Accommodating Information Security in Our Curricula

Ken Surendran
Department of Computer Science
Southeast Missouri State University
Cape Girardeau, MO 63701
ksurendran@semo.edu

Ki-Yoon Kim
Department of Business Administration
Kwangwoon University
Seoul, Korea.
min1203@daisy.kwangwoon.ac.kr

Al Harris
Department of Information Technology & Operations Management
Appalachian State University
Boone, NC 28608
harrisal@appstate.edu

ABSTRACT

When the power of computing and communications technology was unleashed for the benefit of the society, only the good intentions were at heart and not enough attention was paid to the possible illegal and unethical activities in cyberspace. The intrinsic nature of Information Technology (IT) is such that, in today's world, even what is thought to be a simple criminal behavior could cause colossal damage to the society. The need to pay attention to the security issues in IT has been recognized, as evidenced by a major emphasis on security in industry and education. While it may take considerable research and development effort to bring about infrastructures and applications that are fundamentally security-centric, there is need to cope with the prevailing information security problems. Educational institutions, for their part, have responded by initiating security related research and curricula.

Keywords: Information security, information systems education, information systems curriculum.

1. CURRICULA TYPES

Information Security (InfoSec) education has many dimensions, and it comes in several offerings. The dimensions range from stand-alone courses to complete specialized curriculums. The offerings reflect the institutions' educational philosophies and the nature of the programs for which the courses are intended. InfoSec is an area that encompasses courses in Computer Science, Communications Engineering, Information Systems, and Management. The mix of technology and business issues in these courses varies as well. The Common Body of Knowledge (CBK) found on http://www.isc.org seems to reflect the interdisciplinary nature of InfoSec and as such could serve as a good starting point in planning a course or curriculum in this area.

Like many new disciplines, InfoSec was first introduced at the Masters level. As demand for InfoSec personnel grew, courses have become common in the Bachelors' programs. In some cases, contents for the existing courses were modified to include Info Sec components. Some academics envision the need for separate curricula in InfoSec – both at the Masters and Bachelors levels. The ten papers that are presented in this issue fall under these three categories: courses in the Masters program, courses in the Bachelors program, and complete curricula in InfoSec.

2. ISSUE OVERVIEW

In all, ten papers on InfoSec are presented in this special issue. As can be expected, a large majority of the papers presented in this issue describe Masters level courses. Three papers deal with InfoSec curricula at Bachelor and Master levels; another three, which follow this introductory paper, address the Bachelors level courses; and four are concerned with Masters level courses. While each paper has a special message, there are some common themes that may be of interest to note. Most individual courses are project driven, have lab components and, especially the graduate ones, emphasize the business aspects of security. The needs are stressed for stand-alone labs, as well as ethical concerns and legal implications in teaching approaches. Different approaches to designing curricula are discussed; and, in some cases, comparisons with globally existing programs are discussed. One of the main themes that emerge is the interdisciplinary nature of information security. We introduce the ten papers below briefly, starting with those on undergraduate courses.

2.1 Undergraduate Courses

It is perhaps easier in an undergraduate curriculum to include an optional course in InfoSec without upsetting the existing curricula. Another proactive approach is to add a track in InfoSec in an existing program itself. The first paper by Patricia Logan shares her experience in the design and delivery of a capstone course 'Computer Forensics' for the Information Security and Networks track within the Information Systems and Technology major. The need for a separate lab, incorporation of ethics, and collaboration with the Criminal Justice Department are emphasized. Another issue in an InfoSec course in an undergraduate program is to present the technical concepts to the Information Systems students in a palatable way. Qidong Cao, John Davis, Xue Bai and Orlando Katter illustrate how they were able to teach technical concepts (encryption) to business students using less demanding laboratory exercises, requiring simple database knowledge and familiarity with Active Server Pages. The final paper dealing with an undergraduate course is by Michael Grimaila and Inkoo Kim. In this paper, they describe a foundation course in the InfoSec curriculum involving project work in which the students prepare a security plan for an organization and 'sandbox' labs, which allow students to learn through attack/defend modes (For details on a large-scale version of such attack/defend training exercises refer to the paper by Welch et al in IEEE Computer, April 2002 issue on *Training for Information Assurance*.) .

