Winter 12-13-2018

Enhancing Cybersecurity Content in Undergraduate Information Systems Programs: A Way Forward

Rajendra K. Raj
Rochester Institute of Technology

Jean R.S. Blair
United States Military Academy

Edward Sobiesk
United States Military Academy

Allen Parrish
Mississippi State University

Enhancing Cybersecurity Content in Undergraduate Information Systems Programs: A Way Forward

Rajendra K. Raj[1]
Rochester Institute of Technology,
Rochester, New York, USA

Jean R. S. Blair, Edward Sobiesk
United States Military Academy,
West Point, New York, USA

Allen Parrish
Mississippi State University,
Mississippi State, Mississippi, USA

ABSTRACT

The ongoing barrage of data and infrastructure breaches is a constant reminder of the critical need to enhance the cybersecurity component of modern undergraduate information systems (IS) education. Although the most recent undergraduate information systems curricular guidelines (IS2010) highlight security in the context of data, enterprise architecture, and risk management, much more needs to be done. The IS education community needs to identify cybersecurity competencies and curricular content that further integrates cybersecurity principles and practices into IS curricular guidelines. Until this is completed at the IS community level, IS programs will need to fulfill this role individually. This paper contributes to both these efforts by reviewing relevant literature and initiatives – highlighting two primary paths of curricular development: (1) the evolution of IS curricular guidelines, and (2) the development of Cybersecurity as a standalone discipline. Using these resources, the paper summarizes best practices for integrating cybersecurity into curricula and explores the integration of IS into cybersecurity programs.

[1] Corresponding author. Rajendra.K.Raj@rit.edu +1 585 475 2595

Keywords: Information systems education, information systems curricular guidelines, cybersecurity education, information assurance education, computing education.

INTRODUCTION

Around 832 million records were breached because of 619 separate incidents in the first nine months of 2018, and over the past five years 9.3 billion records where breached in 3,700 incidents (Privacy Rights Clearinghouse 2018). This is one example of countless reports of cybersecurity attacks on information systems. These incidents serve as reminders that the cybersecurity component of information systems (IS) education needs to be substantially strengthened, so that IS professionals are prepared to identify, protect, detect, respond, and recover from attacks affecting information systems, while also functioning as part of a larger cybersecurity team.

The most recent undergraduate information systems curricular guidelines (IS2010) are dated as they relate to cybersecurity. The IS education community needs to revise and update them to more thoroughly incorporate cybersecurity principles and practices. Until this is completed at the IS community level, individual IS programs will face the challenge of accomplishing this critical task on their own.

This paper reviews salient literature and initiatives, examining the evolution of IS curricular guidelines, describing the key developments involved in cybersecurity emerging as a standalone discipline, and presenting the latest ABET IS accreditation criteria. Based on these resources and initiatives, a way forward for improving cybersecurity in IS education is presented that includes best practices for integrating cybersecurity into curricula and exploration of integrating IS into cybersecurity programs. The paper advocates that these advances not be done

in a vacuum, but rather need to be purposely constructed to integrate with the cybersecurity efforts of several other technical and non-technical disciplines.

PERTINENT RECENT DEVELOPMENTS IN EDUCATION

This section reviews the most significant recent efforts in computing education relevant to cybersecurity in the context of IS education. The review looks at two primary paths of development: (1) the evolution of IS curricular guidelines, and (2) the development of Cybersecurity as a standalone discipline, which includes a version that is a standalone discipline based on an IS foundation. This section also includes an overview of the integration of cybersecurity into ABET accreditation criteria as it impacts IS.

The Evolution of Information Systems Education

As depicted in Figure 1, IS education has primarily evolved through bachelor-level IS curricular guidelines, the most recent of which is IS2010 (Topi et al. 2010), and masters-level IS curricular guidelines, the most recent of which is MSIS2016 (Topi et al. 2017).

IS2010. Many IS programs rely on the IS2010 curriculum guidelines for the design of their undergraduate degree programs. IS2010 specifies high-level capabilities, with security playing a role in two out of the seven: (1) Securing Data and Infrastructure and (2) Understanding, Managing and Controlling IT Risks. For the former, IS2010 states that organizations have a need to protect their data and IT infrastructure from various security threats and recognizes that IS graduates must understand the threats and be able to identify high-level solutions for protecting information systems. For the latter capability, IS graduates must also have strong capabilities in understanding, managing, and controlling organizational risks

associated with the use of IT-based solutions. These high-level capabilities map onto specific knowledge and skills across three categories: IS-specific, foundational, and domain fundamentals. The security related concepts are briefly touched on in several core courses specified in IS2010: Foundations of Information Security; Data and Information Management; Enterprise Architecture; IT Infrastructure; Systems Analysis and Design; IS Strategy, Management and Acquisition; and in the sample electives: Introduction to Human Computing Interaction; and IT Audit and Controls. Despite the mention of security in these course specifications, IS2010 does not provide a cohesive view of security in terms of the capabilities of IS graduates.

