Developing an Information Security Curriculum for Educational Institutions: An Analysis of Goals, Objectives, and Competencies for the 21st Century

Albert Fundaburk[1]
Business Education and Office Information Systems, Bloomsburg University
Bloomsburg, PA, 17815, USA

and

James Cannady[2]
Computer & Information Science, Nova Southeastern University
Ft. Lauderdale, FL, 33314, USA

Abstract

In recent years, a dramatic shift has occurred in the way computers are used. The advances in computer security have not kept pace with the phenomenal advances in computers and networking. This rapidly evolving information systems environment requires up-to-date information security curriculum. The speed in which the information systems environment changes in regard to security makes it extremely difficult for a university curriculum to prepare students for working in the world of information security. Current engineering and computer science curriculum does not provide students with an understanding of the foundational concepts of information security. Existing undergraduate computer science curriculum focuses on the physical aspect of information security. The goal for developing a comprehensive information security curriculum is to teach the theoretical concepts of information security, and provide a means of applying the concepts to practical applications. This project focuses on rigorous research to define information security and the meaning of a security professional. From this definition, specific knowledge and skill attributes will be determined and a specific curriculum will be developed. This research will consist of three phases: Phase I – Identify Requirements; Phase II – Develop Curriculum Model; and Phase III - Model Implementation, Evaluation, and Review.

Keywords: Information systems security, curriculum development, information security certification, information security curriculum mode

[1] afundabr@bloomsburg.edu
[2] cannady@nova.edu

1. RESEARCH GOAL

In recent years, there has been a dramatic shift in the way computers are used. The advances in computer security have not kept pace with the phenomenal advances in computers and networking. Due to these advances the need is continuous for trained security professionals. However, schools and universities lag behind in providing graduates in the computer security field.

> Recent high-profile computer attacks, like those against the Web sites of Yahoo and Amazon.com, while not necessarily typical, raised security concerns at companies and universities. With the Internet established as a fact of life for businesses, and networked computers increasingly indispensable to our daily lives, people who know how to protect computers are a hot commodity. Unfortunately, academic programs that teach such expertise are lagging far behind this demand (McCollum 2000).

The Internet has allowed a world so interconnected that work cannot be accomplished without computers, and computers cannot perform effectively without a measure of security. Due to the shortage of information security professionals a need exists for a comprehensive program to educate more individuals in the field of information security (Chin 1997). Employers expect graduates to have the proper technical and non-technical skills to ensure success. The rapidly evolving information systems environment requires up-to-date curriculum (Maier 1996). The problem is that a current engineering and computer science curriculum does not provide students with an understanding of the foundational concepts of information security (Bishop 1997).

There is interest in establishing core curriculum and integrating computer security into Computer Information Systems (CIS) curriculum. The National Security Agency has designated institutions that are teaching information security as Centers of Academic Excellence. This recognition involves no support or benefits. The National Plan for Information Systems Protection states its support of education and training; however, it does not allocate funding. Although there seems to be support for the development of an educational program in information security the actual components of that program have yet to be defined.

The speed in which the information systems environment changes in respect to security makes it extremely difficult for a university curriculum to prepare students for working in the world of information security. The challenge in industry is to design, develop, and deploy systems with confidence in their ability to satisfy security requirements. To meet this challenge a fundamental change in thinking is required. The information security professional must shift from a purely physical information technology (IT) environment to include the virtual and operate from both a physical and conceptual level. In defining curriculum the issue of the academic level must be addressed. If defined as an undergraduate program the curriculum must teach broad principles and applications. If defined as a graduate program it must build upon an undergraduate program and apply critical thinking and an in-depth analysis of a particular program. Dr. Blaine Burnham, University of Nebraska, states that because of the requirement of a broad base knowledge in the technical aspects of information systems, an information security curriculum at the undergraduate level would not be viable (B. Burnham, personal communication, December 2000).

Current undergraduate computer science curriculum focuses on the physical aspect of information security (Bishop 1997). The goal for developing a comprehensive information security curriculum is to teach the theoretical concepts of information security, and provide a means of applying the concepts to practical applications. This includes the administration of information security through applicable policies, procedures, and laws.

Contemporary research defines computer security as the detection, prevention, and investigation of actual or potential acts or omissions that threaten a system or data, and includes safeguarding critical resources and sensitive information. As this is a simplistic view, the first step will be a more rigorous look at information security to identify information security specific knowledge and skill attributes. There are two specific problems associated with defining specific knowledge and skill attributes for curriculum within information security: 1) defining the needs of an information security graduate by projecting current needs into the future; and 2) dealing with the time lag required to implement a new academic program in the university system. From the time the curriculum is developed until a student may actually take a course may be as long as two years. The skills and attributes must be viable when the first student graduates in four to six years (Lightfoot 1999). This research will examine existing information security curriculum to determine the level in which skills and attributes are currently being taught. An initial survey will be developed to forecast the future skills and attributes of an effective information security curriculum. Based on this examination, the goal of this research is to develop an effective information security curriculum model grounded in rigorous and empirical research. This curriculum model will consist of the following: 1) identify and describe specific information security learning areas; 2) identify essential student prerequisites; 3) identify and verify knowledge and skill attributes (KSAs); 4) write terminal performance objectives; and 5) sequence KSAs to terminal performance objectives.

