum. There are many "core" courses like Management Information Systems, Database Management, Systems Analysis and Design, Networking and Computer Programming. However, security is not listed as a "required" course in IS 2010 (ACM, 2019). Therefore, a student majoring in an Information Systems program may or may not have taken a security course by the time he/she graduates. Security courses are primarily offered at institutions with specific concentrations or degrees in security. Information Systems programs currently focus on providing students with a broad degree that covers many different technical disciplines.

Three Versus Four Credit Courses

Should security be a required course in CIS curriculum? Should CIS courses be three-credits or four-credits? The curricula of Information Systems programs as well as other college programs include both three-credit and four-credit courses. There are advantages and disadvantages to each approach including the argument of breadth versus depth (Schwartz, Sadler, Sonnert & Tai, 2009). In the Fall of 2017, the new Provost/Vice President of Academic Affairs at our medium-sized, public institution encouraged faculty to consider four-credit courses. At the time, the Computer Information Systems (CIS) program included primarily three-credit courses with a few exceptions in the cognates. The General Education courses had already switched to four-credit courses. It just so happened that the CIS faculty were reviewing the CIS program and in the process of switching to a four-credit curriculum for all CIS courses. During this review, the discussion began as to the importance of security and the need to make it a required course. This would move the course from a restrictive elective and insure that all students take the course before graduation. After careful planning, the CIS faculty submitted the curriculum proposals that switched to all four-credit CIS courses and made security a required course in the program. The changes were approved by the institution's curriculum committee and the administration with an effective date of the Fall 2018 semester. It is unknown if the security course would have become a required course had the change to four-credit courses not happened. So this change was a very important starting point in focusing on security as part of the CIS curriculum.

Security Course Requirements

Making security a required course opened a proverbial and unexpected can of worms. Previously, development of any existing or new CIS course was relatively straight-forward. Most CIS faculty had either graduate-level courses or industry experience in the topic area (e.g. programming, networking, databases). However, this was not the case for the new security course. It had only been taught as an elective by one faculty member, using his particular approach to the course. What would be the best way to teach the course? Should it be taught at a managerial-level covering all possible topics? Should it be a more technical course with hands-on exercises that require computer facilities? Should it focus on security certifications? These questions led to a discussion with the institution's newly appointed Chief Security Officer (CSO), an existing employee of the Information Systems Department who had just recently became a Certified Information Systems Security Professional (CISSP), considered one of the most "prominent" certifications, along with the Systems Security Certified Practitioner (SSCP), administered by the International Information Systems Security Certifications Consortium (IISSCC) or ISC^2 (Merkow & Breithaupt, 2014, p. 36). His recommendation was to focus on ITSec and the Common Body of Knowledge. There was no discussion of the Center for Academic Excellence (CAE) program sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS). This approach was then used in the first offering of the newly required security course.

Fast forward from Fall 2018 to Spring 2019 and the changes in faculty at this institution. There was a new faculty member in the Math and Computer Science Department with a strong background in security/cybersecurity. This new faculty member reached out to the CIS faculty to discuss security curriculum and opportunities for both the institution and the students. Thus began the start of pursuing the CAE designation and attending the CAE workshop.

CENTER FOR ACADEMIC EXCELLENCE

The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program: "The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise" (NSA, 2019). This program is available to all regionally accredited two-year, four-year and graduate level institutions. It focuses on very specific Knowledge Units (learning objectives) that must be covered in a variety of security courses and a list of other criteria to be completed by the institution. If achieved, the recognition comes from the U.S. government. The NSA and DHS do not fund these programs, but institutions may receive funding from other sources, like the National Science Foundation (NSF). However, the NSA and DHS do provide resources through a group of National Resource Centers (CNRC) and Regional Resource Centers (CRRC). The National Resource Centers (CNRC) are a group of institutions that have already received the CAE-CD designation that are willing to help other institutions through the process. There are three national centers that include the Hub, Consultation, and National. The Regional Resource Centers (CRRC) are located in specific geographic locations and provide workshops, seminars and courses for both designated and

candidate institutions. There are six regional centers that include the Central Eastern, New England, South Central, South Eastern and Western Regions. Each of these is located at a special college, university, or community college. As of May 2019, there are over 270 colleges and universities across 48 states that have received the CAE-CD designation. Therefore, it is considered a well-established and organized program.

