ISSN: 1545-679X

Information Systems Education Journal

Volume 7, Number 75 http://isedj.org/7/75/ July 13, 2009

In this issue:

Answering the Need for Information Assurance Graduates: A Case Study of Pennsylvania State University's Security and Risk Analysis Major

Robert L. Marchant
The Pennsylvania State University
University Park, PA 16802 USA

Robert Cole
The Pennsylvania State University
University Park, PA 16802 USA

Chao-Hsien Chu
The Pennsylvania State University
University Park, PA 16802 USA

Abstract: This paper is a case study of the Security and Risk Analysis Major at the College of Information Sciences and Technology (IST) at Pennsylvania State University. Fielded in the fall of 2006, the Security and Risk Analysis Major addresses government and industry needs for graduates better prepared for Information Assurance careers through a unique socio—technical curriculum. The program is the result of a thorough review of existing academic programs, published industry needs analyses, guidance from the federal government and recommendation from an advisory board created specifically for this program. The objectives of the major go beyond simply providing the theoretical framework and skill sets needed for a career in security and related analyses by providing exposure through problem based learning to current, real life challenges and problems. The pedagogy of the major is based on lecture, web-based learning, industry-endorsed case studies, term projects and industry-sponsored practice.

Keywords: information assurance, pedagogy, security, risk analysis, case study

Recommended Citation: Marchant, Cole, and Chu (2009). Answering the Need for Information Assurance Graduates: A Case Study of Pennsylvania State University's Security and Risk Analysis Major. *Information Systems Education Journal, 7* (75). http://isedj.org/7/75/. ISSN: 1545-679X. (A preliminary version appears in *The Proceedings of ISECON 2007:* §3345. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/7/75/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

2009 AITP Education Special Interest Group Board of Directors

Information Systems Education Journal Editors

Information Systems Education Journal 2007-2008 Editorial Review Board

EDSIG activities include the publication of ISEDJ and JISAR, the organization and execution of the annual ISECON and CONISAR conferences held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

Answering the Need for Information Assurance Graduates: A Case Study of Pennsylvania State University's Security and Risk Analysis Major

Robert L. Marchant
marchant@psu.edu

Robert Cole
rcole@ist.psu.edu

Chao-Hsien Chu
chu@ist.psu.edu

College of Information Sciences and Technology
The Pennsylvania State University
University Park, PA 16802 USA

Abstract

This paper is a case study of the Security and Risk Analysis Major at the College of Information Sciences and Technology (IST) at Pennsylvania State University. Fielded in the fall of 2006, the Security and Risk Analysis Major addresses government and industry needs for graduates better prepared for Information Assurance careers through a unique socio—technical curriculum. The program is the result of a thorough review of existing academic programs, published industry needs analyses, guidance from the federal government and recommendation from an advisory board created specifically for this program. The objectives of the major go beyond simply providing the theoretical framework and skill sets needed for a career in security and related analyses by providing exposure through problem based learning to current, real life challenges and problems. The pedagogy of the major is based on lecture, web-based learning, industry-endorsed case studies, term projects and industry-sponsored practice.

Keywords: information assurance, pedagogy, security, risk analysis, case study

1. INTRODUCTION

The need for an Integrated Approach

Information Assurance (IA) is field of practice focused on managing the risks associated with storing, processing, and transmitting information. A superset of information security and security engineering, IA is also concerned with governance (e.g. compliance, privacy, audits, business continuity, and disaster management and recovery). Both corporate executives and government officials around the world have identified countering information security threats as one of their highest priorities, yet they are forced to depend on a small pool of IA professionals that have both technical and business knowledge needed to address these increasingly pervasive and complex threats. The global shortage of experienced IA professionals is further compounded by the intelligence analyst and cyber forensics shortages in organizations like the United State's Department of Homeland Security (DHS) and National Security Agency (NSA) and by increased public and private sector regulatory compliance requirements.

