Towards Changes in Information Security Education

Mariana Hentea and Harpal S. Dhillon
Southwestern Oklahoma State University, Weatherford, USA

mariana.hentea@swosu.edu harpal.dhillon@swosu.edu

Manpreet Dhillon
George Washington University, Washington D.C, USA

dhillonm@gwu.edu

Executive Summary

In the ACM guidelines for curricula at educational institutions, the recommendations for Information Security Assurance (ISA) education do not specify the topics, courses, or sequence of courses. As a consequence, there are numerous ISA education models and curricula in existence at educational institutions around the world. Organizations employing ISA professionals generally base their assessment of an individual's skill level based on academic qualifications or certifications. While academic qualifications support broad knowledge and skills in general, professional certifications may be effective in a limited area of operations. Academic programs exposing the students to theoretical concepts and problem solving experience are critical for preparing graduates for jobs in the information security. The critical importance of information security curriculum at universities is stressed. Therefore, it is appropriate to evaluate the quality of academic information security programs and suggest changes or improvements in the curricula to ensure that undergraduates and graduates have gained the required skills after completing their studies.

Despite a variety of ISA curricula and diverse educational models, universities often fail to provide their graduates with skills demanded by employers. There is a big discrepancy between the levels of skills expected by employers and those the graduates have after completing their studies.

In U.S., many educational institutions defined the educational model and curricula based on standards and guidelines promoted by government or other organizations, resulting in numerous ISA education models and curricula. However, the focus is on practical, low level skills which are identified in various standards. Issues related to Information Security curricula include content, didactic methodology, and degrees in Information Security. In addition, ABET accreditation criteria of 2005-2006 for US computing programs (computer engineering, computer science, information systems) still do not include criteria for evaluating information security education. Information security education in other countries is briefly compared with the ISA educational programs in the U.S.

We identified that there is greater variation and flexibility in the ISA

Editor: Linda Knight

academic programs with universities located outside the U.S. Many universities offer sound curricula to focus on specific skills required for information security systems developers and information security managers. In nearly all countries, the ISA related research is sponsored by universities and "National Laboratories" that can be viewed as counterparts of NIST and NSF.

We briefly discuss changes to approaches, topics, resources, and courses. We discuss the implementation of an effective ISA curriculum based on the curriculum content, methodology, currency, and research. It is necessary to recognize that the curriculum content of an ISA program is multidisciplinary, with inter-related topics coming from computer science, computer engineering, mathematics, management, information systems, business, political science, psychology, sociology, and law. Specific topics should be included about securing critical infrastructure that covers all sectors (agriculture, food, water, public health, emergency services, government, defense, information and telecommunications, energy, transportation, banking and finance, chemical industries and hazardous materials, postal and shipping, monuments and icons).

As organizations build knowledge from a strategic, managerial, and operational perspective, universities and training organizations should teach skills that are mapping to these areas. Scholarly research should explore new technologies and new approaches to obtain more effective and long-term solutions. The timely dissemination and sharing of the results produced by ISA researchers in academic institutions is very desirable. ISA curriculum should cover courses and experiments involving Intelligent Systems and Artificial Intelligence techniques that support intelligent control of security and create the knowledge base for information security domain. Also, there is a need to incorporate ISA topics throughout undergraduate curricula for all computing disciplines. The selection of courses for an ISA program should be based on strategic knowledge because functions and knowledge areas that are of strategic importance, and critical to business of the enterprise, are less likely to be outsourced.

Finally, we suggest actions that should make the ISA curricula in the universities responsive to the needs of the general population and the industry in which graduates with ISA skills and specialization will be employed.

Information Security Education Overview

Non-availability of skilled staff has been identified as the third most significant cause of the failure of users of information technology to ensure the security of their physical assets and information (Furnell & Clarke, 2005). Organizations employing ISA professionals generally base their assessment of an individual's skill level on the following indicators:

- Academic qualifications leading to a diploma and/or degree.
- Professional Certifications (CISSP, SSCP, CISA, GISEC, etc.).
- Vendor-Specific Certifications (MCSE, CCSP, Comp TIA, Security +, TISIA, etc.).

