Information System Security Curricula Development

Ed Crowley
University of Houston
Information Systems Technology
Houston, TX 77204-4023
713-743-4096
ecrowley@uh.edu

ABSTRACT

In this paper, we survey current literature concerning Information Systems Security Training and Education. This paper also describes current Information System Security Training and Education dynamics. Finally, this paper presents a graduate level information system security specialization that was developed using this information.

Categories and Subject Descriptors

K.3.2 [**Computers and Information Science Education**]: Information Systems Education – Information Technology.

General Terms

Keywords

Information technology curricula, Information technology security.

1. INTRODUCTION

In 1996, the National Research Council referred to the growing reliance on vulnerable information systems as the "Information Security Problem." In 1998, Presidential Decision Directive 63 cited the need to protect critical cyber-based systems essential to the minimum operations of the economy and government. More recently, the National Strategy to Secure Cyberspace names "A National Cyberspace Security Awareness and Training Program" as its number three priority.

All of these references indicate a growing awareness that society is increasingly dependent upon information systems that have proven vulnerable. In a quest to increase productivity, organizations connected their internal information systems. To increase productivity even more, they connected their infrastructure to the Internet. Now, organizations are becoming aware that as they increased their connectivity, they also increased their vulnerability. This growing awareness has lead to a demand for Information Systems Security training and education.

Unlike more mature disciplines, such as Computer Science and Computer Engineering, there is neither a universally accepted Common Body of Information Systems Security Knowledge (CBK) nor a model curriculum for Information Systems Security. There are, though, ongoing efforts to define a CBK that could lead to a model curriculum.

Similarly, there doesn't seem to be a clear consensus about what differentiates information systems security training from education. For example, while the National Plan for Information Systems Protection refers to "training and education" in several places, those terms remain undefined. This lack of precision and consensus has created tension.

This paper offers a perspective of how one Information Systems Technology program dealt with these tensions and developed a graduate level information system security specialization.

2. PROGRAM VISION

The Information Systems Security Specialization was developed for the new Masters in Project Management degree. The program design began with a vision of a successful student. Specifically, a vision based upon the knowledge and skills that a successful student would possess. That vision was that a successful student would:

Within a specific organizational environment, provide information assurance.

Information Assurance (IA), as defined by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), is:

> Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [14]

Specifically then, successful students would be able to analyze, develop, implement, and maintain the appropriate information systems services needed by an organization. To understand IA, it is important to understand the context within which it evolved.

Information Assurance evolved from a three component theory of Computer Security. [5] The three components are:

- A precisely articulated security policy describing the management, protection, and distribution of sensitive information by an organization
- A set of functional mechanisms sufficient to enforce the policy and
- Assurance that the mechanisms do enforce the policy

Other models, such as the McComber model, also possess administrative and technical components [13]. It is these components combined with the organizational context that makes Information Assurance Education unique.

2.1 IA Education Attributes

Information Assurance Education has several significant attributes. They include:

- Context sensitive
- Dynamic
- Multidisciplinary
- Active

IA is context sensitive. Security countermeasures need to be based on threat models that include:

- An organization's legal and regulatory context
- The value of informational assets
- Current vulnerabilities
- Potential threats.

From a technical perspective, IA is dynamic. Each day, new:

- Vulnerabilities are discovered.
- Exploits are published.
- Countermeasures may be required.

Consequently, IA Education must prepare students to learn about and understand new concepts.

From a legal perspective, IA is dynamic. Federal Legislation, such as the Health Insurance Portability Act (HIPAA) and Graham-Leach-Bliley specify discrete mechanisms to be applied to organizational data. Also specified are discrete liabilities and penalties for failure to comply. In addition to new administrative law, civil law evolves with each new case. What was legally appropriate today may not be legally appropriate tomorrow.

IA is multidisciplinary. Within an organization, IA is dependent upon computing infrastructure, policies, and people. Consequently, IA as a discipline includes aspects of diverse disciplines including psychology, sociology, law, computer science, computer engineering, and management [7].

Finally, students learn information security by doing it [20]. Unlike some fields, knowing what to do and why to do it may not increase an organization's Information Assurance. To achieve our vision, it is necessary that our students also know how to do IA.

2.2 Institutional Program Goals

Gene Spaford has articulated appropriate goals for different programs. For Science and Technology programs, he articulates that they:

> Teach basic skills with an emphasis on a professional path. [15]

As we are a College of Technology, this is an appropriate program goal. At the same time, Research 1 institutions have a research obligation.