2. THE RESEARCH APPROACH

The initial research will focus on rigorous research to define information security and the meaning of a security professional. From this definition, specific knowledge and skill attributes will be determined from which a specific curriculum will be developed. This research will consist of three phases: Phase I – Identify Requirements; Phase II – Develop Curriculum Model; and Phase III - Model Implementation, Evaluation, and Review.

Phase I - Identify Requirements

In the first phase this research will define information security and summarize its importance to personal, governmental, and corporate information systems. From this definition the research will identify the requirements needed to perform in an information security role. In particular, this research will evaluate existing information security curriculum to determine if these programs are meeting current and foreseeable future information security needs as defined by this research and real-world scenarios.

This phase of the research will be accomplished by:

1) Conducting surveys of information technology professionals in both business and government. These professionals will include Chief Information Officers, Systems Administrators, and other personnel currently working in the Information Technology field.

2) Surveying information security program graduates as to the usefulness of their degrees, determining what, if anything, was missing and comparing their responses against the stated outcomes of the completed program to identify successful curriculum.

3) Reviewing all of the existing information security programs to determine objectives, outcomes, skills, and faculty involvement, including faculty academic and professional background.

4) Reviewing the components of the Certified Information Systems Security Professional (CISSP) exam and Department of Defense Information Technology Certification and Accreditation Process (DITSCAP) for a comparison of the examination topics and the outcomes of existing curriculum.

5) Surveying faculty and administrators at universities that have information security programs to establish the curriculum development process used in determining program content and outcomes, as well as learning resource selection.

Phase II - Develop Curriculum Model

Phase II will be the development of a model information security curriculum using the information obtained in Phase I. This model will define specific courses needed to produce information security professionals, what the prerequisites to these courses should be, and course content by following the steps outlined below:

1) By developing objectives consistent with the needs identified by the analysis of the research in Phase I.

2) By defining instructional methodologies and strategies.

3) By selecting existing materials or developing new materials to support the instructional methodologies.

4) By writing course descriptions and identifying outcomes.

Phase III - Model Implementation, Evaluation, and Review

Some fundamental questions will be addressed in Phase III of this research. The level of implementation must be defined. Will the complexity of the coursework require that the program be designated as a computer science (CS), computer information systems (CIS), or as a management information systems (MIS) curriculum? Should this curriculum be an undergraduate program or will the prerequisite knowledge require that the program be implemented at the graduate level? Will the successful faculty member be an information security generalist, a specialist in some aspect of information security, or a combination? Using the outcomes of the curriculum as defined in Phase II, an evaluation will be performed to ascertain whether the curriculum will provide a generalized education in information security and require that industry provide training in specific needs and requirements, or will the curriculum provide education in specific tools and requirements? Finally, Phase III will address the evolution of the curriculum by developing a recommended revision and evolution plan to ensure that as information systems evolve so shall the information security curriculum.

3. CONCLUSION

The speed at which information technologies have advanced over the past decade has left glaring holes in our ability to protect this resource. Although industry has kept pace by providing exclusive learning tools relating to specific products designed for information security, academe has lagged far behind. As information security is multi-disciplined it is a challenge to determine the specific skills and attributes needed to satisfy security requirements. To meet this challenge this research will develop an effective information security curriculum model grounded in rigorous and empirical research. The proposed three-phase model will provide definitive answers to the development of a general curriculum in information security.

4. REFERENCES

Bishop, Matt, 1997, “The State of INFOSEC Education in Academia: Present and Future Directions.” Keynote speech to the National Colloquium on Information Security Education. May 25 - 27

Chin, Shiu-Kai., Deborah Frincke and Cynthia Irvine, 1997, .An Information Security Education Initiative for Engineering and Computer Science. Syracuse: Syracuse University.

Lightfoot, Jay, 1999, “ Fad versus Fundamentals: The Dilemma for Information Systems Curriculum Design.” Journal of Education for Business, 75(1), pp. 43-51.

Maier, J. Lee, and Stan Gimbill, 1996, “CIS/MIS Curriculum in AACSB-Accredited Colleges of Business.” Journal of Education for Business, 71(6), pp. 329-334.

McCollum, Kelly. 2000, “Colleges Struggle to Train Experts in Protecting Computer Systems.” The Chronicle of Higher Education, March 24, 46(29).