2015

The Homogenization Of Standards Based Information Security Education: An Example Of Differentiation

James Smith
Kennesaw State University, jnsmith@bluereefgroup.com

Adriane B. Randolph
Kennesaw State University, arandol3@kennesaw.edu

THE HOMOGENIZATION OF STANDARDS-BASED INFORMATION SECURITY EDUCATION: AN EXAMPLE OF DIFFERENTIATION

James N. Smith, CISSP
Mercer University, Kennesaw State University
smith_jn@mercer.edu

Adriane B. Randolph
Kennesaw State University
arandolph@kennesaw.edu

ABSTRACT

The development of standards-based information security and assurance (ISA) training in the United States may foster a homogenization in ISA training among post-secondary training and education outlets. This leaves open the question of how bachelor's programs at universities should differentiate themselves from other post-secondary training and education programs and create added value for students pursuing bachelor's degrees with ISA content. In pursuit of an answer, we engaged in an early-stage investigation into the trends among ISA course offerings by technical colleges and universities. With little distinction perceived between certain programs, what resulted was the Survey of Strategic Global Cybersecurity course that was developed in 2014 at Mercer University. The goal of this course was to provide a global, macro-level view of causes and effects as they related to cybersecurity issues, thus taking a higher-level view than what was presented in most standards-based ISA courses.

Keywords

Information security and assurance, information security education, pedagogy, information security standards

INTRODUCTION

In 2003 the Bush Administration issued a report outlining the United States' National Strategy to Secure Cyberspace (White House, 2003). Priority three of that strategy detailed plans for a national cyberspace security awareness and training program and specified that "the Nation must focus resources on training a talented and innovative pool of citizens that can specialize in securing the infrastructure" (White House, 2003, p. 41). This mandate has fostered the development of several programs to standardize and certify cybersecurity education at the post-secondary level. It has also incentivized technical schools, colleges and universities to develop programs that meet these standards in order to develop a workforce with strong, standards-based education in information security and assurance (ISA).

With encouragement to "teach to the standards," a programmatic trend may have evolved that fosters a homogenization in ISA training among post-secondary training and education outlets. This leaves open the question of how bachelor's programs at universities should differentiate themselves from other post-secondary training and education programs. Further, how can these bachelor's programs create added value for their students pursuing degrees with ISA content. It seems the answer may lie within the source of the questions: the curriculum, itself.

We present results of an early-stage investigation into the trends that may be driving homogenization among ISA course offerings by technical colleges and universities. We discuss the need to differentiate university-level ISA education from that of technical colleges and commercial certification training programs. We then describe the Survey of Strategic Global Cybersecurity course that was developed in 2014 for use in the Information Science and Technology program at Mercer University. The goal of this course was to provide a global, macro-level view of causes and effects as they related to cybersecurity issues, more so than what was presented in a standards-based ISA course. We present an overview of this course developed and taught by the first author in the fall.

LITERATURE REVIEW

Following the promulgation of the National Strategy to Secure Cyberspace there was rapid movement by the U.S. national security organizations to establish training standards for information assurance professionals. The Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC), an interagency federal government organization tasked with developing security standards for the federal government, issued a set of training standards for information assurance workers listed in Table 1 ("CNSS History," n.d.; Manson et al., 2009; Schembari and Jochen, n.d.). The "I" following CNSS and NSTISS stands for "Instruction".

Standard Title (All Preceded by "National Training Standard for")	**Standard Number**
Information Systems Security (INFOSEC) Professionals	NSTISSI 4011
Senior Systems Managers	CNSSI 4012
System Administrators (SA)	CNSSI 4013
Information Systems Security Officers	CNSSI 4014
System Certifiers	NSTISSI 4015
Risk Analyst	CNSSI 4016

Table 1. Education Certification Standards Issued by the CNSS

Schools and other training institutions were encouraged to conform their training and coursework to these standards. A process was created through the National Security Agency's (NSA) Central Security Service (CSS) to confer certifications on students who successfully completed certified courses. In addition the designation Center of Academic Excellence (CAE) was created for those schools that implemented multiple courses to the CNSS standards and met various other requirements. At this time there are approximately 180 post-secondary programs in the United States with some level of CAE certification ("Centers of Academic Excellence - Institutions - NSA/CSS," n.d., "CNSS History," n.d.; James Davis and Dark, 2003; Manson et al., 2009).

