

A DRAFT MODEL CURRICULUM FOR PROGRAMS OF STUDY IN INFORMATION SECURITY AND ASSURANCE

Michael E. Whitman, Ph.D., CISSP

Kennesaw State University
mwhitman@kennesaw.edu

Herbert J. Mattord, CISSP

Kennesaw State University
hmattord@kennesaw.edu

Abstract

With the dramatic increase in threats to information security, there is a clear need for a corresponding increase in the number of information security professional. With a lack of formal curriculum models, many academic institutions are unprepared to implement the courses and laboratories needed to prepare this special class of information technologist. This paper provides an overview of lessons learned in the implementation of both individual courses and a degree concentration in information security. It refers to a more comprehensive document, available on the Web, which includes the methodology used in developing the curriculum, individual course syllabi for recommended components, and laboratory development and implementation recommendations..

Keywords: Information Security, Information Security Education, Curriculum Models

Introduction

A major challenge facing modern society is the security and protection of information assets. Advances in information security (InfoSec) have been unable to keep pace with advances in computing in general (Pfleeger & Cooper, 1997) and with the threats that IT systems face. Press accounts of dramatic computer theft, fraud and abuse are often reported as leading to extensive economic loss. Recent attacks on the American IT Infrastructure have highlighted the need for information security (MSNBC, 2001). The 2003 CSI/FBI Computer Security survey found 92% of respondents detected computer security breaches within the last year and 75% reported financial losses due to these computer breaches (CSI/FBI, 2003). According to Dr. Joseph Bordogna, Deputy Director, National Science Foundation in remarks at a June 2002 NSF Workshop “The events of September 11 only accelerated longstanding concerns about the threat of cyberterrorism and the vulnerability of the nation’s information systems and communications networks [...] Questions about the adequacy of the U.S. science, engineering, and technology workforce are also rising to a chorus. Reported shortages of skilled workers in the IT sector are only one example. The need we all recognize, for a cadre of professions in computer security and information assurance, is right at the top of the list” (Bordogna, 2002).

Education of IT students in information security prepares them to recognize and counter information system threats and vulnerabilities (Chin, et al, 1997). The article “Integrating Security into the Curriculum” argues “an educational system that cultivates an appropriate knowledge of computer security will increase the likelihood that the next generation of IT workers will have the background needed to design and develop systems that are engineered to be reliable and secure” (Irvine et al., 1998). The need is so great that the President of the US issued Presidential Decision Directive 63, the Policy on Critical Infrastructure Protection in May 1998, which prompted the National Security Agency to established outreach programs like the Centers of Academic Excellence in Information Assurance Education (CAEIAE). This program’s goal is “to reduce vulnerabilities in our National Information Infrastructure by promoting higher education in information assurance, and producing a growing number of professionals with IA expertise” (NIETP, 2003). According to the US Government document *The National Strategy to Secure Cyberspace*, “Education and outreach play an important role in making users and operators of cyberspace sensitive to security needs. These activities are an important part of the solution for almost all of the issues discussed in the National Strategy to Secure Cyberspace” (White House, 2003).

There are two dominant technology curriculum models currently in use. The first is the ABET-CAC accreditation standard, which allows for security courses in both IS and CS undergraduate programs as electives. The second dominant curriculum guideline is the *IS 2002 Model Curriculum Guidelines for Undergraduate Degree Programs in Information Systems*, co-sponsored by the three largest professional technology organizations: The Association for Computing Machinery (ACM), The Association for Information Systems (AIS) and The Association for Information Technology Professional (AITP). The *IS 2002* guiding principles are revised here for adoption in this curriculum model: 1) The model curriculum should represent a consensus from the InfoSec community. 2) The model curriculum should be designed to help [InfoSec] faculty produce competent and confident entry level graduates well suited to work-place responsibilities. 3) The model curriculum should guide but not prescribe. Using the model curriculum guidelines, faculty can design their own courses. 4) The model curriculum should be based on sound educational methodologies and make appropriate recommendations for consideration by InfoSec faculty. 5) The model curriculum should be flexible and adaptable to most IS/CS programs (ACM et al, 2002). Even established curriculum bodies, like the Association for Computing Machinery (ACM) and the Accreditation Board for Engineering and Technology – Computing Accreditation Council (ABET-CAC), do not have formal models established for curriculum in Information Security at the four-year level. The only recommendation that does exist resulted from a workshop sponsored by the NSF and the American Association of Community Colleges, *Protecting Information: the Role of Community Colleges in Cybersecurity Education* (NSF & AACC, 2002). That report serves as both a starting point for two-year institutions and as a baseline reference for this project. While supportive of the typical mission of a two-year institution, this approach is inadequate for the mission of a four-year institution. The proposed model is designed to allow undergraduate Information Systems (IS) and Computer Science (CS) majors to move toward career fields that include and evolve through technical knowledge areas and into the management of information security.