At a Research 1 institution, in addition to attracting students, the program also has an obligation to enhance the University's research position. Moreover, for Research 1 institutions, any new security curriculum will likely only be seen as successful if it produces quality graduate students and a body of knowledge that will produce two results:

- Increased research result visibility (refereed publications)
- Increased external funding (federal grants) [19]

In addition to research, our students are interested in potential Career Paths. We project three distinct potential student career paths. [15]

Table 1: Potential Student Career Paths

Career Path	Description
Practitioner	Manage enterprise security
Managers/planner	Responsible for enterprise wide security planning and operations, e.g. a CIO
Auditor/Investigator	Audit computing systems or facilitates law enforcement

While a common core of educational competencies underlies each path, there are some differences. The competencies required for Manager/Planner is primarily a superset of that required for Practitioner. An Auditor/Investigator also requires education in Incident Response and Psychology.

Table 2: Career Path Competencies

Practitioner	Manager/Planner	Auditor/ Investigator
Risk management	Risk management	Forensics
Ethics and Law	Ethics and Law	Law and evidence
Computing technology	Software engineering	Privacy
Personnel management	Personnel management	Psychology
Design and test	Design and test	Multinational norms
Telecom and networking	Access control	Access control
	Intellectual property	
	Purchasing and acquisitions	

2.3 Training and Education

The Federal Government divides responsibility for Information Assurance among several groups. The 1987 Computer Security Act assigned the National Institute for Standards and Technology (NIST) responsibility for unclassified systems. It also assigned the National Security Agency (NSA) responsibilities for systems and telecommunications involving classified systems. Providing a policy setting structure for the national security systems community is the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

Several government documents provide insight into security education and training. Among them is NIST SP 800—16 titled "Information Technology Security Training Requirements: A Role and Performance Based Model." This document presents a role-based model based on the premise that learning in the IA field is a constant [18].

In the document, a training environment is where an employee is taught to use specific skills as part of a job or role. In contrast, in an educational environment, the employee is encouraged to examine and evaluate not only work skills and methods but fundamental operational principles as well.

From this perspective, the objective of training is skill development. Training emphasizes the how attribute. Training focuses on developing skills with particular systems, situations, or both. Emphasis is on procedures and technologies. While training is provided to individuals based on their particular job functions, education is intended for designated IT security specialists.

Likewise, the objective of education is understanding. Education emphasizes the why attribute. NIST 800 – 16 describes educated professionals as people that are "capable of vision and pro-active response".

Undergraduate learning focuses on broad principles and how they are applied. In addition to building on undergraduate education, a Masters education enables a student to weigh competing interests and determine the optimum technical solution [4]. These students can analyze problems, envision solutions, as well as make and work, an implementation plan. At this level, education emphasizes applications or applied research.

2.4 Inherent Tensions

While academia, industry, and government are all significant IA education stakeholders, each has a distinct perspective. While the fundamentals of security do not change, the emphasis on and value of a particular service depends, in part, on the context in which it is used. Consequently, each stakeholder views IA through a unique filter.

In Academia, principles that underlie computer security are emphasized. A students understanding of the principles, i.e. the why and what, is generally considered most important. How receives, relatively, less emphasis.

Industry focuses upon applied security. From an Industrial perspective, people, infrastructure, and intangibles such as fiscal Information, availability, and proprietary information all need protection. Consequently, Industry needs effective security mechanisms. Emphasis is upon security's how and what. Principles are considered, relatively, less important.

In contrast to the other sectors, the Government uses computer security to protect the national interest. Specific protections are legally mandated. Consequently, they are not necessarily subject to the same cost benefit analysis as in the other sectors. Here, computer security education focuses on developing policies and systems to implement, laws and regulations. Emphasis is on what and how.

3. PARALLEL CBK EFFORTS

While there isn't a mature academic common body of knowledge, there has been significant work done in governmental, industrial, and academic sectors. Each sector has developed a unique body of knowledge based upon their own unique perspectives. The following sections examine these efforts.

3.1 Government Efforts

In addition to the previously discussed efforts at NIST, the National Security Telecommunications and Information Systems Security Committee (NSTISSC), has developed a series of training standards.

These standards include the 4011, National Training Standard for Information Systems Security (INFOSEC) Professionals, as well as the standards referenced in the following table.

