

Crafting an Undergraduate Information Security Emphasis Within Information Technology

Patricia Y. Logan, Ph.D.
Information Systems and Technologies, Weber State University
Ogden, Utah, 84408-3804
plogan@weber.edu

ABSTRACT

Universities have only recently created an undergraduate course in information security (or related topics) but few have implemented an emphasis or comprehensive program at the undergraduate level. This article explores the creation of an undergraduate emphasis in information security at Weber State University (WSU) within the John B. Goddard School of Business and Economics (JGSBE) that is designed to train students in the skills necessary to implement and manage security. Specifically, the article discusses the skill sets for security management, the lab requirements for the courses in this emphasis and the incorporation of legal elements in the curriculum.

Keywords: Information security, training, security skills sets, undergraduate programs in information security.

1. INTRODUCTION

The security and assurance of our information and communications infrastructure is a national priority. To address this, our nation needs an information-literate work force that is aware of its vulnerability, as well as a cadre of information professionals who are knowledgeable of the recognized "best practices" available in information security and information assurance, as called for in Presidential Decision Directive 63, May 22, 1998. It is the task of American higher education to provide that information-literate work force and to prepare information professionals. To meet this priority, higher education must be informed of the knowledge, skills and attitudes to be taught in the general curricula and in the information curricula of its colleges and universities. www.ncisse.org

Information security is a hot topic in the popular press as well as technical journals. The skills required: investigating, managing, and responding to cyber attacks are sought after by Fortune 500 corporations and the federal government. The increase in reported cyber crime, and the devastating cost of a variety of viruses, worms, Trojans, and DoS (Denial of Service) attacks (see www.gocsi.com/forms/fbi/pdf.html), has underscored the need for information technologists able to effectively manage the security of a complex networked and application environment (Radcliff, 2002a; Vatis, 2002). Universities have responded to

this need by providing courses and certifications in information security.

In the USA, the most recognized initiative to meet the need for information security specialists is the NSA (National Security Agency) program for Centers of Academic Excellence in Information Assurance Education (http://www.ehr.nsf.gov/du/awards/sfs_scholarships.asp). The NSA initiative currently comprises thirty-six universities offering undergraduate and/or graduate curriculum that respond to the federal guidelines for information infrastructure security. Universities designated as Centers of Excellence may participate in a scholarship program, that allows selected students to be admitted for instruction in information security and will prepare them to receive bachelor's or master's degrees in information assurance and computer security. The students have internship opportunities with federal agencies, receive a full tuition scholarship, living expenses, an academic stipend, and upon graduation commit to work for the federal government on the basis of one year of service for each year of scholarship-based education received.

In a review of information systems/computer science department web sites for the 36 schools designated as Centers of Excellence in Information Assurance Education, the researcher found that undergraduates are not a popular target audience for an emphasis in information security. While nearly all schools had a rich offering of classes at the graduate level, only a handful

offered undergraduate course(s) in information security or related topics. Most commonly, universities offered a single course in information security within the undergraduate degree program. The conspicuous absence of undergraduate course offerings is interesting. Students graduating with a bachelor's degree in information systems/computer science are the most likely to be employed as network engineers with responsibilities that include security and the least likely to have attended a program with a rich set of courses in information security. Without access to undergraduate courses that prepare them for the responsibility of managing security, it would appear that an important skill set is missing for employers that hire information systems graduates.

2. DETERMINING THE SKILLS SETS

Security is both a business and technical issue. Industry leaders and security professionals have defined an ideal skill set as including: the capability of conducting detailed forensic investigations; the ability to interface with law enforcement, configure a complex network system securely, enable a detailed security and risk assessment; and additionally the ability to assume leadership in the management of security policies (Weisman, 2002). Security practitioners are increasingly being asked to have well-developed management, cognitive, and communication skills, as well as strong technical expertise (Suydam, 1999). At WSU we have elected to provide the foundation skills for effective security management at the undergraduate level and encourage students to explore relevant certifications to extend their skill set through private organizations in specialized areas of security.

