SECURITY IN THE INFORMATION SYSTEMS CURRICULUM: IDENTIFICATION & STATUS OF RELEVANT ISSUES

JOHN E. ANDERSON and PAUL H. SCHWAGER
Appalachian State University
Boone, North Carolina 28608

ABSTRACT

This exploratory study examined three major issues: 1) Should more emphasis be placed on security issues in the IS curriculum, 2) If yes, should security issues be integrated in all IS courses or should there be a stand-alone course, and 3) Which security issues should be emphasized. A short survey was administered to members of the academic IS community. The results show that security issues should receive more emphasis in the IS curriculum. Ideally, security issues should be integrated into all other courses in the IS curriculum, but strong support for a stand-alone elective security course was also exhibited. Lastly, the relevance of security topics and sub-issues were examined as a guide for implementing a stronger emphasis on security issues in the IS curriculum.

INTRODUCTION

Security is becoming a prominent issue in the information systems (IS) field. Communications in IS, financial losses due to poor security, and future trends will force information systems security to be a central enabling technology.

A third of the popular IS literature is security related. Every week the popular IS practitioner press reports on new viruses or newly found holes in network operating systems. In just a three-month period between June and August of 2001, IS security was the cover story in the popular IS press ten times (Table 1).

TABLE 1
Selected Security Cover Stores in IS Press
June – August 2001

Magazine	Cover Story
Interactive Week, Vol. 8, No. 23, June 11, 2001	Data Privacy Mess
eWeek, Vol. 18, No. 23, June 11, 2001	Security: Think Social Engineering
Business 2.0, June 12, 2001	Who Can You Trust?
eWeek, Vol. 18, No. 24, June 18, 2001	DDoS Attackers Raising the Bar
eWeek, Vol. 18, No. 27, July 16, 2001	Public-key Security Takes Another Hit
Interactive Week, Vol. 8, No. 30, August 6, 2001	WORMS! Think Code Red Was Bad?
eWeek, Vol. 18, No. 31, August 13, 2001	Wireless LANs Dealt New Blow: Security Goes from Bad to Worse
Interactive Week, Vol. 8, No. 31, August 13, 2001	E-commerce in Legal Crosshairs: Lawyers, Lawmakers Target Identity Theft
Interactive Week, Vol. 8, No. 32, August 20, 2001	State of Disunion: Behind the Federal Security Enforcement Mess
Interactive Week, Vol. 8, No. 33, August 27, 2001	Security: Hacks and Wacks

In **Computerworld,** between June 1 and August 31, 2001, 67 articles contained the word "security" in the title and 450 contained the word "security" in the body. In fact, with 450 out of the 1578 total number of articles in the three-month period, 29% of all the articles in **Computerworld** contained "security" issues. After the September 11, 2001 World Trade Center attack, the issue of security received even greater attention in the practitioner literature.

Security breaches are pervasive and incur financial loses. According to the **2001 Computer Crime and Security Survey** (1):

- 85% of respondents detected computer security breaches within the last twelve months.
- 64% acknowledged financial losses due to computer breaches.
- 35% were willing/able to quantify their losses, which totaled to almost $378 million.

Future trends toward virtual teams/organizations, wireless connectivity, and mobile computing will depend on security to be an enabling technology. With decreased business travel in the aftermath of the September 11 terrorist attacks, remote technologies like videoconferencing are surging in popularity. The new emphasis on remote technologies increases remote connectivity security risks (3). Security in wireless LANs has been lacking. The transition from e-commerce to m-commerce has introduced additional security threats. Mobile devices currently lack even basic security; security has been traded for performance (5).

Microsoft has had to confront security fears about its products and training. Analysts have warned that the damage to the credibility of some Microsoft products, especially from the

Code Red and Nimda worms, may be difficult to repair (6). IT professionals have also blamed insufficient security training offered under Microsoft's MCSE program for contributing to the spread of viruses. In the current MCSE curriculum, in-depth security training is not a core requirement but is optional (4).

