Oct 12th, 10:55 AM - 11:20 AM

Proposal for a Joint Cybersecurity and Information Technology Management Program

Christopher Simpson
National University, csimpson@nu.edu

Debra Bowen
National University, dbowen@nu.edu

William Reid
National University, wreid2@nu.edu

James Juarez
National University, jjaurez@nu.edu

Abstract
Cybersecurity and Information Technology Management programs have many similarities and many similar knowledge, skills, and abilities are taught across both programs. The skill mappings for the NICE Framework and the knowledge units required to become a National Security Agency and Department of Homeland Security Center of Academic Excellence in Cyber Defense Education contain many information technology management functions. This paper explores one university's perception on how a joint Cybersecurity and Information Technology Management program could be developed to upskill students to be work force ready.

Location
KSU Center Rm 460

Disciplines
Curriculum and Instruction | Information Security | Technology and Innovation

Comments
I didn't see a place to upload the file on how we addressed reviewer comments, so it's pasted below.

Special thanks to the reviewers for their detailed and thoughtful comments. The following items were addressed in our final revision:

1. First of all I do not know if this proposal written in response to an RFP! And I do not know who is the granter for this proposal because NSF requirements is different from other entity requirements.

- This was written for development of an internal p program

1. Some lingering limitations and concerns include the potential difficulties in some subjects proposed if there are no equipped labs to help the students have a hands on experience.

- Added discussion on current lab use and how adoption of labs increase collaboration between programs.

1. I would like to see if the choice for CAE is explained further since lots of other frameworks were explained.

- Added more details on CAE

1. I suggest replacing "would" with "will" throughout the paper. This will bring the writing out of the passive tense.

Fixed

1. The subtitles under "Frameworks to Consider" each have very short bodies of writing. Each part is around 1-2 sentences, and many of them are fragments. I suggest putting everything into complete sentences and to either add more detail to each section or combine everything into one larger subtitle.

- Added additional details on each framework.

1. The author mentions many similarities in the "Differences in CYB and ITM Curriculum" section. Instead, I suggest waiting to hit on the similarities until that corresponding section. You should focus

more heavily on the differences during the differences section.

- Good point, we try to explain this in paragraph 2 of the differences section.

1. In table 2, I suggest adding more detailed descriptions for the CTM courses. They are very vague at the moment, and for someone with limited knowledge and background in this field, it can be hard to understand.

- Excellent point. We are still in the early research and development and haven't built detailed descriptions yet. The courses will be modeled after the current courses and merged as appropriate to meet KU's and KSA requirements.

INTRODUCTION

The skills gap in cybersecurity continues to be an issue that is creating unique opportunities and challenges for educational institutions. Even though the number of schools designated as Centers of Academic Excellence (CAE) is growing, the ability to prepare enough cybersecurity students cannot meet the demands of the industry (Tsado, 2019). From the perspective of a non-profit university with limited resources we are attempting to develop a cybersecurity focused program, by combining two current bachelor's programs. This new program will need to be flexible enough to adjust as changes in the industry necessitate.

We propose an option of combining a Bachelor of Science in Cybersecurity (BS CYB) program with a Bachelor of Science in Information Technology Management (BS ITM) program to create a single Bachelor of Science in Cybersecurity and Technology Management (BS CTM) program. This new program will combine resources to create an educational program built on a Centers of Academic Excellence in Cyber Defense (CAE-CD) framework, using CAE-CD knowledge areas and knowledge units. The BS CTM program will upskill students to be workforce ready in a variety of information technology/security jobs or to immediately continue into a master's degree program.

FRAMEWORKS TO CONSIDER

There were several frameworks to consider when planning cybersecurity and/or information technology curricula. Finding one or a combination that would be applicable to our current CYB and ITM programs, while simultaneously providing a fundamental foundation for a new CTM program was challenging. We began by examining some of the more well-known cybersecurity and IT frameworks.

National Initiative On Cybersecurity Education (NICE 2.0)

The NICE 2.0 framework is published by the National Institute of Standards and Technology (NIST) and was developed as a fundamental reference to provide a standardized lexicon for cybersecurity job duty categories and descriptions (Newhouse, Keith, Scribner, & Witte, 2017). This framework consists of seven main categories of cybersecurity related functions. There are thirty-three specialty areas of work associated with cybersecurity that are distributed among the seven main categories. These are further divided into a set of work roles that contain a set of knowledge, skill, and abilities required to serve in that role (Newhouse, Keith, Scribner, & Witte, 2017).