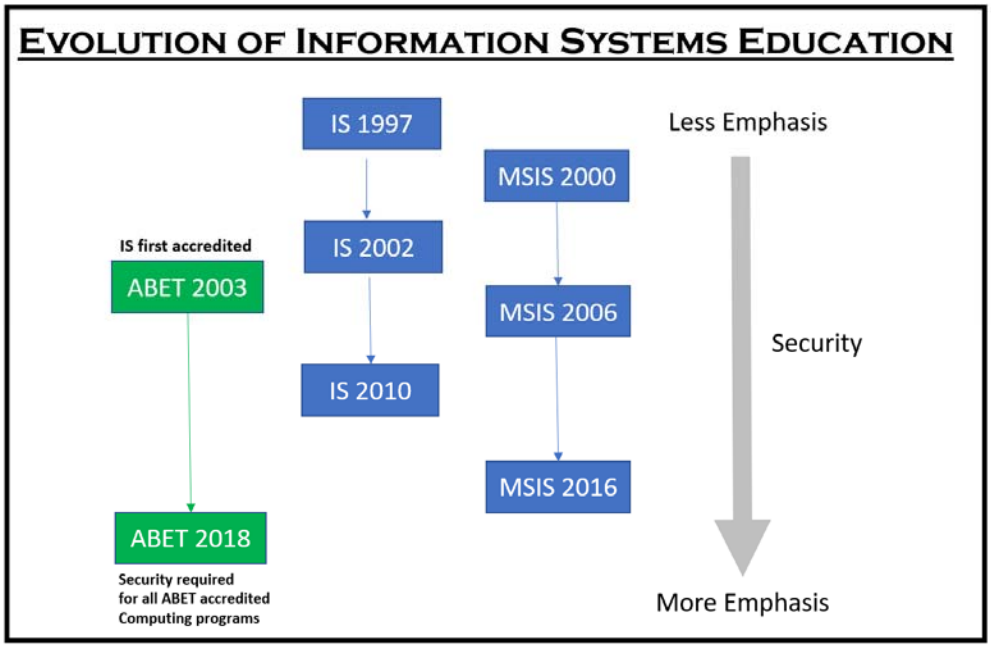

Figure 1. The Evolution of Information Systems Education

MSIS2016 (Topi et al. 2017) uses a competency-based approach to curricular guidance for master's level Information Systems programs; this competency model is also discussed later under IT2017. MSIS2016 divides core competencies into three similar-to-IS2010 categories: IS

competencies, individual foundational competencies, and domain competencies. Among the nine areas defined under IS competencies is *Business Continuity and Information Assurance*. Competencies within this area include managing and implementing cybersecurity, protecting IT assets, developing information assurance strategy, implementing and managing quality audit processes, and assuring safety throughout the systems' lifecycle. The next generation of IS undergraduate curricular guidelines will likely be guided by the direction taken in MSIS2016.

ABET. For over 15 years, the ABET Computing Accreditation Commission (CAC) has accredited IS specific programs. The latest edition of the ABET IS Program Criteria was published in 2018. In this edition, the requirement to integrate cybersecurity is now part of the general criteria for all computing programs, requiring principles and practices for secure computing that must be appropriate for the discipline.

The Development of Cybersecurity as a Discipline

A parallel relevant path of educational guidelines with more recent milestones is cybersecurity as a standalone discipline. As depicted in Figure 2, several initiatives contributed to this journey ultimately culminating in the Cyber Education Project, which led to a Joint Task Force on Cybersecurity Education producing Cybersecurity Curricula 2017 and to ABET producing Cybersecurity Program Criteria. In the subsequent paragraphs, each of these contributions is briefly highlighted.