As the development of ISA courses, emphasis areas, minors and majors has grown, there have been numerous academic articles from scholars who are working to develop these programs. Davis and Dark (2003) developed a four-layer curriculum model that combines a prerequisite body of knowledge, an information assurance body of knowledge, higher order skills and professional level skills as a model for developing students. Cruz and Bonilla (2012) also emphasized the need for a common body of knowledge (CBK) for information assurance and security programs. Manson et al. (2009) and Shoemaker (2014) further emphasized the need for standards-based programs.

Several authors shared narratives of their schools' implementations. Sexton (2008) and Hoag (2013) recounted the development process at the undergraduate level. Schembari and Jochen (n.d.) described the development of a graduate degree program in information assurance that was standards-based. Hawthorne (2013) explored programs at the associate's degree / community college level.

There were two works that deviated from the general theme of the literature reviewed. Davis and Dark (2003) advocated for a holistic approach that embeds security into the breadth of the technology curriculum. Green and Zafar (2013) looked at the effectiveness of non-course-based educational experiences, specifically, cyber-defense competitions.

TRENDS IN ISA CURRICULUM

An early investigation of programs highlighted what seemed to be a natural clustering of how various schools, at all levels, have developed their ISA programs. This led to developing three classifications for academic ISA programs outlined as follows. These classifications were then used as a framework for understanding the practices of several technical colleges and universities with an ISA curriculum.

Program Classifications

Emerging Programs

Emerging ISA programs are highlighted by their lack of a formal major, minor or emphasis area in information security. They generally have a single ISA course that may or may not be NSTISSI 4011 compliant. However, they have not achieved NSA CSS CAE status.

Compliant Programs

Compliant ISA programs have, at a minimum, an ISA course that is NSTISSI 4011 compliant. They seem to have often mapped their equivalent network operating systems course to the CNSSI 4013 system administrators' standard. They generally have a minor, emphasis area or certificate program in ISA, though some have a major. These programs are filled out with network administration and other IS/IT courses from the school's general course offering. Many have a computer forensics course. Courses are generally taught by extant IS and IT faculty and they generally do not have dedicated ISA faculty. Many have achieved the base level of NSA CSS CAE status.

Proficient Programs

Proficient ISA programs have at a minimum a major in information security or ISA. Some have a graduate degree. They generally have dedicated ISA faculty and some have a full department. They have numerous certified courses and all have NSA CSS CAE status, often at advanced levels.

Program Comparisons

Using these three classifications, we then examined the practices of nine technical colleges and universities with an ISA curriculum. These schools were selected based on the authors' personal knowledge and access to their faculty and curriculum known to specifically be engaged in such areas. Knowledge of these two institutions was supplemented by schools reporting on their programs in the extant literature (Hawthorne, 2013; Hoag, 2013; Schembari and Jochen, n.d.; Sexton, 2008). We examined degree layout, course descriptions, textbook usage and published accounts of curriculum development against our classifications. The results are shown in Table 2.

Classification	Number of Schools
Emerging	1
Compliant	6
Proficient	2

Table 2. Distribution of ISA Programs Across Classifications, N=9.

Of particular interest was our comparison of three technical schools in our sample, which rated as compliant against the compliant universities. We found very similar course titles and descriptions, program structure and textbook choice. Here we could not find a distinct metric against which we could differentiate the technical colleges and four-year universities as it related to their ISA program structure.

COURSE OBJECTIVES AND DESIGN

Given the similarities found across certain programs, it seemed an easily-accessible differentiator would come through the curriculum itself and not necessarily through the program infrastructure. Thus, the following describes a course developed to transcend the commonly-employed, standards-based curriculum which any level program could implement.