Table 3: NSTISSI Training Standards

NSTISSI No	Description
4011	National Training Standard for Information Systems Security (INFOSEC) Professionals, 20 June 1994
4012	National Training Standard for Designated Approving Authority (DAA), August 1997
4013	National Training Standard for System Administration in Information Systems Security, August 1997
4014	National Training Standard for Information Systems Security Officers (ISSO), August 1997
4015	National Training Standard for Systems Certifiers, dated 2000

Both NIST 800-16 and NSTISSI 4011 include information that could be useful in defining a CBK for Information Security. Note that the NSA operates the Centers of Academic Excellence (COE) in Information Assurance program. The NSA grants the COE designations following a rigorous review of university applications against published criteria based on training standards established by NSTISSC. The following table lists the security content areas for both documents.

Table 4: NIST vs. NSTISSI Content Areas

NIST 800 -16	NSTISSI 4011
• The Organization and IT Security • System Interconnection and Information Sharing Sensitivity • Operational Controls • Technical Controls • Risk Management • Management Controls Acquisition/Development • Installation/ Implementation Controls • Laws and Regulations	• Communications Basics (Awareness Level) • Security Basics (Awareness Level) • NSTISS Basics (Awareness Level) • System Operating Environment (Awareness Level) • NSTISS Planning And Management • NSTISS Policies And Procedures (Performance Level)

3.2 Industry Efforts

In the industrial sector, (ISC2) the International Information Systems Security Certifications Consortium, Inc. developed a Common Body of Knowledge [CBK] for Information Systems Security Certification. This CBK serves as the basis for Certified Information Systems Security Professional certification.

Table 5: ISC2 Common Body of Knowledge Domains

ISC^2 CBK Domains
Security Management Practices
Security Architecture and Models
Access Control Systems & Methodology
Application Development Security
Operations Security
Physical Security
Cryptography
Telecommunications, Network, & Internet Security
Business Continuity Planning/Disaster Recovery
Law, Investigations, & Ethics

Other groups including, the Information Systems Audit and Control Association (ISACA), the SANS (SysAdmin, Audit, Network, Security) Institute, and the Computer Trade Industries Association (CompTIA) have also developed security certifications. The IETF has developed RFC 2196. The ISO has developed ISO17799. A group working in a related area is the Organization for Economic Cooperation and Development (OECD) which has developed the Generally Accepted System Security Principles (GASSP).

3.3 Academic Efforts

Within the academic sector, there is an ongoing effort to establish a common body of knowledge. The long term objective of the project is to develop a curriculum framework for undergraduate and graduate programs in Information Assurance (IA). The stated goal is to produce a document similar to the Joint IEEE Computer Society/ACM Task Force document “Model Curricula for Computing”.

The Report on Information Assurance Curriculum Development is a working document developed from meetings held in April 02 and July 01. The Framework includes: identification of broad areas of knowledge considered important for practicing professionals in information assurance [7].

As it is a working document, the Framework is expected to evolve. Its goal is to outline the core of an IA graduate program. At the Graduate Level, it defines four areas. The following table summarizes some of the report’s detail concerning each content area.

Table 6: IA Graduate Program Areas

Area Title	Sub-Areas
Management, Policy and Response	Security Policy Guidelines, Security awareness, Ethical decision making and high technology, Employment practices and policies, Operations security and production controls, E-mail and Internet use policies, Using social psychology to implement security policies, Auditing and assessing computer systems, Cyberspace law and computer forensics, Privacy in cyberspace, Protecting intellectual property, Security standards for products, Management responsibilities and liabilities, Developing security policies, Risk assessment and risk management, Incident Response and Recovery
Secure Computing Systems	Access control, Identification, authentication, and authorization, Design of secure systems, Evaluation, Databases and their applications, Software development, Auditing, Operations Management
Network Security	Protocols, Network basics, Vulnerabilities, Attacks, Application layer services, Management, monitoring, auditing and forensics, Infrastructure, Wireless and broadband, Filtering
Cryptography	Development, Fundamentals, Symmetric algorithms, Asymmetric algorithms, Cryptographic protocols, Hardware implementations, Digital signatures, Public key infrastructure and certificate authorities, Implementation issues, Applications, Cryptanalysis, Steganography, Latest Developments

4. SECURITY SPECIALIZATION

This graduate level specialization consists of four, three credit hour courses. Prior to enrolling in the specialization, students are expected to have earned a technical undergraduate degree or to have experience working with information systems security. The Principles Class is a prerequisite for the other three classes.

With the help of local governmental and private organizations, we plan on evolving the specialization to maintain its relevancy. The college is also considering packaging the four courses as a certificate. Longer range goals include submitting the curriculum to the NSA for 4011 certification.