Centers Of Academic Excellence In Cyber Defense Education (CAE-CD)

A framework created in partnership with the National Security Agency (NSA) and the Department of Homeland Security (DHS) to provide guidelines for designating academic institutions. In order to achieve designation as CAE a university must complete administrative requirements that demonstrate a commitment to excellence in cybersecurity education and the designated curriculum must cover a required set of knowledge units (NSA, 2019b). Specific requirements vary based on the level of the program but generally consist a set of three foundational knowledge units (KUs), five technical or non-technical core KUs, and a selection of optional KU's. KUs are maintained by the CAE community. Figure 1 provides a high-level overview of the KU requirements.

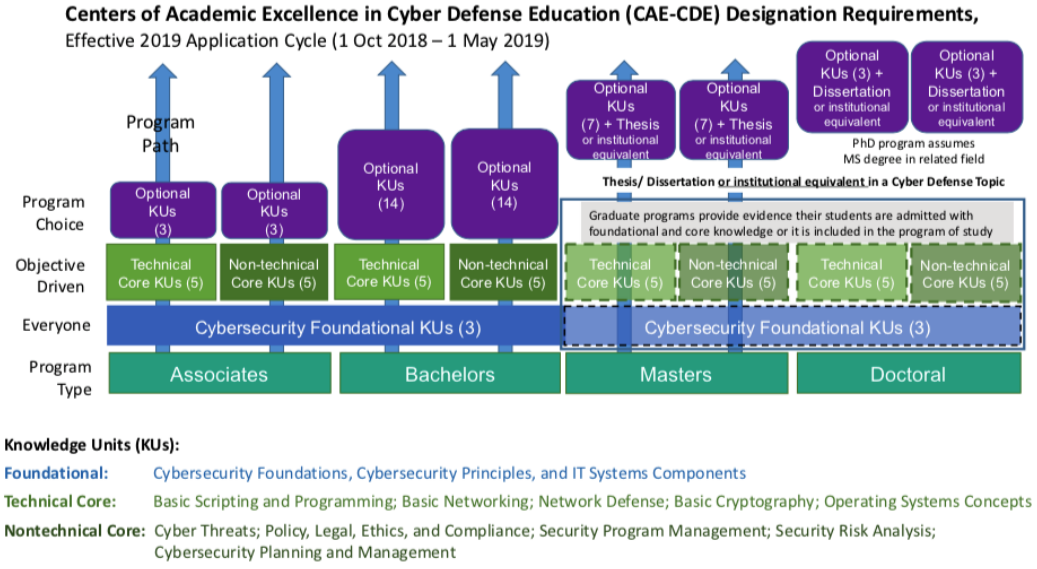

Figure 1 (NSA, 2019a)

A KU consists of a high-level description, required outcomes, a list of required topics, and a vocabulary list. Each KU is mapped to related NICE Workforce Framework Categories. Figure 2 is an example of a KU.

Cybersecurity Foundations (CSF)
The intent of the Cybersecurity Foundations Knowledge Unit is to provide students with a basic understanding of the fundamental concepts behind cybersecurity. This is a high-level introduction or familiarization of the Topics, not a deep dive into specifics.
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)

Figure 2 (NSA, 2019a)

Cybersecurity Curricula 2017 (CSEC2017)

The CSEC 2017 framework is designed for universities creating cybersecurity programs. It provides curriculum guidelines for post-secondary degree programs in cybersecurity. This education-focused framework was developed by a joint taskforce to align cybersecurity curriculum in higher education to industry needs (CSEC2017, 2017). The framework takes an interdisciplinary approach and divides cybersecurity into different knowledge areas. These knowledge areas contain knowledge units and topics along with desired learning outcomes. This framework was developed from other framework including CAE knowledge units and the NICE Workforce framework (CSEC2017, 2017).

Information Technology Curricula 2017 (IT2017)

The IT2017 framework provides guidance for the development of information technology baccalaureate degree programs. This is a student focused framework to prepare IT graduates to be workforce ready or to continue their education (IT2017, 2017). This framework consists of Essential and Supplemental IT domains. Each domain has a defined scope and a set of desired competencies. The domains are further divided into sub domains. This framework contains an essential domain dedicated to cybersecurity principles (IT2017, 2017).