Background

In 2014 the Computer Science department at Mercer University embarked on a redesign of its Information Science and Technology (IST) major. The goal of this redesign was to bring the curriculum into alignment with the Association of Computing Machinery's (ACM) curriculum guidelines for undergraduate degree programs in information technology (Lunt et al., 2008). One of the results of this redesign was the permanent addition of an upper division information security course to the catalog which would be a requirement for the Bachelor of Science in IST major, an elective within the Bachelor of Arts in IST major and would conform to NSTISSI 4011. The next step of this planning is to adapt the Network Operating Systems course to conform to CNSSI 4013. Thus, Mercer University is considered to currently be an emerging program as classified above.

As a result of the early-stage investigation of trends in ISA curriculum, the first author decided to develop and teach an elective course that might serve to augment the ISA component of the new curriculum and serve to meet the Mercer University's mission to develop "leaders who make a positive difference in the world" (*Mercer University Catalog 2014-2015*, 2014, p. 7). He conceptualized a course that would complement the NSTISSI 4011 standardized ISA course and provide students with a global, macro-level view of the emerging cybersecurity environment. Another guiding principle was that the course would be attractive to students from majors outside of the technology disciplines. The course was titled "Survey of Strategic Global Cybersecurity" and the following overview statement and course structure was developed.

Conceptual Overview

From governments and multinational corporations to revolutionaries and not-for profit causes, information technology has evolved from an obscure support role within organizations into a core capability for communications, operations and effecting change. With that evolution cybersecurity has become critical to ensuring organizational success and emerged as an active tool for gaining strategic competitive advantage.

This course looked at the political, military, commercial and criminal uses of technology from global framework. As a class, we explored what capabilities were available to global actors and the strategic choices involved in their use.

While this course was about technology, it was not a technical course. This course was driven by cases and current events. Students were expected to work individually and within groups to prepare deliverables involving both live and written briefings on cases and current issues throughout the semester.

This course hoped to attract a diverse group of students from various programs including Business, International Affairs, Journalism, Law and Public Policy, Political Science and Military Science.

Organizing Framework

The organizing structure of the course was based on three classes of actors in cyber-based conflict. These classes were defined as nation states, criminal actors and non-state actors.

Nation States

This section of the course explored the development of offensive and defensive cyber capabilities among nation states. It focused on the United States Military's Cyber Command and the People Republic of China's Unit 61398 of the People's Liberation Army. We looked at their structure, development and capabilities. We examined prominent events such as the cyber conflict between Russia and Georgia in 2008 and the Stuxnet attack on Iran in 2009-2010.

Criminal Actors

In this section of the course we looked at criminal use of the internet for illicit gain. We excluded terrorism and insurrection from this section and focused on actors that primarily dealt in contraband and crimes for profit. We examined case studies such as the Carder's Market hacking incident from 2007 and the Silk Road darknet. We explored methods by which anonymous transfers of value, such as bitcoin and transfers of digital contraband by means of anonymizers and darknets, took place.

Non-State Actors

In this section of the course we looked at various non state actors such as political movements, terrorist, activists and non-governmental organizations leverage the cyber environment. We examined Al Qaeda's use of the internet for command control and communications (C3) and for propaganda purposes. We examined the Arab Spring and Green Revolution's use of technology to organize and operate. We examined WikiLeaks and Anonymous to understand their tactics for using cyber resources to advance their agendas. Particular attention was paid to events that were asymmetrical in nature and where technology acted as a force multiplier.

Textbook Selection

The first author examined many leading security textbooks, such as Whitman and Mattord (2014) and Smith (2011) and found them to overlap with our standards-based ISA course offering to a great degree. He settled on three mass market books to act as texts. He began with Barnett (2005) to introduce the students to thinking in a global strategic framework. He then added Clarke and Knake (2012) and Singer and Friedman (2014) because of their global viewpoint and lack of focus on technical subjects.

Pedagogical Structure

The course was primarily a lecture course. The first author systematically explored the organizing framework of the course with the help of the texts and numerous articles. A strong emphasis was placed on current events. The first author was fortunate in the fall of 2014 to have ample current events in the news cycle. A heavy discussion and debate component helped the students to develop their critical thinking as to actors' motives and strategic positions. Assessment was in the form of essays on each of the major organizing constructs.