4.1 Principles of Information System Security

This course covers the basic principles of information systems security. Included are specific, administrative and technical, security controls. It also includes the methodologies that organizations utilize to create and achieve security goals. In addition to information systems security legal and regulatory

CITC4’03, October 16-18, 2003, Lafayette, Indiana, USA..
Copyright 2000 ACM 1-58113-000-0/00/0000…$5.00.

aspects, emphasis is placed on management issues and solutions. Specific control measures include system access controls, telecommunications network security, encryption, and physical security.

Class activities are augmented with laboratory activities that provide students the opportunity to apply the principles. Laboratory activities focus on four areas: Operating Systems, Telecommunications, Cryptography, and Management.

Table 7: Class One, Knowledges and Skills

Knowledges	Skills
Management Practices Risk Management and Assessment	Management Policy Policy Generation
Architecture and Models	
Access Control Systems	
Application Development	
Operations Security	Operating System Secure Install Baseline Patch Install/configure/operate Antivirus Spyware scanner
Physical Security	
Cryptography	Cryptography PGP Install/configure/operate Asymmetric Key Pair Generation Document Encryption Hashing Steganography S-Tools JPHS
Telecommunications and Networking	Telecommunications Personal Firewall Firewall Log Analysis Install/Configure/operate Port Scanner Packet Analyzer
Business Continuity Planning/Disaster Recovery	
Law, Investigations, & Ethics	

4.2 Secure Enterprise Computing:

Incident Response and Computer Forensics

This course covers the detection, isolation and response to security incidents. Security incidents may involve crimes using computers as the object of a crime, or they may involve general information systems misuse. This Course presents a detailed examination of the incident response and computer forensic process. Specific procedures required to appropriately respond to a security incident are also presented. Class goals include preparing students to quickly return information systems to normal operation while gathering and preserving evidence in a manner congruent with court presentation.

Class activities are augmented with laboratory activities that provide the students the opportunity to apply the principles. Laboratory activities concentrate on four areas: hard drive and network forensics, document integrity (hashing), password auditing (cracking), and system integrity.

Knowledges	Skills
Incident Response Developing an Incident Response Team Incident Response Process	
Basic Forensics Methodology HD Forensics System Forensics Network Forensics Internet Forensics	HD Forensics • Linux DD Network Forensics • Ethereal
Security Policy and the Law Privacy Law Evidence Rules Cyberspace Law	
Computer Systems Audit	
Intrusion Detection	
Cryptanalysis	Cryptography • MD5-Sum • Win-Hex
Access Control Radius Password Cracking	Access Control • Password Cracking • L0pht Crack • John the Ripper
Malicious Software	
System Integrity	Systems Integrity • Tripwire

4.3 Information Systems Security: Cryptography and Intrusion Detection

This class covers the cryptographic services required to securely send confidential information across the public Internet. It also covers related cryptographic services that provide integrity, authentication, and nonrepudiation. Specific technical topics include: public key infrastructure, digital signatures, certificates, and virtual private networks (VPNs). In addition to applying appropriate cryptographic methodologies to their own communications, organizations need intrusion detection to have assurance that their network infrastructure has not been compromised.

Class activities are augmented with laboratory activities that provide the students the opportunity to apply the principles. Laboratory activities focus on five areas: Public Key Infrastructure, Proxy Servers, Intrusion Detection Systems, building a bastion host, and Remote Access.

Table 9: Class Three, Knowledges and Skills

Knowledges	Skills
Symmetric Ciphers DES AES	
Cryptographic Applications Hashes Digital signatures Key exchange Protocols Cryptographic Protocols	Certificate Server Installation Managing Certificates
Communications Concepts TCP/IP	
Perimeter Devices Firewalls Bastion Hosts Proxy Servers Rules and Restrictions	IPTables Identifying an Nmap Scan
Intrusion Detection System Components Process Preventive Measures Logging Analyzing Intrusion Signatures Identifying Suspicious Events Developing IDS Filter Rules	IDS Installation SNORT Capturing packets with Snort Capturing ICMP Packets Configuring a SNORT rule set Using IDScenter as a Front End for Snort
Virtual Private Networks Tunneling Protocols IPSec/IKE Secure Shell (SSH) Layer 2 Tunneling Protocols	Setting up a Remote Access Server Configuring a VPN Server Establishing a VPN Connection Activating IPSec and Specifying a Policy Configuring L2TP
Web Security TLS/SSL	Building a Bastion host

4.4 Information Systems Security Risk Analysis and Management

This course focuses on the organizational issues of risk management in the legal context of the Internet. Organizational problems involving reliability, safety, security, privacy, and human well-being are addressed here. Particular focus is put on avoiding recurrences of similar events. Legal issues include the current legal context of the Internet. Specific issues covered include: copyright and trademark issues, defamation, privacy, liability, electronic contracts, tax issues, and ethics.

