Reengineering an Information Security Course for Business Management Focus

Sunil Hazari
Robert H. Smith School of Business
University of Maryland
College Park, MD 20740
shazari@umd.edu

ABSTRACT

This paper describes an information security course that evolved from a technology-focused legacy systems course to a current-topics Web commerce course for MBA students with an emphasis on business management issues faced by today's networked organizations. The paper also describes the use of an online component, implemented to enhance student learning in a technology-based environment, which fostered interactivity and discussions among students. Using this course as a model, the paper presents a rationale for revising content and describes the framework, pedagogy and learning materials that were used in the course to meet the changing needs of information security management.

Keywords: Information security management, enterprise security architecture, risk management, business education.

1. INTRODUCTION

The field of information security has traditionally been considered a technical discipline. However, information security is a very broad area that can include topics ranging from mathematical concepts of encryption techniques to physical security of IT systems, risk analysis and human compliance (Highland 1993). According to Summers (1997), information security has three dimensions: application (safety-critical systems, electronic commerce, national security, law enforcement, personal data and e-mail); computing (networks, PCs, decentralization, end-user applications, mobile computing and the Internet); and a social-economic-legal framework (ethics, fraud and abuse, privacy, laws, standards, the global economy, international agreements and public policy). Security and controls enable good business by mitigating risks in a cost-effective manner. In that way, security can be viewed as a component of business operations to help an organization efficiently achieve business goals.

A graduate-level business management course, therefore, must address security beyond its technical aspects. The Robert H. Smith School of Business at the University of Maryland offers an MBA program in information systems (IS) that prepares students to manage enterprises in a Netcentric environment by effectively executing the e-infrastructure transformation, extracting the maximum strategic and tactical advantage from technology use, and designing and implementing electronic marketplaces. (See http://www.rhsmith.umd.edu/dit for program details.) A course called "BMGT727: Security and Control of Information Systems" is offered as an elective in the IS curriculum. The University catalog description for the course reads: "The information security risks faced by corporations. Strategies for maintaining integrity of corporate information resources. Also covers encryption, firewalls, digital certificates, policies, laws, risk management from a business perspective. Actual case studies."

To prepare managers who can compete successfully in the information economy and to provide the education demanded by a workplace that is increasingly driven by technology, MBA information systems curricula should model a structure that reflects business functions and disciplines, supported by technological applications. For an information security course to be effective, it must prepare students to demonstrate and articulate the business value of IT security to senior management. The BMGT727 information security course presented in this paper is being used as a model to demonstrate the changing focus of information security management.

2. CURRICULUM REDESIGN

In the past, this course was taught from a technical perspective and included such topics as the comparison between VAX & Unix operating systems, LAN, WAN, mainframe security, cryptography techniques and access controls. Although these topics are important (and continue to be covered in the course on a limited basis), the usefulness of the course for MBA students was limited. Using the C.I.A. model, information security is concerned with three aspects: Confidentiality (disclosing information according to policy), Integrity (making sure information is not corrupted or destroyed), and Availability (making sure the system's services are available when needed) (Summers 1997; Schneier 2000). Web servers of large organizations are still connected to back-end legacy systems. Therefore, security should not be focused only on Web servers or newer client-server systems, but instead should take a holistic approach. For that reason, the focus of this course has undergone a major shift toward management of security issues in the Internet era.

The e-commerce boom a few years ago led many colleges and universities to redesign their curricula to accommodate courses that focused on conducting business in the digital world. Experts predicted that the Internet would transform businesses around the world by allowing new kinds of interactions among companies, suppliers and customers and new processes within the firms. The vast potential of this area translated into a need for professionals who could explore new business models and who had a broad understanding of the key trends in technology-supported business applications. To focus students' attention on business models of dot-com companies, many business schools started offering e-commerce as a primary concentration, which required changes to the curricula. In a recent survey, AACSB International found that one-fourth of 282 surveyed schools continue to offer e-commerce concentrations with their MBA degrees.