2.1 Two Models of Information Security Management Education

In order to create a robust program at the university-level in information security education, it is necessary to review the course offerings and associated skill sets required by existing programs that are attended by IT practitioners involved in implementing and managing a secure infrastructure. Such a review can provide insight into the skills needed from an industry perspective and identify models for university programs. Two models of information security education for professional IT practitioners are provided by: (1) Private certifying organizations such as federal agencies, ISC² (International Information Systems Security Certificate Consortium), SANS (Systems Administration, Network and Security) and IACIS (International Association of Computer Investigations Specialists); (2) Proprietary sources, including vendors of security products.

The federal government has training standards that are associated with both the National Institute of Standards Publication 800-16 and the [National Security Telecommunications and Information Systems Security Committee \(NSTISSC\)](#) (Federal guidelines NSTISSI

4011, 4012, 4013, 4014, and 4015) standards for Information Systems Security Professionals, Designated Approving Authorities and Information Systems Security Officers (www.ntissc.gov). (These standards are currently undergoing update). Federal law enforcement programs include: FLETC (federal law enforcement training center), the Drug Enforcement Agency (DEA) and Department of Defense program DCITIP (department of defense computer investigation training program) have training courses in information security and forensics available only to qualified applicants from law enforcement or federal employees. The focus of these programs is on investigation, with course content reflecting procedures to investigate and analyze rather than the business need for securing a network against intrusion.

The ISC² model of training represents the attempt of a private organization to aggregate and standardize information security knowledge into a Common Body of Knowledge (CBK). ISC² grants certifications (SSCP, CISSP) only to experienced IT professionals with a bachelor's degree. The ten domains of the CBK (<http://www.isc2.org>) include:

- 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
- Law, Investigations, & Ethics

IT practitioners with a SSCP Certification must have a working knowledge in seven domains of the CBK:

- Access Controls
- Administration
- Audit and Monitoring
- Cryptography
- Data Communications
- Malicious Code/Malware
- Risk, Response, and Recovery

SANS offers a certification program based on network administration and security, GIAC (Global Information Assurance Certification). A significant amount of background knowledge and coursework is required of security practitioners that test for this certification, which covers topics in:

- Operating Systems
- Database Systems
- Data Communication and Networking

- Operating Systems Theory
- Advanced Topics in Database Systems
- Computer Networks and Distributed Processing.

Proprietary courses and vendors of security products represent another source of training for IT practitioners. Vendor sponsored courses include a curriculum heavy on product use, with course length from two to five days, depending on the complexity of the product. Coverage of topics dealing with security management is often brief if the vendor also offers information security consulting services. Proprietary training courses generally use a high-level over-view of security topics that require little technical knowledge, in comparison to the private certifying organizations and vendor sponsored courses. Some popular course options in this category are offered by the following firms: LC Technology, NTI (New Technologies Incorporated), Foundstone, Guidance, CompuForensics, Security University.

What conclusions can be reached by reviewing these models of curriculum from the private sector? Programs leading to certification require the most rigorous background in networks and operating systems, and include topics designed to meet the needs of a network engineer tasked with the responsibility to secure a complex network. Programs from vendors and proprietary sources appear to offer the same topic coverage, but at a lower technical level to accommodate all ranges of class participants.

How are the existing university programs different from these approaches to curriculum? Many universities have followed the federal guidelines required by the NSA in order to receive recognition and funding from the NSA as a Center of Excellence in Information Assurance, Education. In order to be designated as a Center of Excellence in Information Assurance universities must have an academic program tied to the topics covered in federal courses outlined at www.nstissc.gov, perform security research, and have faculty available to teach the courses. Points are awarded for each area of compliance, with the greatest points awarded under academic programs for those at the doctoral and graduate levels. Subject areas offered at the 36 schools that currently hold the NSA designation as Centers of Excellence include a variety of courses such as:

- Secure Electronic Commerce
- Information System Assurance
- Enterprise Security Management
- Secure System Administration and Certification
- Distributed Computing
- Network Security
- Computer and Network Forensics
- Computer Law and Policy

- Advanced Computer Security

The focus of the academic curriculum in these schools reflects the role of the university in providing research and the development of software tools to support the federal concerns with cyber-security and Critical Infrastructure Protection. Their programs reflect a heavy focus on graduate level courses and degree offerings. Few of the schools are focusing this curriculum on the undergraduate IT population.