The demand for IA professionals is clearly a global issue. Extremely attractive incentives are being offered to (and accepted by) IA professionals from emerging markets around the world. For example, a study (IDC, 2006) conducted by IDC for the International Information Systems Security Certification Consortium (ISC)^2 estimates that the number of information security professionals worldwide in 2006 is 1.5 million, an 8.1% increase from 2005. IDC predicts that the demand for IA professionals will grow to in excess of 2 million by 2010. This equates to a worldwide compound annual growth rate of close to 8% (6.4 in the Americas) (IDC, 2006).

In creating the Security and Risk Analysis Major (SRA), the College of Information Sciences and Technology (IST) at Pennsylvania State University performed a benchmark analysis of 67 universities with majors recognizable as being information security and assurance related and recognized (in 2005) as *Centers of Academic Excellence in IA Education* (NSA, 2007) by the NSA and DHS. This analysis indicated that most university programs focused on technology-based security with very few (Liberal Arts) colleges offering programs that included intelligence studies. The conclusion reached from this analysis was that no school reviewed provides a major that integrates Information Technology, Information Assurance, Intelligence Analysis, and Cyber Forensics into one curriculum. Understandably, IST crafted the SRA to be compliant with the criteria defined for recognition as a center of academic excellence (this criterion is maintained by the Committee on National Security Systems (CNSS) (CNSS, 2007).

Developmental Influences

The content of the SRA program was developed under several influences. The first of these, the results of the benchmark analysis, is described above. This analysis showed the need for an integrated, multidisciplinary program going beyond the traditional technical courses to include courses from law, business and liberal arts colleges.

Published industry survey data was a second source of recommendation for the SRA program, in particular a survey from the SANS Institute (www.sans.org), "The SANS 2005 Information Security Salary and Career Advancement Survey" (SANS, 2005). The survey contains the responses of over 4000 security professionals. As part of the survey, the participants were asked to rate the importance of areas of critical skills necessary for advancement as very important, important, not important, or no opinion. Table 1 shows the percentage ratings for the *Very Important* category for each of the 12 areas surveyed. Although interpreting the meaning of the absolute percentages may be problematic, clearly the ranking implied by these percentages indicates the relative importance these highly skilled professionals place on the categories of *critical thinking, communications, teamwork, and ability to lead.* Surprisingly, the responses indicated that slightly more participants feel two of these areas are more important than *technical knowledge*! Based on these findings, IST determined that the SRA major must include training in critical thinking, communications, teamwork, and leadership.

Table 1: "Very Important" response, adapted from (SANS, 2005)

Area	%
Critical thinking and judgment.	69%
Communications (verbal and written).	68%
Technical knowledge.	66%
Teamwork and collaboration.	52%
Ability to lead change.	52%
Business knowledge/acumen.	40%
Cross functional influence.	35%
Influence.	33%
Facilitation.	24%
Mentoring and coaching.	19%
Strategic business planning.	22%
Industry participation.	13%

A third influence on the development (and continued maintenance) of the program was the SRA advisory board. Consisting of representatives of government, industry, and academia, the board emphasized the importance of SRA graduates understanding the following:

- The blending of digital and physical elements of security.
- Contextual aspects of security from a multi-cultural perspective
- Legal, regulatory and ethical issues associated with security (e.g. privacy, intellectual property).
- Critical thinking and problem solving
- Analytical skills (e.g. data mining)
- Communication skills.
- Risk Management, including integration of risk, security, governance, and compliance.
- Methods of cyber crime and cyber warfare
- Policy trade-offs involving protection of data and the sharing of that data with others.
- The use of technologies employed in government and business

Based on the needs identified by the sources described above, IST determined that the SRA curriculum should provide training in:

- Communications
- Leadership
- Crisis management
- Conflict resolution
- Ethics
- Cultural sensitivity
- Human relationship building
- Decision making/problem solving
- Technology impacts on society
- Teamwork balanced with individual assessment

2. THE SRA MAJOR

As discussed above, IST created the SRA major to address the high demand for graduates with solid technical skills, strong interpersonal skills, forensics and analysis training, and an interdisciplinary and global perspective. A minimum of 120 credits is required for a bachelor of science in IST. For the SRA major, these credits are divided into the following categories:

• Electives:	3 credits
• General Education:	23 credits
• SRA – Common:	73 credits
• SRA - Option	21 credits