In 2000, denial-of-service attacks on companies such as Yahoo, eBay and CNN brought the topic of information security to the headlines of national newspapers. Managers and executives began to see a need for stronger information security in their organizations. In light of that awareness, and because of the Internet- and security-related issues that were beginning to emerge, there was a need to shift the focus of information security courses to current topics related to Web commerce security. At the University of Maryland, the BMGT727 information security course fit well with the e-commerce concentration. The area of information security management is relevant to any e-business course because strategic and operational plans are needed to maintain the confidentiality, data integrity, and availability of systems and business processes.

When redesigning this course to prepare students to meet the market demands of hiring managers, it was important to review industry needs. One way to achieve this was to look at certification programs in the industry. Recognizing that the needs of MBA students go beyond the technical domain toward a stronger emphasis on business management issues, the BMGT727 course was designed to have a broader focus than the industry-standard Certified Information Systems Security Professional (CISSP) certification. According to the International Information System Security Consortium (http://www.isc.org), which administers the CISSP examination, "CISSP Certification was designed to recognize mastery of an international standard for information security and understanding of a Common Body of Knowledge (CBK). Certification can enhance a professional's career and provide added IS credibility." Ten CISSP information systems security areas are covered in the certification examination, reflecting the CBK:

- Access Control Systems & Methodology
- Applications & Systems Development
- Business Continuity & Disaster Recovery Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security (Computer)
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications & Network Security – I & II

As seen from the above list, the CISSP certification has limited use for MBA students. The focus is technological issues, and the CBK does not address topics related to organization, finance, and strategy. The BMGT727 course used the CBK but built on it to provide a broader business-based perspective on information security.

3. COURSE CONTENT

The initial portion of this fifteen-week, graduate-level elective exposes students to technical aspects of information security because business decisions depend on a conceptual understanding of technological issues and the products that are available to safeguard organizational assets. Students need to understand techniques such as encryption, firewalls and intrusion detection systems to assess their impact on organizational goals and to justify the cost of maintaining data integrity in the corporate infrastructure.

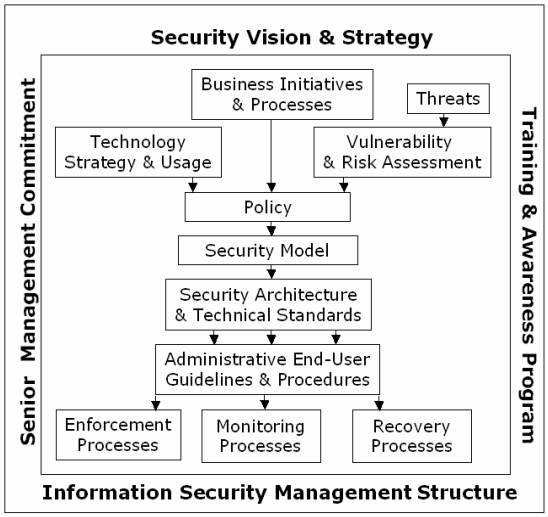
Due to the nature of the course, selecting an appropriate textbook was a challenge, especially the first time the course was taught under the revised curriculum. Although there were many information security books

with a technical focus, there were no books that provided a balanced technology and management approach. Secure Computing: Threats and Safeguards by Summers (1997) were selected because it appeared to meet the needs of the course. Although the book is very comprehensive, at the end of the semester students expressed concerns regarding use of a text that was more technical than managerial, and more theoretical than practical. For the second semester, a different textbook, Defending Your Digital Assets by Nichols, Ryan, and Ryan (2000) was adopted. In addition to the textbook, supplementary articles that provided industry-based case studies on relevant topics were used for information beyond the factual knowledge and technical terminology contained in the textbook. The case studies included cross-functional areas, since information security must be woven throughout the fabric of an organization and every employee should be made to realize the importance of safeguarding corporate information.

As mentioned earlier, since a broad understanding of technical terms is necessary before making business decisions related to security, the course's content reflects a technological focus toward the beginning of the semester. (This was also necessary due to the diverse backgrounds of the students, some of whom lacked adequate technical knowledge.) The technical concepts introduced were made specific to security-related issues. For example, the OSI seven-layer model was explained using an example of how firewall rules permit or deny data between the physical (Layer 1) and application (Layer 7) layers. Lest the students lose sight of the nature of the course, during alternate classes the supplementary readings introduced broader strategic issues faced by organizations.