Developing the Curriculum Model

The development of a sound InfoSec curriculum model would provide direct benefit to academic, business, and governmental agencies that depend on the production of properly trained InfoSec graduates. As the analysis phase of this project evolved, the authors examined existing literature, reviewed other programs of interest and their implementations. They also examined current and emerging national and international standards and guidelines for the training of InfoSec professionals, instructional methods and materials from programs recognized as NSA centers of excellence across the country, and general recommendations and constraints from curriculum supporting organizations such as ACM and ABET. This curriculum model and its pilot project used the “Backward Curriculum Design Process” (Hutton, 2003) a well-known approach to curriculum design that begins with the desired outcomes and goals and works backward to learning objectives grouped into courses. The curriculum model seeks to answer the following question:

What should an information security graduate be qualified to do, and what roles should they expect to be able to fill?

Information Security Position and Roles

Typical position descriptions used by InfoSec organizations were found to be too widely varied to be consistently descriptive of the roles individuals play in the field of information security. So, the next step was to identify *roles* information security professionals typically assume. A typical organization has a number of individuals with various InfoSec responsibilities. While the titles used within any specific organization may be different from one organization to the next, most of the job functions share features typified by the following categories: Chief information security officer (CISO), Security managers, security administrators and analysts, security technicians and general security staff. In the curriculum model presented here these roles were used as surrogates for positions and mapped to knowledge areas.

A Knowledge Area (KA) represents the specific factual knowledge needed for each role. When paired with a multi-level mastery model like Bloom’s taxonomy (Bloom et al, 1964), can be used to identify the level of depth of knowledge for each role. For example, a CISO may need great breadth of knowledge, but not as much depth of knowledge in a specific KA as a technician would. The challenge is to verify the roles, document the knowledge areas, and completely map them to each other along with the levels of mastery needed for each. The resulting map must then be verified across the various interest groups. Knowledge areas can be obtained from key indices like certifications and from training standards and models. Knowledge areas in InfoSec are many and can be very technical; however, there is an agreed upon way to discuss them.

Many programs take the short cut and jump straight to the certifications an information security professional may earn such as: Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP), Global Information Assurance Certification Certified Security Expert (GSE), Security Certified Network Professional or Architect (SCNP/SCNA), Security+, or Certified Information Security Auditor or Manager (CISA/CISM), among others. However,

many programs are hesitant to implement coursework that is focused on a specific applied certification. Universities in general prefer to focus more on the underlying knowledge areas that these certificates draw from, rather than the specifics of the certification exams. However by examining the content of some of the key certifications some of the knowledge areas needed for integrate with the proposed coursework are readily identifiable.

Established Standards, Models and Practices

Another set area of information that can be used to derive the skills needed to become a security professional lies in established standards, models and practices. Among the most accessible places to find a quality security management model are U.S. federal agencies and international organizations. One of the most popular security management models has been ratified into an international standard. The original British Standard 7799 has emerged as two components, each addressing a different area of security management practice. BS 7799:1, now known as ISO/IEC 17799, is called “Information Technology – Code of Practice for Information Security Management.” BS 7799:2 is called “Information security management: Specification with guidance for use.” There are a number of alternatives to BS 7799/ISO17799. The first and foremost of these are free documents provided by the National Institute of Standards and Technology’s Computer Security Resources Center (<http://csrc.nist.gov>). This site contains a number of publications, including ones containing models and practices

Mapping Positions and Roles to Knowledge Areas (KAs)

With this information the curriculum designers can gain a better feel for what a graduate should know upon seeking a specific job category. Figure 1 illustrates this process of mapping. (Note: This figure is exemplary, not definitive. Each curriculum program would be best served to develop its own detailed Title-Role-KA map.) Based on feedback from each institution’s curriculum advisory board, and built on the foundation of existing IT, IS or CS coursework, each program should be focused on preparing future InfoSec graduates so that immediately upon graduation they would be prepared for career progression through positions from entry-level to security manager to CISO. As a result, selected learning objectives should be tied to providing the appropriate level of mastery within each knowledge area felt to be critical to an individual’s success in that program. The pilot project where this mapping has been completed was performed at Kennesaw State University (KSU) using two sets of information: the CISSP Common Body of Knowledge (CBK), and the NSTISSC training standards (www.nstissc.gov).