Within the SRA major, there are three options based on an interdisciplinary curriculum that integrates study in information assurance, intelligence analysis, and cyber forensics. The *Intelligence Analysis and Modeling Option* focuses on developing a more thorough knowledge of the strategic and tactical levels of intelligence collection, analysis, and decision-making. The *Information and Cyber Security Option* focuses on the theories, skills, and technologies associated with network security, cyber threat defense, information warfare, and critical infrastructure protection. The *Social Factors and Risk Option* examines the legal, regulatory, ethical, and other social aspects of security and risk with the intent of providing understanding of the social factors and causes that are linked to transnational terrorism, criminal investigations, and litigation involved in business and other security-related environments. The typical schedule has students taking classes common to all 3 options for the first four semesters followed by option-specific classes in the last four semesters. Summers are designated for supervised experience in business, industry, or the public sector.

Table 2: Common Requirements

Prescribed courses: (43 credits)	
CMPSC 101 (3)	Introduction to algorithmic processes
SRA 111 (3)	Introduction to security and risk analysis
IST 110 (3)	Information, people, and technology
ACCTG 211 (4)	Financial and managerial accounting for decision making
MICRB 106 (3) And MICRB 107 (1)	Elementary microbiology (with lab)
SRA 211 (3)	Threat of terrorism and crime
SRA 221 (3)	Overview of information security

SRA 231 (3)	Decision theory and analysis
STAT 200 (4)	Elementary statistics
IST 495 (1)	Internship (1 required, can have up to 3)
IST 432 (3)	Legal and regulatory environment of IST
SRA 311 (3)	Risk management assessment and mitigation
STAT 460 (3)	Intermediate applied statistics
IST 440W (3)	IST integration
Additional courses: (12 credits)	
AG BM 101 (3) or ECON 002 (3)	Economic principles of agrabusiness, Economics
PL SC 001 (3) PL SC 014 (3) or GEOG 040 (3)	Political Science, Geography
PSYCH 100 (3) Or SOC 005 (3)	Introduction to Psychology Social Problems
ENGL 202C (3) or ENGL 202D (3)	Technical writing Business writing
Supporting courses and realated areas.: (18 credits)	
Third-level proficiency in a foreign language (12)	Various
International Courses (6)	Various

A total of 21 credits are required for each SRA option. These along with the 73 credits common across all SRA options constitute the 94 credit SRA requirement. Details of the common requirements are presented in Table 2.

Intelligence analysis and modeling (IAM)

This option focuses on developing knowledge of the strategic and tactical levels of intelligence collection, analysis, and decision-making. This includes examining the foundations of decision analysis, economic theory, statistics, data mining, and knowledge management. As shown in Table 3, it has 5 required courses (15 credits) and 6 supporting credits selected from 8 alternatives.

Table 3: IAM option requirements

Prescribed courses: (15 credits)	
ADM J 111 (3)	Introduction to the American criminal justice system
ECON 302 (3)	Intermediate microeconomic analysis.
ECON 402 (3)	Decision making and strategy in economics.
PL SC 409 (3)	Quantitative political analysis
PL SC 439 (3)	The policitics of terrorism
Additional courses: (6 credits)	
ADM J 462 (3)	Comparative criminal justice system.
PL SC 442 (3)	American foreign policy
STAT 480 (1)	Introduction to statistical program packages
GEOG 103 (3)	Geography of the developing world
GEOG 121 (3)	Mapping our changing world
GEOG 124 (3	Elements of cultural geography
GEOG 128 (3)	Geography of international affairs
GEOG 357 (3)	Geographic information systems

Information and cyber security (ICS)

In the ICS option, the focus is on network security, cyber threat defense, information warfare, and critical infrastructure protection. As shown in Table 4, it has 4 required courses (12 credits) and 9 supporting credits selected from 8 alternatives.