COVERAGE OF SECURITY ISSUES IN THE IS CURRICULUM

In the current typical IS curriculum, security issues are covered in a piecemeal fashion with parts taught in various classes or not taught at all. Table 2 shows that about 1% of a typical Systems Analysis text covers security issues, about .5% of a Database text discusses security, about 8.5% of an E-Commerce text covers security, and about 9% of a Data Communications text discusses security issues.

It is interesting that while 29% of IS practitioner literature involves security issues, only 4% of the content in the texts of the typical IS curriculum involves security issues. Students read an average of 108 out of 2495 (4.3%) textbook pages that deal with security topics if they take an E-Commerce course (usually an elective). Looking at only the common required courses of Analysis & Design, Database, and Networking, a student will read only 71 out of 1816 (3.9%) textbook pages that deal with security issues.

TABLE 2
Amount of IS Security Issues Coverage in Selected IS Textbooks

Text		# of Pages	Total Pages	% of Book
Systems Analysis & Design				
Systems Analysis & Design - Denis & Wixom		7	506	1.3
Systems Analysis & Design - Witten, Bentley, Dittman		10	694	1.4
Systems Analysis & Design - Satzinger, Jackson, Burd		4	618	0.7
	Average	**7.0**	**606.0**	**1.1**
Database				
Database Processing - Kroenke		21	564	0.4
Database Systems - Rob, Coronel		19	737	0.3
Data Management - Watson		4	570	0.7
Modern Database Management - McFadden, Hoffer, Prescott		13	598	0.2
	Average	**14.3**	**617.3**	**0.4**
E-Commerce				
Creating a Winning E-Business - Napier, Judd, Rivers, Wagner		38	395	10.0
Electronic Commerce - Sneider, Perry		64	443	14.5
E-business & e-Commerc - Deitel, Deitel, Nieto		10	1200	0.8
	Average	**37.3**	**679.3**	**8.4**
Telecommunications/Data Communications				
Business Data Communications and Networking - Fitzgerald, Dennis		59	422	14.0
Business Data Communications - Stamper		37	576	6.4
Data & Computer Communications - Stallings		53	779	7.0
	Average	**49.7**	**592.3**	**9.1**
	Total Average Pages	**108.3**	**2494.9**	**4.3**

PROBLEM AND PURPOSE

While information systems security is becoming a more important issue to the IS practitioner, the coverage of IS security issues in the common IS curriculum is covered only sparingly. The purpose of the present study is to explore the relevance of security issues to the IS curriculum. The following objectives were formulated to accomplish the purpose of this study.

1. Determine the extent security issues are covered in the required and elective courses of the IS curriculum.
2. Determine if an IS curriculum should contain a single course devoted to IS security issues and if such a course should be required.
3. Determine if security issues should be addressed as a single course or integrated into other IS courses.
4. Determine the relative relevance of IS security issues to the IS curriculum.

METHODOLOGY

Due to the exploratory nature of this study, the perceptions of IS faculty members were required in a Web-based survey. An invitation was sent out to members of the ISWorld community via the ISWorld list-serve to complete the survey, followed by a second invitation five days later. The survey questions dealing with the relative relevance of IS security issues were based on the Certified Information Systems Security Professional (CISSP) certification common body of knowledge domains developed by ISC2 (2). CISSP is considered the premier vendor-neutral IS security certification.

PRESENTATION AND DISCUSSION

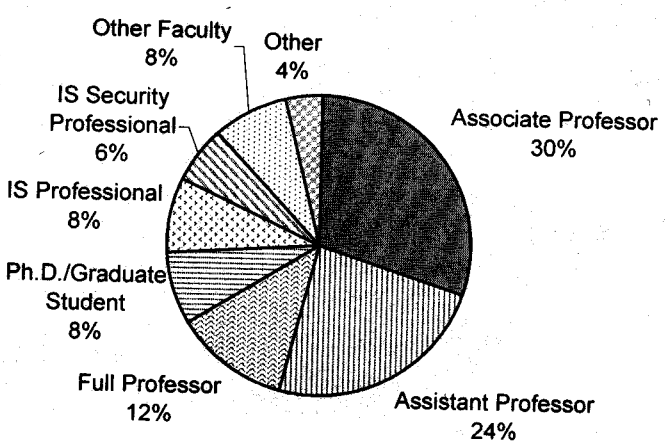
From the request to the ISWorld community 50 usable responses were received. In this section, demographic data will be presented first. The results will then be presented in order of the research questions answered.

