Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

Secure "Information at Your Fingertips" -- Just One Course can Help

Keyu Jiang, Mark Bannister, *Fort Hays State University*

Abstract – This article briefly explains the motive, purpose, feasibility and vision of creating an introductory information assurance course serving not only students seeking to become INFOSEC professionals, but which also reaches out to students from such diverse academic areas as Accounting, Business Administration, Education, and Criminal Justice to provide fundamental knowledge and skills. This course has been successfully mapped to meet 100% of the requirements of National Security Telecommunications and Information Systems Security (NSTISS) standards 4011 and 4013E.

Index terms – Information Assurance, Education, NSTISS 4011, 4013, Certificate.

I. Introduction

As defined in the National Training Program for Information Security Systems Professionals, Information systems security (INFOSEC) is "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats [1]."

According to 2006 Global Information Security Workforce Study, the number of information security professionals in America is projected to reach 0.8 million in 2010, a 6.4 percent compound annual growth rate from 2005 [2]. Despite the growth in the number of professionals, the study notes that both direct employers and "providers of security services are also challenged to find appropriate candidates for vacancies within their security workforces [2]."

The impact of a shortage of INFOSEC professionals can be profound. A simple illustration is the example of a school with three hundred network users paralyzed while waiting for assistance from one INFOSEC professional. Financial institutions, medical providers, small businesses, law enforcement, governmental organizations and many other entities are even more dependent upon maintaining information security and availability. In addition to facing a shortage of talent, cost is another barrier to effective information protection and use when depending heavily on INFOSEC professionals. Even if the gap between supply and demand is closed by increasing the number of available INFOSEC professionals in the workforce, the question arises as to whether employers can financially expand reliance on INFOSEC professionals. On average, more than 41% of information security budgets are spent on personnel, including salaries and benefits, and education and training [2].

The greater the knowledge that accountants, small business owners, teachers, law enforcement personnel, etc. have of information security principles and tools, the more self-reliant these professionals can be in their professional activities. Finally, individual users, from five-year-olds to eighty-five-year-olds, cannot live without Internet-based platforms. Therefore, we present the question: Should educators create an opportunity for individuals to have introductory Information Assurance education in order to protect their own information?

Curriculum designed for INFOSEC professionals has the luxury of distributing key concepts and principles over a sequence of multiple courses. A sequence of coursework is often not plausible for students from other majors seeking basic information assurance knowledge and skills. Therefore faculty at the university created a course that can serve as an introductory course for future INFOSEC professionals and as an awareness level course for students from other disciplines. In effect, this course is designed for the public instead of the expert. Our belief is this strategy may provide the greatest economic benefit to employers seeking to counter information threats.

II. The Trend of Information Interconnectedness and Globalization Creates the Need for an Awareness Course

Thanks to the transition from a PC-based computer platform to an Internet-based platform, we are living in the new generation of the Cyber World. The value of computers and computing devices lies substantially in their interconnection. This concept is described in Metcalfe's law, stating that a network becomes geometrically more valuable as it reaches more users [3].

A recent ComScore Networks study showed that the

quantity of net citizens over 15 years of age numbered 153 million in the United States and 747 million worldwide in 2007 [4]. If younger teenagers and children are taken into account, the figure will be larger. Interconnection allows the movement of vast amounts of data enhancing productivity and providing substantial economic and social benefits. Interconnection and use of a multitude of software and hardware tools create a multitude of information vulnerabilities. Both physical and logical securities are at risk, which mean that security becomes every user's social responsibility. On one hand, an individual in one of many various industry fields who lacks information security awareness may be a frail target of hackers and is vulnerable to losing money, private information or even being used by hackers without notice in a way that puts the user or the organization at risk. Systems can be risked through ignorance as a user inserts a CD, or attaches thumb drive or MP3 player behind the corporate firewall. On the other hand, individuals -- especially teenagers, may be driven by pure curiosity to offend another individual's privacy or to intrude into organizational networks. Irresponsible acts may even threaten a nation's security. These factors point to the need to inform IT users and consumers of the need to take fundamental steps to protect digital assets. They also point to the need to arouse ethical and legal consciousness. Both domestically and internationally, effective electronic commerce, business execution, education, health care, delivery of government services, and even electronic entertainment is dependent on users' capabilities to protect themselves and in discouraging threatening activities.

