Issues in Informing Science and Information Technology

A Perspective on Achieving Information Security Awareness

Mariana Hentea
Southwestern Oklahoma State University, Weatherford, USA

mariana.hentea@swosu.edu

Abstract

The guidelines “Towards a Culture of Security” emphasize a culture of security in all aspects of information systems, from designing and planning through to everyday use, and among all participants, from government down through business to consumers. In response to national needs, Information Security education has become a priority for many educational institutions in US for the past years. More universities and colleges have established courses or specialized programs to teach Information Security skills to students enrolled in degrees related to computers such as computer information systems, computer engineering, and computer science. However, there are aspects of the security education model that need attention. This paper discusses these issues including changes to improve security awareness education. Through close coordination between faculty, industry, government agencies, and universities, the critical education of future graduates, Information Technology professionals, Information Security professionals, and public can be accelerated.

Keywords: information security awareness, education, curriculum.

Overview

In 2002 the Organization for Economic Cooperation and Development (OECD) released the document “OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security” (OECD, 2002). This initiative calls for approaching information security globally, although only 30 countries are members of OECD (OECD, 2004a). United States (US) has been a member of OECD since 1961. This document marked a “new international understanding of the need to safeguard the information systems on which we increasingly depend for our life” (“OECD publishes,” 2002). The guidelines “Towards a Culture of Security” specify that Information Technology (IT) users have “to be aware of the need for security of information systems and networks”. After releasing the initial document, the OECD Working Party on Information Security and Privacy (WPISP) promoted implementation plans, revised plans, and monitored the efforts to promote a “Culture of Security” among all participants who develop, own, provide, manage, and use information systems and networks. The document emphasizes a culture of security in all aspects of information systems, from designing and planning through to everyday use, and among all participants, from government down through business to consumers. The guidelines promote nine principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. In addition, a Web site “Culture of Security” has been created to promote a global “culture of security”. In February 2003, the US government released the final version of the document "National Strategy to Secure Cyberspace" which lays out five public and private sector priorities. Among those priorities is "A national cyberspace security awareness and training program" (Goth, 2003). In June 2003, the US Department of Homeland Security created the National Cyber Security Division (NCSD) that supports creation of cyber security awareness programs for the US public and for various international communities.

However, recent worms, viruses, and denial of service attacks show that the Information Technology (IT) workforce is not prepared to handle such attacks because of "poor security awareness and training" (McConnell & Hamilton, 2002). According to the survey "Hacker Homelands" of third quarter in 2003 provided by Internet Security Systems Inc., approximately 84.95% of cyber attacks originate from North America ("Security log," 2003). Intruders known as hackers may be novices (called also script-kiddies) or vicious criminals. Statistics show that more than 90% of computer attacks are initiated by teenagers. These attacks make security education increasingly important in schools starting at a very early age. Many intruders use social engineering techniques to persuade someone to reveal access codes, passwords, or other confidential information. Threats, such as viruses spread via email, achieve their destructive goal through social engineering. "That is, by psychologically manipulating or tricking the user to do something" (Volonino & Robinson, 2004) quickly that maybe be very dangerous. The success of the mass spread of the ILoveYou virus is because of its attention grabbing email subject. In fact, social engineering is a collection of techniques used to fool the users. These techniques succeed well with uneducated users. In June 2004, the Internet intrusion called a scob attack "exploited a powerful new assault technique" that affected many Web sites (Leavitt, 2004, p. 16). This attack "has computer security officials worried that it could be a harbinger of worse things to come" and it has sent a signal that we can expect "scob-like attacks to become more targeted and sophisticated" in the future (Leavitt, 2004, p. 18). Leavitt (Leavitt, 2004, p. 18) advises that "the best proactive steps involve educating users, system administrators, and software manufacturers".

Although security awareness is one of the most effective security methods for the information security assurance, statistics indicate that the problem of Information Security Awareness is not resolved in all US organizations because many IT users lack the basic security training and organizations do not have the budgets or the strategies in place for training (Furnell, Warren & Dowland, 2003). Subsequent reports periodically released by OECD provide information about the progress made on the implementation of the guidelines for security of information systems and networks. The OECD report of June 2004 suggests the need for greater awareness and understanding of security issues. At the hearing of the House Science Committee of July 21, 2004, both experts and lawmakers agreed that availability of education is crucial for enhancing the nation's cyber security workforce (Reed, 2004).