2.2 Skill Sets For an Undergraduate Emphasis

Weber State University's Information Systems and Technologies department is one of the departments of the John B. Goddard School of Business and Economics. Our Business Advisory Council (BAC) in 2000 recommended we offer a course that focused on information security issues and management. The members of our BAC were unanimous in their interest in hiring graduates of our program with an emphasis in information security.

In preparation for offering an emphasis in information security, we reviewed the university curriculum at the 36 schools awarded the status as Centers of Excellence in Information Assurance Education and found the following:

- Few offered undergraduate courses or an emphasis in information security within the majors of MIS (management information systems) or CS (computer science)
- An absence of specific courses in computer forensics, security policy, security concerns in e-commerce strategy and legal and ethical issues
- Technical subjects did not often include topics such as configuration and hardening of servers, intrusion detection, or planning for incident response

As our focus in the JGSBE is to develop our students to participate in the strategic business initiatives that encompass technology, we set about crafting a different view of an undergraduate emphasis in information security based on the following points:

- Technical and management skills are required in order to effectively implement and manage complex networked systems.
- An alliance with the criminal justice department would facilitate an understanding of forensic investigation techniques, rules of evidence, and applicable law.
- All components of a complex technology environment require security: networks, applications, and desktops.

At WSU, the Information Systems and Technology (IS&T) major requires students to select either a

software development emphasis requiring three (9 units) specialty courses, or the information security and networks emphasis that requires four (12 units) specialty courses. Required courses for the information security emphasis include: data communications, LAN or Internetworks, computer crime (a criminal justice course), advanced hardware/software and computer forensics. All IS&T students complete a foundation of classes that includes data communications, two programming languages (Visual Basic and Java), systems analysis, database design, as well as a rigorous business core in accounting, business law, management, marketing, logistics, and finance. Our goal was to provide a curriculum that included the ability to manage technically a complex computing environment and to be able to participate in the business components of risk assessment and cost analysis of loss. In summary, our program requires hardware, software, network, legal, and management skills.

The required coursework for the information security emphasis focuses on technical skills, emphasizes security issues, and introduces the ethical and legal concerns of managing security. The capstone course IS&T 4600, Computer Forensics, has the following course objectives:

- Develop the knowledge and skills necessary to understand the relationship between information security and business strategy
- Develop advanced competencies associated with technical, supervisory, policy development, and related positions in information security
- Develop core competencies in database and information system design, in operating systems and networks, and in software product development
- Adhere to ethical standards of conduct for analyzing, investigating evidence, and applying the knowledge only for the benefit of an employer

The capstone course includes desktop and network investigations and security implementation. Specialized software used for the course included: the NTI forensic suite, QuickView Plus, Norton Utilities, and Omniquad's Detective. Additional software that performs data recovery, back-up, duplication, search, encryption, data hiding, keyboard logging, password cracking, and hacker tool sets were introduced. The course required students to sign a statement of ethics that acknowledged the importance of the material they were to learn. To prevent students from attempting unauthorized network access under the guise of performing class work, we also stressed to the students that there were no assignments connected with the class that required access to the university network or computers. Students were advised that only their own

home computers and networks were to be used for practice and assignments. The course web site (www.wsuonline.weber.edu/forensics) was password protected to prevent unauthorized access to the software and course content. The final course exercise was a team competition to "break" the secrets of a suspect's computer. The students were divided into teams of three to four students, and each team created a desktop computer with evidence of a probable crime (desktop or network) that another team must "break". Teams supplied no hints, but could leave incriminating evidence in the area of the desktop, or within logs. The course this year (2002) had three teams, and each developed a scenario for another team to solve. The teams had access to the software used in the course for forensic examination and were allowed to use any other tool that they had found (freeware) or purchased (shareware, commercial products). Teams submitted a final report based on their review of the suspect computer and the disk image that they created. Reports were required to include a log of their actions in handling the computer, their findings, and a copy of the image they recovered from the suspect computer.