Desired Outcomes

The desired outcome for students in this course was to engage students in a critical examination of the motives of the various capabilities that are being leveraged in cyberspace. The goal was to provide a durable framework that would provide students a basis for examining future threats and to enable students to think critically about the cybersecurity environment.

DISCUSSION, LIMITATIONS AND FUTURE WORK

While we acknowledge the need for baselines and standards-based ISA education to develop a qualified workforce, we feel that it is in the long range interest of universities to develop an ISA curriculum that is distinct from other technical training

programs. This differentiation places a value on developing critical thought and a leadership worldview in addition to technical skill. It is necessary to develop the next generation of leaders as we develop the next generation of workers. In addition, it will be necessary for university ISA programs to demonstrate a distinct value proposition in order to maintain their value proposition over other training channels.

The primary limitation of this study is the very small sample size of the early-stage investigation. Future work is needed to substantiate the phenomenon of homogenization within ISA programs. To this end, we hope to develop a broad-based survey of ISA programs within the United States. In addition, we see a need in the market place for a broader selection of teaching texts. We envision a periodic casebook of global events to aid in a broader treatment of cybersecurity in the classroom.

REFERENCES

1. Barnett, T. P. M. (2005) *The Pentagon's New Map*, , (Reprint edition.) New York: Berkley Trade.

2. Centers of Academic Excellence - Institutions - NSA/CSS. (n.d.).

3. Clarke, R. A., and Knake, R. (2012) *Cyber War: The Next Threat to National Security and What to Do About It*, (Reprint edition.) New York: Ecco.

4. CNSS History,. ((n.d.).) https://www.cnss.gov/CNSS/about/history.cfm.

5. Cruz, A., and Bonilla, S. (2012) Creating a Common Body of Knowledge (CBK) for Information Assurance and Security Academic Programs and Certificates ICETI 2012, Presented at the ICETI 2012.

6. Davis, J., and Dark, M. (2003) Defining a curriculum framework in information assurance and security, in *Proceedings of the 2003 ASEE Annual Conference*,.

7. Davis, J., and Dark, M. (2003) Teaching students to design secure systems, *Security & Privacy, IEEE*, 1,2, 56–58.

8. Green, A., and Zafar, H. (2013) Addressing Emerging Information Security Personnel Needs. A Look at Competitions in Academia: Do Cyber Defense Competitions Work?, in *AMCIS 2013 Proceedings*, , Presented at the Americas Conference on Information Systems, Chicago, IL.

9. Hawthorne, E. K. (2013) Multifarious initiatives in cybersecurity education, *ACM Inroads*, 4,3, 46–47.

10. Hoag, J. (2013) Evolution of a Cybersecurity curriculum, in *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*, 94.

11. Lunt, B. M., Ekstrom, J. J., Gorka, S., Hislop, G., Kamali, R., Lawson, E., LeBlanc, R., Miller, J., and Reichgelt, H. (2008) Curriculum guidelines for undergraduate degree programs in information technology, *Retrieved March*, 2, 2009.

12. Manson, D. P., Curl, S. S., and Torner, J. (2009) A Framework for Improving Information Assurance Education, *Communications of the IIMA*, 9,1, 6.

13. *Mercer University Catalog 2014-2015*. (2014) Macon, GA.

14. Schembari, N. P., and Jochen, M. ((n.d.).) "Using Information Assurance Curriculum Standards as a Basis for a Graduate Degree,".

15. Sexton, J. (2008) Establishing an undergraduate information assurance (information security) program at a small liberal arts college, *Journal of Computing Sciences in Colleges*, 24,2, 234–240.

16. Shoemaker, D. P. (2014) The colloquium for information system security education (CISSE)–the adventure continues, *ACM Inroads*, 5,2, 50–54.

17. Singer, P. W., and Friedman, A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*, , Oxford ; New York: Oxford University Press.

18. Smith, R. E. (2011) *Elementary Information Security*, , (1e edition.) Burlington, MA: Jones & Bartlett Learning.

19. White House. (2003) The National Strategy to Secure Cyberspace, *Washington, DC: White House*.

20. Whitman, M. E., and Mattord, H. J. (2014) *Principles of Information Security*, (5 edition.) Clifton Park, NJ: Cengage Learning.