Table 4: ICS option requirements

Prescribed courses: (12 credits)	
IST 220 (3)	Networking and telecommunications
IST 451 (3)	Network security
IST 454 (3)	Computer and cyber forensics
IST 456 (3)	Security and risk management
Additional courses: (9 credits)	
ADM J 433 (3)	Computer Security
IST 210 (4)	Organization of data
IST 301 (3)	Information and organizations
IST 302 (3)	IT project management
MGMT 100 (3)	Survey of management
IST 452 (3)	Legal and regulatory environment of privacy and security
IST 402 (3)	Emerging issues and technologies
IST 442 (3)	IT in and international context

Social factors and risk (SFR)

This option includes an examination of the legal, regulatory, ethical, and other theories associated with security and risk focused on understanding the social factors and causes that are linked to transnational terrorism, criminal investigations, and litigation involved in business and other security-related environments. As shown in Table 5, it has 4 required courses (12 credits) and 9 supporting credits selected from 8 alternatives

Table 5: SFR option requirements

Prescribed courses: (12 credits)	
PSYCH 270 (3)	Intro to abnormal psychology
PL SC 410 (3)	Game theory and international relations
IST 452 (3)	Legal and regulatory environment of privacy and security
PSYCH 445 (3)	Quantitative political analysis
Additional courses: (9 credits)	
ADM J 310 (3)	Forensic science I
ADM J 311 (3)	Forensic science II
ADM J 200 (3)	Introduction to security and loss control
ADM J 340 (3)	Fundamental technologies of scientific criminal investigation
INS 301 (3)	Risk and insurance
COMM 180 (3)	Survey of electronic media and telecommunications
COMM 490 (3)	Issues in electronic commerce policy and implementation
IST 453 (3)	Legal, regulatory, policy environment of cyber forensics

The program courseware has also been certified by the Committee on National Security Systems and the NSA as having met national training standards for:

- Information Systems Security Professionals (NSTISSI # 4011)
- Senior Systems Managers (CNSSI # 4012)
- Systems Administrators (CNSSI # 4013)
- Information Systems Security Officers (CNSSI #4014)
- Systems Certifiers (NSTISSI # 4015)

3. PEDAGOGY

The skills taught in the SRA program must be practiced. A problem-based approach with ample case studies, term projects, and labs both provides the Confucius-described prescription of "I do and I understand" and increases the enjoyment of the learning experience. The learning pedagogy of the SRA program has four parts: lecture, practice, project, and experience. Lectures are provided via multi-media in classrooms and enhanced with web-based learning modules. Practice is via case studies, labs, and problem based exercises. Projects are term long and most often require collaboration and teamwork. Experience comes via guest speakers, field trips, and internships.

Even the most basic of SRA classes strive to maintain this pedagogical template. As an example, SRA 111, *Introduction to Security and Risk Analysis*, is an introductory course with a broad focus, spanning security, risk and analysis. In addition to familiarizing the student with basic security terminology, it touches upon social and legal issues, risk analysis and mitigation, crime intelligence and forensics, and information warfare and information assurance.

The lectures/web based learning part of the course is presented in 6 modules:

1. *Motivation*, which addresses the "why" of security and risk analysis, discusses the national strategy to secure cyberspace, and encourages class participation in reviewing current efforts and challenges. The intent of this module is to provide the big picture perspective for the remaining modules of the course.
2. *Basic Concepts*, which covers authentication and encryption methods, PKI and digital signatures, logical and physical security, and operation systems versus application security
3. *Social and legal issues*, which includes topics such as identity theft, social engineering, spam, spyware, and adware
4. *Analysis and methods,* which focuses on vulnerability assessment, intelligence analysis, forensic analysis, risk assessment, risk analysis and risk mitigation
5. *Information warfare and assurance* , which covers topics such as footprinting, sniffing, port scanning, intrusion prevention and detection, Denial of Service (DoS) , and wardriving
6. *Securing the future*, a module which most recently included topics such as security planning and policy, outsourcing and open source security, and the impact of Sarbanes Oxley Act and HIPPA.

In addition, there are guest speaker presentations, videos, and 36 readings. Students are required to complete 3 hands on exercises (risk analysis, backup planning, and vulnerability assessment and mitigation). They must submit current event reports and complete a team based term project on security awareness program development.