Professional and vendor certifications in Information Security validate competencies and skills, but they are not replacing experience or education. While academic qualifications support broad knowledge and skills in general, professional certifications may be effective in a limited area of operations. Academic programs exposing the students to theoretical concepts and problem solving experience are critical for preparing graduates for jobs in the information security. The critical importance of information security curriculum at universities was stressed in (Irvine, Chin, & Fruickle, 1998) as follows:

> An educational system that cultivates an appropriate knowledge of computer security will increase the likelihood that the next generation of Information Technology (IT) workers will

have the background needed to design and develop systems that are engineered to be reliable and secure.

Many educational institutions defined the educational model and curricula based on standards and guidelines promoted by government or other organizations, resulting in numerous ISA education models and curricula. Despite a variety of ISA curricula and diverse educational models, universities often fail to graduate students with skills demanded by employers. Therefore, it is necessary to identify the issues and suggest changes in the curricula to ensure that undergraduates and graduates have gained required skills after completing their studies. We primarily focus on Information Security curricula issues in US, and outline a few distinctions from other parts of the world. We recognize that the international aspects of the Information Security curricula are too broad for a single paper to cover comprehensively. The remainder of the paper is organized in sections that review the ISA programs in US and evaluate the quality of academic information security programs including the requirements for an effective information security curricula implementation as well as future directions for more responsive curricula. In this paper, we suggest the actions that should make the ISA curricula in the universities responsive to the needs of the general population and the industry in which graduates with ISA skills and specialization will be employed.

Information Security Education in US

The National Institute of Standards and Technology (NIST) and the National Security Telecommunications and Information Systems Security Committee (NSTISSC), along with others, contributed to the guidelines for training and education. In addition, ISO 17799 Information Security Management standard of 2000 with additions in 2002 includes requirements for Information security education and training. NSTISSC directive established the requirement for all federal agencies to develop and implement education, training, and awareness programs for national security systems. The required knowledge areas known as Common Body Knowledge (CBK) were defined by International Systems Security Certification Consortium (ISC)². However, the focus is on practical, low level skills which are identified in various standards. In addition, Electronic Develop-A-Curriculum (EDACUM) program supports the development of a curriculum based on NSTISSI standards. Some colleges and universities have been certified to meet one or more NSTISSI standards. Table 1 depicts statistics about institutions where ISA curricula are certified to be in compliance with specific NSTISSI standards. Most universities support the lowest requirement based on NSTISSI 4011 standard. No university certifies higher level skills such as system security engineer and risk analyst that are vital to any organization.

Table 1: Number of universities supporting various skill categories

NSTISSI Standard (Year)	Skill Level	Number of Universities Certified
4011 (1994)	INFOSEC Professionals	53
4012 (1997)	Designated Approving Authority	19
4013 (1997)	Systems Administration in Information Systems Security	23
4014 (1997)	Information Systems Security Officers	12
4015 (2000)	Systems Certifiers	7
4016 (in preparation)	Risk Analyst	0
4017 (in preparation)	System Security Engineer	0

Table 2 shows the scope of ISA programs and the approximate number of institutions supporting ISA programs.

Table 2: Summary of ISA programs

Degree/Certification and/or ISA Activity	Number of Universities
PhD with Concentration in IA	7
MS with Concentration in IA	30
BS with Concentration in IA	22
AAS with Concentration in IA	**
Certificate Programs	22
Research Centers/Institutes	29
Advanced Laboratories	15
Partnerships between Schools	9
Scholarship Offerings in IA	19
Specialized Seminars/Workshops	13
Online Course Offerings	5

** Applied Associate of Science (AAS) degrees are offered by most two-year college degrees programs.

Certificate programs are offered by different entities. The knowledge and skills supported by these certifications are in general limited, and the employers' needs for expertise are not guaranteed. This situation results in hiring more individuals with different certificates causing an increase of costs. In this scenario, higher education institutions need to identify resources for improving the information security education for future work force. It is critical to analyze security education around globe and identify improvements to ISA curricula in universities. The following section is an overview of information security education in other countries.

Information Security Education in Other Countries

Compared with the ISA educational programs in the U.S., there is greater variation and flexibility in the ISA academic programs with universities located outside the U.S. In nearly all countries, the ISA related research is sponsored by universities and "National Laboratories" that can be viewed as counterparts of NIST and NSF. We provide a brief overview of the ISA programs in other countries/regions.