The report of September 2004 (OECD, 2004b) containing a summary of responses to the survey on the implementation of the OECD guidelines, indicates that "awareness raising" is supported in US by common initiatives such as workshops, seminars, training, conferences and associated papers and studies, Web sites, mass media, telephone hotlines. In addition, the Federal Trade Commission (FTC) and the National Institute of Standards and Technology (NIST) promote awareness-raising initiatives (The NIST Handbook. SP 800-12, 1995) including guidelines for building security awareness program (The NIST Handbook. SP 800-50, 2003). Security awareness has to be promoted not only to IT users within organizational settings, but for all users that manipulate a computer and data for a job task or personal use. It is necessary to ensure that Information Security Awareness is achieved at all levels, government, private, and general public. Without a broad understanding of the problem of information security, users will continue to be the victims of cyber attacks. The standard RFC2828 promoted by Internet Engineering Task Force (IETF) defines Information Security as the set of measures taken to prevent the unauthorized use, modification, or denial of use of data (Internet Engineering Task Force [IETF], 2000). Security Awareness refers to owners, providers, users and other parties that should readily be able to gain knowledge about the information security, be aware of the importance of information security, and be consistent with maintaining security (The NIST Handbook. SP 800-14, 1996). Information Assurance is a procedure that ensures a system is developed and operated as intended by the system's security policy (IETF, 2000). Information security is a process and it "is in many ways a mindset" (Maiwald, 2004, p. 4).

In response to national needs, Information Security education became a priority for many educational institutions in the US for the past years. Many universities and colleges have established courses or specialized programs to teach Information Security skills to students enrolled in degrees related to computers such as computer information systems, computer engineering, and computer science. However, there are aspects of the education model that need further attention as described in the next section.

Information Security Awareness Education Issues

First, most universities teach one or more Information Security courses in the final year of undergraduate study or at the Masters level. This curriculum model is not efficient because students have already learned how to use computers without paying much attention to the basics of information security and computer ethics (Bintziou, Alexandris & Chrissikopoulos, 1999). It is becoming obvious that information security awareness has to be provided to students at an earlier age. If we teach children security awareness earlier, they will be prepared to pay attention to security matters as well as to avoid getting engaged in illegal behavior. In addition, education on information security awareness must be provided to teachers and parents. These are the most important people in the youngsters' lives. If we teach educators and parents how to handle information security issues and how to use computers, they will be better prepared to provide training to youngsters. A few OECD member countries have established education and training programs for youngsters. For example, Norway supports educational packages for elementary and middle schools (OECD, 2004b). Hungary is preparing to survey the educational field of informatics. Korea is supporting a "Study Material Contest" for elementary/middle/high-school teachers in preparation for providing a standard curriculum on security of information systems and networks. Hong Kong recognized that "schools become Hacking Centre" and published the document "Managing IT Security in Schools" to promote security programs in schools ("Managing," 2004). A program for introducing IT security awareness into the secondary education in Greece is discussed by at the 1st World Information Security for Education (Bintziou & Chrissikopoulos, 1999). In the US, the National Cyber Security Awareness (NCSA) agency launched a program during the National Cyber Security Awareness Month of October 2004. This initiative was structured in four week-long components – targeting Home Users in week one, Small Businesses in week two, Education audiences (K-12 and higher education) in week three, and focusing on Child Safety Online in week four. The mission for this initiative was to raise awareness of cyber security with the goal of persuading users to improve their cyber security preparedness. Top Ten Security Tips (a self test) was posted on the Web. The effectiveness of this program has yet to be seen.

Second, it is common that many disciplines of study in a higher education environment require students to use a computer to write essays, seek for information, store or process the results of experiments. Although computer literacy is included in the curriculum of the general education in more universities and colleges, Information Security education is not required or it is left at the student's choice. Very few universities teach a course on Information Security during first year of study, and this is mostly offered only to students enrolled in specialized computing programs.

Third, there is a need for the reinforcement of continuing education for the Information Technology (IT) users and IT professionals. Cyber security cost effectiveness, and impact on productivity and quality demand an assessment of the education and training needs of the Information Technology (IT) users and IT professionals. Continuing education is very important for the IT professional to keep up with emerging technologies and business demands for new technology knowledge and skills. As of September 2003, there were approximately 3.5 million employees hired in specific IT positions and more millions of employees perform significant functions using computers (Chabrow, 2003).