Accreditation Board For Engineering And Technology (ABET)

Guided by CSEC 2017, along with input from the computing community, ABET created cybersecurity accreditation criteria that allowed for flexibility to support individual program outcomes as well as the ability to continually improve a cybersecurity program (ABET, 2019).

FRAMEWORK SELECTION

Since the NICE 2.0 framework focused on job duties in the cyber workforce, using this framework by itself for an educational curriculum, did not seem practical. However, we were able to gain valuable insight from the survey conducted by Jones, Namin, and Armstrong (2018) regarding knowledge, skills, and abilities (KSAs) most important to incorporate into a cybersecurity curriculum to upskill students to meet industry needs. Additionally, schools seeking CAE designation must identify which NICE Workforce Framework categories are covered in the designated program. CAE KU's have already been mapped to NICE Framework categories.

While the CSEC2017 and the IT2017 describe different aspects of cybersecurity education and domains of IT education respectively, they did not appear to be the best framework for our unique accelerated four-week per class structure. ABET was one of the newer frameworks we explored, however with

limited dedicated faculty we needed a framework that was familiar and one we could implement in less than 18 months.

Designation of our Masters of Cybersecurity program as a CAE provides significant benefits to the program and the university. These benefits include access to grant opportunities, providing students a list of knowledge units they have completed that can be shared with potential employers, and the ability to participate in the broader CAE community. Because of these benefits the university will seek CAE designation for our current BS Cybersecurity and BS Information Technology Management programs. The knowledge units for these programs will be used to build and model the new CTM program with online and onsite modalities.

DIFFERENCES IN CYB AND ITM CURRICULUM

Similar in their concentration on information as the core of organizational operations, cybersecurity and information technology majors view this core element from slightly different perspectives and approaches. The focus of ITM has been appropriate facilitation of operations and communications throughout an organization to meet and enhance business objectives (Mardis et al., 2018). Correspondingly, CYB perspective relies on the idea of appropriately protecting surrounding organizational technology, people, and process in order to appropriately facilitate confidentiality, integrity, and availability (CIA) within the business objectives (LeClair, Abraham, & Shih, 2013; Sobiesk, Blair, Conti, Lanham, & Taylor, 2015). The broader spectrum of ITM program content identifies data, files, users, access, and connectivity across the organizational function and provides the necessary software, hardware, network, security, and managerial procedures to facilitate that information towards organizational goals. CYB program content takes much of the ITM content and asks the question, is this individual technology, procedure, or personnel secure, vulnerable, or compromised?

Fundamentally, the ITM and CYB programs are similar in their use of technology for stakeholders, infrastructure, and systems of the organization. However, that similarity was differentiated by the approach (direction, timing, intensity) and perspective of these foundations towards operations and security. As an example, the ITM curriculum was geared towards assessing the user experience and ease of access for secure business information of an employee within an organization provided by its network and system (nu.edu/ITM, 2019). On the other hand, the CYB curriculum concentrated on assessing the vulnerability and threats created by the individual towards the system at various phases and conditions of access (nu.edu/CYB, 2019). Although the programs examined the same system and user, their direction, timing, intensity, and perspective was unique.

To build on the comparison of the expected outcomes between the ITM and CYB programs, the concept of breadth versus depth becomes the obvious touchpoint. The ITM and CYB programs were most similar at the lower division and capstone courses but diverge at the upper-division courses which are the specializations for the CYB program. Examining the program and course learning outcomes (PLOs/CLOs) for key identifiers and underlying knowledge units (KUs) reveal the degree of overlap in information security and technology concepts and practice both in number of learning interactions and depth of knowledge (DoK) within those interactions. Although primarily written using Bloom's Taxonomy, Norman Webb's DoK with four levels (Recall and Reproduction, Skills, and Concepts, Strategic Thinking, Extended Thinking) provided a cursory tool for quickly comparing PLOs/CLOs and KUs across both programs (Aungst, 2014; Patten & Harris, 2016). Appendix A contains an example of KU's similar across cybersecurity and information technology management programs.

