Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

A Draft Model Curriculum for Programs of Study in Information Security and Assurance

Michael E. Whitman, Ph.D., CISSP & Herbert J. Mattord, CISSP

Abstract – As Information Security and Assurance programs are designed and implemented throughout the country, many academicians begin to struggle with the development of this new and exciting curriculum. Information Security represents an area distinct from traditional Information Systems, Computer Science or Information Technology fields, yet shares some of the same challenges in managing a technology-based field. Those not familiar with the specifics of the Information Security professional will find it difficult to develop curriculum without outside support. The purpose of this draft model curriculum is to provide best practices and lessons learned from a study of numerous programs throughout the country. It is an ongoing project that welcomes outside input.

Index terms – Information Security Education
Information Security Curriculum
Curriculum Models
Curriculum Development

I. INTRODUCTION

One of the continuing challenges facing society is the security and protection of information assets. According to Dr. Joseph Bordogna, Deputy Director, National Science Foundation, "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 […] The need we all recognize, for a cadre of professions in computer security and information assurance, is right at the top of the list" [1].

Education in information security prepares IT students to recognize and combat information system threats and vulnerabilities [2]. 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" [3].

The dominant technology curriculum guidelines and established curriculum bodies currently in use do not provide specific guidance for information security coursework. The ABET-CAC accreditation standards, and the IS 2002 Model Curriculum Guidelines for Undergraduate Degree Programs in Information Systems, co-sponsored by the three largest professional technology organizations: Association for Computing Machinery (ACM), Association for Information Systems (AIS) and Association for Information Technology Professional (AITP), both provide a model curriculum for undergraduate degree programs in Information Systems. Educational institutions and their faculties are searching for guidance and advice on designing and implementing information security curriculum to meet anticipated demand for information security courses. The Model Curriculum for Programs of Study in Information Security and Assurance is based on studies of other programs and experiences gained in implementing a number of information security courses. It builds upon the IS 2002 model by creating information security curriculum following the IS 2002 template: "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" [4].

Until recently, most university-level courses have been designed for graduate-level coursework in computer science and engineering programs. Most other curriculum development has been in practitioner training programs oriented towards certificate programs. The only documented curriculum recommendation that does exist resulted from a workshop sponsored by the NSF and the American Association of Community Colleges, resulting in the draft recommendation *Protecting Information: the Role of Community Colleges in Cybersecurity Education* [5]. While supportive of the two-year institution's mission, this level of approach is inadequate for the mission of the four-year institution.

The proposed model is designed to allow undergraduate Information Systems (IS) and Computer Science (CS)

ISBN 0-87145-192-1/04/$15.00

majors to move toward career fields that include and evolve through technical knowledge areas and into the management of information security, an area not addressed at the two-year level.

II. Goals and Objectives

This model is designed to increase the quality of baccalaureate-level information security education by documenting curriculum in information security that provides students with technical and managerial skills needed for information security positions in the IT workforce. The curriculum can be adopted by institutions with undergraduate information technology degree programs as individual courses, minors or concentrations in information security. It is intended to provide adopters with the means to deliver quality coursework with breadth and depth of the information security common body of knowledge. The curriculum adapts existing U.S. government standards for security training programs. However there are no existing baccalaureate education models with the closest match being *The Role of Community Colleges* described earlier. There is a clear lack of recommendations for managerial and administrative education that this curriculum has identified and will continue to develop.

III. Designing and Implementing Information Security Curricula

There are five approaches that academics may use to implement information security curricula:

1. Elements added to existing courses.
2. Elements added to a capstone course or courses.
3. Independent information security courses.
4. Information security certificates / minors.
5. Information security degree programs.

Which of these approaches should be considered? Available resources, time, faculty, money, technology and student demand must be the determining factors. It may be useful to begin with the first two approaches to gain experience and gauge demand and then expand using the additional approaches as resources are made available.

The development of a curriculum model provides direct benefit to the various academic, business, and governmental agencies that support formal education efforts. During the preparation of the draft curriculum the authors examined existing literature, reviewed other programs of interest and how they were implemented. They also examined current and emerging national and international standards and guidelines for the training of information security professionals [5,6,7], instructional methods and materials from programs recognized as NSA centers of excellence across the country [8,9], and general recommendations and constraints from curriculum supporting organizations such as ACM and ABET.