Class activities are augmented with projects that provide the students the opportunity to apply the principles. Projects focus on three areas: creating a policy handbook, planning a security audit, and creating an organization disaster recovery plan.

Table 10: Class Four, Knowledges and Skills

Knowledges	Skills
Threat identification process	Create a contingency and disaster recovery plan.
The current Information Systems Security regulatory and legal environment.	Create a security auditing and monitoring plan for an enterprise.
Contemporary issues in computer security regulations and laws, including: Contract law Intellectual and other property law Criminal law Constitutional law Liability law Regulatory law	Create a policy handbook.
Principal ethical issues with relationship to legal standards.	
Distinguish the legal issues in an information architecture that can be analyzed by a computer security professional from those that require an attorney.	

5. REFERENCES

[1] Bishop, M., "Teaching Computer Security," SEC 1993: 65-74.

[2] Bishop, M., "Computer Security Education: Training, Scholarship, and Research," IEEE Computer 35 (4) Privacy and Security Supplement pp. 30-32 (Apr. 2002).

[3] Bishop, M., "What Do We Mean By 'Computer Security Education'?," Proceedings of the 22nd National Information Systems Security Conference p. 604 (Oct. 1999).

[4] Bishop, M., "Academia and Education in Information Security: Four Years Later," Fourth National Colloquium on Information System Security Education (May 2000).

[5] D. L. Brinkley and Schell, R. R., Concepts and Terminology for Computer Security, in Information Security: An Integrated

Collection of Essays, ed. Abrams and Jajodia and Podell, IEEE Computer Society Press, Los Alamitos, CA, 1995, pp. 40-97.

[6] Chin, S.-K., Irvine, C. E., and Frinke, D., "An Information Security Education Initiative for Engineering and Computer Science," Technical Report NPSCS-97-003 ,Naval Postgraduate School, Monterey, CA, December 1997.

[7] Dark, M., and Davis, J., "Report on Information Assurance Curriculum Development", June 2002.

[8] Davis, J. and Dark, M., "Defining a curriculum framework in Information Assurance and Security", 2003 ASEE Annual Conference, Nashville, TN, June 2003.

[9] Davis, J., "Building an IA Program: A Few First Steps," NCISSE Boot Camp, June 2002.

[10] Fundaburk, A. (in review) Assessing the Need for Teaching Information Security in an Office Information Systems Curriculum. Information Technology, Learning, and Performance Journal.

[11] Irvine, C.E., Warren, D. F., and Clark, P. C. The NPS CISR Graduate Program in INFOSEC: Six Years of Experience. In Proceedings of the 20thNational InformationSystems Security Conference, pp. 22-30, Baltimore, MD, October 1997.

[12] Laswell, B., Simmel, D., and Behrens, S. "Information Assurance Curriculum and Certification: State of the Practice," CMU/SEI-99-TR-021, Software Engineering Institute, Carnegie Mellon, Pittsburg, PA, Sept. 1999.

[13] Maconachy, V., Schou, C., Ragsdale, D., and Welch. D., "A Model for Information Assurance: an Integrated Approach," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, (West Point, NY), 2001.

[14] NSTISSI, "No. 4011 - National Training Standard for Information Systems Security (INFOSEC) Professionals," 1994.

[15] Spaford, E., "Teaching the Big Picture of InfoSec," National Colloquium For Informationsystems Security Education (NCISSE), VA. 1998.

[16] Vaughn R., "Ware to Start?," National Colloquium For Informationsystems Security Education (NCISSE), 2001.

[17] Vaughn R., Henning R., and Fox K., "An Empirical Study of Industrial Security - Engineering Practices," Journal of Systems and Software, vol. 61, no. 3, pp. 225-232, June 2002.

[18] Wilson, Mark, ed. Information Technology Security Training Requirements: A Role- and Performance-Based Model, NIST Special Publication 800-16, National Institute of Standards and Technology, U.S. Department of Commerce, 1998.

[19] Yasinsac, A. Information Security Curricula in Computer Science Departments: Theory and Practice. Manuscript, 2001.

[20] Yurcik, W. and Doss, D., "Different Approaches in the Teaching of Information Systems Security," Information Systems Education Conference (ISECON), Cincinnati, OH, 2001.