Further examining the concentrations, or specializations, in the majors, there are further indicators of differences of depth and breadth. For the ITM program, there is a general focus on technological components, from the system management and project perspectives. However, the ITM major does not currently offer any specializations. Conversely, the CYB program provides two concentrations that dive deeper into Computer Network Defense (CND) or Digital Forensics (DF). Specifically, the CND concentration provides additional time and practices with hardening virtual and physical systems and networks. The DF concentration examines the specific rules, regulations, and procedures for investigations on networked computing systems. Of the two, the DF concentration is more technically focused.

In addition to differences in depth and breadth of information technology topics versus cybersecurity topics in the ITM and CYB programs, there is also a matter of perspectives or tools, techniques, and procedures (TTPs) used to address these topics. As a comparison, the ITM program touches on many of the topics in the CYB-CND concentration through its core courses in Local and Wide Area Networks (LAN/WAN), Wireless LAN Administration and Security, and Information Security Management and Security Technology courses. However, the CYB-CND focusses on additional TTPs to facilitate security planning as well as additional security testing, while ITM approaches these topics with TTPs for long term planning, project planning, daily operations, and management.

As an example, the CYB-CND content and practice include TTPs for penetration (pen) testing hardened networks, red and blue team activities for real-time incidence test and response, and exhaustive document for information assurance. Additionally, the CYB-NF takes the information security concepts of confidentiality, integrity, and availability (CIA) and expands them to an extensive

look at the TTPs for non-repudiation, traceability, and legal policy. Although these topics are found in the ITM program the concepts are limited to DoKs at the first and second level, where CYB-CND explores these at all four levels.

SIMILARITIES IN CYB AND ITM CURRICULUM

For the larger picture of information communication technology (ICT) education, industry, and accrediting authorities view these disciplines as related across learning, training, and profession for much of the technological areas of the field (Hudnall, 2019). As previously mentioned, the ITM and CYB programs share many of the same PLOs/CLOs, knowledge areas (KAs), and knowledge units (KUs). This was largely due to the shared focus on information, technology, people, and process for the broad scope of an organization and in support of its continued operations (LeClair et al., 2013).

In terms of the academic journey both the ITM and CYB programs follow similar course structures, methods of teaching, and lab resources, allowing the mapping of similarities to be mostly straightforward and exhibited similar scaffolding (nu.edu/CYB, 2019; nu.edu/ITM, 2019). When we look at the lower division courses it was clear that identical topics were being covered at the same DoK levels (1 through 4). For example, in the course ITM340 – IT Clients Using MS Windows, there were CLOs that covered Examining the Structures of Client-Server Environment and Demonstration of Features within a Client Operating System. These same CLOs can be found at the depth for CYB332 Secure Windows Administration. However, although the CLOs are the same and similar DoKs are achieved, there was a difference in perspective and focus with ITM towards operations and CYB exploring more of protection.

Both programs have a hands-on lab component and the labs used in each program are provided by the same vendors. The migration to common lab environment has reduced costs while delivering an approved educational experience for students.

The ICT foundations for both programs were consistently built on the same scaffolding for TTPs as well as theoretical concepts at the lower division and later in the capstone courses. Each of the undergraduate programs concludes the academic journey with a series of capstone courses, 490 A, B, and C (499 for the CYB program). Just like the lower division courses, the capstone series focusses largely on the same principles and CLOs for conducting a sponsored real-world project and employing the program PLOs through the project management process. Examining the KAs and KUs for the capstones also yield identical project focused outcomes at the same DoKs. However, consistent with the trends in the lower

division courses, the capstone takes on the perspective changes between operations versus protection.

Bridging the gaps and merging the ITM and CYB programs started to make sense as the difference between the two remained largely at the perspective or view of the organization level. Realizing that the similarities throughout the programs lent themselves to a stronger more unified academic and practical experience once the perspective for both programs could be elevated to a more comprehensive and balanced view of the discipline and the enterprises it serves. Once the programs are merged and prescribed to a larger perspective, like the Enterprise Security Lifecycle (ESL), then concentrations or specializations can be established in order to address more granular needs within a functioning and protected ICT environments (Bhardwaj, Subrahmanyam, Avasthi, & Sastry, 2016).