Europe

Because of the large number of nations in this region, there are no documented standards for ISA education in Europe. Studies show that approximately 119 undergraduate and graduate courses in ISA are being taught, resulting in considerable variation in curriculum content among universities (Manson & Curl, 2003; Rosseli, 2003). Several courses related to information security aspects such as legal issues and biometrics are being offered. In Russia, many universities have schools and departments for information security studies at undergraduate and graduate level. Specifically, many courses are focused on cryptography topics.

Other Parts of the World

In other regions of the world (Canada, Africa, Asia, Australia) there is a considerable diversity in considerations for creating ISA curricula and strategies for implementing the curricula. While many universities offer ISA education through stand-alone courses, a majority of universities cover ISA related issues as parts of courses that are centered on generic hardware/software and systems design topics. In Australia, universities offer both postgraduate diplomas and a variety of master degrees for areas such as Internet Security Management, Commerce, Information Security and Computer Crime, Information Technology Security, Security Risk Management, Forensic Computing (Armstrong & Jayaratna, 2002; Stevens & Jamieson, 2002). The master programs require a suite of security courses from eight to twelve courses for one year full-time or more years for part-time enrollment. The topics cover three areas of skills and knowledge: generic, specialist, and practical.

In Korea, many universities offer sound curricula to focus on specific skills required for information security systems developers and information security managers (K. Y. Kim & Surendran, 2002; S. Kim & Choi, 2002). Although the skill sets are mostly the same, there are some differences in the requirements for a specialization and programs are structured differently. These programs offer important skills required for any employer that needs to design and implement its own software applications and information needs as well as to manage the security infrastructure. More specific curriculum issues are discussed in next section.

Information Security Curriculum Issues

Although ACM provides guidelines for Computer Science, Information Systems, and Computer Engineering curricula used by educational institutions, the recommendations for Information Security Assurance do not specify the topics, courses, or sequence of courses. This situation resulted in different education models and curricula and many institutions around the world continue to change or define new educational models and curricula. Issues related to Information Security curricula include content, didactic methodology, and degrees in Information Security. In addition, ABET accreditation criteria of 2005-2006 for US computing programs (computer engineering, computer science, information systems) still do not include criteria for evaluating information security education (Hentea, 2005b). Other issues are summarized as follows:

- Information Security Education supports basically federal government concerns with cyber infrastructure rather than a more generic set of skills needed by private industries and the public (Logan, 2002; Hentea, 2005b).
- Security architecture relies on the Orange Book criteria that advocate a perimeter of defense around a centralized system, which does not work in today's distributed computing environment (Paulson, 2002).
- The current ISECON undergraduate model curriculum in information systems is still focused on information systems (Manson & Curl, 2003).
- Many colleges and universities have codes of conduct such as plagiarism, snooping, piracy, and file-sharing, but these are not enforced.
- Teaching security is based on either defensive or offensive approach. The offensive approach allows students to understand how systems fail, but it also trains more hackers.
- Acceptance of teaching difficult topics such as cryptography is not the norm.
- Information Assurance cannot be viewed strictly as a Computer Science subset and scholars recommend that Information Security education should include both technical

and non-technical aspects. Scholars recognize that "interdisciplinary education" is a rising demand for combining the technical, social, and contextual aspects of security (Gritzalis, Theoharidou & Kalimeri, 2005). Efforts are underway to combine limited aspects of several disciplines such as information technology, law, political science, sociology, psychology, management, etc. However, the challenge is how to expand the disciplines interaction, and under which department the responsibilities should be managed.

In response to the shortcomings of education models based on NSTISSI standards, there are many attempts to define a curriculum for undergraduate and graduate programs. Examples include:

- Davis' curriculum framework based on what students should know and be able to do as information assurance practitioners (Davis &Dark, 2003).
- Whitman and Mattord's draft curriculum model complying with NSTISSI standards and hands-on laboratory projects (Whitman & Mattord, 2004).
- International conferences (WISE).
- Model based on interdisciplinary approach (Gritzalis, Theoharidou & Kalimeri, 2005) and industry needs (Smith, Kritzinger, Oosthuizen, & von Solms, 2005).