Demographics

To determine organizational and respondent characteristics, the respondents were asked to disclose their position in the organization, the type of organization with which they were affiliated, and the location of their organization.

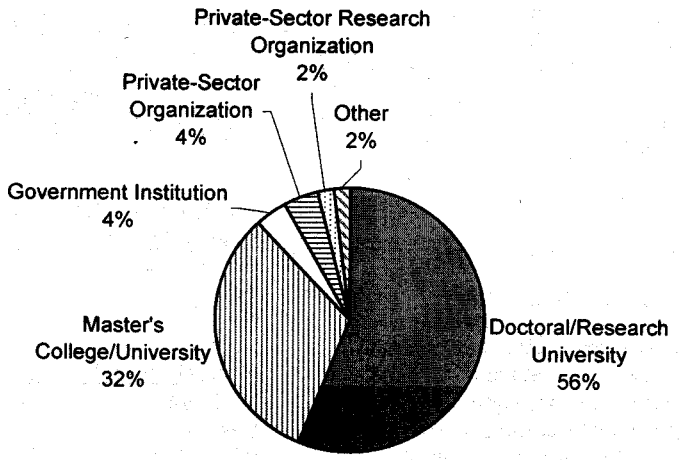
The majority (82%) of the respondents were academics: Associate Professors (30%), Assistant Professors (24%), Full Professors (12%), Ph.D./Graduate Students (8%), and other faculty (8%) as seen in Figure 1. The IS profession accounted for 15% of our respondents: IS Professional (9%), and IS Security Professional (6%).

FIGURE 1
Position



The majority (88%) of the respondents were from universities: Doctoral/Research Universities (56%), and Master's College/Universities (32%) as seen in Figure 2. Government Institutions accounted for 4%, and Private-Sector Organizations accounted for another 6%.

FIGURE 2
Organization



The majority (66%) of the respondents were located in North America as seen in Figure 3. Europe accounted for 18% and Australia/New Zealand accounted for 10%, while Africa, Asia, and South America accounted for the remaining 6%.

Objective 1: Determine the extent security issues are covered in the required and elective courses of the IS curriculum.

Objective 1 was measured by two questions: 1) "Approximately what percentage of the security issues above are in your REQUIRED IS curriculum?" and 2) "Approximately what percentage of the security issues above are in your ELECTIVE IS curriculum?" The number of respondents reported covering the security issues in their required and elective IS curricula is presented as frequencies for no opinion and 10% intervals ranging from 10% to 100% in Table 3.

In the required curriculum, Table 3 shows that not a single IS required curriculum covered all of the security issues listed. The table shows that 50% of the respondents' required IS curricula covered less than 40% of the security issues, while only 2% of the respondents' required IS curricula covered more than 80% of the security issues.

In the elective curriculum, Table 3 shows that 8% of the respondent's elective IS curricula covered all of the security issues. The table shows that 34% of the respondents' elective IS curricula covered less than 40% of the security issues listed, while 22% of the respondent's elective curricula covered more than 80% of the security issues listed.