Centers of Academic Excellence. The National Security Agency and Department of Homeland Security (NSA/DHS) designate National Centers of Academic Excellence in Cyber Defense (CAE-CD) based on institutional criteria. Each institution shows a mapping of its curriculum to the core knowledge units (KUs), optional KUs, and focus areas. These CAE-CD designations focus on ensuring an appropriate cybersecurity curriculum is available at the

institution. However, these designations do not require an institution to formally assess and evaluate the performance of their graduates against the KUs and focus areas. Complementing the CAE-CD effort, the NSA also designates National Centers of Academic Excellence for Cyber Operations (CAE-Cyber Operations) programs to increase the number of cybersecurity trained professionals. Unlike the CAE-CD effort, the CAE-Cyber Operations designates a student based on their transcript or degree satisfying all mandatory knowledge units and at least four of the optional knowledge units.

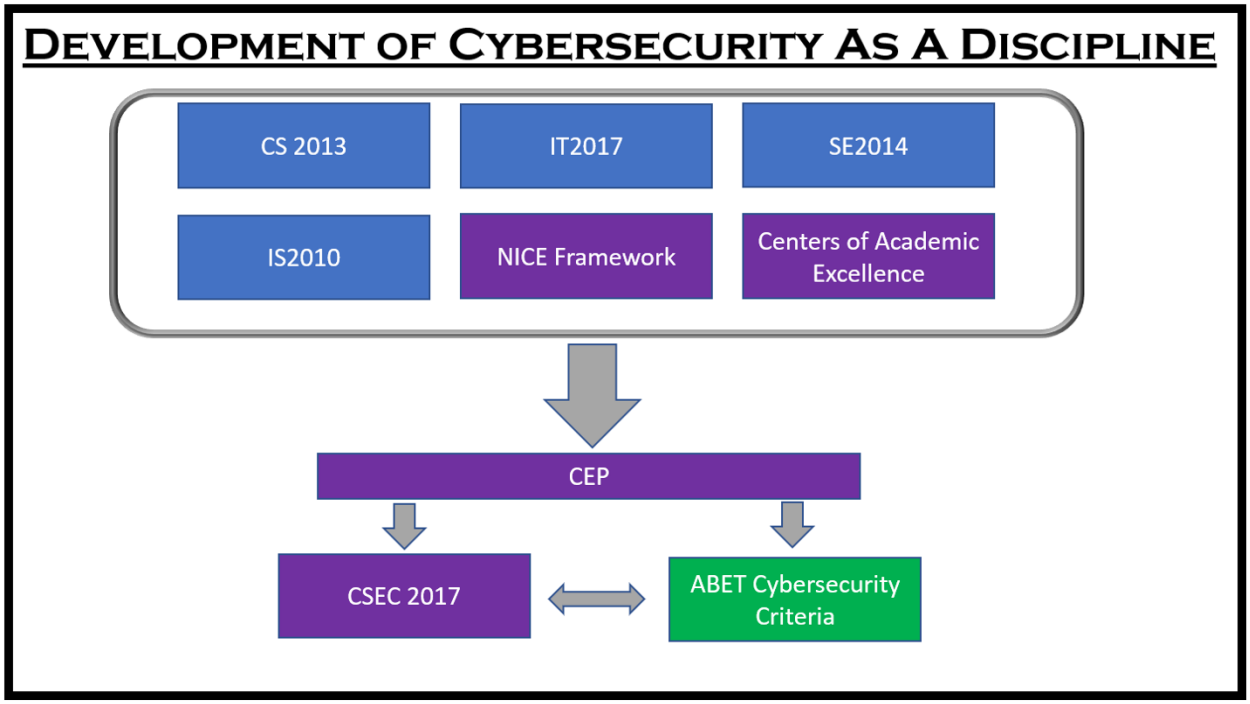

Figure 2. The Development of Cybersecurity as a Discipline

NICE Framework. The National Initiative for Cybersecurity Education (NICE) framework (Newhouse 2012) from the National Institute of Standards and Technology (NIST) "serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen cybersecurity posture of an organization" (Newhouse 2012). NICE's primary goal

is to support employers' plans and guide career development and workforce enhancement so that they can respond rapidly to market needs for cybersecurity professionals. The Skills Framework for the Information Age (SFIA) has similar goals of defining the workforce context for the application of cybersecurity skills and competencies (von Konsky 2016).

The Association for Computing Machinery (ACM) continues to provide greater integration of cybersecurity into the five classical computing disciplines: computer science, information systems, information technology, computer engineering, and software engineering. IS2010 was discussed above and the other three most relevant are discussed below.