In developing the draft curriculum the "Backward Curriculum Design Process" [10] was used. This is a well-known approach to curriculum design that begins with the desired learning outcomes and works backward to develop learning objectives which are grouped into courses. The curriculum model seeks to answer the following question:

> What should an information security graduate learn from a comprehensive program, what work will they be qualified to do, and what positions should they expect to be able to hold?

A. Information Security Position and Roles

Employment position descriptions are not usually sufficient to describe the roles the individuals play when employed in the information security industry. It is necessary to identify the roles information security professionals assume and then map these roles to the information security positions often used in industry. A study of information security positions by Schwartz, Erwin, Weafer, and Briney found that positions can be classified into one of three types: those that define, those that build and those that administer.

"Definers provide the policies, guidelines and standards […] They're the people who do the consulting and the risk assessment, who develop the product and technical architectures. These are senior people with a lot of broad knowledge, but often not a lot of depth. Then you have the builders. They're the real techies, who create and install security solutions. [...] Finally, you have the people who operate and administrate the security tools, the security monitoring function, and the people who continuously improve the processes" [11].

A typical organization has a number of individuals with information security responsibilities. While the titles used within any specific organization may be different from one organization to the next, most of the job functions fit one of the following categories: Chief Information Security Officer (CISO), Security Managers, Security Administrators and Analysts, and Security Technicians, and Security Staffers.

Why is it important to understand these roles? In this draft curriculum model these roles were used as surrogates for specific named positions and mapped to knowledge areas. Knowledge areas represent the specific knowledge needed for each role, and when paired with a multi-level mastery model like Bloom's taxonomy [12], can be used to identify the level of depth of knowledge for each role.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

The challenge is to completely map and verify the roles, knowledge areas, and levels of mastery needed. Knowledge areas can be obtained from key indices like certifications [13], and from training standards and models [14]. Knowledge areas in information security are many and can be very technical but, there is an agreed upon way to discuss them. Some programs may take a short cut and jump straight to the dominant certifications that information security professional earn such as the Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP) from ISC2, the SANs Institute's Global Information Assurance Certification (GIAC), the Security Certified Professional (SCP) and the Certified Information Security Auditor (CISA) and Certified Information Security Manager (CISM) from ISACA to name a few. However, other programs are hesitant to implement coursework that is focused around delivering a specific certification. Universities in general prefer to focus more on the content of knowledge areas that these certificates test, rather than the specifics of these exams. However, if the content of some of the key certifications are examine, the underlying topics within the knowledge areas needed to integrate with the desired coursework will be revealed.

B. Established Standards, Models and Practices

Another source of information used to discern the skills needed to become a security professional lies in established government and industry 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. BS 7799:1, now known as ISO/IEC 17799, is "Information Technology – Code of Practice for Information Security Management." BS 7799:2 is "Information security management: Specification with guidance for use." These documents are discussed in detail in the following sections. They are proprietary, and organizations wishing to adopt them must purchase the right to use them. There are a number of alternatives. The first and foremost of these are the widely referenced free documents provided by the National Institute of Standards and Technology's Computer Security Resources Center (http://csrc.nist.gov).

C. Mapping Positions and Roles to Knowledge Areas

The sources noted above provide curriculum designers with a background of what a graduate should know when seeking a position in industry. The next step used in the process of developing the draft model is to map the roles the individuals are expected to perform to the knowledge areas previously documented, taking into consideration the levels of mastery each role is expected to possess, as illustrated in Figure 1 below.

The draft model presented here is based on inputs from the Kennesaw State University CSIS Department curriculum advisory board. It was their guidance that information security coursework should be focused on preparing security administrators so that immediately upon graduation they would be prepared for career progression through positions leading to Security Manager and then to CISO. As a result, learning objectives were tied specific levels of mastery within the knowledge areas felt to be critical to an individual's future success. Two sets of information informed this mapping process: the CISSP Common Body of Knowledge (CBK), and the NSTISSC training standards (www.nstissc.gov). From each, introductory and advanced knowledge areas essential to career progression were documented based on guidance from the advisory board.