FIGURE 3
Location

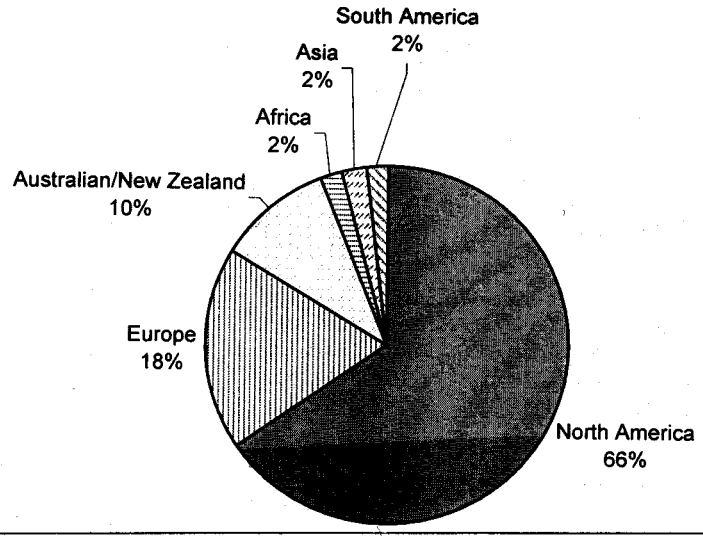


TABLE 3
Frequencies and Percentages of Security Issues Covered in the Required and Elective IS Curriculum for Selected Intervals

	Required Curriculum		Elective Curriculum	
Intervals	4	%	F	%
No Opinion	14	28	13	26
10%	11	22	8	16
20%	7	14	5	10
30%	7	14	4	8
40%	3	6	1	2
50%	2	4	2	4
60%	3	6	2	4
70%	2	4	4	8
80%	0	0	6	12
90%	1	2	1	2
100%	0	0	4	8

Figure 4 shows a visual representation of the frequencies in Table 3. Both the table and the figure show that more IS security issues are covered in elective courses than in required courses. However, the majority of respondents' required or elective curricula covered half or less of the IS security issues listed.

Objective 2: Determine if an IS curriculum should contain a single course devoted to IS security issues, and if such a course should be required

Objective 2 was measured by two questions: 1) "Should an IS curriculum contain a single course devoted to IS security issues?" and 2) "If yes, should it be an elective or required?" The responses to the questions are summarized in Table 4. Most (80%) of the respondents held that there should be a single dedicated IS security course in the IS curriculum. There was a more even split concerning whether the dedicated course should be elective or required with 48% of the respondents holding that it should be an elective and 32% that it should be required.

Objective 3: Determine if security issues should be addressed as a single course or integrated into other IS courses.

Given the choice of integrating security issues into the curriculum or addressing them in a single course the majority (70%) of the respondents held that security issues should be integrated into the curriculum, while 22% held that security issues should be addressed in a single course. The complete results are shown in Table 5.

TABLE 4
Single IS Security Course Issues
N=50

	f	%
Should an IS Curriculum contain a single course devoted to IS security issues?		
No Opinion	2	4%
Yes	40	80%
No	8	16%
If yes, should it be an elective or required?		
No Opinion	10	20%
Elective	24	48%
Required	16	32%

Responses to objectives 2 and 3 reveal an interesting tension between perceiving security as a discreet area within IS and security as a foundational element of all areas of IS. The comment of a respondent sheds some light on the matter. The respondent stated:

> In a perfect world security would be integrated across the curriculum. However, this requires a level of coordination that is very difficult to achieve. In addition, many professors do not have the background to present the security aspects of an area in addition to their expertise in that area. Therefore, while sub-optimal, it is probably better to have a single course where security can be added to existing knowledge

rather than being taught in an integrated fashion.

Ideally then, IS security issues should be integrated into the curriculum. However, a single elective course is also useful.

Objective 4: Determine the relative relevance of IS security issues to the IS curriculum

The frequencies and percentages of the relative relevance of common security issues to an undergraduate information systems security course are shown in Table 6.

The weighted sum of the frequencies may be seen in Figure 5. The four security issues the respondents held as most important to an IS security course are in order: 1) Telecommunications & Network Security, 2) Security Management Practices, 3) Access Control Systems & Methodology, and 4) Business Continuity & Disaster Recovery Planning. The next most important security issues to an IS security course were in order: 5) Security Architecture & Models, 6) Law, Investigations, & Ethics, 5) (tie) Applications & Systems Development Security, 7) Operations Security, 8) Physical Security, and 9) Cryptography.