CAE KU Mapping and Criteria Workshop

The purpose of the CAE Workshop is to provide resources and guidance to institutions pursuing the CAE designation. The workshop is considered part of the Assistance Program, one of the many items provided by the National Resource Centers (CNRC). The agenda included an overview of CAE, a description of the CNRC and CRRC, program eligibility, benefits of the CAE, submission expectations, and the application process. However, the primary focus is on the Knowledge Units (KUs) mapping (curriculum) and Criteria for Measurement (outreach and collaboration). Not surprising, the KUs and criteria are rigorous being somewhat similar to other accreditation standards. Fortunately, the workshop included several faculty members from CAE institutions that had in-depth knowledge and experience going through the process.

Overview of Knowledge Units (KUs)

The Knowledge Units (KUs) are specific topics that must be covered in courses and the expected outcomes. Four year institutions must "map" to 22 KUs. Mapping means that the topics in each KU is linked to its coverage in at least one specific course (e.g. CIS 440 Issues in Computer Security). This is best tracked using an Excel spreadsheet with the KUs/topics in column A and the course numbers listed across the top in the header row. There are three *Foundational KUs* required by all institutions (Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components). Each institution must then choose between a *Technical* or a *Non-Technical Core*, each having five KUs. The Technical Core includes Basic Cryptography, Basic Networking, Basic Scripting and Programming, Network Defense, and Operating Systems Concepts. The Non-Technical includes Cyber Threats, Cybersecurity Planning and Management, Policy/Legal/Ethics and Compliance, Security Program Management, and Security Risk Analysis. Lastly, there are dozens of *Optional KUs* from which institutions may choose to complete the required 22 KUs - Foundational (3), Core (5), Optional (14) as shown in Figure 1, which is provided by the CAE documentation (CAE-CD, 2019). Figure 1, the Knowledge Unit Usage Notional Structure, summarizes the requirements of the four program types that can become CAEs in one combined graphic. The program types include Associates, Bachelors, Masters and Doctoral. The figure also includes a listing of the foundational, technical and non-technical KUs with color coding to show where these fit in each type of program. Lastly, the arrows show the program paths for both the technical and non-technical core.