CS2013 curricular guidelines (ACM/IEEE - CS2013) provide an exemplar of the way other computing disciplines are integrating substantial computer security content throughout the breadth of their curriculum. CS2013 recommends nine lesson-hours on "concepts where the depth is unique to Information Assurance and Security" and an additional 63.5 lesson hours of Information Assurance and Security content that is "integrated into other knowledge areas that reflect naturally implied or specified topics with a strong role in security concepts and topics" (ACM/IEEE-CS 2013). These CS-based cybersecurity curricular recommendations are mostly technical in nature and apply most significantly to the technical aspects of the curriculum.

IT2017 emphasizes that knowledge by itself is not sufficient and needs to be supplemented by both technical skill and human disposition to ensure successful practice. Competency focuses on performance in professional context:

Competency = Knowledge + [Technical] Skills + [Human] Dispositions

IT2017 recommends the cybersecurity content constitute around a tenth of the IT curriculum. Moreover, the material needs to be covered throughout the curriculum instead of just in a course or two. The cybersecurity integrated throughout IT2017 led to the proposition that any IT degree

program conforming to IT2017 will have substantial overlap with Cybersecurity Curricula 2017 (Ekstrom et. al 2017).

Both CS2013 and IT2017 are examples of the agreed on best practice of covering cybersecurity content throughout the entire curriculum, and not simply as something to be bolted on afterwards.

SE2014 (Leblanc, et al 2014) was written for software engineering. It contains 10 knowledge areas, including security. The security knowledge area is technical in nature, and contains 20 hours covering secure software design and development, network security and cryptography.

CEP and CSEC2017. The culmination of cybersecurity as a standalone discipline was the Cybersecurity Curricula 2017 report known as CSEC2017 (Burley et al. 2017). This report is meant to be "the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level" (Burley et al. 2017). CSEC2017 followed from the Cyber Education Project (CEP) grassroots effort to build consensus on cybersecurity education (Blair et al. 2015).

The CSEC2017 report presents a model of cybersecurity with three dimensions: knowledge areas, crosscutting concepts, and disciplinary lenses (see Table 1). The knowledge areas are the "basic organizing structure for cybersecurity content." The first five (Data, Software, System, Component, and Connection) primarily represent technical content, and the last three (Human, Organizational, and Societal) primarily represent social science and contextual content. Crosscutting concepts span all knowledge areas, while disciplinary lenses—when applied to a particular knowledge area and associated topics—impact what competencies and learning outcomes can reasonably be expected for that knowledge area.

Table 1. The three major components of CSEC2017 (Burley et al. 2017)

Component	Description
Knowledge Areas	Data Security, Software Security, System Security, Component Security, Connection Security, Human Security, Organizational Security, and Societal Security.
Crosscutting Concepts	Confidentiality, Integrity, Availability, Risk, Adversarial Thinking, and Systems Thinking.
Disciplinary Lenses	Computer Science, Computer Engineering, Information Systems, Information Technology, Software Engineering, and Mixed Disciplinary.

CSEC2017 disciplinary lens "represents the underlying computing discipline from which the cybersecurity program can be developed. The disciplinary lens drives the approach, depth of content, and learning outcomes resulting from the interplay among the topics.…The application of the crosscutting concept and/or the level of depth taught within each knowledge unit may differ depending upon the disciplinary lens. For instance, coverage of *Risk* in the context of *Data Security* may differ for students in a computer science cybersecurity program and those in an information systems cybersecurity program" (Burley et al. 2017). A program that is consistent with CSEC2017 guidelines is considered to be a cybersecurity program.

ABET is an organization dedicated to disciplinary accreditation in computing, engineering, engineering technology, and applied and natural science. Organized around the concept of commissions, ABET's Computing Accreditation Commission (CAC) currently accredits 59 undergraduate IS programs (as of September 2018), with 42 of these programs in the U.S. and 17 in other countries. An IS program accredited by the CAC must meet both a set of General Criteria (required of all computing programs) and a set of IS-specific Program Criteria.

Table 2 shows the current ABET student outcomes for IS programs; the first row shows the outcomes required of all computing programs while the second row shows the one outcome that is distinct to IS programs. Table 3 similarly shows the curricular requirements for IS

programs. As shown in Table 3, it is the CAC General Criteria that now include a significant cybersecurity curricular requirement (ABET 2017).