The model based on industry needs (Smith et al., 2005) identifies a CBK divided in two broad areas: technical knowledge (technical security controls, database security, programming, design) and tools; and non-technical aspects. This model is similar to Korean model for educating information security systems developers and information security managers (K.Y. Kim & Surendran, 2002; S. Kim & Choi, 2002). These specific curriculum frameworks can be consolidated and adopted by educational institutions to ensure the skills required by the employers. Scholars in academia argue that ISA education is distinct from training (Bishop, 2002). Therefore, it becomes necessary to evaluate the requirements for quality academic programs in the following section.

Effective Information Security Curriculum

We discuss the implementation of an effective ISA curriculum based on the curriculum content, methodology, currency, and research.

Curriculum Content

The university's mission is likely to be heavily influenced by the needs of the government, industry, and public. In addition, the emerging Information Technologies (IT) should guide the courses and activities in an ISA curriculum such that the list of courses and topics are enhanced beyond the comprehensive CBK to include domains such as E-Commerce, Multimedia, Ubiquitous and Pervasive computing, Wireless applications, Intelligent Information Technologies, Safety and Security, Software Assurance, Fault-tolerance and Survivability, Knowledge Management, etc.

Methodology for Implementing ISA Curriculum

A good balance must be maintained between the time and effort devoted to the study of theory and the time and effort associated with hands-on activities in the laboratory and/or in a real operational environment (i.e. Cooperative or Internship activities) as described in (Furnell & Clarke, 2005; Gritzalis, Theoharidou & Kalimeri, 2005; Hentea, 2005a). The adoption of courses that link theory and practice is vital for some courses offered for information security education such that "the individual acquires the ability to put theories into practice" (Hsu & Blackhouse, 2002). The emerging and growing field of computer and network forensics require designing undergraduate curricula and specialized laboratories to support multidisciplinary education of forensics profes-

sionals (Yasinsac, Erbacher, Marks, Politt, & Sommer, 2003). For institutions forced to implement new ISA programs with limited funding and other assets, it is feasible to operate an ISA program even on a low budget without degrading the scope and quality of instruction (Dhillon & Hentea, 2005).

Tactically, it is necessary to recognize that the curriculum content of an ISA program is multidisciplinary, with inter-related topics coming from computer science, computer engineering, mathematics, management, information systems, business, political science, psychology, sociology, and law. Specific topics should be included about securing critical infrastructure that covers all sectors (agriculture, food, water, public health, emergency services, government, defense, information and telecommunications, energy, transportation, banking and finance, chemical industries and hazardous materials, postal and shipping, monuments and icons). Activities in broader ISA curricula should include workshops and projects to enable students of diverse backgrounds to become computer security and ISA professionals (Cicalese, DeWitt & Martin, 2005). It is necessary to develop a curriculum that integrates the technical content with the ethnic, social, and legal considerations. Also, different approaches (offensive or defensive) in teaching information security enhance the effectiveness of the courses and improve the learning process (Dornseif, Gartner, Mink & Pimenidis, 2005; Yurcik & Doss, 2001). However, students have to learn how to design and develop technologies on cyber attacks prevention, information security management, and how to make decisions and take actions to control the cyber space.

Currency of ISA Curriculum

A few trends need to be addressed by an ISA curriculum to maintain its currency. These include technology changes, threats and attacks, standards, teaching methods, and non-IT degree enrollment that we describe as follows:

I. Technology changes

The preferred hardware system architectures and components choices are dynamic, and as these choices change, the information security requirements also change. New paradigms in the form of Intelligent Information Systems, Object-Oriented Software Engineering, Web Services, Smart Clients, and User-centered HCI design, Knowledge Management Systems are emerging.

II.Threats and attacks

A continuous stream of new viruses, worms, spam attacks, denial of service attacks, and unauthorized intrusion keep the ISA specialists on alert all the time. The ISA curriculum in universities must be updated to maintain the currency of the education and training of the students with regard to prevention of information security threats, attacks, and mitigation/response methods.

III. Information security standards

It is evident that the standards and guidelines for ISA practices and education, set by organizations like IEEE, IETF, and ISO, are a critical determinant of the framework within which an ISA curriculum/training program should be formulated and implemented. Therefore, any changes in these standards and/or guidelines must be reflected in the ISA curriculum with minimal delay.

IV. Teaching methods

Classes based on e-learning (e.g. Interactive TV, Web-based distance learning systems) are rapidly replacing traditional face-to-face classes. The distance learning classes have unique ISA requirements, and in view of the fast growth of this method of instruction, the ISA curriculum should stay in step with new teaching methods.