A framework was also needed to provide a foundation on which business issues of information security could be studied and students could acquire a logically coherent perception and knowledge of topics in the course description. The Enterprise Security Framework used for the course is the Price Waterhouse Coopers (PWC) model (Murphy et al. 2000). The PWC model is comprehensive and has been incorporated extensively in the course because it addresses the entire enterprise of security architecture. The model emphasizes information security strategies within the organization using a holistic rather than a piecemeal approach. The framework (see Figure 1) is based on four pillars: Security Vision and Strategy, Senior Management Commitment, Information Security Management Structure, and Training and Awareness.

Figure 1: PWC Enterprise Security Model



Since each organization is different, reviewing the business model determines the level of effort required to achieve security while reflecting a company's vision and strategy. The commitment of senior management, in the form of political and financial support, guides the security policy of an organization by keeping in mind the business goals and risks associated with maintaining the confidentiality, integrity, and availability of information. Typically, an organization's chief security officer is in charge of IT and usually reports to the chief information officer. The PWC model suggests an alternative approach: placing the security department under the responsibility of the chief financial officer because of the direct relationship between information and monetary assets. This provides for better transitioning from computer security to information security and places IT in the risk management domain, which makes use of internal audits as well as traditional security departments. In class, this idea generates spirited discussions between students with IT and non-IT backgrounds, who consider the pros and cons of each scenario. Security awareness relates to the behavioral (such as human nature related) aspects of information security and includes instructional methods (such as using newsletters, videos, presentations, and posters) that demonstrate the importance of protecting information from social engineering techniques commonly used by hackers. (Social engineering refers to using non-technical means to get confidential or protected information from other people.) As part of group discussions in class, students design a security awareness program to supplement new employee orientation in an organization. Group programs are then compared and discussed. The PWC model is introduced early in the semester and is reinforced throughout the course in lectures, case studies, group discussion, and the online environment.

Going beyond technical topics, the PWC model is referenced throughout the course in other areas such as policy development, risk management, conflict resolution, funding, ROI of security products and programs, and budgeting [Senior Management Commitment]; security goals and objectives, organizational business models, and project management [Security Vision and Strategy]; departmental staffing

issues [Management Structure]; and employee orientation, password use, anti-virus programs, compliance and monitoring, and acceptable use guidelines [Training and Awareness]. Additionally, case studies deal with organizational aspects of denial-of-service attacks, auditing, employment screening, e-mail monitoring by employers, privacy, encryption debates, and the security management issues that surround emerging technologies such as mobile applications and Web services. A complete list of topics and case studies related to the PWC model is available online at http://sunil.umd.edu/bmgt727. Three examples are explained below in further detail.

Example 1: Risk Management and Information Security

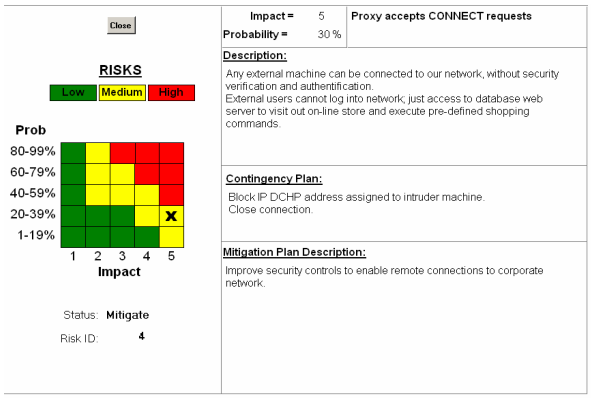
Risk management plays an important role in information security (Troutt 2002). An organization must understand the value of assets that need protection, the consequences of losing confidentiality or operational capability, the vulnerabilities that could be exploited to bring about the losses, the existing threats that could exploit the vulnerabilities, the likelihood that a threat might occur, and the availability and appropriateness of options and resources to address risks and concerns (Allen et al. 2000). The students had no problems pointing out technical threats and vulnerabilities that could result in losses, but most IS/IT students lacked the background to identify non-technical controls and factors affecting the risk scenario. Measurement models such as external audits, internal audits, capability maturity, and defect elimination – which can be used to provide an assessment of overall security of the IT environment (Bayuk 2001) – were explained to students. Different types of security assessments that can be performed using the above-mentioned models were also discussed. In addition, differences between penetration testing, auditing, and assessment (Winkler 2000) - which can be used for risk mitigation - were discussed in class to give students ideas of how to maintain systems security. Students then had a theoretical framework to address a case study of a financial services organization, which further aided discussion in this area. The goal of the risk management case study was to impress upon students the idea that advances in technology and business methods increase risks for organizations, and that appropriate preventive, detective, and corrective controls must be in place to mitigate those risks (Murphy et. al. 2000).