Fourth, there is no standard integration between information security topics and different topics taught for programs related to computing such as computer engineering, computer science, and computer information systems. Unfortunately, Information Assurance has not been a formal part of computer and information systems programs. It is also surprising that information security awareness is not a body of knowledge required by ABET even during the 2005-2006 Accreditation Cycle (ABET, 2004).

Fifth, the security professional entering the work force is expected to have more information security skills, and be more proficient in problem solving. Caputo and Kovacs surveyed professional corporate IT professionals in a regional corporate community to identify the technological skills considered essential to higher education curricular offerings (Caputo & Kovacs, 2004). The results of the survey should not surprise anyone. Information security skills are identified as a critical skill by 42% of large corporations, a key skill by 33% of small corporations, and a key skill by 48% of health care, government, and not-for-profit organizations. Information security skills were identified as presenting the most significant growth by a percentage of 71% while skills in Web services were ranked by 63% and database application skills ranked by 54% (Caputo & Kovacs, 2004). Studies indicate that university education in information security will be on the increase, both in terms of introductory courses and whole degree programs (Janczewski, 2004). Many universities offer programs in Information Security, but the areas of specialization in Information Security may be diverse. Although a common set of skills is desired, universities emphasize one or more areas of Information Security. Still there is no uniform curriculum or standard Common Body of Knowledge (CBK) for teaching Information Security professionals. Within government, the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC), developed a series of training standards (NSTISSC, 2004). The industrial sector (International Information Systems Security Certification Consortium, Inc.) has developed CBK for Information Systems Security certification. There is ongoing work to define a model curriculum promoted by a group of scholars within academia. It is becoming mandatory to have a uniform curriculum for Information Security Assurance programs. Although, there is a long term objective to produce a document similar to the Joint IEEE Computer Society/ACM Task Force document "Model Curricula for Computing" (Crowley, 2003) within academia, the release date of this document is not set.

In addition, minimum standards for security literature could benefit both governmental and educational institutions. A recent survey indicates that many books used for teaching computer security lack depth coverage of important concepts such as "cyber terrorism", which is a pressing issue nationally and globally (Prichard & MacDonald, 2004).

These issues affect the objectives and the means to achieve better Information Security Awareness. The following section discusses Information Security Awareness Education needs.

Information Security Awareness Education Needs

Significant changes to security education and training are needed and should be expected because IT is growing rapidly and new applications and security technologies are emerging. The new trend is toward more unified networks and more secure networks, both public networks and home networks, as well as wireless networks and the Internet. Stajano and Anderson emphasize that "promoting awareness of the security issues that we face, will contribute to the deployment of a ubiquitous computing infrastructure designed to minimize the corresponding economic and social risks" (Stajano & Anderson, 2002).

Emerging patterns of growth in the information security disciplines must be identified through research, and then promptly integrated into curriculum. Higher education institutions have to update curricular offerings in response to corporate and government needs. The next section discusses a framework for changes to improve Information Security Awareness education in the universities.

Achieving Better Awareness Education in Information Security

Both IT professionals and non-IT professionals must understand Information Security Awareness. In order to achieve Information Security Awareness for future graduates, it is necessary to introduce at least one introductory course "Fundamentals of Information Security" to teach basic security awareness methods to all students enrolled in a university or college program. The future graduates will make up the work force that is required to have skills in information security. This course must be introduced in the first year of study. The course is a comprehensive coverage of important concepts related to threats and vulnerabilities, protection (authorization, access control, and privacy integrity), detection (accountability), response and recovery (availability), security technologies, managerial policies, and legal and ethical issues. With the introduction of biometric devices into various sectors of economy, there should be more education on this technology (Moody, 2004). More education and simple tips on how users should choose and manage passwords may avoid the problem of weak passwords, human errors, and exposure to intruders (Carstens, McCauley-Bell, & DeMara, 2004). The course has to be based on the model of teaching students a combination of theoretical concepts and hands on practice of security. To achieve a broad Information Security Awareness, changes to the education requirements are needed. Recently, the United States Military Academy introduced Information Assurance education as a critical component for all graduates (Conti, Hill, Alford, & Ragsdale, 2003; Schumacher & Welch, 2002).