Table 2. The 2019-20 CAC Information Systems Accreditation Criteria – Student Outcomes (The first row is from the General Criteria and the second row from the IS Program Criteria)

Graduates of the program will have an ability to: 1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions. 2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline. 3. Communicate effectively in a variety of professional contexts. 4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles. 5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
6. Support the delivery, use, and management of information systems within an information systems environment. [IS]

Table 3. The 2019-20 CAC Information Systems Accreditation Criteria – Curriculum (The first row is from the General Criteria and the second row from the IS Program Criteria)

The program's requirements must be consistent with its program educational objectives and designed in such a way that each of the student outcomes can be attained. The curriculum must combine technical, professional, and general education components to prepare students for a career, further study, and lifelong professional development in the computing discipline associated with the program. The curriculum requirements specify topics, but do not prescribe specific courses. The program must include mathematics appropriate to the discipline and at least 30 semester credit hours (or equivalent) of up-to-date coverage of fundamental and advanced computing topics that provide both breadth and depth. The computing topics must include: 1. Techniques, skills, and tools necessary for computing practice. 2. Principles and practices for secure computing. 3. Local and global impacts of computing solutions on individuals, organizations, and society.
The curriculum requirements specify topics, but do not prescribe specific courses. These requirements are: a) Information systems: At least 30 semester credit hours (or equivalent) that include coverage of fundamentals and applied practice in application development; data and information management; information technology infrastructure; systems analysis, design and acquisition; project management; and the role of information systems in organizations. b) Information systems environment: At least 15 additional semester credit hours (or equivalent) of a cohesive set of topics that provide an understanding of an information systems environment. c) Quantitative analysis or methods that must include statistics.

The combined IS accreditation criteria also describe the notion of the IS environment, which is defined as "an organized domain of activity within which information systems are used to support and enable the goals of the activity. Examples of information systems environments include (but are not limited to) business, healthcare, government, not-for-profit organizations, and scientific disciplines."

In summary, the combined IS accreditation criteria require the curricular content stated in the bottom row of Table 3 to be informed by the "principles and practices of secure computing."

THE WAY FORWARD

The way forward for undergraduate IS programs can be summarized thus: until IS2010 is revised and updated, undergraduate IS programs must integrate the above cybersecurity education best practices and paradigms themselves. Each program must also determine whether its constituents would benefit most from remaining an IS program that has increased cybersecurity content or by becoming a cybersecurity program that has an IS lens.

Based on the related literature discussed above, several IS cybersecurity education best practices emerge:

- **Don't work in a vacuum.** Build on the work and best practices of others.
- **Integrate cybersecurity throughout the entire breadth and depth of the program**. This is prevalent in several of the exemplar curricular guidelines and could now be categorized as common knowledge. While there may be reasons to have a special course addressing cybersecurity specific foundations and topics, the days are past of bolting on cybersecurity after covering functionality and theory.

- **Include interdisciplinary cybersecurity content**. Computing professionals can no longer function exclusively in a technical silo. Interdisciplinary skills are a personal approach to knowledge development and problem solving that involves synergy across disciplines within an individual. Programs must prepare IS professionals to deal with the professional, legal, ethical, policy, cognitive, mathematical, societal, global, business, and emerging technology aspects of cybersecurity that are beginning to significantly manifest themselves.
- **Assume an intelligent, adaptive, and ever-present adversary**. This is one of the great contributions of CSEC2017. Making this assumption forces one to assess risk and to address security throughout all networks and infrastructure as well as in terms of people, organizations, and processes.
- **Consider competencies**. Both MSIS2016 and IT2017 have paved the way to think not just in terms of learning outcomes, but also in terms of competencies, which combine knowledge, technical skills, and human dispositions. Moreover, the layout of the IS curriculum in MSIS2016, albeit at the masters-level, provides guidance to undergraduate IS programs. This perspective will better account for the need of IS professionals to continue to grow and increase their level of knowledge and abilities, including in cybersecurity.
- **Integrate with the multidisciplinary cybersecurity team**. Although some efforts are being made to fight against disciplinary siloes, there is still significant need for improvement in all computing disciplines (including IS) identifying their discipline's role as part of a larger cybersecurity team effort – and then ensuring their actions and efforts tie in with the rest of the team. A multidisciplinary approach involves a team of individuals with diverse disciplinary expertise working together to create solutions that can only be developed by integrating aspects of the disciplines at a team level. Multidisciplinary team efforts mitigate

the fact that the greatest vulnerabilities are often at the boundaries between various disciplines.

- **Maintain a global mindset**. The continued increase of IS programs in the rest of the world shows that an international perspective toward IS education is mandatory. As the numbers indicate, almost a third of the IS programs accredited by ABET are now outside the U.S. It will be crucial to engage an international audience when incorporating cybersecurity content into undergraduate IS education. Parrish et al. (2018) provide a recent instance of such an international engagement, where global perspectives in cybersecurity education were discussed. Several more such events are needed.