V. Increasing interest in information security by students outside the IT learning area

Because utilization of information technology is becoming an essential requirement for all university students, the ISA curriculum must be designed to support the needs of increasing numbers of students outside the IT learning area who are interested in learning how to protect their information assets and resources. The ISA curriculum designers should play a role in helping liberal arts majors to become as technically and security literate as possible (Davidson, 2005; Piotrowski, 2005). User awareness and education are the most critical elements because many successful security intrusions come from simple variations of the basics: social engineering and user complacency. Since information security is a concern for students outside the university environment also, the Southwestern Oklahoma State University has introduced a two-hour course in which lower-level students are introduced to ISA in the context of identity theft threats, protection measures, and ethics. Learning about computer security and ethics will minimize the occurrence and/or impact of information security breaches.

Information Security Research

Members of a panel on Information Security Research and Development in Academia (Hoganson, 2005) highlighted the lack of ISA research programs in universities, and made suggestions for dealing with this deficiency. At the 4th National Colloquium on Information Security Education in 2000, Bishop warned that the current Information Security programs are focusing on short-term or medium-term planning and recommended focusing on basic research and higher education (Bishop, 2000). Also, Paulson made the following observations (Paulson, 2002):

- A lack of adequate research eventually could cause the US to experience an "electronic Pearl Harbor" in which a cyber attack could damage the public networks causing serious losses.
- Most US network security research occurs in the private sector and is usually related to the development of products such as antivirus software, cryptography, and intrusion detection systems.
- More research has to be supported in programming languages. "Academia has done a very poor job in developing core courses and core research of a more practical nature".
- There is a need for more graduates in computer security, but there are still relatively few institutions that offer ISA degrees or emphasize computer security in their programs.
- There is a substantial shortage of researchers and practitioners who have gained a broad knowledge of security. More researchers in the field are needed.

Adequate cyber infrastructure is critical for the success of joint research ventures. The timely dissemination and sharing of the results produced by ISA researchers in academic institutions is very desirable. In the policy/strategy area, universities should conduct research to evaluate the benefits of IT certificates (particularly, ISA certifications) because a certification does not have a lasting value and the rapidly changing knowledge base may render these certifications irrelevant or unacceptable within a short time (McGill & Dixon, 2004). Other issues/realities that should be investigated are absence of an unbiased/neutral group for creating exams and approving examiners, absence of an unbiased/neutral group for determining content, heavy vendor involvement in the certification process, and the impact of interference with the academic programs by certification organizations. The following section provides suggestions for changes and actions to improve ISA curriculum.

A Perspective for Changes

There is a big discrepancy between the levels of skills expected by employers and those the graduates have after completing their studies. In order to address these problems, the academic community must restructure the curricula for computing related degrees (Computer Science, Information Systems, Computer Engineering, Information Technology) to generate interest and research in several areas of computer science, informatics, applied mathematics, hardware, formal methods, simulation and modeling, intelligent agents, etc. We briefly discuss changes to approaches, topics, resources, and courses.

New Approaches

Scholars argue that Information Assurance cannot be viewed strictly as a Computer Science subset and recommend that:

I. Information Security education should include both technical and non-technical aspects, and

II. Keep up with security requirements for public, industry, and government.

We are moving to the Intelligence Age in which we should have "systems that can intelligently gather and analyze data" (Watson, 2004). Information security management based on knowledge management models can be used for security auditing because they include organizational subsystems: people, technology, and structure (Zaliwski, 2005). ISA curriculum should cover courses and experiments involving Intelligent Systems and Artificial Intelligence techniques that support intelligent control of security and create the knowledge base for information security domain.

Students in ISA programs should be able to study how people assign credibility to the information they collect, in order to invent and develop new credibility systems to help consumers manage the information overload often "incomplete and even incorrect" (Pattanik, 2004). A new area of learning, concentrated on the behavior of information users, called Human Information Behavior (HIB) may assist ISA specialists in fine-tuning the designs of systems and training programs for specific groups of information systems users. Also, students in computing disciplines need to learn how to develop information security tools. Small and medium-sized enterprises employ Information Security professionals possessing skills to use and enhance security tools (Jennex, Walters & Addo, 2004).