IT professionals need to design and use systems that implement security measures. At the Congressional Hearings on Intelligence & Security in January 1997, Spafford's testimony emphasized that "To ensure safe computing, the security (and other desirable properties) must be designed in from the start. To do that, we need to be sure all of our students understand the many concerns of security, privacy, integrity, and reliability" (Spafford, 1997). Knowledge and skills in security issues are required in any IT position regardless of job focus in either one or more of the following areas: analysis, programming, systems engineering, software engineering, system administration, network administrator, database specialist, web developer, etc.

Within academia, scholars argue how to teach information security and what curricula to follow. Yasinsac mentions that Information Security curricula within Computer Science departments have to meet diverse needs of the federal government, industry, and academia (Yasinsac, 2002). Vaughn and Boggess (1999) emphasize that "the computer science community has an obligation to train its graduates in known protection requirements, causes, vulnerabilities, current research, needed research, and to some extent, computing ethics". Byrne and Staehr stress the importance of teaching computer ethics in undergraduate curricula as well as designing strategies to evaluate the success of these programs (Byrne & Staehr, 2004). These issues imply that Computer Science and Computer Information Systems curricula have to be updated to "match the latest developments of computing technologies in the past decade and endure through the next decade" (Piner, 2001, p. 75). It is observed that teaching Information Security is a "difficult course" (Yurcik & Doss, 2004) and finding the best approach for helping students learn is the key (Crowley, 2003). A combination of traditional lecture approach with laboratory projects enables students to become more interested and active in analyzing problems (Bishop, 2002; Hentea & Conners, 2003; Hill, Carver, Humphries, & Pooch, 2004; Labruyere & Knight, 2004; Pandya & Frazin, 2004). Techniques for teaching the subject are in their infancy, and there is a clear need to accelerate the development of pedagogical tools and teaching techniques so that graduates will be prepared as information professionals to avoid and defend against such attacks.

In addition, parallel efforts have been recognized within academia to define the Common Body of Knowledge (CBK) for Information Systems Security professionals as well as to define a model curriculum for Information Security Education for students enrolled in computer science and computer engineering (Crowley, 2003; Davis & Dark, 2003). A similar model curriculum for the undergraduate computer science and information systems majors was proposed by Whitman and Mattord (2004). This model curriculum is currently used for teaching students enrolled at Kennesaw State University, Georgia. Crowley (2003) proposes a graduate specialization in Security consisting of four three credit hour courses that have to be certified by National Security Agency (NSA) for conformance to 4011 standards.

However, there is no uniform curriculum or standard CBK for teaching Information Security at the undergraduate level. There is a long term objective to produce a document similar to the Joint IEEE Computer Society/ACM Task Force document "Model Curricula for Computing." There should be more efforts to accelerate the process of defining the Common Body of Knowledge (CBK) for Information Systems Security to educate students enrolled in computing disciplines as well as other disciplines. Within academia it is necessary to define a model curriculum for Information Security Awareness Education that is recognized by corporations, government, public, and accreditation agencies. The following subsection discusses specific topics of Information Security Awareness that could be integrated within different courses to improve Information Security curricula.

Examples of Changes and Outlines

Information Security Awareness is not only about defense, it is about skills in designing and programming with security protection. The security professional that enters the work force is expected to have more skills and be more proficient in problem solving skills. The next-generation networks are going to need management systems that move beyond simply fixing problems and monitoring quality of service. The future IT professional will need to use sophisticated tools for management, decision making, and prediction. The management employee of the future needs to be able to control security services and traffic loads, predict network performance in a given situation, and optimize service levels on a continuous basis. Decision making processes that determine security policies, traffic engineering, routing, device loads, service levels, and restoration under failure scenarios will require use of predictive network management tools (Monahan, 2003; Sykes, 2001) based on simulation capabilities.

Based on these requirements, education institutions have to provide consistent teaching of knowledge and skills on Information Security Awareness. This can be accomplished only by including and keeping records of the OUTLINE FOR EDUCATION ON INFORMATION SECURITY as a component for each course offered. Security concepts were included in the undergraduate computer science curriculum at the University of Maryland Baltimore County (Cress, Roberts, &

Simons, 2003). The educators included so called defensive programming concepts within the framework of four classes (Computer Science I, Computer Science II, Data Structures, and Software Engineering). A set of security concepts are added as learning modules in the existing courses to expose the students early and often in their coursework.