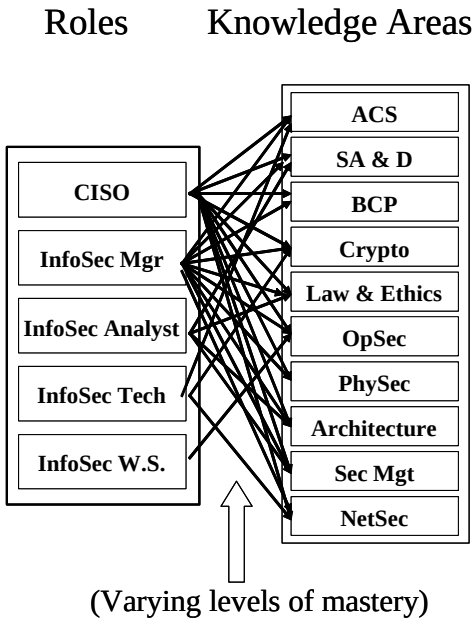

Figure 1 Knowledge Area Map

D. Mapping the CISSP Common Body of Knowledge

The mapping of the CISSP CBK began with use of the general categories indicated as knowledge areas in Figure 1. Since the 10 domains of the CBK are too broad to be useful as learning objectives, subordinate topic areas were collated from each domain. The authors then assured the list was exhaustive by reviewing the National Security Telecommunications and Information Systems Security Committee (NSTISSC) now known as the Committee for National Security Systems (CNSS) documents on training

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

information security professionals (http://www.nstissc.gov/html/library.html) for additional specific topics not previously included. While the draft model is not focused on training per se, this source was useful in two ways: 1) to provide information not found elsewhere and 2) to lay the foundation for eventual certification in the NSA's Information Assurance Courseware Evaluation program.

E. Defining the Focus of the Program

A single approach to curriculum will not work for all institutions. To be successful within the local environment, it is essential to define the general thrust of the intended program and develop overall program objectives. What is the student to learn from the program? This is articulated in the process of defining the focus of the program. In general, there are three general types of information security programs:

1) A managerial program seeks to emphasize the 5 "Ps" of Information Security: People, Planning, Policy, Programs and Projects. These programs will focus more on the administration and management of information security, than the technological aspects. The student in a managerial program should have an understanding of the types and purposes of various technical security controls, but may not be able to configure, implement or maintain them. Managerial information security programs are frequently found in Colleges of Business, Information Systems programs or related areas.

2) At the other end of the information security spectrum, the technical program focuses more on the control technologies of information security. Students in these programs are expected 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 management. Technical InfoSec programs are frequently found in Colleges of Science, Computer Science programs, technical colleges and schools, or related areas.

3) The balanced InfoSec program is a combination of the managerial and technical programs that seeks a balance between the two. Programs in this category generally will not have the level of depth in either management or technology, but will seek to provide an approach that prepares the student for further education or employment.

F. Levels of Mastery

Using the detailed list of domains and knowledge areas mapped above, the desired level of mastery for each knowledge area has been identified. The taxonomy used was derived in part from Bloom's taxonomy, but simplified to a great extent, resulting in four levels of mastery, defined as follows:

1. Understanding: the student can identify key concepts when presented with a list of alternatives.
2. Accomplishment: the student can demonstrate the process necessary to use the knowledge area in a given scenario.
3. Proficiency: the student can generate new examples of the application of the knowledge area.
4. Mastery: the student can not only freely create new knowledge of the area, but can also evaluate and critique new knowledge created by others.

G. Determining Numbers of Courses Needed

Determining how many courses are needed depends on the targeted level of mastery within the clustered of knowledge areas developed above. Depending on the breadth of topic coverage and the degree of mastery required, courses will have to be split or combined to achieve the proper balance of topics within courses that allow sufficient instruction to achieve the level of mastery.