As organizations build knowledge from a strategic, managerial, and operational perspective, universities and training organizations should teach skills that are mapping to these areas. Scholarly research should explore new technologies and new approaches to obtain more effective and long-term solutions.

Teaching Information security management related on-line exercises and assessment requires that students and faculty have access to Web-based laboratories in a Web-based educational environment such as VITELS laboratory at Berne University in Switzerland (VITELS, 2005) and the laboratory at Arcada Polytechnic in Finland (Bergstrom, Grahn, Karlstrom, Pulkkis, & Astrom, 2004). In the virtual setting, innovative laboratory projects should be designed to teach students complex problem-solving skills, rather than limited experiments involving firewalls, intrusion detection, server configuration, etc.

New Topics and Resources

There is a need to incorporate ISA topics throughout undergraduate curricula for all computing disciplines. "Software security and reliability cannot effectively be added as an afterthought –

they must be built in from the start" and "students with such background will be ready and prepared for more specialized information assurance courses" (Bhagyavati, 2005; Hentea, 2005b).

Pedagogical tools, based on simulations that support interactive step-by-step demonstrations of the protocols, processes, and algorithms, can facilitate the students' learning. For example, encryption processes for various algorithms can be described with simulation tools (McNear & Pettey, 2005). Also intelligent tutorials built with Artificial Intelligence constructs, that support interactive step-by-step demonstrations and concepts, can make learning easier and faster. Topics addressing the role of Intelligent Systems, as assistants in learning security concepts, and providers of personalized feedback to the student, and usage of systems for remedial skill building, are needed in the Information Security curricula.

Courses

The selection of courses for an ISA program should be based on "strategic knowledge". Effective utilization of strategic knowledge in the formulation, upgrading, and enhancing ISA education are necessary to position computing programs to counter the outsourcing movement of IT jobs (Hoganson, 2005). Functions and knowledge areas that are of strategic importance, and critical to business of the enterprise, are less likely to be outsourced. Examples of these knowledge areas include Information Security, Software Engineering, Networking, Database, Embedded Computing, Bioinformatics, Computer Graphics, Multimedia, Knowledge Management, and Game Design. Undergraduate programs gain by adding concentrations or degrees on Information Security Management or Telecommunications. For example, these concentrations may be designed as follows:

- **Information Security Management**

Assuming that an introductory course in information security is provided during the second semester of first year of study in CS or IS programs, the following courses are suggested: Security Design and Architecture, Disaster Recovery and Contingency Plans, Computer Forensics, Wireless Security, Information Security Management, Elective (any of the following: Legal Issues and Code of Ethics, Information Technology Risk Assessment, Emerging Technologies and Impacts, Introduction to Cryptography).

- **Telecommunications**

Assuming that an introductory course in data communications and computer networks is provided during the second year of study in CS or IS programs, the following courses are suggested: Internetworking and TCP/IP Protocols, Broadband Services, Wireless and Mobile Computing Applications, SOHO/Home networks, Network Management, Elective (any of the following: Voice Over Internet Protocol Services, Storage Area Networks, Emerging Technologies and Impacts, Web Server Management, Introduction to simulation and modeling).

Conclusion

So far, government and professional organizations, and employers of ISA specialists have been the drivers of the ISA curricula and programs at our universities. There are numerous ISA education models and curricula in existence at educational institutions around the world. The market place for the products, services, and personnel is now global, and ISA curriculum should be based on national and international standards. In addition, we observe several majors trends that will change the way in which university ISA programs are designed and operated.

The specific curriculum frameworks can be consolidated and adopted by educational institutions to ensure the skills required by the employers. Security education and specific security topics

should be incorporated in all relevant courses of computing programs such as Computer Science, Information Systems, Informatics, Information Technology, Computer Engineering as well as business major programs (Management of Information Systems). Security education, specific career tracks or degrees, should be offered at undergraduate, graduate, and postgraduate level in any academic institution.

There is a need to cope with prevailing information security problems around the globe. However, bringing curriculum and infrastructures for undergraduate and graduate programs to common designs and universal models will take effort, research, and collaboration at national and international levels. Future work should focus on specifying the recommended topics, courses, and sequence of courses for Information Security Assurance curricula appropriate for particular degrees.