Mapping the CISSP Common Body of Knowledge (CBK)

In mapping the CISSP CBK, the KSU pilot project curriculum model begins with the CISSP general categories used as KAs (as indicated in the rightmost column shown in Figure 1). Each KA is then linked to the applicable roles and the varying levels of mastery are identified for each relationship. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) now known as the Committee for National Security Systems (CNSS) documents on training information security professionals were also examined to insure that all critical areas of knowledge were included. While the pilot project is focused on education and was not focused on training needs per se, it was felt that the CNSS documents were useful in two ways: 1) to provide verification of the completeness of the CISSP CBK information not found elsewhere and 2) to lay the foundation for eventual certification of the KSU curriculum in the NSA’s Information Assurance Courseware Evaluation program.

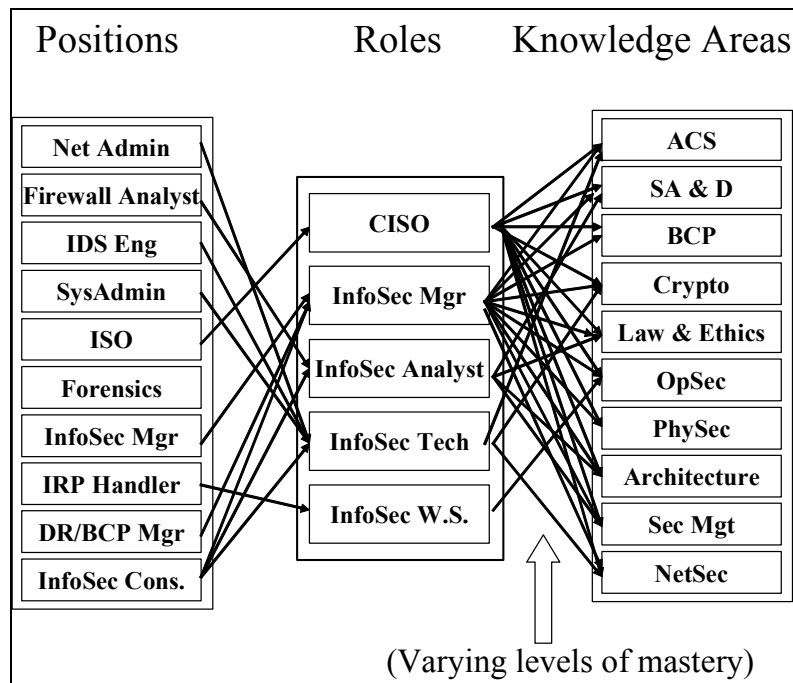


Figure 1: Mapping Roles to Knowledge Areas

Defining the Focus of the Program

As each curriculum development effort progresses, it is necessary to align the deliverables with the overall program objectives and the primary focus of the program. This implies that the project’s investigators have defined the focus of the program and articulated the program objectives. Based on an broad evaluation of existing programs in InfoSec, it has been observed that most programs tend to cluster into one of three general types, Managerial, Technical and Balanced.

Managerial InfoSec Programs

The managerial program seeks to emphasize five principles of InfoSec management: People, Planning, Policy, Programs and Projects. Students emerging from these programs should have an understanding of the types and purposes of technical security controls, but may not be able to configure, implement or maintain them.

Technical InfoSec Programs

At the other end of the security spectrum, the technical program focuses more on InfoSec technologies. Students in these programs should graduate with skills that enable them to design, install, configure, test, and maintain various technical security controls and equipment. They should understand the role and purpose of the managerial aspects, as the technical implementations are guided by the managers in InfoSec, but may not have mastery of the managerial knowledge areas.

Balanced InfoSec Program

The balanced InfoSec program is a combination of the two and seeks to balance between them. Programs in this category generally will not provide depth in either aspect of InfoSec, but will provide an approach that prepares the graduate for entry-level as a practitioner or for further education.

Levels of Mastery

Using the detailed list of domains and knowledge areas from the CISSP as verified using other sources, the authors identified the level of mastery desired for each knowledge area. The taxonomy used was derived using a greatly simplified version of Bloom’s taxonomy. Four levels of desired mastery were chosen and defined: Understanding, Accomplishment, Proficiency,

and Mastery, as described here.

Understanding

At the understanding level, the student can identify key concepts when presented with a list of alternatives. The student has familiarized themselves with the selected knowledge area and can discuss key concepts.

Accomplishment

At the accomplishment level, the student can demonstrate the process necessary to use the knowledge area in a given scenario. The student has a deeper grasp on both theoretical and practical applications of the knowledge area.

Proficiency

At the proficiency level, the student can generate new examples of the application of the knowledge area. The student has demonstrated the ability to critically discuss knowledge area concepts and can easily relate their learning to others.

Mastery

At the mastery level, the student can not only freely create new knowledge within the area, but can also evaluate and critique new knowledge created by others. This level is typically obtained through graduate level coursework, or extensive and highly specialized depth of curriculum.