Education of computer engineering, computer science, and computer information systems professionals can provide software development skills in security issues as they relate to each concept taught in undergraduate programs. It is necessary to teach students the development of applications and systems with built-in application and system level security. In addition, it is necessary to teach students programming skills for the implementation of the important protocols such as TCP/IP and Web protocols. Programming exercises and projects to design software for the IP, TCP, UDP and application level protocols can be included in the operating system, script programming, and network courses.

At the software development level, a professional needs knowledge of

- Behavior of viruses and other malicious programs
- Overview of TCP/IP and other network protocols
- Cryptographic algorithms, protocols, and standards
- Methodology for the development of a secure, or trusted, distributed system
- Analysis and design of security requirements
- Access controls, authorization, and permissions for data, files, and databases
- Security vulnerabilities and protection for different OS platforms (Windows, Linux, Unix, VxWorks, HP-Unix, Sun Solaris, etc)
- Open standards
- Freeware and open source
- Ethics and social responsibility in the information age.

Programming classes should include assignments for avoiding buffer overflow, malicious programs, behavior of viruses, cryptographic algorithms, etc. For example, the Open Source library contains a collection of C and C++ functions that can be used for teaching programming with security protection. Also, visual programming tools offer kits for smart card programming (smart cards are key technology for e-commerce). Script programming (Java, Linux, etc.) courses can use toolkits to demonstrate the secure messaging protocols.

Students need to understand and practice good programming techniques to avoid format-string bugs, heap-based memory corruption bugs, or integer errors (Wheeler, 2003). These types of errors create vulnerabilities that are easily exploited by intruders. There is a “rising threat of vulnerabilities due to integer errors” (Ahmad, 2003) and programmers should know how to prevent this threat. In addition, information systems courses must emphasize e-commerce and e-service security requirements, design, and implementation. The architecture for secure transmission of data between e-services has to be provided before any e-service is implemented and methodologies for the development of trusted information systems must be followed when the information system is built (Fugini & Plebani, 2003). Web development courses should include security protocols (HTTPS, S-HTTP, PCT, PGP, secure APIs), regulations for security. On the other hand, it becomes difficult to teach these technical concepts in Information Security courses only because students cannot understand all the details.

Conclusion

Accreditation agencies for Information Security Assurance provide input and guidance in assessing and implementing academic curricula. Through close coordination between faculty, industry, government agencies, and universities, the critical education of future graduates, IT professionals, Information Security professionals, and the public can be accelerated.

Besides providing courses in Information Security, institutions that provide education in computing must teach their students security software development skills. Educators could provide teaching modules on Information Security Awareness as components to be included in each course offered that deals with computers and information. Also, more efforts should be focused on accelerating the process of defining the Common Body of Knowledge (CBK) for Information Systems Security as well as on defining a model curriculum for Information Security Education and Training.

References

ABET. (2004, November 1). *Accreditation criteria 2005-2006*. Retrieved on November 12, 2004 from http://www.abet.org/images/Criteria/C001%2005-06%20CAC%20Criteria%2011-29-04.pdf

Ahmad, D. (2003). The rising threat of vulnerabilities due to integer errors. *IEEE Security & Privacy, 1* (4), 77-82.

Bintziou, A., Alexandris, N., & Chrissikopoulos, V. (1999). Introducing IT-security awareness in schools: the Greek case, *IFIP WG 11.8 1st World Conference on Information Security Education WISE1,* (Stockholm, Sweden). Retrieved on October 2, 2004 from http://citeseer.ist.psu.edu/correct/460292

Bishop, M. (2002). Computer security education: training, scholarship, and research. *Security&Privacy Suplement to IEEE Computer Society*, *35* (1), 30-32.

Byrne, G.J. & Staehr, L.J. (2004). The evaluation of a computer ethics program. *Journal of Issues in Informing Science and Information Technology, 1,* 935-939.

Caputo, D. & Kovacs, P. (2004). Identifying the critical information technology skills, functions and business intelligence parameters assessed by regional corporate community. *Proceedings of 2004 International Resource Management Association* (New Orleans, Louisiana), 280-283. Idea Group Inc.