Since risk management is such an important topic, with an interdisciplinary focus, it was also beneficial for students to learn a tool with which they could analyze and quantify risks faced by organizations, using a project management approach. Working in pairs, students used the Risk Radar tool (http://www.iceincusa.com/RR2000.exe) to quantify security risks faced by an e-commerce organization that has implemented a new system that ties into back-end databases. (See Figure 2 for one student's risk assessment model.) The Risk Radar tool received positive comments from students, who felt that it helped them understand and apply risk management to an information security related business problem.

Example 2: Cyberterrorism and the law

According to Denning (2001), "The next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyberterrorism than the terrorists of today, and their level of knowledge and skill relating to hacking will be greater" (pp. 77). Students of information security must be prepared to deal with these challenges by understanding the political, social, and behavioral agendas that affect operations of computer systems. They must also be able to deploy countermeasures and safeguards to protect communication over networks. Terrorism has an impact on how organizations deal with information. Taking lessons from the World Trade Center attacks, students in the course are made aware of the importance of disaster recovery and enterprise continuity planning, which are tied to information security. During case study discussions, students realize that cyberterrorism poses an imminent threat in the future since utility, water supply, and transportation systems rely heavily on networked computer systems. As managers, students could be in charge of developing InfoSec policies for organizations, and they must be familiar with new legislation such as the PATRIOT Act and Health Information Portability and Accountability Act (HIPAA), which affect policy development. As an example, during class discussion on HIPAA, students critique the practices of consulting companies with regard to HIPAA composition, goals, benefits and compliance, and they review technical, legal, privacy, trust, and financial aspects of the law's implementation. They also discuss a mock scenario about a healthcare organization that involves assessing

Figure 2: Student Risk Management Assignment



The company's current environment, adherence to privacy rules, and relationship with trading partners; assigning a chief security or privacy officer; developing training programs for employees; conducting a risk

evaluation; and creating an action plan for HIPAA compliance.

Example 3: Mobile computing and information security

For current issues and emerging technologies such as mobile computing and wireless security, discussions center on implementation and are especially important in the course. As an example, new developments in wireless standards (such as 802.11a) have allowed mobile devices to make inroads to the corporate environment because of their portability, compact size, and ability to access the corporate network from any place at any time. However, IT managers remain reluctant to deploy wireless access technologies because of seemingly weak authentication and authorization tools at the handheld level (Chen 2001). Using lectures, discussions, case studies, and hands-on exercises (such as one using the NetStumbler software program), students in the course are made aware of wireless technologies and protocols. They follow up with group discussions on management issues (such as risk analysis and secure online behavior) related to the deployment of wireless LANs in the corporate environment.

Additionally, guest lecturers are invited to class to offer an industry perspective that goes beyond book learning and academic case studies. During the past two years, guest speakers with position titles such as Network Administrator, Webmaster, Director of Policy and Planning (Education), Manager of Information Security (at a dot-com company), Deputy Director of IT for the federal government, and CEO of a managed security services firm have offered students insight on the operational and strategic responsibilities of their roles. In course evaluations, students noted this aspect of class as one of the course's strong points.