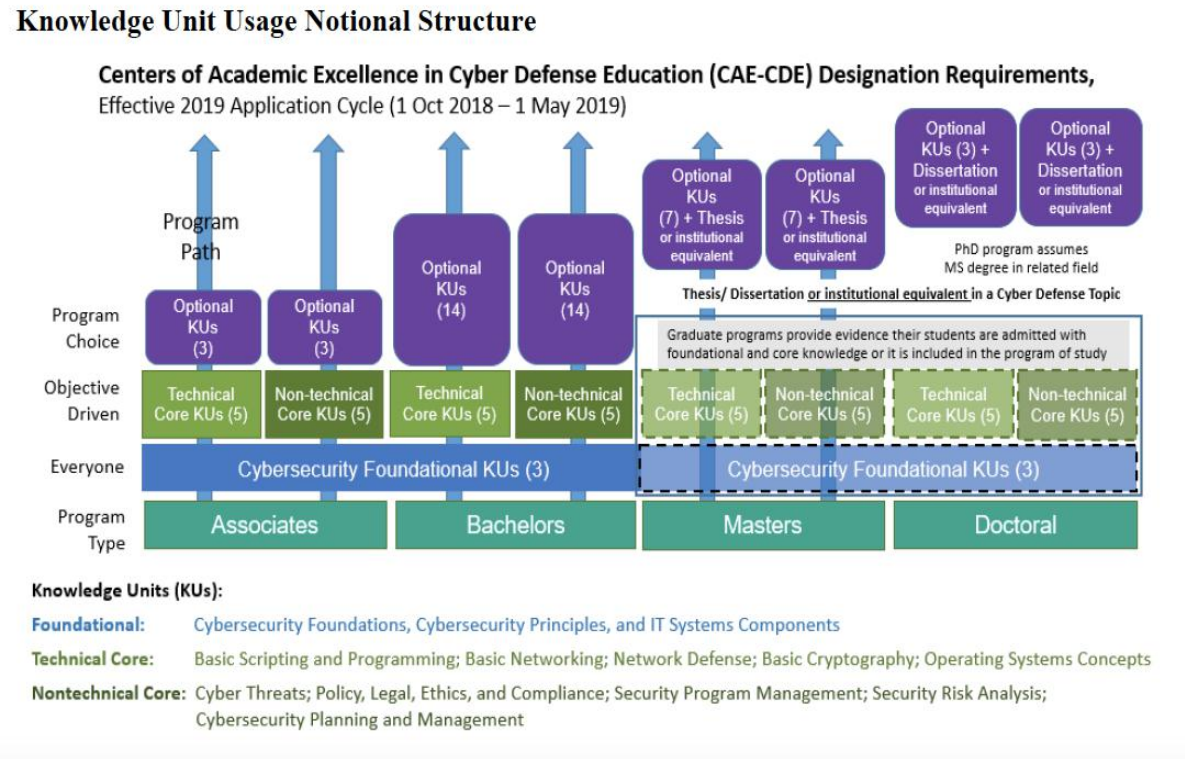

Figure 1. CAE Knowledge Unit Model

Sample Knowledge Unit (KU) Detail

The CAE-CD Knowledge Unit guide provides in-depth detail for each Knowledge Unit. This includes the name, description, outcomes, topics, vocabulary, related KUs, specialization, and the National Initiative for Cybersecurity Education (NICE) framework categories. The name identifies each KU along with a three-letter key for indexing (e.g. CSF for Cybersecurity Foundations) and a description. The outcomes are a description of the student-based outcomes for that particular KU. The number of outcomes vary by KU. The topics are a list of elements that are part of the KU. The vocabulary and related KUs are self-explanatory. The specializations provide a list of IT areas directly related to this KU. Finally, the NICE framework categories also provide a list of the items related to this KU. NICE is part of the National Institute of Standards and Technology (NIST) and has developed a framework for the cybersecurity workforce, which is a guide "categorized and describes cybersecurity work" (NICE, 2019). This framework includes categories, specialty areas, and work roles. Whereas the KUs focus on pedagogy and education, the NICE framework focuses on the IT industry and specific job/work roles. A sample Knowledge Unit detail is shown in Table 1.

Table 1. Sample Knowledge Unit Detail

Cybersecurity Principles (CSP)
The intent of the Cybersecurity Principles Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.
Outcomes
To complete this KU, students should be able to: 1. Describe the fundamental concepts of the cyber security discipline and use to provide system security. 2. Describe potential system attacks and the actors that might perform them. 3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks. 4. Describe appropriate measures to be taken should a system compromise occur. 5. Properly use the Vocabulary associated with cyber security.
Topics
To complete this KU, all Topics and sub-Topics must be completed 1. Threats and Adversaries (threat actors, malware, natural phenomena) 2. Vulnerabilities and Risk management (include backups and recovery) 3. Common Attacks 4. Basic Risk Assessment 5. Security Life-Cycle 6. Applications of Cryptography and PKI 7. Data Security (in transmission, at rest, in processing) 8. Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security) 9. Access Control Models (MAC, DAC, RBAC, Lattice) 10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy 11. Session Management 12. Exception Management 13. Security Mechanisms (e.g., Identification/Authentication, Audit) 14. Malicious activity detection / forms of attack 15. Appropriate Countermeasures 16. Legal issues 17. Ethics (Ethics associated with cybersecurity profession)
Vocabulary
Advanced persistent threat (APT), attacker, Block ciphers, DoS, DDoS, malware, mitigations, residual risk, risk, stream ciphers, vulnerability
NICE Framework Categories
Securely Provision (SP) Operate and Maintain (OM) Oversee and Govern (OV) Protect and Defend (PR) Analyze (AN) Collect and Operate (CO) Investigate (IN)

Criteria for Measurement

The second requirement of the CAE-CD designation is the Criteria for Measurement (aka program requirements), which focuses on the outreach and collaboration of the program. These necessitate a significant time commitment by the faculty and strong institutional support. There is a point system used to "grade" the activities with mandatory points for seven criteria. In addition, the reviewers require justification and evidence for each criterion resulting in the need for detailed record keeping and administrative activities. There are very detailed and specific items required by the seven criteria that cannot be included in this paper due to the length limitations. A summary of the criteria is shown in Table 2. However, a few samples in italics are included in the table.