PROPOSAL FOR NEW CTM PROGRAM

As stated by Logan (2002) and still true today, it is the responsibility of higher education to prepare a workforce that is ready to secure our nations information and infrastructure. The success of any Information Security program may rest on shifting focus from implementation and administration of network technologies (e.g. Information Technology Management degree programs) to a program that emphasizes theory, abstraction, and design of secure network infrastructures designed to protect information assets (Cybersecurity degree programs). We believe one way to upskill students to be workforce ready is to combine the knowledge units from these two programs into a single program so that information security management professionals are also information technology relevant. This combining of such skills can be noted in several ABET accredited schools that are infusing cybersecurity into their engineering curricula.

In addition to mapping curriculum to required CAE knowledge units, many CAE institutions map their curriculum to professional certifications like the International Information Systems Security Certification Consortium's (ISC^2) Certified Information Systems Security Professional (CISSP). Mapping curriculum to professional certifications may increase employment opportunities for graduates (Wierschem, Zhang, & Johnston, 2010).

Our proposal for developing a new Bachelor of Science program started with examining our existing CYB and ITM bachelor programs for similarities of content. Currently our CYB program has 23 courses and the ITM program has 19 courses. For each program three courses encompass a Capstone project that all students must take to receive the degree. Our intention is to create a new CTM program that can be completed in 18 months (or less if taught in a competency-based modality).

Table 1 provides an example of some of the courses that share similar knowledge units that would be combined into a new CTM bachelor's program.

CYB Course	**Description**	**ITM Course**	**Description**
CYB212	Introduction to Networking	ITM230	Computer Network Overview
CYB216	Programming for Cybersecurity	ITM438	Role of Programming in IT
CYB332	Secure Windows Administration	ITM340	IT Clients using MS Windows
CYB331	Secure Linux Administration	ITM345	IT Servers using Linux

Table 1: Similarities between existing CYB and ITM content.

The basic premise is to create a CTM program that encompasses the CAE knowledge units for cybersecurity and information technology management that can provide students with industry ready skills as quickly as possible (depending on a student's individual capability). In addition, the program must maintain rigor and quality to meet accreditation standards. Table 2 represents a potential list of core courses for a potential CTM program.

CTM Course	**Description**
CTM200	Hardware and Software
CTM201	Introduction to Cybersecurity
CTM202	Introduction to Networking
CTM203	Introduction to Operating Systems
CTM300	Secure Linux Administration
CTM301	Secure Windows Administration
CTM302	Wireless LAN Administration
CTM400	Network Defense
CTM401	Fundamentals of Cloud and Virtualization
CTM402	Programming Concepts for Cybersecurity
CTM425	IT Project Management

CTM499A	Capstone Project I
CTM499B	Capstone Project II
CTM499C	Capstone Project III

Table 2: Potential core courses for a new CTM program.

In addition to the suggested core courses, there will be specializations, allowing for students to pursue their area of interest. Each specialization will entail four or five additional courses to enhance a student's skill. Currently there are three specializations being considered, which are Digital Forensics, Computer Network Defense, and Information Technology Management. These three specializations will allow students to focus on either technology management or information security, complementing the core courses so that both cybersecurity and technology are a part of the overall program.

CONCLUSION

There are many different frameworks that can be used to guide a successful cybersecurity or IT program. The common goal is to prepare enough skilled cybersecurity workers to meet the demands of the industry. However, the industry is continually changing and with limited resources to keep curriculum content up to date our goal is to have one CAE designated bachelor's program that provides the skills and knowledge students need to either immediately enter the workforce or to continue with their education. Although KUs are sure to change, having a program aligned with a CAE framework will take less effort and resources to adjust when industry needs necessitate a curriculum change.

REFERENCES

ABET Criteria for Accrediting Computing Programs, 2019-2020; https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2019-2020/#2. Accessed 2019 Jul 17.

Aungst, G. (2014). Using Webb's Depth of Knowledge to Increase Rigor. Retrieved July 12, 2019, from Edutopia website: https://www.edutopia.org/blog/webbs-depth-knowledge-increase-rigor-gerald-aungst

Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Design a Resilient Network Infrastructure Security Policy Framework. Indian Journal of Science and Technology, 9(19). https://doi.org/10.17485/ijst/2016/v9i19/90133

CSEC2017, "Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity," version 1.0 report, 2017. doi:10.1145/3184594

Hudnall, M. (2019). Educational and Workforce Cybersecurity Frameworks: Comparing, Contrasting, and Mapping. Computer, 52(3), 18–28

IT2017, "Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology". (2017) ACM/IEEE-CS. doi:10.1145/3173161

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. ACM Transactions on Computing Education (TOCE), 18(3), 11.