4. ONLINE COMPONENT

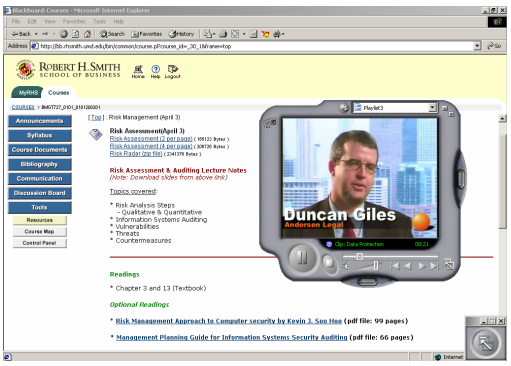
Business schools have been under constant pressure to provide students the skills and experience they need to effectively use the emerging technologies (Hilldebrand 1995) that businesses are using for competitive advantages (Leidner and Jarvenpaa 1993). With the acceptance of business models that integrate online technologies for business-to-business and business-to-consumer transactions as well as the exponential growth of e-commerce, it is imperative to increase students' proficiency with interactive Web-based applications. An online environment provides opportunities for students to work in teams to accomplish tasks and projects using collaborative software that has built-in tools to facilitate content creation and document sharing. Webster and Hackley (1997) identified previous studies of business schools that have adopted computer-mediated distance learning for business cases and simulations. Many business faculty have realized the advantages of using online technology to supplement face-to-face instruction. The Internet has quickly evolved from being merely a distribution channel to an interactive environment that encourages collaborative learning. In a partial response to Frost and Fukami's (1997) challenge to think in deep ways about management education and teaching, business faculty have realized the tremendous potential of actively engaging students in the online environment. Students have also appreciated the benefits and convenience of accessing course materials online. A technology component is now being integrated into almost every functional area of business education.

For technology-mediated learning environments to be pedagogically effective, faculty should incorporate interactive features such as online discussions, assessment, and feedback that directly contribute to student learning (Hazari 2000). Over the past three years, two online course systems have been used in BMGT727 to accommodate emerging technologies. Initially, the course was taught with a tool based on the Lotus Notes groupware environment. Recently, however, the course has used a commercial course development tool (Blackboard, http://www.blackboard.com) that offers additional features and is integrated with the School Portal. Alavi, Yoo, and Vogel (1997) believe that the integration of information technology into management is by no means trivial. With organizations increasingly using online tools (such as e-mail, instant messaging, desktop video conferencing) for internal and external communications, the online component of this course was designed to provide students experiential learning (Rogers and Freiberg 1994) while using the online environment. The online portion of this course used features and teaching methodologies that go beyond convenience-based features such as providing the syllabus, schedule, and other course documents. The goals in using online components are to develop students' communication skills and ability to work well in teams (including virtual teams), as well as their analytical and problem-solving skills.

Interaction and feedback have also been shown to have a significant impact on learning by improving the quality and success of online courses (Hazari and Schnorr 1999). Moore and Kearsley (1996) and Cornell and Martin (1997) have specifically identified interaction and feedback as factors that influence student motivation in completing a course. A feedback mechanism was integrated into this course, allowing students to comment anonymously on the amount of material, pace of lectures, use of examples and illustrations, and other concerns relevant to the instructional process. This helped the instructor monitor student reactions, control the pace of learning, and evaluate teaching strategies. Use of online testing, multimedia materials, and an interactive discussion board provided value-added features that kept the class connected as a virtual community between class meetings. It is becoming the norm at many colleges and universities to supplement face-to-face classes with an online course component. In this course, students have consistently rated the online environment as one of its strengths. A sample online format for the delivery of

course information on the topic of risk management is shown in Figure 3: The commercial web-based online environment itself was critiqued for security features such as appropriate use of digital certificates, access controls in private

Figure 3: Sample Online Environment



group discussion boards, identity spoofing using anonymous postings, use of cookies to maintain state, and authentication with university's directory services for single sign-on to the portal. Follow-up discussions resulted in identifying factors to be considered when designing secure intranets for corporations.

5. COURSE EVALUATION

The course uses tests, group presentations, and business research reports to evaluate students and assign grades. Class participation (face-to-face as well as online) also counts for a portion of students' overall course grades. The tests included questions related to factual knowledge, problem solving, what-if situations, scenarios, and case studies.