Table 2. CAE-CD Program Requirements

Criteria	Description
1. Cyber Defense Curriculum Path	Clearly defined curriculum path that maps to KUs - *Curriculum path existence for at least 3 years*
2. Student Skill Development and Assessment	Student development and assessment in Cyber Defense - *Student participation in cyber competitions*
3. "Center" for Cyber Education	Established focal point for cyber curriculum and practice - *Website with specific information and a board of advisors*
4. Cyber Faculty Qualifications and Course Taught	Demonstrated faculty support of the program - *Faculty CVs, cyber defense publications*
5. Cyber Defense is a Multidisciplinary Practice	Demonstrated cybersecurity integrated across disciplines - *Cyber defense principles taught in other depar*tments
6. Institutional Security Plan	Demonstrated implemented institutional security plan - *Security plans, officers, and implemented practices*
7. Cyber Outreach/Collaboration Beyond Institution	Demonstrated practices extend beyond boundaries of institution - *Sharing curriculum with other schools, participation in CAE community*

CAE Workshop Activities

The CAE KU mapping and criteria workshop that the authors attended in March of 2019 began with an overview of the CAE process, then focused on the KU mapping and criteria (program requirements). The KU mapping session provided an overview of how to complete the mapping and then allowed participants to try mapping their actual courses. This required participants to first select whether their programs would use the technical or non-technical core. In this particular workshop, there were participants from institutions at different stages of the CAE process. Some were at the beginning stages (us) and several were already a year or two into the process. At first this was intimidating but later turned out to be very helpful in being able to see real examples and benefit from advice on how to get started. It would have been even more helpful to have completed some items prior to attending the workshop. This includes selecting the technical or non-technical core and having a complete list of all courses for the mapping. However, the faculty members hosting the workshop were extremely patient and helpful, allowing each participant/institution to move at their own pace. One item of interest that emerged from the mapping is the requirement that *only one program per institution* can be used for the CAE process. In our case, one faculty member from the Computer Science program and one from the Computer Information Systems program attended the workshop. It was assumed before the workshop that a collaboration was possible, but this is not the case. The CAE designation is given to the entire institution but only one program (CS or CIS) can be used for the evaluation process.

The second session of the workshop focused on the criteria, which are also known as program requirements. The workshop hosts took a different approach here by discussing one of the seven criteria at a time then allowing participants to document possible activities that would apply to each one. The hosts then reviewed each of the participants "answers" and provided possible scoring. It highlighted many weak areas but also offered ideas and examples from the other workshop participants. At the conclusion of this exercise, the hosts concluded the workshop and participants shared contact information and offers of assistance to one another.

CAE Workshop Summary
Overall the workshop was vital and highly recommended for any faculty member considering the CAE designation for their institution. Reading the CAE website and documents alone would not be sufficient preparation before taking on this enormous task. The hosts of the workshop were very supportive and encouraging to all participants. It was not a competitive environment at all. The workshop hosts stressed that as many institutions as possible gaining the CAE designation is seen as a very positive goal for the NSA and DHS. Faculty and institutions should know that this process takes a minimum of two years to complete and substantial administrative support. There are many benefits for faculty and institutions to pursue this designation. The most important is the impact it could have on the skillsets of students. However, there are many other factors to consider as well. These relate mostly to the larger picture of Information Systems curriculum and programs. These reflections are discussed in the following section.

REFLECTIONS

Reflection #1 - What security curriculum *framework* best serves the needs of students majoring in CIS?
With multiple frameworks and technical certifications available to students and professionals, it is very challenging for faculty to choose the one best suited to serve the needs of the students. The Information Technology industry includes many different and complex disciples. The most common of which are technical support, software development, database management, network and systems administration and security (OOH, 2019). Each of these have varying frameworks and technical certifications.

For the security discipline, there are at least three current approaches to the required topics that should be covered to meet the demands of industry. The ISC^2 's Common Body of Knowledge has 10 domains, which include: (1) Governance and Risk Management; (2) Security Architecture and Design; (3) Business Continuity Planning and Disaster Recovery Planning; (4) Law, Investigations and Ethics; (5) Physical Security Control; (6) Operations Security; (7) Access Control Systems; (8) Cryptography; (9) Telecommunications, Networks and Internet Security; and, (10) Software Development Security (ISC^2, 2019). This takes a higher level and managerial approach to security topics and uses the nomenclature of ITSec. It is an international and nonprofit membership association that administers the CISSP certification. The Computing Technology Industry Association (CompTIA) is another approach and provides the Security + certification. This includes six main topics in the areas of (1) Threats, Attacks and Vulnerabilities; (2) Technologies and Tools; (3) Architecture and Design; (4) Identity and Access Management; (5) Risk Management; and, (6) Cryptography and PKI (CompTIA, 2019). This is more technical in nature and requires two years of experience but has many similar topics to the CISSP certification. CompTIA is also a non-profit organization, like ISC^2, and is considered one of the IT industry's top trade associations, providing vendor-neutral certifications. The CAE has its own topics called KUs, as described above, and is aligned closely with the NIST/NICE framework. These refer to security as cybersecurity and cyber defense.

