JOURNAL OF INFORMATION SYSTEMS
Vol. 21, No. 1
Spring 2007
pp. 123–148

A Draft of an Information Systems Security and Control Course

L. Melissa Walters
The University of Tampa

ABSTRACT: Proficiency with information systems (IS) and their supporting information technologies has become a core competency for accounting professionals; and because of its close relationship to internal control, IS security has evolved into a critical aspect of that competency. Unfortunately, IS security is not widely included within the core body of knowledge typically offered by business curriculums. This essay is intended first, to make a case for the importance of explicitly addressing IS security as part of an accounting curriculum and second, to provide some practical guidance to accounting information systems (AIS) educators who would like to develop and offer an IS security and control course (or otherwise incorporate more comprehensive coverage of information security topics into an already existing systems course). The course draft presented here is based on the author's experiences in designing, developing, and teaching an IS security course as a core course within an AIS curriculum.

Keywords: accounting; information systems; information security.

I. INTRODUCTION

What is Information Systems (IS) Security?

In the broadest sense, IS security (also commonly referred to as "information security") refers to organizational measures taken to protect and control IS resources, so as to reduce the risks and impacts of system vulnerabilities and threats to a level that is considered acceptable by an organization. IS resources would typically include people, procedures, technology (hardware, software, and netware), facilities, and perhaps most importantly, the data or information processed by, accessible via, or transmitted through the system. Information security concepts are rooted in principal concerns for confidentiality (regarding access to and privacy of data/information), integrity (regarding accuracy, authenticity, validity, completeness, and consistency of data/information), and availability (regarding reliability of and timely access to information resources) (see Harris 2003; Hansche et al. 2004; Krutz and Vines 2003; Whitman and Mattord 2005). Information security practices encompass formal (security governance and management), technical (technological safeguards, countermeasures, and controls), and informal (awareness, education, and ethics) aspects of securing organizational IS (Dhillon 2007). The field of information security is vast, dynamic, and above all, exceedingly complex; however, most

The author thanks the editor, an associate editor, and an anonymous reviewer for *Journal of Information Systems* (*JIS*), as well as two anonymous reviewers for the 2005 American Accounting Association (AAA) Information Systems (IS) Section Mid-Year Meeting for their insightful comments and helpful suggestions on improving earlier versions of this manuscript. The author would also like to thank the participants at the AAA IS Section Mid-Year meeting and the 2005 AIS Educator's Conference for their enthusiastic interest and supportive feedback. Last but certainly not least, the author would like to acknowledge her students for their hard work and constructive comments on improving the course.

security professionals would probably agree that the relevant common body of knowledge would encompass at least ten key domains of study: security management; security architecture and models; access security; application and systems development security; communications, network and Internet security; cryptography; operations security; physical security; continuity planning; and law, investigation, and ethics.[1]

Why Teach IS Security to Accounting Students?

Because evolving business processes and practices are so inextricably tied to IS and their supporting information technologies, IS proficiency has become a core competency for accounting professionals (see AICPA 1999; IFAC 2003a, 2003b); IS security has evolved into an obligatory component of that competency (see Boritz 1999; IFAC 2003a, 2003b). Indeed, information security has earned a place at the top of the American Institute of Certified Public Accountants' (AICPA) *Top Ten Techs* (for the fourth consecutive year) as the most important technology issue affecting the accounting profession (see AICPA 2003, 2004, 2005, 2006).[2] There are a number of interrelated reasons for the growing importance of information security to accounting professionals; among the most significant are the proliferation of the IS threats, the relationship between information security and internal control, and the corollary relevance of information security for Sarbanes-Oxley compliance.

One of the consequences of greater connectivity and expanded reliance on information technology is exposure to a broader spectrum of IS threats and risks. Computer and Internet abuse have evolved into serious problems with significant operating and financial consequences (e.g., see Gordon et al. 2005). Threats to IS resources have increased at an alarming rate and have become ever more virulent; over 180,000 known programmed threats exist today (McAfee AVERT Virus Information Library http://vil.nai.com/vil/) with 7 to 10 new viruses discovered *each day* (F-Secure http://www.f-secure.com/products/radar/). Moreover, methods employed by cyber criminals to gain unauthorized access, attack networks, exploit system vulnerabilities, or otherwise threaten system availability and information integrity have evolved in sophistication (along with advances in information technology) and have become progressively more perilous. Successful attacks can result in incapacitated web servers, crippled networks, theft of proprietary data, corrupted or lost financial and operating data, and financial fraud with costs of recovery and/or remediation often amounting to millions of dollars (Gordon et al. 2005). Due to the increasing importance of IS resources to business functions and the unrelenting proliferation of such IS threats, information security has become a key enabler of business (Dhillon 2007, vi); *and* because many of these threats have the potential to significantly impact the accuracy and reliability of financial data processed by an organization's IS, an understanding of IS risk management and control is now requisite to the development of sound internal control practices.

Indeed, there is a close relationship between internal control and IS security; and in many cases, information security is requisite to ensuring the reliability of financial data. For most organizations, the accuracy and reliability of financial information will be directly dependent upon the information technology that forms the basis of an organization's IS

[1] These ten domains are based on the International Information Systems Security Certifications Consortium (ISC)^2 Common Body of Knowledge (CBK).

[2] Interestingly, information security actually encompasses five of the ten technologies on the AICPA's *2006 Top 10 Technologies* list (#1 Information Security, #3 Disaster and Business Continuity Planning, #5 Privacy Management, #6 Digital Identity and Authentication Technologies, and #10 Spyware Detection and Removal) as well as three of the honorable mention technologies (#11 Email Filtering Including Spam and Malware Scanning, #13 Storage and Backup Technologies, #14 Patch and Network Management Tools).

(Fox and Zonneveld 2003); information technologies are used to initiate and execute financial transactions, process and house the data resulting from those transactions, and report and disseminate financial results. Because information security is directed at protecting and controlling these information technology resources, it has a *pervasive* impact on the integrity of information processing activities as well as the accuracy and reliability of the resulting information. For instance, strong system access controls prevent unauthorized individuals from accessing system data and in turn, protect that data from unauthorized alteration, corruption, or destruction. Good network security reduces the risk of data being intercepted or altered by unauthorized parties during transmission from one network host to another. Proper software application controls minimize the likelihood of data inaccuracies during processing. This pervasive impact on data integrity makes information security a close ally to internal control. Moreover, because of this relationship to internal control, IS security becomes a requisite consideration for Sarbanes-Oxley compliance and as such, of fundamental interest to accounting professionals.

The Sarbanes-Oxley Act of 2002 (SOX) redoubles the importance of internal control, and while information security was not explicitly considered in the development of the Act (Regan 2003); it is emerging as an obligatory aspect of compliance (Byrum 2003; Harrison 2005a, 2005b, 2005c; Proctor and Vignaly 2004). IS security concerns are relevant to Section 404, regarding management responsibility for internal control, as well as Section 302, regarding corporate responsibility for financial reports (Byrum 2003). Section 404 requires management to establish and maintain an adequate internal control structure and assess the effectiveness of internal controls over financial reporting on an annual basis; and Section 302 requires corporate officers to certify the accuracy of both financial and other nonfinancial information contained in quarterly and annual reports. Because most organizations' transaction processing and financial reporting functions are heavily dependent on IS (and their supporting information technologies), information security controls that promote the reliability of IS resources and as a corollary, the confidentiality, integrity, and availability of the resulting financial data are encompassed by the requirements of SOX Sections 404 and 302 and, therefore, must be considered and assessed by management (see Byrum 2003). Section 404 compliance necessitates confidence in the reliability of the systems and technologies that house, process, and transmit financial data; and Section 302 compliance necessitates confidence in the accuracy of the data that relies on those IS resources for processing, storage, and accessibility. Without proper information security, organizations cannot confidently validate the effectiveness of their internal controls nor can they confidently certify the integrity of their financial information (Byrum 2003; Proctor and Vignaly 2004).

The general role of information security in SOX compliance is in the provision of a safe and reliable IS infrastructure within which financial processing and reporting can be conducted. Key to appreciating the complexity of this charge is in understanding that financial data does not reside in a single place within an organizational IS; financial data may reside in (or be transmitted across) numerous computers, systems, databases, and/or network hosts during collection and processing (Harrison 2005c). Identifying which systems and technologies make up or impact financial reporting systems and then designing information security controls to protect the integrity of financial information that resides in or passes through those systems is a daunting task (Harrison 2005c), a task that necessitates the convergence of two traditionally distinct disciplines: information technology (i.e., information security) and accounting (i.e., internal control). SOX compliance requires an amalgam of strong accounting practices *and* good information technology controls. Information technology professionals do not typically possess the requisite accounting competencies and knowledge of internal control processes necessary to assess the impact of IS security vulnerabilities on internal control (Fox and Zonneveld 2003), so the task falls heavily on accountants (making information security a requisite competency for accounting professionals).

Unfortunately, IS security is not widely included within the core body of knowledge typically offered by business curriculums (Whitman and Mattord 2006a), and coverage of information security topics within traditional AIS courses is constrained by competing subject matter and time constraints. There is a *need* for explicit, *comprehensive* coverage of IS security topics within an accounting curriculum because of the close relationship between IS security and internal control and the corollary importance of IS security to SOX compliance. IS security has become an integral part of the professional accountant's requisite body of knowledge as well as a significant aspect of what practicing accountants do.[3] An IS security and control course (such as the one described in this paper) would address this need and provide accounting graduates with a more pragmatic, more inclusive understanding of this critical topic.

The purpose of the remainder of this essay is to provide some guidance to AIS educators who would like to develop an IS security and control course (or otherwise incorporate more comprehensive coverage of information security topics into an already existing AIS course). The next section addresses issues of course design, including course objectives, recommended core topics, and suggested assignments. The following section presents various preparatory resources designed to assist prospective instructors in developing course materials and assignments. The final section presents reflections on the development and implementation of the course along with a few closing remarks.

II. COURSE DESIGN

Course Framework

The IS security and control course described here is intended to provide a broad but pragmatic view of the field of information security for accounting/business students. The International Information Systems Security Certifications Consortium $(ISC)^2$ Common Body of Knowledge (CBK) provides a useful as well as widely referenced, widely recognized framework for constructing course objectives and developing core topical content to accomplish this general goal. The $(ISC)^2$ is a nonprofit organization that exists for the stated purposes of standardizing and maintaining a CBK for information security professionals, providing an international standard for professional certifications in the area of information security, providing education and administering certifications for information security professionals and practitioners, and ensuring that professional competencies are maintained through continuing education and periodic recertification requirements (www.isc2.org). As the $(ISC)^2$ administers the two primary and most sought-after certifications for IS security professionals, the *Certified Information Systems Security Professional (CISSP)* certification

[3] For instance, IS audits to assess the proper implementation, operation, and control of IS resources are becoming a significant component of both internal and external (financial) audits (Hall 2007). Information security topics (Protection of IS Assets, Business Continuity and Disaster Recovery) constitute approximately 45 percent of the Information Systems Audit and Control Association (ISACA) *Certified Information Systems Auditor* (CISA) content knowledge areas (effective 2006; see www.isaca.org/certification). The closely related area of Information Technology Governance, which includes knowledge of IS risk management methods and tools as well as IS control frameworks (COSO, CobiT, and ISO/IEC 17799), accounts for a further 15 percent of the CISA knowledge requirements.

and the *System Security Certified Practitioner (SSCP)* certification, its CBK has become widely regarded and generally accepted as an international base knowledge standard for information security managers and practitioners.

The (ISC)^2 CBK domains required for the CISSP certification address what are generally regarded by most information security texts and professionals as the most business critical aspects of IS security (Whitman and Mattord 2005); the (ISC)^2 CISSP CBK encompasses ten key domains of knowledge (see www.isc2.org; also see Harris 2003; Hansche et al. 2004; Krutz and Vines 2003). Table 1 provides a list of these ten CBK domains along with a brief description of what each domain encompasses.[4]

Course Objectives

Specific course objectives are based on the general scope chosen for the course, the knowledge standard provided by the ten (ISC)^2 CISSP CBK domains, as well as consideration for the type of students that would most likely be taking the course. The IS security and control course described in this essay is primarily intended for upper-level, undergraduate accounting students (juniors and seniors) who have already taken a foundational AIS

TABLE 1
(ISC)^2 CISSP CBK Ten Knowledge Domains

Domain 1: Information Security Management (encompasses security management concepts, security policy, security awareness, risk management, data classification, personnel roles and responsibilities).

Domain 2: Security Architecture and Models (encompasses system architecture, protection mechanisms, trust assurance, security models).

Domain 3: Access Control Systems and Methodology (encompasses access control methods; administrative, logical, and physical access controls; monitoring and audit mechanisms).

Domain 4: Applications and Systems Development Security (encompasses systems development methods, application software controls, database management system controls, change controls).

Domain 5: Operations Security (encompasses computer operation controls, system resources controls, media controls, data processing controls, administrative/personnel controls, monitoring/auditing of controls).

Domain 6: Cryptography (encompasses cryptographic technologies, cryptographic standards, key distribution and management, public key infrastructure, security applications).

Domain 7: Physical Security (encompasses perimeter and site security, facility and data center security, emergency procedures, and environmental controls).

Domain 8: Telecommunications, Network, and Internet Security (encompasses physical security of netware, network and data access security, network traffic management and security, remote access management, intrusion detection, network availability and recovery planning).

Domain 9: Business Continuity Planning (encompasses plan initiation, business impact analysis, recovery strategies, plan implementation, plan testing, and plan maintenance for continuity plans such as incident response, contingency, and disaster recovery plans).

Domain 10: Law, Investigations, and Ethics (encompasses computer crimes, cyberspace law, investigations of computer crime, incident handling, ethical computing).

[4] Note that the ten CBK domains presented appear in different sequences across different security texts and resources; moreover, the specific content of each of the ten domains is subject to a certain amount of interpretation. Table 1 describes the content of each domain based on three widely recognized CISSP prep texts (Harris 2003; Hansche et al. 2004; Krutz and Vines 2003) and presents the order of the domains as they are presented in the Hansche et al. (2004), the official CISSP prep textbook sanctioned by the (ISC)^2.

course. As such, specific learning objectives (and topical content) were constructed to address those aspects of information security most relevant to contemporary business practices, to facilitate the development of core accounting and business competencies, and to accommodate relatively nontechnical accounting students. Suggested objectives for the course and how they correspond to the ten (ISC)^2 CISSP CBK domains (from Table 1) are presented in Table 2.

Course Content

Core content for the course was developed by adapting the subject matter covered by the ten (ISC)^2 CISSP CBK domains to accommodate a pragmatic business focus as well as the technology skills that could reasonably be expected of accounting students. Table 3 provides a suggested list of core topics and indicates the (ISC)^2 CISSP CBK domains (from

TABLE 2
Suggested Course Objectives

The objectives of the IS Security and Control Course are to:

1. Provide students with an articulate working understanding of the technical language of information security (all ten CBK domains).
2. Develop students' awareness of the practical importance of information security for individuals and organizations (CBK domains 1 and 10).
3. Provide students with a pragmatic understanding of foundational information security concepts (all ten CBK domains but especially domains 1 and 10).
4. Provide students with an understanding of the nature and implications of information technology as it relates to specific threats and/or domains of information security (all ten CBK Domains).
5. Familiarize students with the nature of, the potential for harm from, and the potential business implications of the principle vulnerabilities of and threats (nonsubversive and subversive) to IS resources (all ten CBK domains but especially domains 1 and 10).
6. Familiarize students with the information security methods and practices necessary to protect IS resources (all ten CBK domains).
7. Provide students with a pragmatic understanding of the real-world particulars associated with the application of information security concepts and practices (all ten CBK domains but especially Domain 1).
8. Develop students' critical awareness of an organization's institutional, legal, ethical, and social responsibilities regarding IS security (CBK Domain 10).
9. Develop students' critical awareness of the potential implications of significant prevailing and/or emerging issues related to or affecting information security concepts and practices (CBK domains 1 and 10).
10. Provide students with a forum for demonstrating and honing their oral and written communications skills, practical application skills, critical evaluation skills, ethical reasoning skills, foundational business technology skills, and electronic research skills (CBK Domain 1, see footnote).[a]

[a] Objective 10 does not correspond *directly* to any of the ISC^2 CISSP CBK domains; although it does corresponded *indirectly* to Domain 1 (security management practices) as both security managers and practitioners need to possess sound communication skills, assessment skills, technology skills, and research skills. This objective was intended as a general educational objective directed towards core competencies generally expected of accounting and business graduates. Traditional accounting curriculums have oft been criticized for failing to provide the necessary individual skills and abilities demanded by the accounting profession; written and oral communication skills, critical thinking skills, ethical reasoning skills, information technology skills, and research skills are often cited as wanting in accounting graduates (For further discussion, see Albrecht and Sack 2000).

Table 1) and course objectives (from Table 2) to which each topic corresponds. Note that this suggested list of core topics is comprehensive and relatively independent of course textbook selection. Appendix A presents suggested modules along with brief subject matter descriptions and content suggestions for each of the core topics listed in Table 3.[5]

Suggested Assignments and Activities

This section briefly describes a number of suggested student assignments and activities. Suggested assignments and course activities are designed to support course objectives (Table 2) and address core topics (Table 3).

Online Research

There is an almost unlimited amount of information relating to information security topics available online at no cost. Online research assignments may be used to specifically address prevailing or emerging issues, compensate for lack of text coverage, or to promote in-depth study of selected topics beyond coverage in the course text. Students may be asked to investigate technical topics via online resources, peruse assigned websites addressing a particular subject, supplement their course text readings with articles or white papers available online, or simply surf the web for interesting information related to course topics. Web

TABLE 3
Suggested Core Topics

Topical Area	CBK Domain	Course Objective
Information Security Foundations		
1. Introduction to Information Security	1	1, 2, 3, 4
2. Information Security Principles	1	1, 3, 4, 6
3. IS Threats, Vulnerabilities, and Exposures	1	1, 2, 3, 4, 5, 9
Information Security Management		
4. Security Management Responsibilities	1, 10	3, 6, 7, 8, 9
5. Information System Risk Management	1	1, 2, 3, 5, 7
6. Security Policy and Awareness	1	1, 3, 7
7. Information Security Standards/Frameworks	1, 2	1, 3
Security Methods and Controls		
8. Access Security	3	1, 3, 4, 6, 7
9. Application and System Development Security	4	1, 3, 4, 6, 7
10. Network and Internet Security	8	1, 3, 4, 6, 7
11. Cryptography	6	1, 3, 4, 6, 7
12. Operations/Data Center Security	5	1, 3, 4, 6, 7
13. Physical Security	7	1, 3, 4, 6, 7
14. Remediation Practices	9	1, 3, 4, 6, 7
Special (Optional) Topics		
15. Computer Crime Investigation	10	2, 3, 7, 8, 9
16. Ethical Computing	1, 10	2, 3, 6, 7, 8, 9
17. IS Auditing	1, 5	3, 6, 7
18. Legal Aspects of Information Security	10	2, 3, 7, 8, 9
19. Personal Computer Security	Aspects of All	2, 7
20. Privacy Issues	10	2, 3, 7, 8, 9

[5] In the interests of space and to avoid redundancy, the author's syllabus for this course is not reproduced here; interested instructors should contact the author.

research assignments require student initiative, support active learning, and encourage critical reasoning by affording students the opportunity to explore available resources, ferret out key issues, analyze information, form their own opinions, and synthesize their own understanding of the subject matter based on a variety of resources. An illustrative example of a web research assignment on malware is presented in Appendix B.

Security News Summaries

News events are valuable for initiating and enhancing participative class discussions, promoting interaction between students, and emphasizing particular events or topics that are either lacking or have been afforded only cursory coverage in the primary course text. Students may be asked to search for, summarize, and comment on news events of relevance to course topics or material. Searching for relevant news events promotes awareness of prevailing and/or emerging issues related to or affecting information security concepts and practices. Moreover, selecting news events to bring to class affords students a measure of control over course content and class discussions and as such, may encourage students to develop a more active interest in the subject matter.

Practical Assignments and Lab Exercises

Professional accountants need both conceptual IS understanding and practical IS skills (IFAC 2003b). Practical assignments provide students with the opportunity to apply IS security concepts to specific problems; and hands-on lab exercises provide students with the opportunity to develop pragmatic IS security skills. Practical assignments may be designed as short-term projects, team assignments, or in-class exercises (an illustrative example of a practical team assignment on security policy development is presented in Appendix C). Lab exercises may be constructed to provide hands-on experience downloading, installing, configuring, and/or using common security tools and products. Use of free online tools such as McAfee's *FreeScan*, *Wi-Fi Scan*, and *My SecurityStatus* (http://us.mcafee.com/root/catalog.asp?catid=free) or freeware such as *Zone Alarm* or *Ad-Aware* facilitates the development of useful lab exercises and makes access to requisite software convenient for students. The Whitman et al. (2006) *Lab Manual* (discussed below) provides a number of hands-on lab exercises utilizing freeware products; alternatively, exercises may be constructed according to individual instructor needs or preferences.

Team Project

A team project may be used to give students the opportunity to study real-world IS security policies and practices and apply IS security concepts to real-world system problems. Team projects may be constructed in a number of different ways and may vary with respect to comprehensiveness; an overview of one possible team project (developed for the course) is presented in Appendix D. The comprehensive project described in Appendix D addresses security management practices (security policy and risk assessment) and security methods and controls consistent with course objectives and core topics suggested for the course.

III. COURSE DEVELOPMENT RESOURCES

This section provides a brief description of preparatory resources that may assist instructors to develop an IS security and control course.

Primary Course Text and Supplements

Although a course text is not absolutely necessary (as the course can be taught utilizing online resources and supplementary readings, see below), it provides structure for the course and a place for instructors to start. The ideal text would be consistent with the framework (Table 1) and objectives (Table 2) selected for the course, provide reasonable coverage of desired core content (Table 3), and be written at a technical level appropriate for upper-level, undergraduate accounting students. A number of different texts from different publishers were reviewed based on the following dimensions: pragmatic focus, topical coverage, technical complexity, and instructor support. The following texts are suggested: Whitman and Mattord (2005) *Principles of Information Security* (as a primary course text), Whitman and Mattord (2006) *Readings and Cases in the Management of Information Security* (as a supplementary course text), and Whitman et al. (2006) *Hands-On Information Security Lab Manual* (as a supplementary course text). A brief description and rationalization for each text is discussed below.

The Whitman and Mattord (2005) *Principles* text provides a broad view of the field of information security with enough technical detail to afford a sound understanding of subject matter; and as both of the authors are CISSP holders, its contents are heavily influenced by the (ISC)^2 CBK, the framework recommended above as a base knowledge standard for developing course content. The text is well written and organized, provides a reasonable table of contents for an introductory information security course,[6] effectively balances the managerial and technical aspects of the subject matter, and approaches information security from a practical real-world perspective. The text is not *overly* technical and as such, it is appropriate for junior/senior undergraduate accounting majors with a foundational understanding of IS concepts (as would likely be acquired through an introductory AIS or MIS course). Additionally, the text is well supported with online resources (e.g., an instructor's manual, illustrations files, PowerPoint presentations, solutions to exercises, and recommended syllabi), provides reasonable end-of-chapter pedagogy (discussion questions, hands-on exercises, and minicases), and provides insightful material for further study throughout the chapters. Moreover, the text may be easily supplemented by both a readings and cases text and a lab exercises manual (both designed to compliment the *Principles* text).

The Whitman and Mattord (2006) *Readings and Cases* text provides a set of supplemental readings (articles, best practices, and cases) based on real-world scenarios, pragmatic security issues, and real-world practices. The readings do a nice job of providing insights into the real-world relevance and pragmatic importance of information security as well as the logistics and difficulties of formulating and implementing good information security practices. The readings also provide a good resource for developing research assignments whereas the cases are valuable for use as class discussion material, writing assignments, or team assignments.

The Whitman et al. (2006) *Lab Manual* includes a number of detailed hands-on lab exercises as well as a CD-ROM containing full versions of the requisite freeware used in the lab exercises. The lab exercises compliment the Whitman and Mattord (2005) *Principles* text nicely, addressing topics such as footprinting, network security tools, information security management, and computer forensics. Lab exercises range from simple introductory

[6] Although the Whitman and Mattord (2005) *Principles* text does *not* provide comprehensive coverage of *all* of the security methods and controls areas suggested as core topics for the course (see Table 3), it provides a sound foundation to start from and may be supplemented via readily available web resources (see Table 5 for an illustrative list of helpful websites), online readings, and supplementary readings from other texts (see Table 4).

exercises to more technical security-specific exercises; and each lab section includes detailed descriptions of the relevant software tool or tools, step-by-step instructions and explanations of procedures, sample screenshots, and practice questions.

Other Information Security Texts

There are countless texts on information security available. Although most are oriented towards practitioners (many specially designed for professional certification exam preparation), narrowly focused on a particular aspect of information security (such as firewalls or cryptography), or are a bit too technical for use as a course text (for an accounting course); a number of these texts are excellent resources for course development and instructor preparation, and a few provide useful supplementary readings for students. For example, the Bosworth and Kabay (2002) *Computer Security Handbook*, is a helpful preparatory resource and in addition, is a particularly suitable source of supplementary readings for students. Table 4 provides an illustrative list of potentially helpful information security texts.

Web Resources

Online resources are invaluable for developing an information security course. Sites such as the Computer Ethics Institute (CEI) (http://www.brook.edu/its/cei/cei_hp.htm), the Computer Security Institute (www.gocsi.com), the Electronic Privacy Information Center (EPIC) (www.epic.org), and FraudWatch International (http://fraudwatchinternational.com) provide a number of informational resources useful for developing course content, preparing class lectures/discussions, or constructing student assignments. In

TABLE 4
Illustrative List of Information Security Texts

- Bosworth, S. and M. E. Kabay, 2002. *Computer Security Handbook*. New York, NY: John Wiley & Sons.[a]
- Brewer, D. C. 2005. *Security Controls for Sarbanes-Oxley Section 404 IT Compliance: Authorization, Authentication, and Access*. Indianapolis, IN: Wiley Publishing.
- Campbell, P., B. Calvert, and S. Boswell. 2003. *Security + Guide to Network Security Fundamentals*. Boston, MA: Thomson Course Technology.
- Ciampa, M. 2004. *Security Awareness: Applying Practical Security in Your World*. Boston, MA: Thomson Course Technology.
- Dhillon, G. 2007. *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ: John Wiley & Sons, Inc.
- Erbschloe, M. 2003. *Guide to Disaster Recovery. Canada*: Boston, MA: Thomson Course Technology.
- Gollmann, D. 2006. *Computer Security*. 2nd edition. New York, NY: John Wiley & Sons.
- Hansche, S., J. Berti, and C. Hare. 2004. *Official (ISC)^2 Guide to the CISSP Exam*. Boca Raton, FL: Auerbach/CRC Press.
- Harris, S. 2003. *All-in-One CISSP Certification Exam Guide*. Second edition. Emeryville, CA: McGraw-Hill/Osborne.
- Holden, G. 2003. *Guide to Firewalls and Network Security*. Boston, MA: Thomson Course Technology.
- Krutz, R. L., and R. D. Vines. 2003. *The CISSP Prep Guide*. Gold edition. Indianapolis, IN: Wiley Publishing, Inc.
- Maiwald, E. 2004. *Fundamentals of Network Security*. Burr Ridge, IL: McGraw-Hill.
- Tipton, H. F., and M. Krause. 2003. *Information Security Management Handbook*. Fourth edition. Boca Raton, FL: CRC Press.

[a] This edition of the Bosworth and Kabay (2002) *Computer Security Handbook* is a bit dated; however, according to Wiley, a new edition is planned for Spring 2008.

addition, online dictionaries such as *Netlingo* (www.netlingo.com), *Whatis*? (http://whatis.techtarget.com/), and *Webopedia* (http://www.webopedia.com/) are good resources for students as they are easy to use and contain many, if not most, technology terms students will be likely to come across in their studies; moreover, entries often contain links for related terminology or links directing the reader to other resources on the topic. An illustrative list of helpful security-related web resources is included in Table 5.

In addition, there is a plethora of electronic texts, white papers, reports, and articles available online; these online texts may be used to support instructor preparation or otherwise supplement the primary course text. For instance, the *CSI/FBI Computer Crime and Security Survey* (an annual report on computer crime and security trends based on the results of a survey of computer security practitioners) is particularly good supplemental reading material for students; the CSI/FBI report is available each year and may be downloaded in PDF format at no cost from the CSI site (see http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml). Additionally, the CERT Coordination Center at Carnegie Mellon (www.cert.org) offers a selection of online articles, reports, and papers; and the SANs Institute's Reading Room (http://www.sans.org/rr/) offers a number of useful whitepapers on a variety of security topics, all of which may be downloaded in PDF format at no cost.

Security News Events

There are almost limitless online sources of information security news. For example, news services such as CNN (www.cnn.com/TECH/) and online trade publications such as *Computerworld (*www.computerworld.com), *EWeek* (http://www.eweek.com/), *Infoworld* (www.infoworld.com), and *PC World* (www.pcworld.com) regularly contain information security-related news; and on occasion, professional business publications such as *Business Week Online* (www.businessweek.com), *CFO-IT* (www.cfo.com), *Strategic Finance*

TABLE 5
Illustrative List of Information Security Web Resources

- Association of Certified Fraud Examiners (ACFE)—http://www.cfenet.com/home.asp
- Computer Center Response Team (CERT) at Carnegie Mellon University—www.cert.org
- Computer Ethics Institute (CEI): http://www.brook.edu/its/cei/cei_hp.htm
- Computer Professionals for Social Responsibility (CPSR): http://www.cpsr.org/
- Computer Security Institute—www.gocsi.com
- Computer Security Resource Center (CSRC)—http://csrc.nist.gov/fasp/
- Computer Incident Advisory Capability (CIAC)—www.ciac.org/ciac/
- Electronic Privacy Information Center (EPIC)—www.epic.org
- F-Secure: http://www.f-secure.com/
- Fraud Watch International: http://www.fraudwatchinternational.com/
- Happy Hacker—http://www.happyhacker.org/indexb.shtml
- Information Systems Audit and Control Association (ISACA)—www.isaca.org
- Information Systems Security Association (ISSA)—www.issa.org
- Infragard (private industry and FBI)—http://www.infragard.net/
- International IS Security Certifications Consortium (ISC^2)—www.isc2.org
- IT Governance Institute (ITIG)—http://www.itgi.org/
- Internet Security Alliance—http://www.isalliance.org/
- On Guard Online (FTC site)—www.onguardonline.gov
- MacAfee: http://www.mcafee.com/us/default.asp
- Online Dictionaries—www.netlingo.com, http://whatis.techtarget.com/
- Symantec—www.symantec.com/
- SANS Institute—http://www.sans.org/
- Miscellaneous—www.informit.com, www.securityfocus.com, www.securitystats.com

(www.strategicfinancemag.com), and the *Wall Street Journal* (www.WSJ.com) also carry security relevant news items.

In addition to security-related news items, there are numerous information security notification/alert services available online, many available at no cost. Such services help to keep instructors up to date on the most recent threat activity and security news and often provide for interesting topics for class discussions. For instance, the *US-CERT/CC Advisories* (http://www.cert.org/advisories/us-cert-announcement.html) provide updates on frequent and or high-impact security vulnerabilities or incidents being reported; and *Microsoft Technical Security Notifications* provide security updates concerning Microsoft products (http://www.microsoft.com/technet/security/bulletin/notify.mspx). *Network Associates' ADVERT Alerts* (http://vil.nai.com/vil/content/alert.htm) and *F-Secure's Security Center* (http://www.f-secure.com/security_center) provide email alerts concerning malware threats; and *FraudWatch International* (http://www.fraudwatchinternational.com/) provides news and email updates on Internet frauds.

Freeware

Freeware and other free online tools are superb resources for in-class illustrations and /or hands-on lab exercises.[7] These free applications and tools are, for the most part, easily accessible and user friendly and provide an opportunity for students to gain hands-on experience downloading, configuring, and/or working with a variety of computer security-related products. A short illustrative list of available freeware and free online tools is included in Table 6.

Gurus and Sages

Outside experts are invaluable resources for acquiring knowledge and insights into the practical aspects of information security. Guest speakers give students a greater appreciation for course topics by reinforcing the real-world relevance of the subject matter and by providing insights into the day-to-day logistics and difficulties of managing information system security. Moreover, engaging guest speakers often provides for excellent coverage of subject matter (especially where an instructor's technical or practical knowledge may be

TABLE 6
Illustrative List of Freeware/Free Online Tools

- Ad-Aware (anti-adware/spyware): http://www.lavasoftusa.com/software/adaware/
- Firefox (web browser): http://www.mozilla.org/products/firefox
- F-Secure (online virus scanner): http://www.f-secure.com/
- McAfee (scan tools): http://us.mcafee.com/
- McAfee (Stinger malware removal): http://vil.nai.com/vil/stinger/
- NMAP: http://www.insecure.org/nmap/
- Privacy Bird and Privacy Finder (privacy check): http://www.privacybird.com
- Sam Spade (utility program): www.samspade.org
- Spybot S&D (anti-spyware software): http://www.safer-networking.org/en/home/index.html
- Spyware Nuker: http://www.nuker.com/
- Symantec (malware removal tools): http://www.symantec.com/avcenter/tools.list.html
- Zone Alarm (firewall software): http://www.zonealarm.com/

[7] The Whitman et al. (2006) *Lab Manual*, recommended as a supplementary course text above, bases its lab exercises on available freeware products and tools such as the free utility program *Sam Spade* (www.samspade.org), the free spyware scanner *Spybot Search & Destroy* (http://www.safer-networking.org/en /home/index.html), and the free personal firewall program *Zone Alarm* (http://www.zonealarm.com/).

somewhat limited); and offers the added bonus of allowing instructors to further their own knowledge and understanding of such subjects. University information technology departments, local consulting firms, and local businesses often provide a valuable untapped source of information security expertise and in-the-trenches experience; and many individuals may be more than willing to serve as guest speakers on specific areas of security.

Supplementary texts written by industry experts may also add dimension (and interest) to the course. For instance, Mitnick et al. (2002) *The Art of Deception: Controlling the Human Element of Security* and Mitnick and Simon's (2005) *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers* provide real-world insights into the mindset and techniques of computer crackers. These two texts also provide a basis for discussing security awareness, security policy, as well as specific practices for mitigating the threats associated with such cyber villains. Moreover, both texts offer compelling and fascinating reading.

The Silver Screen

Films involving information security-related issues and implications may also be used to stimulate interest and provide a starting point for reflective discussions on particular topics. Not only do films (that may be viewed during extended class sessions, special sessions, or assigned as outside viewing) provide subject matter for student critique and contemplative dialogues in class, but they also make the class compelling. Films provide insights into social perceptions of the digital age and cyber culture and are particularly useful for broaching and deconstructing myths (especially Hollywood-based myths) regarding cybercrime and information security practices. Suggested films include: *Enemy of the State*, *Firewall*, *Hackers*, *The Net*, *NetForce*, and *Sneakers*.

IV. EXPERIENCES AND REFLECTIONS

Instructor Burden

The dynamic, technological nature of the course subject matter makes it difficult to keep current and places a heavy burden on the instructor in both knowledge and prep time; this burden is exacerbated by difficulties with text selection (discussed below). Use of web research assignments and security news discussions will help to keep instructors current and may relieve instructors of some predatory burden.

As for technical knowledge, it should be noted that the course described here, was not intended to teach technical expertise in specific security applications nor was it designed to enable students, upon completing the course, to become IS security *experts*. The course was designed primarily to provide a broad introduction to IS security concepts and practices. As such, while some foundational technological knowledge is necessary, one does not need to be a computer programmer, network engineer, systems auditor, or certified security professional to effectively teach an IS security course. However, some information security topics are *inherently* more demanding and call for specific requisite technical knowledge; network security and cryptography are good examples. The supplemental information security texts listed in Table 4 are helpful for extended study of specific information security areas as are many of the web resources listed in Table 5. Individuals on staff at university information technology departments may be particularly helpful and more than willing to answer questions or provide helpful suggestions. Additionally, engaging guest speakers in certain areas, such as cryptography, will relieve instructors of some technical preparatory burden, provide excellent coverage of subject matter, and allow instructors to further their own knowledge and understanding of difficult topics.

Finding a Course Text

Finding a primary course text turned out to be a particularly difficult challenge. One of the problems encountered was that many of the information security texts available address a particular specialized topic or a narrow subset of topics (such as network security, firewalls, or disaster recovery planning) making them inadequate for the broad scope chosen for the course; and those with a broader focus often lack detailed coverage of certain topics. Furthermore, a key difficulty lay in balancing the pragmatic focus chosen for the course and technical aspects of the subject matter with the technological skills that could reasonably be expected of accounting students. Pragmatic security texts are often overly technical, too technical for the average accounting student. On the other hand, information security texts oriented towards management often lack sufficient technical detail to afford a sound, pragmatic understanding of the subject matter.

As mentioned above, the Whitman and Mattord (2005) *Principles* text was chosen, despite the fact that it lacked desired coverage of some core topics, because it had a pragmatic focus while still presenting topics at an appropriate technical level for accounting students. Difficulties with text selection place an even greater preparatory burden on the instructor. Supplementary web resources and online readings may be helpful to compensate for lack of topical coverage in the course text and furthermore, allow topical breadth and technical depth for different topics to be adjusted to accommodate instructor (and student) needs. Moreover, once an instructor compiles a good list of supplementary texts, white-papers, and/or other web resources, reading lists may be constructed almost entirely from those resources to supplement or perhaps even replace the need for a primary course text.

Course Format

Instructors may choose to structure the course primarily as a lecture course, a discussion course, a lab-based course, or a project-based course, or alternatively, as some amalgam of the four. This instructor employed a discussion format supported by preparatory web-research and practical/lab assignments; in addition, the team project described in Appendix D provided a pragmatic focus for the course. Customary lectures were kept to a minimum and students were given preparatory notes along with readings, web research, and/or short practice/lab exercises to prepare. Students were expected to prepare assignments before attending class so that each assignment could be used as basis for interactive class discussions. Write-ups for assignments were collected and assignment grades were closely linked to active involvement on the part of *each student for each assignment and each class period*; that is, each class period and each assignment had a participation and contribution component as part of the grade. Students were also asked to keep and turn in an informal web journal summarizing web research performed each week,[8] find and summarize a limited number of news events over the course of the semester,[9] and be prepared to discuss periodic informational emails sent out by the instructor.[10] Despite the increased prep work required by the discussion format, students seemed to embrace the format and most of them participated keenly and eagerly on a class-by-class basis.

[8] The web journal was informal and undemanding; students were simply required to keep track of websites they visited and then turn in their web log at midterm and then again at the end of the term.

[9] Students were required to turn in very short write-ups (one page double-spaced maximum) and briefly introduce (two–three minutes) their news events during class; class time was reserved at the beginning of each class for news event discussions.

[10] This instructor sent out weekly informational emails (typically on security terminology for the week, information security alerts of special relevance, and/or links to interesting course-relevant news) to use as a basis for class discussions.

Project Management

Managing the comprehensive team project (see Appendix D) is a challenge and can become onerous (especially with larger class sizes). The suggested team project for this course was managed by dividing the project up into five individual parts; each part of the project was graded individually and instructor feedback was returned to students before the next part of the project was due. Standardized score sheets based on a simple assessment scale for each section of the project were used to facilitate grading and communicate scores to project teams.[11] Project progress was monitored throughout each stage of the project by requiring brief, mandatory team-instructor check-ins and in-class progress reports during which teams were required to summarize and discuss their project progress to date.

Dividing the project up into separate parts due at different times throughout the semester seemed to simplify project management for student teams; it also spread project grading out over the semester and provided students with feedback on their work before they continued on to the next part of the project. Project check-ins seemed to help eliminate confusion over project requirements and keep student teams on track; and in-class progress reports gave teams the opportunity to discuss their progress with their classmates and possibly gain from what other teams were doing.

Computer Access

It would be nice if all class sessions could be scheduled in a computer lab or alternatively, if each student had access to a computer with Internet access during class; unfortunately, depending on the university, this is not always the case. Computer labs are often too small to accommodate class sizes and are frequently unavailable during class sessions. Some universities have addressed this by instituting laptop requirements whereby students purchase a laptop upon entering the university (relieving the burden on lab resources); and many universities now have wireless networks allowing for Internet access from most, if not all, classrooms on campus.[12] On the whole, access to a computer during class is not *absolutely* essential for *every* class session; use of distance learning tools (such as Blackboard) to supplement traditional class sessions in addition to the use of web-based research assignments, blogs, instructor demonstrations by means of multimedia equipment, and/or self-directed lab exercises lessen somewhat the need for computers in the classroom.[13]

Undergraduate versus Graduate Level

The course described here was originally designed for junior- or senior-level, undergraduate accounting students. However, the course could be structured to accommodate the needs of either an undergraduate or graduate level course by adjusting assignment workload, topical depth and emphasis, technical detail, and assignment structure, but without radically altering the base knowledge standard and core content constructed for the course. For instance, undergraduate instructors may choose to focus on a combination of short web-based research assignments and simple practical/lab exercises in lieu of a more in-depth,

[11] Instructors who would like to see the full text of the project document along with scoring sheets should contact the author.

[12] Allowing students to bring laptops to class combined with wireless Internet access is a double-edged sword and can create its own unique set of problems; for instance, students may be less apt to pay attention in class electing instead to check their email, send instant messages to their friends, browse the web, or play computer games.

[13] Many of the lab exercises in the Whitman et al. (2006) *Lab Manual* contain enough detail, explanation, and instruction to allow them to be performed by students or student groups outside of class with minimal preparatory instruction.

comprehensive project while graduate instructors may choose to limit other assignments and structure the course around the completion of a real-world consulting project.[14]

V. CONCLUSION

IS security and control has rapidly grown into a critical problem for organizational management, a problem carrying significant regulatory implications and economic consequences for which management is now held accountable (Gordon et al. 2005; Whitman and Mattord 2005). Because of its' close kinship to internal control and the acute emphasis placed on internal control by Sarbanes-Oxley, information security has also evolved into an integral part of the accountant's professional body of knowledge.

This essay provides some justification for making IS security an explicit part of an accounting curriculum as well as some practical suggestions on the design and implementation of an IS security and control course. While the focus of this essay is on the development of a *stand-alone* IS security course, the suggestions and resources presented here could also be used to incorporate more comprehensive coverage of information security concepts into an already existing AIS or IS auditing course. It is hoped that this essay will encourage accounting educators to consider the importance of information security to their accounting graduates and consequently, motivate them to develop and offer similar IS security content within their own curriculum.

APPENDIX A
SUGGESTED MODULES AND SUBJECT COVERAGE

This appendix presents brief subject matter descriptions and content suggestions (presented in outline form) for each of the core topics listed in Table 3. Subject matter coverage and coverage times will, of course, vary based on instructor preference and course delivery.

Information Security Foundations (300 minutes)

(1) Introduction to Information Security (75 minutes): This module is designed to provide a foundation for studying information systems security by exploring the evolution and practical significance of the field.
    (1) Definition of Information Security
    (2) History and Evolution of Information Security
    (3) Practical Importance of Information Security
    (4) Significance for Accounting Professionals
    (5) Internal Control and Information Security
    (6) Sarbanes-Oxley Compliance

(2) Information Security Principles (75 minutes): The module is designed to provide a broad introduction to the field of IS security by introducing foundational terminology, concepts, and principles.
    (a) Information Protection Environment
    (b) IS Resources (People, Procedures, Technology, Facilities, Data)
    (c) C. I. A. Triad (Confidentiality, Integrity, Availability)
    (d) Other Central Information Security Concepts and Principles
    (e) Overview of Primary Information Security Domains

[14] This author used the comprehensive team project described in Appendix D in an undergraduate course; and while student teams performed commendably, in retrospect, the project might be better suited for a graduate-level course owing to the workload and project-management skills required. Alternatively, the project presented in Appendix D could be scaled back to provide a workload more suitable for an undergraduate course.

(f) Types of Security Measures (Directive, Preventative, Detective, Corrective, Recovery)

(3) IS Threats, Vulnerabilities, and Exposures (150 minutes): This module is designed to provide a broad introduction to potential security vulnerabilities, threats, and exposures as a basis for discussing the need for information security.

(a) Non-Subversive Threats (Unintentional or Passive Threats)

(b) Subversive Threats (Intentional or Active Threats)

(c) Vulnerabilities (Exploitable Resources and Control Weaknesses)

(d) Business Exposures (Undesirable Consequences and Financial Impacts)

Information Security Management (450 minutes)

(4) Security Management Responsibilities (75 minutes): This module is designed to position information systems security as a management issue (rather than an information technology issue alone) and to provide students with an overview of information security management responsibilities and practices.

(a) Information Security as a Management Problem

(b) Regulation and Compliance

(c) Due Diligence of Care

(d) 10 Deadly Sins of Information Security Management (Solms and Solms 2004)

(e) Information Security Governance

(f) Information Security Risk Management

(g) Information Security Program Development

(h) Information Security Administration, Monitoring, Auditing, and Review

(i) Business Continuity and Response Management

(5) Information System Risk Management (150 minutes): This module is designed to introduce the principles of risk management and to familiarize students with fundamental risk assessment methods, risk computations, and risk control strategies.

(a) Definitions of Risk

(b) Risk Identification (Asset Valuation, Threat Analysis, and Vulnerability Assessment)

(c) Risk Assessment (Quantitative and Qualitative Risk Analysis Methods)

(d) Risk Mitigation Strategies and Controls

(e) Best Practices and Due Diligence of Care

(6) Security Policy and Awareness (150 minutes): This module is designed to provide an introduction to security policy concepts and development and to situate security policy as a basis for sound security practices.

(a) Information Security Policy Objectives

(b) Types of Policies (Senior Management, Regulatory, Advisory, Informative)

(c) Policies, Standards, Procedures, and Guidelines

(d) Information Security Policy Development

(e) Information Security Policy Implementation and Management

(f) Information Security Awareness and Education

(7) Information Security Standards and Frameworks (75 minutes): This module is designed to familiarize students with key information security standards and guidelines, their evolution, their principle attributes, and their significance for security management.

(a) Security Architecture

(b) Assurance, Trust, and Confidence

(c) International Organization for Standardization (ISO) 17799
(d) Trusted Computer Security Evaluation Criteria (TCSEC) (A.K.A. *The Orange Book*)
(e) Trusted Network Interpretation (TNI) (A.K.A. *The Red Book*)
(f) Other Rainbow Series Standards
(g) Information Technology Security Evaluation Criteria (ITSEC)
(h) Common Criteria (CC)
(i) National Institute for Standards and Technology (NIST) Security Documents
(j) Control Objectives for Information and Technology (COBIT)
(k) Other Standards and Guidelines

Security Methods and Controls (825 minutes)

(8) Access Security (75 minutes): This module is designed to introduce access control concepts and familiarize students with various methods for controlling access to system resources.
(a) Access Control Protection Environment and Concepts
(b) Access Control Threats
(c) Remote, Centralized, and Decentralized Access Control
(d) Administrative, Technical, and Physical Controls
(e) System Access Methods and Controls (e.g., Passwords, Biometrics, Tokens)
(f) Data Access Methods and Controls (e.g., Access Control Lists)

(9) Application and Systems Development Security (75 minutes): This module is designed to familiarize students with security issues and methods relevant to operating systems, applications software, application development, and databases.
(a) Application Security Protection Environment and Objectives
(b) Software Security Threats
(c) Operating Systems Security
(d) Application Software Controls
(e) Database Security and Controls
(f) Malware Controls
(g) Systems Development and Change Management Controls

(10) Network and Internet Security (150 minutes):[a] This module is designed to introduce network and network security concepts and familiarize students with security measures for managing and protecting network resources.
(a) Network Security Protection Environment and Objectives
(b) Network Technologies (Data Transmission Technologies, Components, Topologies, Protocols, Types, Internet Technology)
(c) Network Security Threats
(d) Physical Security of Netware
(e) Network and Data Access Security
(f) Network Traffic Management and Security
(g) Firewalls and Perimeter Security
(h) Intrusion Detection
(i) Remote Access Security
(j) Virtual Private Networks
(k) Network Availability, Incident Response, and Recovery Planning

(11) Cryptography (150 minutes): This module is designed to introduce the fundamentals of cryptography and to familiarize students with basic cryptographic methods, systems, and applications.

(a) Cryptography Concepts and Objectives
(b) History of Cryptography
(c) Fundamentals (Terminology, Purposes, Process, Method and Key)
(d) Basic Methods (Block, Stream, Substitution, Transposition, Polyalphabetic)
(e) Cryptanalysis and Attacks
(f) Cryptographic Systems and Standards (Secret Key/Symmetric, Public Key/Asymmetric, Hybrid)
(g) Digital Signatures and Certificate Authorities
(h) Key Distribution and Management
(i) Security Applications

(12) Operations/Data Center Security (150 minutes):[b] This module is designed to familiarize students with various controls for securing the computing environment, for ensuring that computer systems function appropriately, and for ensuring the integrity of normal transaction processing.
(a) Operations Security Protection Environment and Objectives
(b) Operations and Data Center Security Threats
(c) Hardware Controls
(d) Software Controls
(e) Operation Controls
(f) Data and Media Controls
(g) Telecommunications Equipment Controls
(h) Information/Transaction Processing Controls
(i) Support Systems Controls
(j) Personnel Controls
(k) Monitoring/Auditing of Controls

(13) Physical Security (75 minutes): This module is designed to familiarize students with various controls designed to protect information systems resources from physical harm and theft.
(a) Physical Security Protection Environment and Objectives
(b) Physical Security Threats
(c) Layered Defense Model
(d) Administrative Controls
(e) Perimeter and Site Security
(f) Facility/Building Security
(g) Data Center/Server Room Security
(h) Environmental Controls
(i) Fire Prevention, Detection, and Suppression
(j) Power Supply Controls

(14) Remediation Practices (150 minutes): This module is designed to provide an introduction to remediation planning and to familiarize students with controls, procedures, and recovery strategies necessary to preserve the continuity of critical information system functions in the event of some major disruption.
(a) Remediation Protection Environment and Objectives
(b) Types of Remediation Plans (e.g., Incident Response, Continuity, Contingency, Disaster Recovery)
(c) Plan Initiation and Management
(d) Business Impact Analysis
(e) Recovery Strategies (Business, Facility, Supply, User, Technical, Data)
(f) Plan Development and Implementation

(g) Plan Testing and Maintenance
(h) Remediation Plan Awareness and Training

Special Topics[c] (up to 300 minutes)

(15) Computer Crime Investigation (150 minutes): This module is designed to familiarize students with major types of computer abuse and fraud and to introduce the evolving area of computer forensics.
(a) Types of Computer and Internet Crimes
(b) History of Computer Crime Investigation
(c) Legal Aspects of Computer Crime Investigation
(d) Computer Crime Investigation Concepts
(e) Investigative Procedures, Methods, and Tools
(f) Digital Evidence and Computer Forensics

(16) Ethical Computing (75 minutes): This module is designed to introduce the ethical dimensions of information systems security and to imbue in students a sense of ethical computing.
(a) Ethics Concepts
(b) Computing Ethics and Social Responsibility
(c) Ethics and Security Culture
(d) Breaches of Computing Ethics
(e) Ethical Computing Practices
(f) Professional Codes of Ethics

(17) IS Auditing (150 minutes): This module is designed to introduce the principles of IS auditing and familiarize students with the elements of the IS audit process.
(a) IT Governance (CobiT)
(b) IS Auditing Standards (ISACA Standards and Guidelines)
(c) Legal/Ethical Considerations (ISACA Code of Professional Ethics)
(d) The Certified Information Systems Auditor (CISA)
(e) Risk-Based Analysis
(f) Types of IS Audits
(g) Audit Planning (Objectives and Scope)
(h) The IS Audit Process (The IS Audit Life Cycle)
(i) Computer Assisted Auditing Techniques (CAATs)
(j) Relationship Between Financial and IS Audits

(18) Legal Aspects of Information Security (75 minutes): This module is designed to familiarize students with the legal dimensions of information security and to introduce key pieces of U.S. legislation that have an impact on the field.
(a) Categories and Types of Laws
(b) Information Technology and Law
(c) U.S. Legislation Relevant to Information Security
(d) International Law
(e) Due Care, Liability, and Litigation

(19) Personal Computer Security (150 minutes): This module is designed to familiarize students with basic PC maintenance and prudent PC security practices and to provide a forum for focused hands-on practice with common PC security tools.
(a) PC Security protection environment
(b) Laptop Security
(c) Basic PC Maintenance

(d) OS Security
(e) Applications Security
(f) Data/File Security
(g) Internet and Web Security
(h) Email Security
(i) Password Management
(j) Privacy Protection
(k) Troubleshooting
(l) PC Security Tools

(20) Privacy Issues (75 minutes): This module is designed to familiarize students with privacy issues related to cyberspace and information security.
(a) Privacy in Cyberspace
(b) Privacy Concepts and Interpretations
(c) Privacy Law
(d) Threats to Individual and Business Privacy
(e) Monitoring/Surveillance Technologies
(f) Privacy Ethics and Policies
(g) Privacy Protection Methods and Tools

[a] Instructors may find it necessary to spend more time on this section depending on the extent to which networking concepts and technologies have been covered in requisite courses.

[b] Instructors may want to devote more/less time to this module depending on desired coverage of information/transaction processing controls.

[c] Special topics are presented alphabetically, not in order of preference or importance. Note that there will not be enough time in a typical semester to cover *all* of these topics in great detail. These topics might be assigned as group or self-study research assignments or alternatively, instructors might choose one or two topics of particular interest for focused study. Note that some of these topics are closely related to other areas of security and in some cases, subject matter will overlap.

APPENDIX B
ILLUSTRATIVE WEB ASSIGNMENT (MALWARE)

This appendix presents an assignment that requires students to perform online research on malware and related topics; the assignment may serve as supplemental knowledge acquisition to compensate for lack of coverage in the course text and/or as a preparatory assignment for a participative class discussion on the subject.

The following resources may be provided to students as a starting place for web research on malware:

Online Dictionaries

- IT Dictionaries: www.netlingo.com, http://whatis.techtarget.com/, http://www.webopedia.com/
- MacAfee Virus Glossary: http://us.mcafee.com/virusInfo/default.asp?id=glossary
- Symantec Security Glossary: http://symantec.com/avcenter/glossary/index.html

Information on the Latest Threats and Security Advisories

- CSI/FBI Survey: http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml
- Symantec AV Center: http://www.symantec.com/avcenter/
- MacAfee Threat Center: http://www.mcafee.com/us/threat_center/default.asp
- Spyware Warrior: www.spywarewarrior.com
- Spyware Guide: http://www.spywareguide.com/

Required:

(1) What is *malware*? How does a malicious program differ from a legitimate program? What are the most prevalent forms of malware? How serious and widespread of a problem is malware? Provide stats and discuss.

(2) What is a computer *virus*? What is a *virus signature*? How do viruses "infect" a system? How are viruses spread? What is meant by the *payload* of the virus? What is a *polymorphic virus*? What is a *retrovirus*? What is a *self-encrypting virus*? What is a *macro virus*? What potential business exposures (undesirable consequences and business implications) are associated with viruses? As part of your research, see what you can find out about the *Melissa virus*. What type of virus was *Melissa*? How was it spread and what did it do? Why do you think that this particular virus is infamous?

(3) What is a *worm*? How does a worm differ from a virus? How do worms "infect" a system? How are worms spread? Infamous worms such as *Code Red*, *Nimda*, *Slammer*, and *Blaster* have in the past attacked computer networks around the globe paralyzing networks and/or leaving infected computers vulnerable to future attacks. Visit one or more of the sites provided and research each of the worms above; provide a very brief description of what each worm was designed to do, how the worm spread, and what system(s) they targeted. Why do you suppose that attackers targeted the systems they targeted? As part of your research, access the following article on the Slammer worm: Boutin 2003. Slammed! An inside view of the worm that crashed the Internet in 15 minutes, *Wired Magazine*, Issue 11.07 (July) (Available at: http://www.wired.com/wired/archive/11.07/slammer_pr.html). Why do you suppose that the Slammer worm, *in particular*, is infamous?

(4) What is a '*blended' threat*? Why are blended threats particularly troublesome? Visit www.symantec.com/avcenter and/or http://vil.nai.com/vil/default.aspx (or another resource of your choosing) and select and describe an example of a blended threat.

(5) What exactly is *spyware*? How does a system become infected with spyware? What potential business exposures (undesirable consequences and business implications) are associated with spyware? Visit http://www.spywareguide.com/ (or another resource of your choosing) and select a spyware application; briefly describe how the spyware application works and what it is used for.

(6) Visit www.symantec.com/avcenter and/or http://vil.nai.com/vil/default.aspx (or another resource of your choosing) and select and describe at least two *recent* malware threats. Provide a brief description of what the malware was supposed to do, how it was designed to spread, what systems it affected, and what the specific potential business exposures (undesirable consequences and business implications) were.

(7) List and explain at least three security/control measures that would protect a system from harm due to malware. Be explicit. Would the security measures you have suggested be classified as directive, preventative, detective, corrective, or recovery? Explain.

(8) What specific security products or tools are available for securing a system against various forms of malware? List and describe at least two. Provide the name of the product, the developer/vendor, a brief description of the tool/product, and the URL for the web site where you found your information.

APPENDIX C
ILLUSTRATIVE PRACTICAL ASSIGNMENT (SECURITY POLICY)

This appendix describes an assignment that requires student teams to develop an issue-specific security policy. The assignment was designed to provide students with a practical appreciation for the pragmatics of constructing and communicating security policy guidelines. This assignment may serve as short-term project or simply as a preparatory assignment for participative class discussion on the subject of security policy.

Required:

Draft an issue-specific security policy governing the protection of the University's information system resources against malware.[a] Your policy statements should be definite, unambiguous, and directive and contain rational explanations for the reasons behind them. Be sure to stipulate the manner in which your policy statements should be disseminated (e.g., email, web) and presented to users (e.g., printed text, electronic text), and the manner in which they should be maintained (e.g., periodic reviews, change/revision process, methods for disseminating changes to affected users). Your security policy will be graded on organization, clarity, reasonableness, content, and rhetorical force. In drafting your malware policy, consider the following:

(1) Security policies provide the foundation for security awareness, a responsive state of understanding of what should and should not occur. Policy statements may also establish responsibility and accountability for resource protection; and may, as a corollary, stipulate disciplinary action for failure to comply (especially if damage results). As such, your policy statements should contain the rules governing how an organization's security resources should be protected; that is, they should focus on desired results and the organizational expectations of students, staff, and faculty, not necessarily on the technical means for achieving those results.

(2) Remember that the objective of information system security is to reduce risks and impacts of security vulnerabilities and threats—*while still allowing an open exchange of information*. Your policy should focus on desired results and behaviors but should be tempered somewhat by a pragmatic understanding of what is realistic in terms of University security expectations. If your policy is *too restrictive*, it will impair the usefulness of information resources and preclude the open exchange of information. However, just because you realize that not all faculty, staff, and students will comply with a policy does ***not*** mean it should ***not*** be policy. Your policies then, should be somewhat idealistic (such as "All students shall maintain updated virus protection software" or "No faculty shall download unauthorized software") but not so unrealistic that they preclude necessary use of systems resources or flow of information (such as "No student or faculty member shall access the Internet").

[a] This assignment was designed as a follow-up to a web research assignment on malware (see Appendix B).

APPENDIX D
INFORMATION SYSTEMS SECURITY PROJECT OVERVIEW

This appendix describes a comprehensive team project requiring student teams to perform a systematic analysis and critical evaluation of the information system security for a subsystem of a real-world information system. The project described focuses on key domains of security consistent with core topics suggested for the course. The suggested project is recommended for five to six students each per team and involves five major parts (which may be assigned at different times over the course of a typical semester); the project culminates in a team presentation and a final team report that would be either delivered or presented to the host organization for feedback. An overview of the project objectives and requirements appears below.[a]

Project Objectives

The objectives of the team project are to give students the opportunity to:

(1) Study real-world IS security policies and practices.
(2) Systematically assess IS risk by identifying specific threats and vulnerabilities associated with a particular real-world IS.
(3) Systematically analyze and evaluate the adequacy and effectiveness of IS security practices corresponding to specific IS threats identified and/or associated with the peculiarities of a particular real-world IS.
(4) Make specific recommendations for improvement of real-world IS security and control.
(5) Present findings and recommendations to the class and obtain feedback on the team's work.
(6) Present findings and recommendations to the host organization and obtain real-world feedback on the team's work.

Project Requirements

Part 1: The Proposal

Part 1 of the project takes the form of a project proposal and requires each project team to identify a willing host organization and organizational contact, get formal written permission to study the information security for a subsystem of the organization's IS, provide some basic information about the host organization and it's IS, describe the particular IS subsystem that the team has decided to focus on, specify a scope and purpose for the project work, stipulate team policies and dynamics, and plan the team's project work.

Part 2: Risk Analysis

Part 2 of the project requires each team to provide a detailed risk analysis for the organizational IS assets/resources relevant to the selected subsystem. More specifically, Part 2 requires each team to conduct and provide an asset identification and valuation analysis, a threat assessment, a vulnerability assessment, and a risk assessment for the selected organizational subsystem.

Part 3: Security Analysis and Evaluation

Part 3 requires each team to conduct a systematic analysis and critical evaluation of the adequacy and effectiveness of the IS security measures and transaction processing controls relevant to their selected subsystem. Part 3 also requires teams to make specific recommendations for improvement. The specific requirements for this portion of the project require teams to evaluate the selected subsystem based on foundational information security objectives (concerns for confidentiality, integrity, and availability), basic information processing objectives (input integrity, processing integrity, and output integrity), and key domains of information system security (security policy and awareness, access security, applications security, network and communications security, cryptography, operations security, physical security, and remediation practices).

Part 4: Presentation of Findings and Recommendations

Part 4 requires the team to prepare and make a formal presentation to the class consisting of the key aspects of the team's analyses, evaluations, recommendations, and (if available) feedback received from the host organization.

Part 5: Final Deliverable

Part 5 is the concluding section of the team's analysis. Part 5 requires teams to revise previous sections of their work based on instructor comments and class feedback, discuss the host organization's responses to their analysis and recommendations, prepare a thank-you letter to the host organization, and write an executive summary for the project document. Instructors may also require teams to either present their analysis and findings or deliver a copy of their finalized project report to the host organization (depending on the host's preference) for feedback.

[a] In the interest of space, the entire project document is not reproduced here; instructors who would like to see the full text of the project document should contact the author.

REFERENCES

Albrecht, S., and R. Sack. 2000. *Accounting Education: Charting the Course through a Perilous Future.* Sarasota FL: American Accounting Association.

American Institute of Certified Public Accountants (AICPA). 1999. *The AICPA Core Competency Framework for Entry into the Accounting Profession.* New York, NY: AICPA. Available at: http://www.aicpa.org/edu/corecomp.htm.

———. 2003. *2003 Top Technologies.* New York, NY: AICPA. Available at: http://infotech.aicpa.org/Resources/Top++10+Technologies/.

———. 2004. *2004 Top Technologies.* New York, NY: AICPA. Available at: http://infotech.aicpa.org/Resources/Top++10+Technologies/.

———. 2005. *Information Security Top Tech Issue for 2005 According to Annual AICPA Survey.* New York, NY: AICPA. Available at: http://www.aicpa.org/download/news/2004_01_05.pdf.

———. 2006. *Top 10 Technologies 2006.* New York, NY: AICPA. Available at: http://infotech.aicpa.org/Resources/Top++10+Technologies/.

Boritz, J. E. 1999. *The Accounting Curriculum and IT.* International Federation of Accountants. Available at: www.ifac.org.

Bosworth, S., and M. E. Kabay. 2002. *Computer Security Handbook.* New York, NY: John Wiley & Sons.

Byrum, S. 2003. *The Impact of the Sarbanes-Oxley Act on IT Security.* SANS Institute. Available at: http://www.sans.org/rr/whitepapers/casestudies/1344.php.

Dhillon, G. 2007. *Principles of Information Systems Security: Text and Cases.* Hoboken, NJ: John Wiley & Sons.

Fox, C., and P. A. Zonneveld. 2003. *IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting.* Rolling Meadows, IL: IT Governance Institute. Available at: www.itgi.org.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and R. Richardson. 2005. *2005 CSI/FBI Computer Crime and Security Survey.* Computer Security Institute. Available at: www.gocsi.com.

Hansche, S., J. Berti, and C. Hare. 2004. *Official (ISC)² Guide to the CISSP Exam.* Boca Raton, FL: Auerbach/CRC Press.

Harris, S. 2003. *All-in-One CISSP Certification Exam Guide.* Second edition. Emeryville, CA: McGraw-Hill/Osborne.

Harrison, R. 2005a. Understanding the role of security in compliance. *Sarbanes-Oxley Compliance Journal* (March 23). Available at: http://www.s-ox.com/feature/article.cfm?articleID=694.

———. 2005b. Understanding the needles in the haystack of security and compliance. *Sarbanes-Oxley Compliance Journal* (May 23). Available at: http://www.s-ox.com/feature/article.cfm?articleID=827.

———. 2005c. Security and compliance. *Sarbanes-Oxley Compliance Journal* (August 11). Available at: http://www.s-ox.com/feature/article.cfm?articleID=997.

International Federation of Accountants (IFAC) Education Committee. 2003a. *International Education Standard for Professional Accountants, IES 1-6.* International Federation of Accountants. Available at: www.ifac.org.

———. 2003b. *International Education Guideline 11 (IEG-11): Information Technology for Professional Accountants.* International Federation of Accountants. Available at: www.ifac.org.

Krutz, R. L., and R. D. Vines. 2003. *The CISSP Prep* Guide. Gold edition. Indianapolis, IN: Wiley Publishing, Inc.

Mitnick, K. D., W. L. Simon, and S. Wozniak. 2002. *The Art of Deception: Controlling the Human Element of Security.* Indianapolis, IN: Wiley Publishing, Inc.

———, and ———. 2005. *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders & Deceivers.* Indianapolis, IN: Wiley Publishing, Inc.

Proctor, P., and J. Vignaly. 2004. The security implications of Sarbanes-Oxley. *Symantec Enterprise Solutions Webcast* (February 19). Available at: http://www.symantec.com/press/2004/n040218c.html.

Regan, K. 2003. The non-security security law. *Information Security Magazine* (May). Available at: http://infosecuritymag.techtarget.com/2003/may/oxley.shtml.

von Solms, S. H., and R. von Solms. 2004. The 10 deadly sins of information security management. *Computers and Security* (23): 371–376.

Whitman, M. E., and H. Mattord. 2005. *Principles of Information Security.* Second edition. Boston, MA: Thomson Course Technology.

———, and ———. 2006. *Readings and Cases in the Management of Information Security.* Boston, MA: Thomson Course Technology.

———, H. Mattord, and D. Shackleford. 2006. *Hands-On Information Security Lab Manual.* Second edition. Boston, MA: Thomson Course Technology.