Carstens, D.S., McCauley-Bell, P.R. & DeMara, R.F. (2004). Evaluation of the human impact of password authentication Practices on Information Security. *Informing Science Journal*, *7*, 67-85. Retrieved from http://inform.nu/Articles/Vol7/v7p067-085-229.pdf

Chabrow, E. (2003, October 20). Jobless recovery. *InformationWeek*.

Conti, G., Hill, J., Alford, K. & Ragsdale, D. (2003). A comprehensive undergraduate information assurance program. In C. Irvine & H. Armstrong (Eds.), *Security Education and Critical Infrastructures IFIP TC11/WG11.8 Third Annual World Conference on Information Security Education (WISE3)*, (pp 243-260), Monterey, California. Kluwer Academic Publishers.

Cress, D., Roberts, B. & Simons, J. (2003). A strategy to integrate defensive programming into the undergraduate computer science curriculum at UMBC. Retrieved December 3, 2004 from http://www.cs.umbc.edu/~cress1/ia/Deliverables/Final-Report

Crowley, E. (2003). Information security curricula development. *Proceedings of CITC4 2003*, (West Lafayette, Indiana), 249-255.

Davis, J. & Dark, M. (2003). Defining a curriculum framework in information assurance and security. *Proceedings of the* 2003 *ASEE Annual Conference* (Nashville, Tenesse) 2003. Retrieved November 16, 2004 from http://www.ee.iastate.edu/~davis/papers/ASEE-6-2003.pdf

Fugini, M.G. & Plebani, P. (2003). A methodology for developing trusted information systems: The security requirements analysis phase. In R. Azari (Ed.), *Current Security Management & Ethical Issues of Information Technology*. Hershey, PA: IRM Press.

Furnell, S.M., Warren, A.G. & Dowland, P.S. (2003). Improving security awareness through computer-based training. In C. Irvine & H. Armstrong (Eds.), *Security Education and Critical Infrastructures IFIP TC11/WG11.8 Third Annual World Conference on Information Security Education (WISE3)* (Monterey, California), 287-302. Kluwer Academic Publishers.

Goth, G. (2003). Questions about strategy to secure cyberspace. *IEEE Security & Privacy*, *1* (3), 8-9.

Hentea, M. & Conners, S. (2003). Network security course model. *Proceedings of Information Resources Management Association International Conference* (Philadelphia, Pennsylvania), 800-803.

Hill, J.M. D., Carver, C.A.Jr., Humphries, J.W., & Pooch, U.W. (2004). *Using an isolated network laboratory to teach advanced networks and security*. Retrieved on October 15, 2004 from http://citeseer.nj.nec.com/499204.html

Internet Engineering Task Force [IETF]. (2000). *Internet security glossary*. Retrieved on October 30, 2004 from http://www.ietf.org/rfc/rfc2828.txt?number=2828

Janczewski, L.J. (2004). University training in information security. *Proceedings of 2004 International Resource Management Association* (New Orleans, Louisiana), 1003-1005. Idea Group.

Labruyere, J.P. & Knight, L.V. (2004). Designing a controlled environment for the simulation of an enterprise security infrastructure. *Proceedings of 2004 International Resource Management Association* (New Orleans, Louisiana), 29-32. Idea Group.

Leavitt, N. (2004). Scob attack: a sign of bad things to come? *IEEE Computer, 37* (9), 16-18.

Managing IT security in schools. (2003). Retrieved on November 8, 2004 from http://www.ited.emb.gov.hk

Maiwald, E. (2004). *Fundamentals of Network Security*. New York :McGraw-Hill Technology Education.

McConnell, M. & Hamilton, B.A. (2002). Information assurance in the twenty-first century. *Security&Privacy Suplement to IEEE Computer Society*, *35* (1), 16-19.

Moody, J. (2004). Public perceptions of biometric devices: The effect of misinformation on acceptance and use. *Journal of Issues in Informing Science and Information Technology, 1*, 753-761.