For academia, the IS 2010 recommended curriculum for Information Systems programs is the only framework available and does not include security as a required course. It does provide a course description, learning objectives, and topics for an elective course called IT Security and Risk Management (ACM, 2019). The main topics include (1) Inspection of Assets; (2) Detection/Protection Techniques; (3) Risk Assessment Frameworks; (4) Security Engineering (e.g. Access Control, Cryptography); (5) Physical Security; (6) Network Security; and, (7) Policy and Management Issues. As side note, CAE/NIST and IS 2010 are based in the United States, whereas ISC^2 is an international organization. CompTIA's headquarters are in the United States, but its certifications are considered international.

The varying terminology can be confusing to students and may cause misunderstandings of the required skillsets needed. The U.S. Department of Labor's Occupational Outlook Handbook (OOH) provides its own list of what Information Security Analysts do as part of that particular occupation (OOH, 2019). To add to this, a popular job board uses both security and cybersecurity in its job titles and lists a variety of job requirements (Dice, 2019).
Therefore, there are many frameworks and approaches available for security curriculum. Currently, there is no clear standard from which faculty can choose. Faculty face many challenges in choosing the one that best fits their students' needs. How do faculty choose? Which of the frameworks best cover the necessary security topics?

Reflection #2 - What *resources* are available to support security curriculum in CIS programs?
Security, like all of the IT disciplines, requires a dedicated faculty and solid curriculum to cover the complex topics thoroughly. The higher-level and more managerial topics require current examples, up-to-date case studies and solid context (Merkow & Breithaupt, 2014). Students benefit from reading how these principles are applied to real situations and by real organizations. For example, recent data breaches at well-known businesses help reinforce the key security topics, like business continuity planning and disaster recover. As with most computer courses, the content needs to be constantly changing and evolving in order to keep pace with Information Technology industry. This alone is challenging in and of itself. In addition, it is ideal if faculty have direct experience in security topics and in the field, if possible.

The more technical topics require a similar but also a very different approach. These demand hands-on exercises in computer laboratories outfitted with proper hardware and software (CompTIA, 2019). Students need the opportunity to use the tools of the trade, like cryptography and network sniffers. Computer laboratories must be monitored, maintained and upgraded on a regular basis. These labs require physical space and security, creating a need for faculty to work closely with the institution's IT and administrative staff. In many cases, faculty must also balance this with their teaching loads and research projects, again creating an issue with limited time and resources.

All of these resources must be funded by the institution or through an external grant. In addition, these resources must compete with other in-demand areas, like data science, as well as the courses that still need to be taught as part of CIS programs. Data science is one of the fastest growing segments of the IT industry (Granville, 2014). CIS programs would be remiss in not providing curriculum in this area. Data science, like security, requires faculty to have significant dedication, focus, and knowledge. Security skills are also in demand and the need is increasing each year (Kauflin, 2017). Can public institutions provide detailed coverage in all areas of IT with limited resources? If not, then where should faculty focus the resources?

Reflection #3 - What type of security *curriculum* is appropriate in CIS Programs?
CIS programs can only include a limited number of CIS courses in order to meet the overall requirements of the institution. In most cases, institutions require all students to take some type General Education or Core Courses. The remaining courses are part of specific programs, like CIS or CS. This limits the number of credits available to CIS-only courses and does not allow the ability of most programs to offer multiple courses in a specific discipline, like security. Faculty can be creative with electives and cognates, but this still may not be enough to meet the requirements of certification the CAE. Nor does it provide students the chance to take courses in other lesser-in-demand disciplines or special topics. Faculty face challenges in providing flexibility in their programs if one specific discipline, like security, has more of a focus.

The CAE-CD designation is a time-consuming process that demands complete dedication by faculty and administration of the institution for a minimum of two years. Of course, most faculty would like to have such a designation, but the reality is that there may not be enough resources at many institutions. Since only one program can be used to pursue the CAE certification per institution, Computer Science programs may have more electives available and be more suited. In many cases, CS programs have less "business" course requirements and more flexibility for students to take electives (CS, 2019). The downside is that many CIS majors may like to take more security courses. The security job market is strong but so is the market for software developers, database administrators and website designers (OOH, 2019). Again, the issue becomes depth versus breadth and whether students have the flexibility to choose from several disciplines or focus just on security.