As programs apply these best practices, they also need to methodically reflect on what the right amount of cybersecurity is for their constituent needs. In some (perhaps many) cases, this will mean remaining an IS program and integrating further cybersecurity content appropriately. In other cases, IS programs that include a substantial amount of security content may become standalone cybersecurity programs with an IS disciplinary lens and program titles such as cybersecurity, information security, and cyber operations. Both types of IS programs — IS with increased security throughout, and cybersecurity with an IS disciplinary lens — will play important roles.

CONCLUSION

This paper highlighted the most salient aspects of recent developments in cybersecurity education and proposed a way forward for integrating cybersecurity content holistically into

undergraduate IS programs. The paper advocates that these advances be coordinated with the increased integration of cybersecurity content into other technical and non-technical disciplines.

REFERENCES

ABET. 2017. "Criteria for Accrediting Computing Programs, Effective for Review During the 2019-20 Accreditation Cycle." (http://www.abet.org/wp-content/uploads/2018/11/C001-19-20-CAC-Criteria-11-24-18.pdf)

ACM/IEEE-CS. 2003. "Computer Science Curricula 2013." Technical Report. ACM Press and IEEE Computer Society Press. (https://doi.org/10.1145/2534860)

ACM/IEEE-CS. 2017. Information Technology Curricula 2017. Technical Report. ACM Press and IEEE Computer Society Press. (https://doi.org/10.1145/3173161)

Blair, J., Buck, S., Burley, D., Parrish, A., and Phillips, A. 2015. "The Cyber Education Project: Defining Educational Standards for an Emerging Discipline" (2015). WISP 2015 Proceedings. 15. (https://aisel.aisnet.org/wisp2015/15)

Burley, D. L., Bishop, M., Buck, S., Ekstrom, J. J., Futcher, L., Gibson, D., Hawthorne, E. K., Kaza, S., Levy, Y., Mattord, H., and Parrish, A. 2017. "Cybersecurity Curricula 2017, Version 1.0." ACM, IEEE Computer Society, AIS SIGSEC, and IFIPS WG 11.8. (https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf)

Ekstrom, J. J., Lunt, B. M., Parrish, A., Raj, R. K., and Sobiesk, E. 2017. Information Technology As a Cyber Science. In *Proc. of 18th Annual Conf. on Information Technology Education (SIGITE '17)*. ACM, New York. (https://doi.org/10.1145/3125659.3125697)

Leblanc, R., Sobel, A., Ben-Menachem, M., Lethbridge, T., Diaz-Herrera, J., Hilburn, T., "Software Engineering 2014: Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering," IEEE Computer Society, ACM.

Newhouse, W., Keith, S., Scribner, B., and Witte, G. 2012. "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." US National Institute of Standards and Technology. (https://doi.org/10.6028/NIST.SP.800-181)

NSA/DHS. 2018. "National Centers of Academic Excellence in Cyber Defense (CAE-CD) Designation Program Guidance." (https://www.iad.gov/NIETP/documents/Requirements/CAE_Program_Guidance.pdf)

Parrish, A., Impagliazzo, J., Raj, R. K., John, Santos, H., Asghar, M. R., Jøsang, A., Pereira, T., and Stavrou, E. 2018. "Global perspectives on cybersecurity education for 2030." *ITiCSE 2018 Companion*. Larnaca, Cyprus. (https://doi.org/10.1145/3293881.3295778)

Privacy Rights Clearinghouse. 2018. "Chronology of Data Breaches: Security Breaches 2015—2018." (http://www.privacyrights.org/data-breach)

Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K. M., Nunamaker, Jr., J. F., Sipior, J. C., and de Vreede, G. J. 2010. "IS 2010: Curriculum Guidelines for Undergraduate Degree Programs in Information Systems." (https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf)

Topi, H., Karsten, H., Brown, S. A., Carvalho, J. A., Donnellan, B., Shen, J., Tan, B. C. Y., and Thouin, M. F. 2017. MSIS 2016: Global Competency Model for Graduate Degree Programs

in IS. (https://www.acm.org/binaries/content/assets/education/msis2016.pdf)

Topi, H. 2017. IS EDUCATION: Role of information systems in the CC2020 initiative. ACM Inroads 8, 4 (October 2017), 43-44. (https://doi.org/10.1145/3148549)

Von Konsky, B., C. Miller and A. Jones, "The Skills Framework for the Information Age: Engaging Stakeholders in Curriculum Design," *Journal of Information Systems Education*, vol 27(1), Winter 2016.