2.2 Graduate Courses

The next four papers deal with courses in Masters level programs. Security and Control of Information System is an MBA course that was reengineered from a conventional technology course. Sunil Hazari explains how this course was evolved to provide the necessary management focus. Discussion on Risk Radar – a software tool for risk assessment - and sample case studies are the highlights of this paper. Sophie Cockcroft's paper discusses a course 'Securing the commercial internet' for those specializing in e-commerce. The delivery of the course includes: research activities, security audit of a firm, and emphasis on privacy, guest lectures and lab work. The course is compared against the elements of CBK. The course is validated using the industry expectations observed from job advertisements. The theme of the next paper is the application of situated learning strategy in an InfoSec course (Security in Information Systems for Organizations) to help students apply classroom knowledge in real world environments. In this, Carol Hsu and James Backhouse elegantly describe the concepts of situated learning, illustrate its application in the InfoSec course, and evaluate, using student feedback, the tools used in the course facilitation. Ken Stevens and Roger Jamieson use a variety of tools for making a graduate InfoSec course popular: industry involvement, web resources, software tools (Audit Risk Language), case studies, research assignments, and consultancy assignments involving assessment of risk exposure of an organization. They also discuss strategies to handle the breadth vs. depth, and include of new topics without overloading the course.

2.3 Curricula Related

These papers address the area of InfoSec curricula design. While it may be simple to use Computer-Based Education as the basis for a curriculum, one needs to fine tune it based on the institution's educational philosophy and also the actual industry requirements. A practical curriculum in Information Security management can be designed collaboratively when specialists from industry and academicians brainstorm together. Ki-Yoon Kim and Ken Surendran present the results of a job analysis of Information Security Managers that led to the identification of seven courses to form the core of a curriculum in Information Security Management. In the following paper, Sehun Kim and Myeong-Gil Choi take a finer look at the educational requirements of Information Security Managers and Information Security System Developers. They used a variation of Delphi technique for gathering this information from both practitioners and academicians. While the above two papers are concerned with undergraduate curricula, the final paper describes a set of graduate curricula. Helen Armstrong and Nimal Jayaratna first identify the elements of generic, specialist and practical skills and then formulate a set of three graduate level programs specializing in Internet Security Management. They describe the contents of all the courses offered under these programs and also compare these programs against other InfoSec programs that are offered elsewhere in the world.

3. LOOKING AHEAD

Listening to international speakers at the 6th National Colloquium for Information Systems Security Education (NCISSE) held this year in Seattle, it was clear that educational Institutions all over the world have programs in Information Security Research and Education. The number of international contributions to this special issue may also evidence this. In the USA, the National Security Agency (NSA) has recognized about 50 educational institutions as Centers of Excellence in Information Assurance Education, including 13 new ones this year. Seven of them were recognized for Advanced Information Security programs. NSA granted these designations following a rigorous review of university applications against published criteria based on training standards established by the Committee on National Security Systems (CNSS). Looking at the number of academic attendees in the Information Security Education Boot Camp that preceded the Colloquium, more institutions may work toward NSA recognition.

4. ACKNOWLEDGEMENT

Special issues like this owe a lot to the reviewers. There were some 30 reviewers who helped us in the preliminary reading of the manuscripts. We would like to thank them for their time and valuable observations. They will be recognized in Issue 4 of Volume 13. Ken Surendran would to thank his Computer Science Department colleagues in Southeast Missouri State University, and in particular Dr. Helen Hays, for their support in this special issue initiative.

AUTHOR BIOGRAPHIES

Ken Surendran is an Associate Professor in the Department of Computer Science at Southeast Missouri State University. His research interests include Software Engineering and Security Management Education. His industrial experiences in IT were with Indian Space Research Organization and Zambia Consolidated Copper Mines. His previous academic assignments in IT were with Rose-Hulman Institute of Technology; UNITEC Institute of Technology, New Zealand; Copper-belt University, Zambia; and PSG College of Technology, India. Surendran received a B.E. in Electrical Engineering from University of Madras, India, M. Tech. in Electrical Engineering from Indian Institute of Technology, Madras, India, and Ph. D. in Applied Analysis from State University of New York at Stony Brook. He is a senior member of IEEE and a member of ACM.

Ki-Yoon Kim is a Professor in and the Chairman of the Department of Business Administration at Kwangwoon University, Seoul, Korea. . His research focuses on Security Management, Software and Information System Risk Management. He received his Ph.D. in Management Science at the Korea University in Korea

Al Harris is a Professor in the Department of Information Technology and Operations Management in the John A. Walker College of Business at Appalachian State University, Boone, NC. He is also the Editor of the Journal of Information Systems Education. He received his Ph.D. in Management Information Systems (MIS) from Georgia State University, his Master's degree in Systems Management from George Washington University, and his B.S. in Quantitative Business Analysis from Indiana University. He had over 15 years of information systems consulting experience before joining the academic ranks. He teaches a variety of undergraduate and graduate IS courses. He has published articles in numerous journals and in over 25 international, national and regional proceedings. Dr. Harris has served as Treasurer of AITP's EDSIG, Secretary of Southeast chapter of DSI, and has participated in numerous regional, national, and international meetings.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

Copyright ©2002 by the Information Systems & Computing Academic Professionals, Inc. (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to the Editor-in-Chief, Journal of Information Systems Education, editor@jise.org.

ISSN 1055-3096