Developing concentrations or minors may be a better approach for CIS programs instead of focusing on the CAE. Recently, this approach has been very successful at the authors' institution with a new Data Science Minor available in Fall 2018. As of the end of the Spring 2019 semester, over 20 students had already added the minor to their curriculum. This group includes many CIS majors, but also majors in Accounting, Computer Science, Finance and Management. Creating a concentration or minor in security would require minimal resources and provide students across disciplines the opportunity to learn valuable skills and an easily obtained credential to add to their transcripts and resumes. Should faculty focus their resources on developing minors or concentrations instead of pursuing discipline-specific designations like the CAE? Which type of security curriculum would better serve the needs of students? Which of security curriculum would align better with the resources available at public institutions?

SUMMARY

There are many benefits from pursuing and obtaining the CAE-CD designation but also many other considerations faculty should take into account. The process is very demanding and time consuming, requiring significant resources. With the breadth of IS programs, it is very challenging to focus resources on only one of the many disciplines covered in a Computer Information Systems (CIS) program. In addition, other approaches like minors or concentration could provide similar benefits to students as would the CAE designation. Therefore, faculty should take into consideration the student body of their respective institutions before selecting a framework for developing the security curriculum in IS programs.

In addition, future reflections and/or considerations in this area should address what type of programs (e.g. IS, CIS, CS) have received this designation as well as its impact on the institutions in terms of enrollment and job placement. The breakdown of programs would provide valuable insight as to the percentage of CIS versus other programs. This could answer many questions about the types of courses in CIS programs and whether they are suited to this type of specialized designation. Enrollment and job placement data would shed light on the impact of having such designations and its overall benefits to the institution and students. This would require significant assistance with enrollment reports and possible alumni organizations.

REFERENCES

ACM (2019). Curricula Recommendations. Accessed May 8, 2019. Retrieved from https://www.acm.org/education/curricula-recommendations.

Bain, L.Z., Bhatnagar, N. & Chapman, T. (2017). How Do Information Systems (IS) Programs Prepare Students for Entry-Level Occupations in the Computer and IT Industry? *Issues in Information Systems Journal* (IIS), (XVIII) 3, 78-88.

CAE-CD (2019). CNRC - Knowledge Unit Development. Accessed May 8, 2019. Retrieved from https://www.caecommunity.org/ogcnrccrrc/cnrc-knowledge-unit-development.

College Board (2019). AP Courses. Accessed May 10, 2019. Retrieved from https://apstudent.collegeboard.org/apcourse.

CompTIA (2019). Certification. Accessed May 1, 2019. Retrieved from https://certification.comptia.org/.

CS (2019). Computer Science Program and Computer Information Systems Program. Accessed April 9, 2019. Retrieved from http://www.ric.edu/mathcomputerscience/Pages/Computer-Science-Program.aspx and http://www.ric.edu/accountingcomputerinformationsystems/Pages/Computer-Information-Systems-Program.aspx.

Dice (2019). Find Jobs in Tech. Accessed May 4, 2019. Retrieved from https://www.dice.com/.

Granville, V. (2014). The growth of data science over the last two years: 300%. *Data Science Central*. Accessed May 10, 2019. Retrieved from https://www.datasciencecentral.com/profiles/blogs/the-growth-of-data-science-in-the-last-two-years.

ISC^2 (2019). Cybersecurity and IT Security Certifications. Accessed May 13, 2019. Retrieved from https://www.isc2.org/.

Kauflin, J. (2017). The Fast-Growing Job With A Huge Skills Gap: Cyber Security. *Forbes Online*. Accessed May 10, 2019. Retrieved from https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#618defe55163.

Merkow, M. S. & Breithaupt, J. (2014). Information Security Principles and Practices, 2nd Edition. Pearson Education, Inc. Indianapolis, IN.

NICE (2019). NICE Cybersecurity Workforce Framework. Accessed May 8, 2019. Retrieved https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

NSA (2019). National Centers of Academic Excellence. Accessed April 9, 2019. Retrieved from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/.

OOH (2019). Computer and Information Technology Occupations. Access April 9, 2019. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/home.htm.

Schwartz, M. S., Sadler, P. M., Sonnert, G. & Tai, R. H. (2009). Depth versus breadth: How content coverage in high school science courses relates to later success in college science coursework. *Science Education*, 93 (5), 798-826.