References

Armstrong, H. & Jayaratna, N. (2002). Internet security management: A joint postgraduate curriculum design. *Journal of Information Systems Education, 13*(3), 249-258.

Bergström, L., Grahn, K.J., Karlström, K., Pulkkis, G., & Åström, P. (2004). Teaching network security in a virtual learning environment. *Journal of Information Technology Education, 3*, 189-217. Available at http://jite.org/documents/Vol3/v3p189-217-038.pdf

Bhagyavati, S., Naugler, D., Olan, M., & Frank, C.E. (2005). Information assurance in the undergraduate curriculum. *Proceedings of 43rd ACM Southeast Conference*, Kennesaw, GA, March 2005.

Bishop, M. (2000). Academia and education in information security: Four years later. *Proceedings of the 4th National Colloquim on Information Security Education.* Retrieved November 5, 2005 from http://seclab.cs.ucdavis.edu/projects/history/ourpapers/2000c.html

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

Cicalese, C., DeWitt, J., & Martin, C.D. (2005). Ethics across the computer science curriculum. *Proceedings of 43rd ACM Southeast Conference*, *Kennesaw, GA,* March 2005.

Davidson, M.A. (2005). Leading by example: IT security. *EDUCAUSE Review*, *40* (1), 14-22.

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

Dhillon, H., & Hentea, M. (2005). Getting a cybersecurity program started on a low budget. *Proceedings of the 43rd Annual ACM Southeast Conference,* Kennesaw, GA, March 2005, 294-300.

Dornseif, M., Gartner, T., Mink, M. & Pimenidis, A. (2005). Teaching data security at university degree level. In N. Milovslaskaya & H. Armstrong (Eds.), *Proceedings of the IFIP TC11 WG 11.8, Fourth World Conference Information Security Education (WISE4)* (pp. 213-222)*,* Moscow, Russia.

Furnell, S. & Clarke, N. (2005). Organizational security culture: Embedding security awareness, education, and training. In N. Milovslaskaya & H. Armstrong (Eds.), *Proceedings of the IFIP TC11 WG 11.8, Fourth World Conference Information Security Education (WISE4)* (pp. 67-74), May 2005, Moscow, Russia.

Gritzalis, D., Theoharidou, M. & Kalimeri, E. (2005). Towards an interdisciplinary information security education model. In N. Milovslaskaya & H. Armstrong (Eds.), *Proceedings of the IFIP TC11 WG 11.8, Fourth World Conference Information Security Education (WISE4)* (pp. 22-35), May 2005, Moscow, Russia.

Hentea, M. (2005a). A framework for teaching information security with laboratory projects. In N. Milovslaskaya & H. Armstrong (Eds.), *Proceedings of the IFIPTC11 WG 11.8, Fourth World Conference-Information Security Education (WISE4)* (pp. 174-178), Moscow, Russia.

Hentea, M. (2005b). A perspective on achieving information security awareness. *Issues in Informing Science and Information Technology Journal, 2*, 169-178. Available at http://2005papers.iisit.org/I14f89Hent.pdf

Hoganson, K. (2005). A strategic approach to computer science curriculum. *Proceedings of 43rd ACM Southeast Conference*, Kennesaw, GA, 1, 365-370.

Hsu, C. & Backhouse, J. (2002). Information systems security education: Redressing the balance of theory and practice. *Journal of Information Systems Education, 13*(3), 211-218.

Irvine, C., Chin, S.K. & Fruickle, D. (1998). Integrating security into the curriculum. *Computer, 31*(12), 25-30.

Jennex, M.E., Walters, A. & Addo, T.B.A. (2004). SMEs and knowledge requirements for operating hacker and security tools. *Proceedings of International Resource Management Association*, New Orleans, Louisiana, May 2004, 276-279.

Kim, K.Y. & Surendran, K. (2002). Information security management curriculum design: A joint industry and academic effort. *Journal of Information Systems Education, 13*(3), 227-235.

Kim, S. & Choi, M. (2002). Educational requirement analysis for information security professionals in Korea. *Journal of Information Systems Education, 13*(3), 177-182.

Logan, P. Y. (2002). Crafting an undergraduate information security emphasis within information technology. *Journal of Information Systems Education, 13*(3), 227-247.

Manson, D. & Curl, S. S. (2003). A comparison of academic and government information security curriculum standards. *Proceedings ISECON 2003*, San Diego, 1-6.