LeClair, J., Abraham, S., & Shih, L. (2013). An interdisciplinary approach to educating an effective cyber security workforce. Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, 71. ACM.

Logan, P. Y. (2002). Crafting an undergraduate information security emphasis within information technology. Journal of Information Systems Education, 13(3), 177.

Mardis, M. A., Ma, J., Jones, F. R., Ambavarapu, C. R., Kelleher, H. M., Spears, L. I., & McClure, C. R. (2018). Assessing alignment between information technology educational opportunities, professional requirements, and industry demands. Education and Information Technologies, 23(4), 1547–1584.

NSA. (2019a). 2019 Knowledge Units. National Security Agency Retrieved from https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

NSA. (2019b). CAE Requirements and Resources. Retrieved from https://www.iad.gov/nietp/CAERequirements.cfm

Newhouse, W., Keith, S., Scribner, B., and Witte, G. National Initiative for Cybersecurity Education (NICE), 2017. Cybersecurity Workforce Framework. Report NIST.SP.800-181, 2017. doi:10.6028/NIST.SP.800-181

nu.edu/CYB. (2019). NU: Bachelor of Science in Cybersecurity. Retrieved July 12, 2019, from National University website: https://www.nu.edu/ourprograms/schoolofengineeringandtechnology/computerscienceandinformationsystems/programs/bs-cybersecurity/

nu.edu/ITM. (2019). NU: Bachelor of Science in Information Technology Management. Retrieved July 12, 2019, from National University website: https://www.nu.edu/ourprograms/schoolofengineeringandtechnology/computerscienceandinformationsystems/programs/bsinformationtechnology/

Patten, K. P., & Harris, M. A. (2016). Evaluating Student Learning in an IT Curriculum Using Bloom's–Webb's Curriculum Taxonomy. Proceedings of the 17th Annual Conference on Information Technology Education, 111–114. ACM.

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). Cyber education: A multi-level, multi-discipline approach. Proceedings of the 16th Annual Conference on Information Technology Education, 43–47. ACM.

Tsado, Lucy (2019) "Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach," Journal of Cybersecurity Education, Research and Practice: Vol. 2019 : No. 1 , Article 4.

Wierschem, D., Zhang, G., & Johnston, C. R. (2010). Information technology certification value: An initial response from employers. Journal of International Technology and Information Management, 19(4), 89.

APPENDIX A

CAE Knowledge Units	**Information Technology Management (ITM) and Cybersecurity (CYB) Overlap**
IT Systems Components (ISC) The intent of the IT Systems Components Knowledge Unit is to provide students with a basic understanding of the components in an information technology system and their roles in system operation. This is a high-level introduction or familiarization of the Topics, not a deep dive into specifics.	This material is typically covered in a 200 level ITM and CYB class
Basic Networking (BNW) The intent of the Basic Networking Knowledge Unit is to provide students with basic understanding of how networks are built and operate, and to give students some experience with basic network analysis tools. Students are exposed to the concept of potential vulnerabilities in a network.	There is an introduction to networking class in each program.
Policy, Legal, Ethics, and Compliance (PLE) The intent of the Policy, Legal, Ethics, and Compliance Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.	Information Technology and Cybersecurity staff must meet common compliance requirements including that are in this knowledge unit: a. Computer Security Act b. Sarbanes – Oxley c. Gramm – Leach – Bliley d. Privacy (COPPA) HIPAA / FERPA e. USA Patriot Act

	f. Americans with Disabilities Act, Section 508 g. Other Federal laws and regulations
Windows System Administration (WSA) The intent of the Windows System Administration Knowledge Unit is to provide students with skill to perform basic operations involved in system administration of Microsoft Windows based systems.	This knowledge unit conations core system administration knowledge required of both Information Technology and Cybersecurity staff.
Linux System Administration (LSA) The intent of the Linux System Administration Knowledge Unit is to provide students with skill to perform basic operations involved in system administration of LINUX based systems.	This knowledge unit conations core system administration knowledge required of both Information Technology and Cybersecurity staff.