The positions of Chief Information Officer and Chief Security Officer have gone from the technical ranks to management, and interpersonal skills now form an important component of these roles. Good communication and interaction are needed to discuss issues and solve problems related to technology and management. Therefore, group presentations were required so students could gain experience in presenting information, such as justifying expenditures on an information security product or process. No written assignment was required for the group presentations, but students were asked to make slides available to other students prior to the presentations. Grading for this major project used peer-evaluation. Kingsuk and Patel (2001) encourage peer-evaluation in an open-ended manner on work assignments. This assignment simulated students presenting information on an information security topic to a corporate board. Rubrics used to assign grades were based on presentation (voice, eye contact, organization theme, time management, transition between speakers, enthusiasm, and audience participation); content (topic background, interactivity, explanation of technical details, business/management issues, security focus, evidence of research, and depth of presentation); visual aids and handouts (clear layout, organization, ease of understanding); and Q&A (ability to answer questions from students). Some examples of presentation topics addressed by student groups in the past are: Applications of Smart cards in Travel Industry, Security for Wireless Computing, Developing Privacy Policies in Organizations, Security of Enterprise Information Portals, Issues in Outsourcing Security to Managed Security Service Providers, and PKI Infrastructure Development, Secure Online Payment Business Models.

The business research report (20% of the course grade) was specifically designed to meet the objective of addressing management and organizational issues that go beyond technology. It was recommended that students address topics such as cost/benefit analysis, risk management, security awareness training and issues of social engineering, along with technical issues. To create a sense of consistency for peer-reviewers, the format for research reports included the standard chapters of Introduction, Review of Literature, Methodology, Data Analysis, and Summary/Conclusions/Recommendations. Some examples of research reports submitted by students in the past are: Impact of BS7799 Information Security Standard, Applications of Electronic Signatures in Organizations, e-Database Security in dot-com Business, PGP and the Debate Between Strong Encryption and National Security, Computer Forensics in Corporate Environment, Managed Security Service Providers Business Model and ROI, Electronic Signatures and the Law, Use of Biometrics in Business and Government, Mobile Computing & Vulnerabilities of Wireless Application Protocol, MP3 and the Protection of Intellectual Property on the Internet. The research reports and group presentation topics reflect the holistic approach to information security in this course and the broad nature of the information security discipline.

6. CONCLUSIONS

Security is about managing risks. A security officer must be a technology manager, a legal expert, a policymaker, a negotiator, a salesperson and an evangelist (Hayes 2002). To prepare for emerging roles, students in this area must be able to see past the technical boundaries of information security. As more executive-level positions are created to manage risk, graduates may be placed in decision-making roles to develop enterprise security architecture or to meet policy and legal requirements (such as HIPAA data security standards). The rapidly growing security area has ramifications for technology-dependent organizations in which employees connect to corporate networks from remote sites, using a variety of computing devices. Security officers should be aware that the e-boundaries of corporate networks go beyond physically wired networks in a corporate building or campus, and policies must be established to maintain the

confidentiality, integrity, and availability of information. Information is the most valuable asset in an organization and must be protected.

To address these issues and to provide a balance between the technology and management of information security, a course model was presented here that demonstrates the business value of information security. After going through several iterations and reviewing feedback from students and other faculty members, this course has evolved to emphasize security as a process rather than a product. Due to the changing nature of information security, the course is updated every time it is offered to reflect current topics and business cases (e.g., changing laws involving privacy, terrorism, encryption, and cybercrime). In Spring 2001, the course was rated among the top 15% for excellence in teaching of all the business management courses offered in the school. Use of face-to-face meetings along with a strong online component has provided students an opportunity to interact and discuss the issues of information security that drive business in the knowledge economy.

As the area of information security management gains increased importance due to the strategic role of technology in organizations and current events that impact areas such as disaster recovery and enterprise continuity planning, it is hoped that courses such as the one described in this paper can be adapted by other educators to meet emerging needs of the discipline. Increased enrollments in information technology and e-business programs have created an opportunity for security related courses to be offered in the curriculum either as required courses or as electives. Further research into curriculum development and best practices in this area is needed because of the mission-critical nature of security for today's Netcentric organizations.