Term Projects

Term projects typically incorporate exercise of skills relating to knowledge of people, of business environments and processes, and of technology. The term project for IST 451, *Network Security*, provides a good example. The term project revolves around a small company that manufactures gloves. The company is just becoming large enough (automated enough) to require connection of internal networks to the Internet. The students, working in teams, must help the company navigate through the stressful process of safely connecting its networks at multiple sites, allowing remote employee access, and hosting an e-commerce site. The students must perform a vulnerability analysis, create a security policy, and design a firewall and VPN deployment strategy.

The IST 451 term project requires delivery of 4 separate reports. Several business processes for the company must be detailed (showing knowledge of business processes). These processes are then used to create a topology for each relevant department participating in each business process. The students must then perform a vulnerability analysis identifying the major goals of possible attack. For each major goal they must create penetration scenarios using the blind remote attack, the user-level attack and a physical attack. The first report required for the term project is the results of this vulnerability analysis.

The second report takes the results of the vulnerability analysis and requires the students to create a global security policy. A global security policy is required as it involves an understanding of human nature, management responsibility, and organizational structure in addition to security technology. The completed global security policy must be comprehensive yet practical, usable, expandable (adaptable), concise, clear, and enforceable. From the technology perspective it must include descriptions of firewalls, intrusion detection systems, access controls, authentication methods, auditing, computing systems security physical security, and operational security.

The third and fourth reports are more technology focused. The third report is centered on firewalls, and the fourth on VPN. In these two reports, the students must define the requirements for the firewalls and VPN, design the deployment of the firewalls and VPN, and create the management and maintenance plans for the firewalls and the VPN. Once again, the reports are not considered complete unless the people focused management and maintenance plans are adequate.

Hands-on Exercises

The SRA program takes full advantage of the lab environments at the college of IST including a Cyber Security Lab, Cyber Defense Lab, Cyber Forensics Lab, Mobile Computing, Sensor Network Test Bed, and RFID Test Bed to create abundant opportunities for hands-on exercises. These exercises incorporate hands-on experience with technology in a context incorporating collaborative and action learning elements of problem-based learning. For example, IST 454, *Computer and Cyber Forensics*, includes seven laboratory exercises that illustrate different aspects of computer and cyber crime and ways in which to uncover, protect, exploit, and document digital evidence. Through these exercises, students are exposed to various hardware and software tools along with forensic techniques and procedure. Working in groups, the students utilize these resources to perform rudimentary forensic investigations. Table 6 lists the lab exercises for this course along with a brief description of the objectives of each exercise. Like most SRA courses, IST 454 also requires a term project; in this case revolving around mobile forensics (cell phone, PDA).

Table 6. IST 454 Lab Exercises

Exercise	Objectives
Data Acquisition (imaging)	Use imagning tools to obtain a forensically sound image of a suspect's hard disk
Forensic Analysis	Use analysis tools to perform forensic analysis of a suspect's hard drive
Investigating Windows Systems	Use analysis tools to perform forensic analysis of the registry from a windows machine
Hostile Code	Understand virus behavior through interaction with and analysis of a virus sample
Network Forensics	Use network scanning, sniffing intrusion detection and protocol analysis tools to analyze a network packet capture file.
PDA Forensics	Use tools to acquire data from a mobile device and perform subsequent forensic analysis
Steganography	Use tools to hide and recover data in multimedia files

4. CONCLUSION

The IST SRA program is designed to meet industry and government needs for security professions possessing a wide range of skills. As shown in Figure 1, the program has the elements that meet the requirements derived from a review of existing academic programs, industry inputs, and direction from our advisory board. Our common requirements courses (Table 2) provide the foundation that allows SRA graduates to understand how IT works, gives them practical analytical thinking skills and experience, and provides a working understanding of the legal and social issues they will encounter. Our learning pedagogy emphasis teamwork and leadership skills, and provides ample opportunity for practice. The program's three options provide focused material on specific, but high-demand needs of industry, government and academia. This multidisciplinary, socio-technical focus of the SRA program is producing graduates with the diverse skills required for effective leadership in a secure global digital economy.