H. Mapping Mastery Depth to Courses

Three courses were chosen for the pilot program. While there may be substantial overlap both within and between courses with regard to the level of mastery, in some cases, duplication of certain levels would be necessary. Duplication between courses also serves to reinforce the desired level of mastery. It was then a simple matter to re-organize learning objectives in each of the pilot courses and begin searching for learning materials that would support each course. Since the initial deployment of the pilot model, learning objectives have evolved to a more complete understanding of what the student should be learning in each course. The end state of these learning objectives for each course in the pilot are presented with the course descriptions in the next section.

As a final note to this process of developing a model curriculum, the following is recommended. Courses and programs should be created in ways that:

- Involve all critical stakeholders.
- Create employable students or students who can advance academically.
- Capitalize on available resources (faculty, classrooms, labs).
- Are flexible in early implementations to permit fine tuning adjustments as courses are deployed.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

- Support local / state / national program objectives like the National Strategy to Secure Cyberspace.

IV. The Draft Curriculum Model

Outcomes from a limited pilot deployment 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 (such as the movement of all forensics material from the technical course to the computer forensics course and the movement of most non-technical forensics content from the introductory and management courses to the computer forensics course). Additional outcomes strengthened existing course relationships, adjusted prerequisite course requirements and validated instructional approaches.

A. Implementation of the Draft Curriculum Model

Preliminary findings suggest that if an institution has the ability to implement only two courses, the best result comes from implementing an introductory course, and then either a technical or managerial course depending on the nature of the program and the preferences of the stakeholders. If the institution can implement more courses, an analysis of the intent of the program as described in previous sections will provide additional course recommendations. Some suggestions based on institutional intent include:

Scenario 1: A one course program
For a general or technical program:
- Introduction to InfoSec

For a managerial or business program:
- Management of InfoSec (emphasis on foundation).

Scenario 2: A two course program
For a general or technical program:
- Introduction to InfoSec
- Technical InfoSec

For a managerial or business program:
- Introduction to InfoSec
- Management of InfoSec

Scenario 3: A three course program:
For all programs:
- Introduction to InfoSec
- Management of InfoSec
- Technical InfoSec

Scenario 4: A four course program:
For a general or technical program:
- Introduction to InfoSec
- Management of InfoSec
- Technical InfoSec
- Advanced Technical topic such as:
  - Firewalls, IDS & VPNs
  - OS Security (Unix/Windows)
  - Computer Forensics

For a managerial or business program:
- Introduction to InfoSec
- Management of InfoSec
- Technical InfoSec
- Advanced Managerial topic such as:
  - Contingency Planning
  - Computer Law & Ethics
  - Security Policy

As additional courses are possible, additional technical or managerial topics can be added. Institutions can then begin drafting specific programs to include electives, existing courses etc. to support their desired outcomes.

B. The Next Step: Design Revision and External Evaluation

It is the intent of the authors to obtain outside input on this model, and additional insight as to the quality of the learning objectives, course content and supporting materials needed to complete the curriculum model, as well as further explore prerequisite knowledge areas (i.e. data communications, programming, operating systems etc). Questions remaining include:
- What areas should be emphasized in each of the three program variants?
- What other courses should be added to each area, and what should they entail?
- Are the proposed levels of knowledge appropriate or should additional depth be pursued?
- Are there sub-domains below the major and minor topics listed?

To answer these questions the authors intend to consult with other experts in the field and obtain their insight. They plan to take the preliminary implementation and draft curriculum model to outside experts for commentary at national information security education conferences. Information from these conferences will be used to shape an InfoSec curriculum development workshop.

The Information Security Curriculum Development conference, planned for September 2004 will invite industry and academic experts to validate and extend the data already collected and begin the process of formulation of the finalized curriculum standards. The workshop will be part of a two-day conference, organized around curriculum issues, working to develop the findings for this study. Additional data collection efforts will focus on curriculum discussions with state and federal

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

agencies and local commercial and non-profit organizations, as these organizations have indicated interest in this project. After this conference all inputs and commentary from the workshop will be synthesized and formalized into a revised model.