Monahan, B. (2003). From security protocols to systems security: Making a case for systems security modeling. Retrieved on September 29, 2004 from http://www.hpl.hp.com/techreports/2003/HPL-2003-147.pdf

NSTISSC. (2004). Retrieved on November 3, 2004 from http://www.nstissc.gov/html/library.html

OECD. (2002). *OECD guidelines for the security of information systems and networks: Towards a culture of security*. Retrieved on October 2, 2004 from http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

OECD. (2004a). *OECD member countries*. Retrieved on October 15, 2004 from http://www.oecd.org/document/58/0,2340,en_2649_201185_1889402_1_1_1_1,00.html

OECD. (2004b).*Summary of responses to the survey on the implementation of the OECD guidelines for the security of information systems and networks: Towards a culture of security*. Retrieved on October 30, 2004 from http://www.oecd.org/sti/security-privacy

OECD publishes cyber-security guidelines. (2002). *ITworld.com.* Retrieved on November 15, 2004 from http://www.itworld.com/Sec/2052/020808oecd/

Pandya, P. & Frazin, R. (2004). Information Security Management: A research project. *Journal of Issues in Informing Science and Information Technology, 1*, 1065-1072.

Piner, M-L. G. (2001). Defining computing curricula for the modern age. *IEEE Computer, 34* (6), 75-77.

Prichard, J.J. & MacDonald, L.E. (2004). Cyber terrorism: A study of the extent of coverage in computer Security Textbooks. *Journal of Information Technology Education, 3*, 279-289.

Reed, M.A.T. (2004). Experts: Cybersecurity needs education, standards, partnerships. *Federal Computer Week.* Retrieved November 15, 2004, from http://www.fcw.com/fcw/articles/2004/0719/web-cybersec-07-21-04.asp

Schumacher, J. & Welch, D. (2002). Educating leaders in information assurance. *IEEE Transactions on Education, 45* (2), 194-201.

Security log. (2003, November 23). *Computerworld.* Retrieved on December 8, 2004 from http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C87365%2C00.html?f=x73

Spafford, E.H. (1997). One view of a critical national need: Support for information security education and research. Retrieved on December 2, 2004 from http://www.fas.org/irp/congress/1997_hr/h970211s.htm

Stajano, F. & Anderson, R. (2002). The Resurrecting Duckling: Security Issues for Ubiquitous Computing. *Security&Privacy Suplement to IEEE Computer Society, 35* (1), 22-25.

Sykes, E. (2001). Simulations illuminate the new-wave network. *Fiber Systems Journal, 4,* 59-62.

The NIST Handbook. SP 800-12. (1995). An introduction to computer security: The NIST handbook. Retrieved on December 12, 2004 from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

The NIST Handbook. SP 800-14. (1996). Generally accepted principles and practices for securing information technology systems. Retrieved on December 12, 2004 from http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

The NIST Handbook. SP 800-50. (2003). Building an information technology security awareness and training program. Retrieved on December 12, 2004 from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Vaughn, R. & Bogess, J. (1999). Integration of computer security into the software engineering and computer science programs. *The Journal of Systems and Software, 49* (2-3), 149-153.

Volonino, L. & Robinson, S.R. (2004). *Principles and Practice of Information Security*. Upper Saddle River, New Jersey: Prentice Hall.

Yasinsac, A. (2002). Information security curricula in computer science departments: Theory and practice. Retrieved on November 2, 2004 from http://www.cs.fsu.edu/~yasinsac/Papers/Yas01b.pdf

Yurcik, W., & Doss, D. (2004). Different approaches in the teaching of information systems security. Retrieved on November 1, 2004 from http://colton.byuh.edu/isecon/2001/04a/Yurcik.Doss.sec.doc

Wheeler, D. (2003). Secure Programming for Linux and Unix HOWTO. Online. Retrieved on September 15, 2004 from http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html

Whitman, M.E. & Mattord, H.J. (2004). A model curriculum for programs of study in information security and assurance (draft). Retrieved on December 10, 2004 from http://infosec.kennesaw.edu/presentations/InfoSecCurriculumModel.pdf

Biography

Dr. **Mariana Hentea** is an Associate Professor in the Department of Computer Science and Information Systems at Southwestern Oklahoma State University. Dr. Hentea teaches courses in Information Security, data communications and networks. Prior to entering academia, Dr. Hentea designed networks and security systems for telecommunications industries and government. Her research interests are in the areas of computer and network security, wireless technologies, home networking, and use of Artificial Intelligence techniques for intrusion and prevention systems, network management, quality of service, and computer process control in manufacturing.