McGill, T. & Dixon, M. (2004). Information technology certification: A student perspective. *Proceedings of International Resource Management Association*, New Orleans, Louisiana, 302-306.

McNear, C. & Pettey, C.C. (2005). A free, readily upgradeable, interactive tool for teaching encryption algorithms. *Proceedings of 43rd ACM Southeast Conference*, Kennesaw, GA, *1*, 280-285.

Pattanik, D. (2004). Impacts of information technology on society. *Proceedings of International Resource Management Association*, New Orleans, Louisiana, May 2004, 1429-1431.

Paulson, L.D. (2002). Wanted: More network-security graduates and research. *IEEE Computer*, *35* (2), 22-24.

Piotrowski, V. (2005). Information assurance curricula and certifications. Retrieved April 28, 2005 from http://www.micsymposium.org/mics_2003/Piotrowski.PDF

Rosseli, F. (2005). Observatoire des sciences et des techniques, Cyber security curricula in European Universities: Final Report. Study commissioned by the Institute for Prospective Technological Studies, Retrieved on May 30, 2005 from http://www.fondazionerosselli.it/DocumentFolder/Cyber.pdf

Smith, E., Kritzinger, E., Oosthuisen, H.J. & Von Solms, S.H. (2005). Information security education: Bridging the gap between academic institutions and industry. In N. Milovslaskaya & H. Armstrong (Eds.), *Proceedings of the IFIP TC11 WG 11.8, Fourth World Conference Information Security Education (WISE4)* (pp. 45-55), Moscow, Russia.

Stevens, K.J. & Jamieson, R. (2002). A popular postgraduate information systems security course. *Journal of Information Systems Education, 13*(3), 219-225.

Yasinsac, A., Erbacher, R.F., Marks, D.G., Politt, M.M., & Sommer, P.M. (2003). Computer forensics education. *IEEE Security & Privacy, 1*(4), 15-23.

Yurcik, W. & Doss, D. (2001). Different approaches in the teaching of information systems security. Retrieved November 11, 2005 from http://colton.byuh.edu/isecon/2001/04a/Yurcik.Doss.sec.doc

VITELS, Retrieved September 10, 2005 from http://vitels.ch/project/overview.php

Watson, J.B. (2004). The coming of the intelligence age: Enhancing education through assessment. *T.H.E Journal*, *31*(9), 32-33.

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

Zaliwski, A.J. (2005). Computer network simulation and network security auditing in a spatial context of an organization. *Issues in Informing Science and Information Technology Journal, 2*, 159-168. Available at http://2005papers.iisit.org/I13f38Zali.pdf

Biographies

Dr. Mariana Hentea is an Associate Professor in the Department of Computer Science at Southwestern Oklahoma State University. She received a MS and Ph.D. in Computer Science from the Illinois Institute of Technology at Chicago, Illinois and a B.S. in Electrical Engineering and MS in Computer Engineering from Polytechnic Institute of Timisoara, Romania. Dr. Hentea has been involved in the research and development of novel products based on various emerging technologies, engineered networks and security systems for telecommunications industry and government for almost thirty years. Her research focuses in computer and network security, network design and architecture, wireless technologies, and Artificial Intelligence techniques for intrusion and prevention systems, information security management, quality of service, and intelligent control. For the past four years, Dr. Hentea has been involved in security awareness education and academic curricula related to information security and networking programs.

Dr. Harpal Dhillon is currently the Director of the Center for Telemedicine and Web-based Distance Learning at Southwestern Oklahoma State University. He is a Professor in the Department of Computer Science and Information Systems. Dr. Dhillon received his Ph.D. degree in Operations Research and Systems Engineering from the University of Massachusetts. He has been involved in academic activities and research related to Information Security for 10 years.

Dr. Dhillon is a Health Information Technology consultant for a number of medical information systems development companies.

Manpreet Dhillon is a doctoral candidate in the School of Business at The George Washington University. She is currently working on her doctoral dissertation for the PhD degree in Information and Decision Systems. Her primary research interests include Information Quality and the Decision Making Process and Technology Adoption and Use in Healthcare. Prior to starting her graduate studies, Ms. Dhillon worked as a business process analyst at HCA Corporation and a research associate at The Advisory Board Company.