As noted by Ellen Roth-Perreault and Brenda Oldfield, at present, courseware to prepare information security professionals is offered by over one hundred universities and/or institutes in America [5]. Curriculum designed to prepare INFOSEC professionals is typically multiple course and unavailable to the end user who is suffering from real information threats (e.g., fraud, hostile intelligence service, malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring). The challenge to post secondary (and perhaps secondary education) is whether information assurance education and training is reserved for the traditional Information Security professional or can it be expanded to end users, the weakest linkage of the Internet-based platform?

III. Statistic Data of Information Security Workforce Supports the Call for One Course

We propose classifying users in five categories based upon their knowledge of information security:

- Security Innocent End User – little to no knowledge of information security.
- Security Know-how End User – awareness of key concepts, practices, and principles.
- Information Security Worker – an INFOSEC professional with a depth of academic preparation and/or industry training and certifications.
- Information Security Researcher – an INFOSEC professional conducting research and rising above implementation to development of theories, practices, and tools for information security protection.
- Information Security Faculty – an INFOSEC professional conducting research, developing theories, practices, tools, and educating others on information security.

We hereby boldly forecast that future information security knowledge buildup will be like table below:

Year / Increased Percentage (%) / Personnel	2007	2017	2037
Security Innocent End User	0	-9.5	-60
Security Know-how End User	0	9095	67641
Information Security Worker	0	397.5	150
Information Security Researcher	0	-42.9	-28.6
Information Security Faculty	0	0	9

The above data is based on the IDC study on 2006 Global Information Security Workforce Study.

Our assumption is that as the mainframe computer was once monopolized by a unique group of highly educated users who were displaced by a sea of personal computer users, information security will move from being the responsibility and tool of a handful of specialized INFOSEC professionals to being a common practice among users from a variety of professions. These will be "Security Know-how End Users." INFOSEC professionals will move to performing higher level strategic activities within an organization.

IV. Yesterday, Today and Tomorrow' One Course

The Department of Information Networking and Telecommunications decided to design an information security course to first be offered in 2004. The course entitled INT 684 Foundations of Information Systems

Security initially was to be offered solely to Information Networking and Telecommunications students. In consultation with a team of full-time faculty, an adjunct faculty member with extensive military intelligence and information security experience created the initial course design. The faculty team decided that the course's learning objectives would be modeled on the Certified Information Systems Security Professional (CISSP) 10 Common Body of Knowledge (CBK) Domains. The class would be offered to upper division undergraduate students and to graduate students.

The CBK Domains include [6]:
Access Control Systems and Methodology
Telecommunications and Network Security
Security Management Practices
Applications and Systems Development Security
Cryptography
Security Architecture and Models
Operations Security
Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
Laws, Investigation, and Ethics
Physical Security

After the faculty began to offer multiple information security courses and had developed concentrations in Information Assurance, the department and university decided to certify curriculum under the Committee on National Security Systems (CNSS) National Standards 4011 and 4013E. The faculty provided syllabi and course materials from several courses to its consultant. The consultant began mapping with the introductory course and to her surprise and to the pleasure of the faculty found that this course systematically met all of the 4011 and 4013E Standards. These standards are:

Information Systems Security (INFOSEC) Professionals, NSTISSI 4011
Communications Basics (Awareness Level)
Automated Information Systems (AIS) Basics (Awareness Level)
Security Basics (Awareness Level)
NSTISS Basics (Awareness Level)
Systems Operating Environment (Awareness Level)
NSTISS Planning and Management (Performance Level)
NSTISS Policies and Procedures (Performance Level) [7]

System Administrators (SA), CNSSI 4013E
Function 1 – Secure use
Function 2 - Incidents
Function 3- Configuration
Function 4 – Anomalies and Integrity
Function 5 - Administration [8]

On February 22, 2008, the university received notice from the National Security Administration (NSA) Information Assurance Center of Excellence Program Manager that the curriculum has been certified as mapping 100% to the Committee on National Security Systems (CNSS) National Standards 4011 and 4013E.