The ultimate purpose of this curriculum development project is to assist in the advancement of information security education at the national level. It is likely that many educational organizations are struggling with the same problems as practitioner organizations. The unanswered questions require understanding what is needed to support the security of information, and what skills and qualifications are needed in a quality information security applicant. The core of this project is to improve education, by assisting administrators and instructors in understanding what must be taught. It seeks to enhance and support educational infrastructure, by providing a curriculum model that provides structure and guidance in the implementation of this critical coursework. Many instructors will be able to master the basics of organizational information security policy, planning and staffing. The technical components of any curriculum are often the most difficult to master for the instructional staff. A framework for the instruction of this technical content will provide strong guidance on the instruction of a wide variety of technical security components. Society will benefit as more qualified security personnel are created, improving the level of security of personal information in organizations around the country.

V. How you can help

This draft curriculum model is an ongoing effort to improve information security curriculum. Through presentations and discussion across the US, the authors have spoken with a number of faculties, all eager to learn about developing and implementing information security curriculum. Help is requested in two ways:

1) Provide critical but constructive reviews of the curriculum model and materials presented here, asking the following questions:

- Does the curriculum model seem comprehensive, robust and scalable? Why or why not?
- Does the curriculum model follow established curriculum development guidelines, especially when an institution has established development requirements in place?
- Does the curriculum model work within established curriculum models for technology (or non-technology) baccalaureate programs?
- What could be improved in the curriculum model?

2) Let the authors know if you like or are using the curriculum model by sending feedback using a formal letter on letterhead and, when appropriate, supporting the curriculum model developed to the authors.

VI. References:

[1] Bordogna, J. “Remarks and Introduction of the Honorable Howard A. Schmidt AACC/NSF Workshop on the Role of Community Colleges in Cybersecurity Education.” June 26, 2002. Viewed online 4/22/2003 at http://www.nsf.gov/od/lpa/forum/bordogna/jb020626aaccnsfcyber.htm

[2] Chin, S-K, Irvine, C.E., & Frinke, D. “An Information Security Education Initiative for Engineering and Computer Science.” Naval Postgraduate School Technical Report, NPSCS-97-003. Naval Postgraduate School, Monterey, CA. 12/1997.

[3] Irvine, C., Chin S-K., & Frincke, D. “Integrating Security into the Curriculum.” Computer. 31(12). 12/1998. 25-30.

[4] ACM, AIS & AITP. “IS 2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems.” Viewed Online 5/8/2003 at http://www.aisnet.org/Curriculum/IS2002-12-31.pdf.

[5] National Science Foundation and the American Association of Community Colleges Protecting Information: the Role of Community Colleges in Cybersecurity Education Community College Press, Washington D.C. June 2002.

[6] NSTISSI No. 4011 – National Training Standard for Information Systems Security (INFOSEC) Professionals. 06/1994. Viewed Online 02/12/2002 at http://www.nstissc.gov/Assets/pdf/4011.pdf.

[7] “NSTISSI No. 4014 - National Training Standard for Information Systems Security Officers (ISSO).” 08/1997. Viewed Online 02/12/2002 at http://www.nstissc.gov/Assets/pdf/4014.pdf

[8] National InfoSec Education and Training Program (NIETP). “Centers Of Academic Excellence in Information Assurance Education.” Viewed Online 04/6/2003 at http://www.nsa.gov/isso/programs/coeiae/index.htm .

[9] National InfoSec Education and Training Program (NIETP). “NSA Designates Centers of Academic Excellence in Information Assurance Education.” Viewed Online 2/10/2002 at. http://www.nsa.gov/isso/programs/nietp/newspg1.htm#Universities.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

[10] Hutton, G. “Backward Curriculum Design Process” Viewed Online 5/1/2003 at http://www.g4v.com/~glen.hutton/ED3601/BackwardDesignFeb11_03.pdf.

[11] Eddie Schwartz, Dan Erwin, Vincent Weafer, and Andy Briney. “Roundtable: Infosec Staffing Help Wanted!” Information Security Magazine Online. April 2001.

[12] Bloom, Bengamin S., Bertram B. Mesia, and David R. Krathwohl (1964). Taxonomy of Educational Objectives. New York. David McKay.

[13] KSU “Professional Security Certifications” Viewed Online 5/10/2003 at. http://infosec.kennesaw.edu/certifications.html.

[14] KSU “Security Models and Training Standards” Viewed Online 5/10/2003 at http://infosec.kennesaw.edu/tngstandards.html.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE