# DESIGN AND DEVELOPMENT OF AN INTRODUCTORY INFORMATION SYSTEMS SECURITY COURSE FOR COLLEGES OF BUSINESS

Al Fundaburk
Bloomsburg University

## ABSTRACT

Using the research from Kim and Choi, Dark and Davis, the Certification of Information Systems Security Professional Domains, and the Organization Systems Research Association curriculum model, Bloomsburg University developed an introductory course in Information Security Management to meet the needs of business majors across the curriculum. The recommended instructional methods for presenting this course include case-based applications supplemented by lecture discussion. The course introduces the basic concepts of information security, specific security contexts, technologies and practices, and the broader implications and ramifications of information security practices as they apply to legal and ethical issues in a general business setting, and emerging trends in information systems security.

## INTRODUCTION

Of interest to business educators are the 2003 CSI/FBI Computer Crime and Security Survey. This survey clearly shows a marked increase in computer security incidents and a significant rise in financial losses. It identifies an increase in total annual losses attributed to computer security incidence from $100 million in 1997 to $456 million in 2002. Over the past five years the total losses have exceeded $1 billion. In 2002, 91% of the respondents detected security breaches compared to 90% detected in 1999. Comparisons of the surveys from 1996 through 2003 show a significant increase in the Internet as a frequent point of attack (POA) (Power, 2001). The IT Risk Survey, compiled by Ernst & Young, found 66% of the respondents not using the Internet would begin to utilize it, and 83% respondents using the Internet would increase usage, if security concerns were adequately addressed (Earnst & Young, 1999).

In an environment in which these risks are inherent it is important that business students entering the workforce understand the ways to mitigate these risks (Grimaila, 2002). Many professional organizations have recommended model curriculum guides used by schools, colleges and universities in the design of programs in information technology. Office Systems Research Association's (OSRA) redefined model curriculum for organization and end-user information systems recognized the need for an introductory course in information systems security and has added the course as a recommended elective.

## COURSE DESIGN

The baseline in this curriculum design is the study guide for the Certified Information Systems Security Professional (CISSP) common body of knowledge (CBK) domains. The CISSP is a broad top-down certification (Dugan, 2001) created by the International Information Systems Security Certification Consortium (ISC)$^2$ which is supported by the Computer Security Institute, Information Systems Security Association, the Canadian Information Processing Society, as well as other industry presences (Yang, 2001). This study guide outlines CBK requirements for certification as an Information Systems Security Professional. Ronald Krutz has written extensively on mastering the ten domains listed in the CISSP CBKs. His *CISSP Preparatory Guide* is one of the few books with detailed knowledge of the requirements needed to become a CISSP certified security professional. An analysis of the CISSP guide identified five domains applicable to an end-user information security curriculum:

1. Domain one: Security Management Practices.
2. Domain three: Telecommunications and Network Security.
3. Domain six: Operations Security.
4. Domain eight: Business Continuity Planning and Disaster Recovery Planning.
5. Domain ten: Physical Security (Krutz, 2001).

Kim and Choi (2002) were instrumental in determining actual information security requirements in Korean industry. They identified the work actually performed by information security professionals in the field. Their research on identifying the educational requirements for information security professionals in Korea identified the following as essential for practitioners of information security. In order of importance they are:

1. establishing information security policy,
2. establishing managerial security measures,
3. analyzing security environments,
4. risk analysis and assessment,
5. understanding basic cryptology,
6. acknowledging laws and regulations,
7. testing vulnerabilities in information security systems,
8. designing physical security measures,
9. coping with hacking,
10. managing intrusion check and detection,
11. privacy and ethics,
12. handling computer viruses,
13. knowledge of information security standards,
14. managing security education programs, and
15. knowledge of security system evaluation.

Dark and Davis (2002) reported on the output of two curriculum development workshops. The first was held in July 2001, and the second was held in April 2002. The workshops were sponsored in part by the National Science Foundation Grant *DUE # 0124409.* The undergraduate skills and knowledge from the requirements workshops were analyzed to determine applicability to the goals and objectives of an information systems security curriculum. The following skills and knowledge requirements, taken from Appendix C of the Dark and Davis (2002) report, were determined to fit the ongoing requirements in an end-user information systems curriculum:

**General information assurance knowledge and skills**

A knowledge of basic IT and traditional definitions of INFOSEC, history and concepts, information assurance mindset, survey/overview of the field, survey/overview of the context/environment, crimes and laws, business fundamentals of authentication and authorization, awareness of INFOSEC hardware products and E-commerce.

**Risk assessment**

A skill of identifying threats and vulnerabilities, classes of attacks, classes of attackers, methods and models for testing systems, assessing risk methods, models, and theories and how these interweave into IA, asset classification, cost benefit analysis, ROI of INFOSEC investments, security posture assessment, testing, validation, and verification.

**Information security management**

The knowledge of security policy, policy development process, classifications of policies, policy implementation and management, organizational behavior, cultural, societal, and ethical implications of information systems.

**Legal and ethical**

A knowledge of privacy, intellectual property, investigation, digital evidence, legal aspects of computing practices, forensic examination and associated tools, seizure concepts, legal principles of computer related investigations, presenting evidence in court, ethics, prepared to engage in discussion on ethical issues that remain open/not yet resolved.

**Intrusion defense and response**

The functions of IDS, types of IDS, Anomaly Misuse, advantages and drawbacks of different IDS, vulnerability scanners, firewalls, proxy, filtering, application, incident response, notification, manual response, automated response, disaster recovery, back up, redundancy, replicated sites, post attack network analysis and computer forensics.

**Emerging technologies**

These include hardware, biometrics, digital cash, wearable computing, and other emerging hardware and software in information systems.

## COURSE DEVELOPMENT

Using the identified undergraduate skills and requirements from the CISSP Guide, Kim and Choi (2002), and Dark and Davis (2002), Bloomsburg University's Business Education and Office Information Systems Department developed a course titled Information Security Management. The course description is indicative of its end-user emphasis.

This course is an introduction of end-user systems security from a management aspect. The course emphasizes the methods for the management of information security through the development of policies, procedures, audits, and logs. It also provides an understanding of the methods used for identifying threats and vulnerabilities, as well as analysis of the legal, ethical, and privacy issues in information systems and discusses emerging technologies related to systems security.

The objectives of this course include:

1. Understand and apply the concepts and theories underlying the administration of information systems security.
2. Examine and use current methodologies for information systems security design, implementation, and monitoring.
3. Undertake review of information systems security practices, techniques, and methods for securing an organization's information assets.
4. Consider and analyze the impact of information systems security on organizations and society.

The course outline includes:

1. Introduction: Definitions, history of IS security, current concerns, and implications of IS security.
2. Information Systems Security Management: Key principles, management's role, standards, policies, procedures and risk management.
3. Systems Security: Exposures and threats, approaches to attack and penetration, exploitation, audits, and logs.
4. Legal and Ethical Issues: Protection of computer assets, copyright, computer abuse, and legal aspects of privacy.
5. Emerging Trends in IS Security: biometrics, smart cards, digital signatures, digital cash, etc.

The recommended instructional methods for presenting this course include case-based applications supplemented by lecture discussion. Learning begins with an understanding of the fundamental concepts of IS security. The first section introduces the basic concepts of information security in information systems. The next two sections deal with specific security contexts, technologies, and practices. The last two sections deal with the broader implications and ramifications of information security practices as they apply to legal and ethical issues and emerging trends in information security.

## CONCLUSIONS

Although primarily an Office Information Systems course, Information Security Management was designed to meet the elective requirements of all majors in the College of Business. The outcomes have applicability to Finance, Accounting, Management, Marketing, and Information Systems majors. Further research is needed to develop more information security curricula that focus on end-user systems practitioners and cross departmental lines.

## REFERENCE LIST

Dark, M. &. Davis, J.(2002) Report on Information Assurance Curriculum Development.

Dugan, P. &. Loretta, W. (2001). Certifiably Secured. InfoWorld, 23(28), 36.

Earnst & Young. (1999) IT Risk Management Series [Web Page]. URL www.ey.com/security [2002, January].

Grimaila, M. &. Kim, I. (2002). An undergraduate business information security course and laboratory. Journal of Information Systems Education, 13(3), 189-196.

Kim, S. &. Choi, M. (2002). Educational Requirement Analysis for Information Security professionals in Korea. Journal of Information Systems Education, 13(3), 237.

Krutz, R. & Vines, R. (2001). The CISSP Prep Guide. New York: Wiley.

Power, R. (2001). 2001 CSI/FBI Computer Crime and Security Survey. Computer Security Journal, 16(2), 33-49.

Yang, T. (2001). Computer Security and Impact on Computer Science Education. Proceedings of the Sixth Annual CCSC Northeastern Conference on the Journal of Computing in Small Colleges.