Coalescing Courses

The final activity is to generate the set of courses needed and identify the prerequisite relationships. This is done so that graduates of the program will emerge with the desired level of mastery in each KA. In the pilot project, this step was accomplished by organizing related content with similar levels of mastery into courses. While this seems to be a subjective process, in fact there is a certain degree of affinity within the KAs and levels of mastery that results in a natural coalescing of courses. Once formed into courses, the final step is to articulate prerequisites among the courses and between the InfoSec courses and the legacy courses of the host curriculum.

For the purposes of the current draft curriculum model, and the implementation of the pilot project, it was determined that three courses would provide the depth needed. The final detail is the organization of specific learning objectives for each of the target courses and for the discovery of learning materials to support each course. Since the initial development of the three-course model, learning objectives in each specific course have continued to evolve as feedback from courses delivered allows the movement of detailed learning objectives between courses to meet the needs of practicality and student capabilities.

Lessons Learned

At this point in the pilot project, the developers are prepared to make the following recommendations for those interested in undertaking a similar curriculum development project: Courses and programs should be created in ways that:

- Involve all critical stakeholders. Just as in systems development, the use of representative groups from all constituencies (faculty, students, and industry advisors) will serve to improve the final product.
- Create employable students or students who can also advance academically. Create a graduate that will be in demand. Unless students can expect employability upon completion, they will not be attracted to it and may lose interest in the program after an initial surge of interest due to the novelty of the program.
- Capitalize on available resources (faculty, classrooms, labs). Existing labs can be easily modified to support the information security laboratory's unique requirements and exercises. There are also a significant number of low-cost or free software products that provide realistic and valuable experiences to students. Cultivating industry contacts can also result in valuable donations of software and/or hardware.
- Support local / state / national program objectives like the National Strategy to Secure Cyberspace. Contributing to these types of programs not only provides visible and demonstrable credibility to the program, but serves as a basis for increasing the validity of your program should you decide to submit for grants and industry support.

The Current State of the Draft Curriculum Model

Outcomes from the pilot program have been incorporated into the proposed curriculum model. These outcomes included the adjustment of specific learning objectives across all core courses, adjusted use of laboratory exercises within each course, and the movement of some core material to more advanced classes (like computer forensics). Additional outcomes strengthened existing course relationships, and validated instructional approaches.

The complete Draft Curriculum Model totals over 100 pages, and is available from <http://infosec.kennesaw.edu>.

References

- ACM, AIS & AITP. IS 2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems. Retrieved 5/8/2003 from <http://www.aisnet.org/Curriculum/IS2002-12-31.pdf>.
- Bengamin S. Bloom, Bertram B. Mesia, & David R. Krathwohl (1964). *Taxonomy of Educational Objectives* (two vols: The Affective Domain & The Cognitive Domain). New York. David McKay.
- Bordogna, J. (2002). Remarks and Introduction of the Honorable Howard A. Schmidt AACC/NSF Workshop on the Role of Community Colleges in Cybersecurity Education. Retrieved 4/22/2003 from <http://www.nsf.gov/od/lpa/forum/bordogna/jb020626aacnsfcyber.htm>
- Chin, S-K, Irvine, C.E., & Frinke, D. (1997). An Information Security Education Initiative for Engineering and Computer Science. Naval Postgraduate School Technical Report, NPSCS-97-003. Naval Postgraduate School, Monterey, CA.
- CSI/FBI. (2003). 2003 Computer Crime and Security Survey. Retrieved 5/10/2003 from <http://www.gocsi.com>.
- Hutton, G. (2003). Backward Curriculum Design Process. Retrieved 5/1/2003 from http://www.g4v.com/~glen.hutton/ED3601/BackwardDesignFeb11_03.pdf.
- Irvine, C., Chin S-K., & Frincke, D. (1998). Integrating Security into the Curriculum. *Computer*. 31(12). 25-30.
- MSNBC. (2001). Chinese hackers call truce in China-U.S. cyberwar. Retrieved 5/12/2001 from <http://www.msnbc.com/news/571091.asp>.
- National InfoSec Education and Training Program (NIETP). (2003) Centers Of Academic Excellence in Information Assurance Education. Retrieved 04/6/2003 from <http://www.nsa.gov/isso/programs/coeiae/index.htm> .
- National Science Foundation & American Association of Community Colleges (NSF & AACC). (2002). *Protecting Information: the Role of Community Colleges in Cybersecurity Education*. Community College Press, Washington D.C.
- Pfleeger, C. & Cooper, D. (1997). Security and Privacy: Promising Advances. *IEEE Software*. 27-32.
- White House, (2003). National Strategy to Secure Cyberspace. Retrieved 2/10/2003 from <http://www.whitehouse.gov/pcipb>.