2.3 Computer Lab Requirements

Implementing an information security emphasis requires a significant investment in separate computing facilities. At a minimum, a computer lab that has a closed network with multiple servers, a router, switch, and software tools for investigation are needed. We have created a lab with 3 servers running Windows 2000 and BSD UNIX. We have removable hard disks that allow us to use different desktop operating systems and tool sets for forensic investigations. Many common hacking tools are available on the Internet for download, and these are used to demonstrate and assist students in creating secure defenses against outside attack. A lab assistant is dedicated to our school and was used to assist with configuration changes to the room and for imaging the removable drives. A critical component in developing courses that require "hands-on" exercises is the exclusive use of the lab for these courses. Due to the nature of the tools and the need to tear-down and rebuild the network during the course, the lab used for security classes should not be available to students outside the course.

3. ENSURING RESPONSIBILITY

Early in our development of the curriculum we found resistance to the program when it became known that we would be discussing the methodology of hacking into a network. There was considerable discussion at the university curriculum committee about the course content and the issue of teaching something potentially dangerous to a company's (or university's) security. We have also had at least one complaint from a business that hires our students as interns voicing the concern that the training in information security provided too great a risk for a student left alone with a network. Our solution to

these concerns has been to stress in the final capstone course the ethics required of security practitioners, to discuss case studies of successful prosecution of cyber-criminals and hackers, and to require completion of a criminal justice course that emphasizes the legal consequences of cyber-crime.

We believe that the content needs to be carefully designed to provide the technical background required by the discipline but without a specific focus on simply refining hacking skills. Implementing an undergraduate emphasis will require addressing the distrust of others that the course will provide a sandbox for hacking and assist in perfecting criminal skills sets. Arguments that teaching information security content at the undergraduate level is educating hackers can be countered by:

- Offering an ethics component (we suggest using the ISC² principles for security professionals and the ACM Code of Ethics and Professional Conduct) and requiring students to sign a statement of ethics
- Placing information security as a last course (senior capstone) to train students that have matured in the curriculum
- Requiring pre-requisites to courses that include network security content to discourage outside attendance by those that could use the information improperly
- Including criminal justice courses in procedures, law, and privacy to improve a student's understanding of the legal process for criminal prosecution
- Using case studies of prosecutions to teach, not only the methods of entry and detection, but legal outcomes.

Perhaps the reason for so few undergraduate level courses in information security is an unwillingness to provide screening of student attendees for maturity, the potential risk to the university infrastructure, and the ability to supervise student activities. Graduate courses may be preferred for program offerings in information security because they can be taught at a higher level (avoiding the risky issue of hands-on practice of hacker tools) and they can be offered to a select population through enrollment in a master's degree program.

The U.S. government has helped to make the security profession visible and attractive by offering scholarships to high school students for undergraduate training in order for them to pursue security as a career option and to provide skilled technical security professionals for government jobs (Saita, 2002). These initiatives, connected with Homeland Security, appear to be aimed at training our IT student population in this skill set at the earliest possible point in their collegiate education—the undergraduate level. There is additional effort required to design and offer courses in information

security to undergraduate IT majors. Creating a robust program of information security at the undergraduate level will ensure a population of skilled IT practitioners that are able to administer security policies as systems/network engineers and fulfill the need for qualified security professionals for employment in both the public and private sectors.