7. ACKNOWLEDGEMENTS

The author would like to acknowledge the assistance of Antra Arora, Database Consultant, for research and development of the Risk Management exercises used in the course.

8. REFERENCES

Alavi, M., Y. Yoo, and D. Vogel (1997) "Using information technology to add value to management education", Academy of Management Journal, 40(6), pp.1310-1333.

Allen, J. et. al. (2000) Improving the security of networked systems, Available from: http://www.stsc.hill.af.mil/crosstalk/2000/oct/allen.asp

Bayuk, J. (2001) "Security metrics: How to justify security dollars and what to spend them on", Computer Security Journal, 17(1), pp. 1-12.

Chen, A. (2001) "M-commerce security: A moving target", eWeek, 18(2), pp. 46-60.

Cornell, R. and B. Martin (1997) "The role of motivation in web-based instruction" in Khan, B. A. (ed.), Web-Based Instruction, Englewood Cliffs: NJ: Educational Technology Publications, pp. 93-100.

Denning, D. (2001) "Cyberwarriors: Activists and terrorists turn to cyberspace", Harvard International Review, 23(2), pp. 70-75.

Frost, P. J. and C. V. Fukami (1997) "Teaching effectiveness in the organizational sciences", Academy of Management Journal, 40(6), pp. 1271-1281.

Hayes, M. (2002, February 25) "Impact player" Information Week, issues 877, pp. 34-41.

Hazari, S. I. (2000) "Implementation and Outcomes of Business Course Development Tool", Journal of Business, Education, and Technology, 2(1), pp. 30-39.

Hazari, S. I. And D. Schnorr (1999) "Leveraging Student Feedback to Improve Teaching in Web Based Courses", Technological Horizons in Education Journal, 26(11), pp. 30-38.

Highland, H. (1993). "A View of Information Security Tomorrow" in Dougall, E (ed.), Computer Security. Holland: Elsevier Science Publishers.

Hildebrand, J. E. (1995) "Videoconferencing in the business curriculum", Journal of Business and Technical Communication, 9, pp. 228-240.

Kinshuk, J. C. and A. Patel (2001) "Implementation issues in web-based training" in Khan, B. A. (ed.) Web-based training. NJ: Educational Technology Publications.

Leidner, D. E. and S. L. Jarvenpaa (1993) "The information age confronts education: Case studies on electronic classrooms", Information Systems Research, 4 (25-54).

Moore, M. and G. Kearsley (1996) Distance Education: A Systems View, Belmont, CA: Wadsworth Publishing.

Murphy, B., R. Boren, R. and S. Schlarman (2000) Enterprise Security Architecture, CRC Press. Available from http://www.pwcglobal.com

Nichols, R., Ryan, D. J., and Ryan, J. C. (2000) Defending your digital assets, New York, NY: McGraw-Hill.

Rogers, C.R. & Freiberg, H.J. (1994) Freedom to Learn (3rd Ed). Columbus, OH: Merrill/Macmillan.

Schneier, B. (2000) Secrets and lies: Digital security in a networked world, New York, NY: John Wiley

Summers, R. (1997) Secure computing: Threats and safeguards, New York, NY: McGraw-Hill.

Troutt, M. (2002) "IT Security issues: The need for end user oriented research", Journal of End User Computing, pp. 48-49.

Webster, J. and P. Hackley (1997) "Teaching effectiveness in technology-mediated distance learning", The Academy of Management Journal, 40(6), pp.1282-1309.

AUTHOR BIOGRAPHY

Sunil Hazari is Adjunct Professor in the Robert H. Smith School of Business and Faculty Research Associate in the Office of Information Technology at University of Maryland, College Park. His teaching and research interests are in the areas of Information Security, Infrastructure Design of E-commerce sites, Web Usability, and organizational aspects of eLearning. He has authored several peer-reviewed journal publications in Information and Instructional Technology areas, has presented at national conferences, and has been technical editor of over a dozen Internet Technology books. He is also a certified online instructor, and has been project manager for application software development, managed IT facilities, and conducted technology training workshops for industry professionals. For further details see http://sunil.umd.edu

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.

ISSN 1055-3096