In the course's first offerings from 2004 to 2006, the course was offered simply as an upper division elective in Computer Networking and Telecommunications. Faculty made three curricular changes prior to the 2007 fall semester. First, the course was incorporated in a concentration at both the undergraduate and the master's level. Secondly, it was opened to students other than those seeking to be INFOSEC professionals. Finally, the initial pre-requisites of nine credit hours of Internetworking classes were dropped. The only remaining prerequisite is MIS 101 Introduction to Computer Systems a basic general education computing fundamentals course required of all university students. The Department of Justices Studies and the Department of Accounting and Information Systems at the university are now interested in using Foundations of Information Systems Security as a master's level elective course.

From 2004 to 2007, a total of 52 students enrolled in this course. Eleven students enrolled for the fall 2007 semester. Most of the fall 2007 students were from non-information security majors and had limited to no information security knowledge background. Eighty-two percent of students passed the course. Twenty-two percent earned a grade of an "A" and forty-four percent earned a grade of a "B." A few excellent students after completing this course choose to pursue their study as security professionals for additional education and training in the areas of information risk management, business continuity/disaster recovery planning, and forensics. Students evaluated the course using a locally developed evaluation tool. Student evaluations were uniformly positive. Much of student feedback from the course relates that students believe it will help them as a useful tool in their professional and personal lives.

What we should contribute now or in the future through one course? Information Security Science or Information Assurance is a relatively new, very dynamic and rapidly changing subject, which makes it very interesting and challenging to teach and learn. We expect this course to evolve as the CISSP, NSTISSI 4011, and CNSSI 4013E standards evolve. The highest priority of the class is to establish a pattern of life-long learning so that graduates will continue to adopt systems and methodologies preventing and minimizing security risks. It will be effective in training the "Security Know-How End User" and will serve as a starting point for future INFOSEC professionals.

A current priority is that that the course should be widely available to the public through distance learning offerings

distributed by the university's Virtual College in addition to on campus offerings. Distance learning will help achieve the goal of providing access and reaching the current professional workforce. Web based distance learning is most the economically efficient and effective method of sharing and educating students in a geographically boundary free and time asynchronous manner. Students from remote areas can afford to join the course hosted by an accredited university thousands miles away. Through self-learning, group discussion and individual communication with the professor, students can be provided a quality learning experience.

V. Conclusion

Academic institutions have the opportunity to offer an effective information security survey course at the awareness level to help students who will enter professions other that INFOSEC to identify problems and risks, implement precautions and countermeasures, and evaluation individual behavior correctly, to boost the cyber world order.

VI. References

[1] The "National Training Program for Information Systems Security (INFOSEC) Professionals" 16 November 1992. http://www.cnss.gov/Assets/pdf/nstissd_501.pdf, Last Accessed: 1 March 2008.

[2] IDC, "White Paper 2006 Global Information Security Workforce Study." October 2006. https://www.isc2.org/download/workforcestudy06.pdf, Last Accessed: 2 March 2008.

[3] Robert Metcalfe, "Metcalfe's Law: A network becomes more valuable as it reaches more users," *Infoworld*, Oct. 2, 1995.

[4] ComScore "Measuring the Digital World" press release 6 March 2007. http://www.comscore.com/press/release.asp?press=1242, Last Accessed: 6 March 2008.

[5] Ellen Roth-Perreault and Brenda Oldfield, "Strengthening the Security Workforce: A Competency and Functional Framework for Information Technology Security Professionals," Proceedings of the 11th Colloquium for Information Systems Security Education, Boston, MA, June 4-7, 2007, ISBN 1-933510-96-7, pp22-27.

[6] Harris, Shon, (2005) All in One CISS, Exam Guide, 3rd Ed. (pp. 4-6).

[7] NSTISS. (1994). National Training Standard for Information Systems Security (INFOSEC) Professionals. [Online]. Available: http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf, Last Accessed: 8 March 2008.

[8] NSTISSI. (2004). Nation Information Assurance Training Standard for System Administrators (SA), [Online], Available: http://www.cnss.gov/Assets/pdf/cnssi_4013.pdf, Last Accessed: 8 March 2008.