4. COLLABORATION WITH CRIMINAL JUSTICE

We have forged a successful collaboration with the criminal justice department at WSU for this emphasis in information security. Criminal justice has traditionally been focused on the sociological aspects of crime research and police work. With more cases being prosecuted based on electronic data discovery (Radcliff, 2002b) there is a need for collaboration of criminal justice and information technology. The report from Dartmouth University in June 2002 on assessing the needs of law enforcement in the area of security education found that 90% of the responders surveyed stated that the need for additional training was urgent (Vatis, 2002). Offering an undergraduate emphasis in information security that cross-lists courses in information systems and criminal justice would enable students interested in careers in law enforcement to acquire the needed skill set.

Our information security emphasis requires an upper division criminal justice course in Computer Crime (CJ 3130) as a prerequisite to the senior capstone course in the program. Students learn the law with respect to investigation, search and seizure, prosecution, and privacy. They have the opportunity to explore cases that have been successfully prosecuted and to understand how the evidence was constructed and presented at trial. Additionally, the criminal justice department and IS&T are discussing a joint masters certification in information security that will benefit both MBA and graduate students in the criminal justice department.

5. OUTCOMES

The Information Security emphasis graduated the first majors in 2002 and has proved a popular emphasis despite requiring one course more than the software emphasis.

The reality of the Utah job market for students at Weber State University is that their employment options will be limited to small or medium size companies that are able to hire two or three network administrators and require them not only to provide network management, but to implement security correctly on the network, within applications, and the desktop, as well as to provide recommendations for security policies and procedures. Students without training in information security will not be prepared for the expanded role expected of them as network administrators by their future employers.

Additionally, providing information security education only at the graduate level requires students to attend graduate school (an expensive and lengthy endeavor) in order to learn the information security skills.

The information security emphasis is a critical component in the information technology major. Students receive training that prepares them for both an informed security role as a junior network administrator and for a management role in implementing security. Universities seeking to provide this training should carefully plan for the costs of implementation which includes a specialized lab with hardware and software. Additionally, a robust program of courses in information security topics will require faculty who have had significant practical experience in information security. In order to implement a program similar to WSU, adjunct faculty may need to be recruited or funding for additional training to existing faculty may be required.

6. CONCLUSIONS

Information security is a critical component of an information technology education. Students at the undergraduate level represent the audience most likely to implement and manage a complex network, application, and desktop environment. Offering a program in information security to undergraduate students will meet the current need for trained security professionals. Universities should consider including an undergraduate emphasis in information security that provides a rigorous technical approach, discussion of security as a business strategy within information technology, and provides for an examination of the ethical issues necessary for professionals in this field. Providing a comprehensive emphasis at the undergraduate level insures that IT students will be able to serve a role in implementing security and providing the secure infrastructure required to resist costly intrusions and business losses.

7. REFERENCES

- Radcliff, D. [2002a], "Clarke Warns Educators about Need for Better Security", Computerworld, <http://www.computerworld.com/security/securitytopics/security/story/0,10801,71714,00.html> [Accessed June 5, 2002].
- Radcliff, D. [2002b], "Cybersleuthing Solves the Case", Computerworld, http://www.computerworld.com/cwi/Printer...y_Version/0,1212,NAV47_STO67299-,00.htm [Accessed April 9, 2002].
- Saita, A. [2002], "Bridging the Gap," InfoSecurity Magazine, www.infosecuritymag.com/2002/apr/infosecprofession.shtml, [Accessed July, 2002].
- Suydam, M [1999], "Tapping the Security Job Market", Information Security, October 1999, pp.40-44.
- Vatis, Michael, "Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A

National Needs Assessment", Institute for security Technology Studies at Dartmouth College, June, 2002.

- Weisman, R.[2002], "The Heart of a Killer Network Security System", NewsFactor Network, <http://www.newsfactor.com/perl/story/17321.htm> [Accessed April 18, 2002].

AUTHOR BIOGRAPHY

Patricia Y. Logan is an associate professor in information systems and technologies at Weber State University. She has worked in the field of information technology management for over fifteen years. Dr. Logan held senior IT management positions in the banking and insurance industries. Her primary teaching responsibilities include data communications, networks, information security, and information systems management. She is content director for a graduate program in chief information security officer training www.weber.edu/CISO.