Table 7. Enrollment

Course	Fall 2006	Spring 2007	Fall 2007
SRA 111	75	101	85
SRA 211	-	56	70
SRA 221	-	-	40

To be successful, the SRA program must attract students in order to provide capable graduates. Although it is too early in the program's development to predict graduate levels, our initial data indicates strong interest and participation in the program. Table 7 shows the enrollment for key courses for the SRA major and indicates the SRA major is off to an excellent start.

5. REFERENCES

IDC, "2006 Global Information Security Workforce Study", accessed June 15, 2007 https://www.isc2.org/download/workforcestudy06.pdf

NSA, "National Security Agency Central Security Services Centers of Academic Excellence", accessed June 15, 2007 http://www.nsa.gov/ia/academia/caeiae.cfm

CNSS, "Committee on National Security Systems", accessed June 15, 2006 http://www.cnss.gov/

SANS, "The SANS 2005 Information Security Salary and Career Advancement Survey", accessed June 15, 2007 http://www.sans.org/salary2005/

APPENDIX

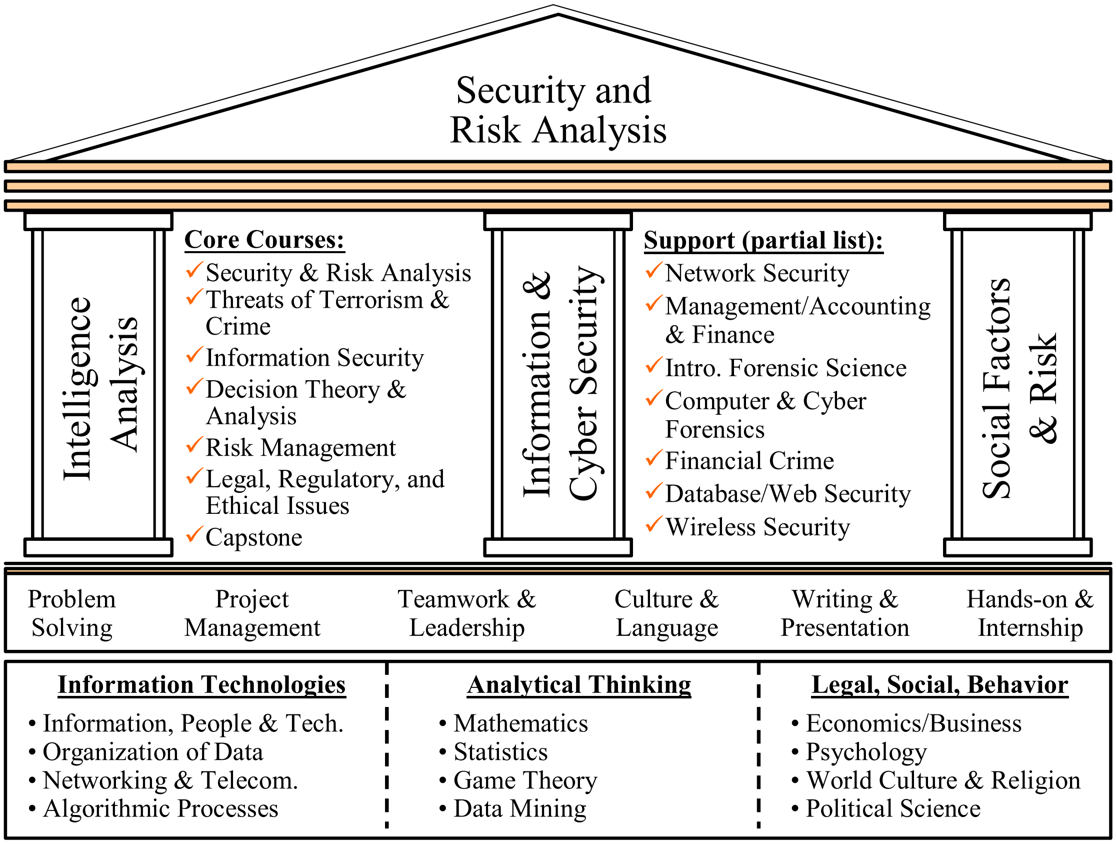

Figure 1. The SRA Major