FIGURE 4
Frequencies for % of Security Issues Taught

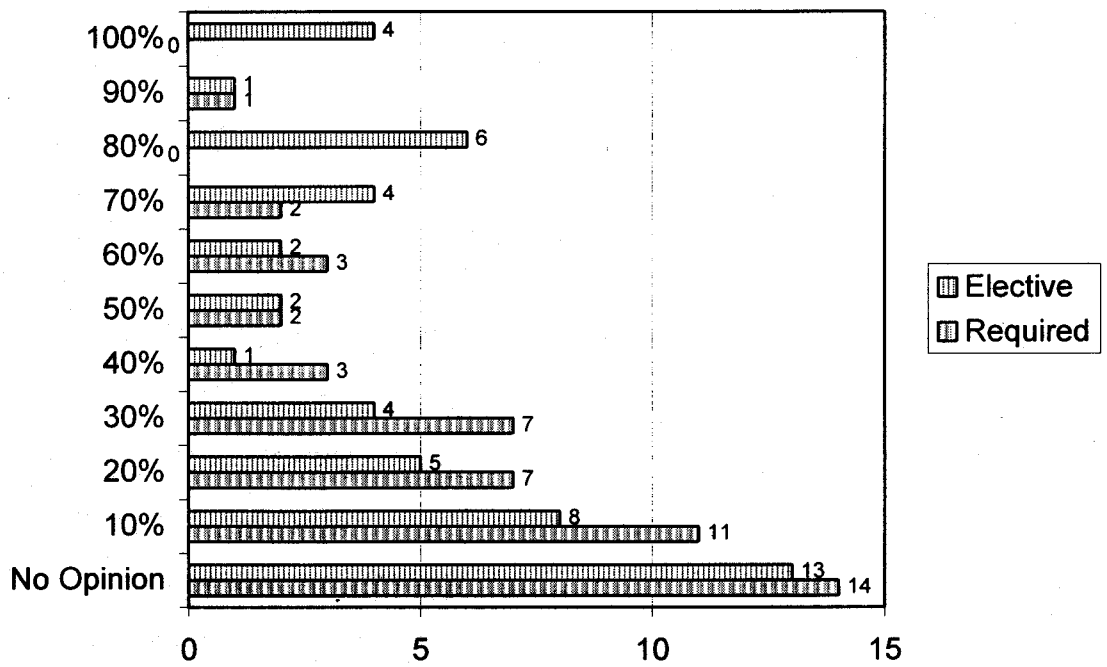


TABLE 5
Single Course vs. Integrated
n = 50

Response	f	%
No Opinion	4	8%
Single	11	22%
Integrated	35	70%
Both	0	0%

It is interesting that Cryptography was considered the least important security topic that should be covered in an undergraduate IS security course. In most Networking textbooks, cryptography is the security topic that receives the most attention (especially the emphasis on private-key and public-key encryption/decryption). The respondents' emphasis on security issues other than cryptography may be illustrated by some of the respondents' comments. One respondent suggested that a security curriculum should be "focused on Managerial Strategies and Policies." Another respondent thought that "it is most important that students understand concepts, basic countermeasures and management rather than technical details and legal issues." The comment of a third respondent stated that "security processes are more important than covering a specific technical threat or solution: the threats/solutions change but the basic processes remain fairly constant."

The respondents' emphasis on security processes rather than technology can also be seen in their choice of ranking the two security topics that could be labeled as the most "processes" oriented (Security Management Practices and Business Continuity & Disaster Recovery Planning) in the top four security issues that should be covered in an IS security course.

Table 7 shows the ten security topics divided into sub-issues with the weighted sum of the relative relevance of each sub-issue in relation to the major security topic and also the rank. These results are not surprising. However, they are useful for planning which subtopics are most important when covering a major topic in teaching a course or in writing course material.

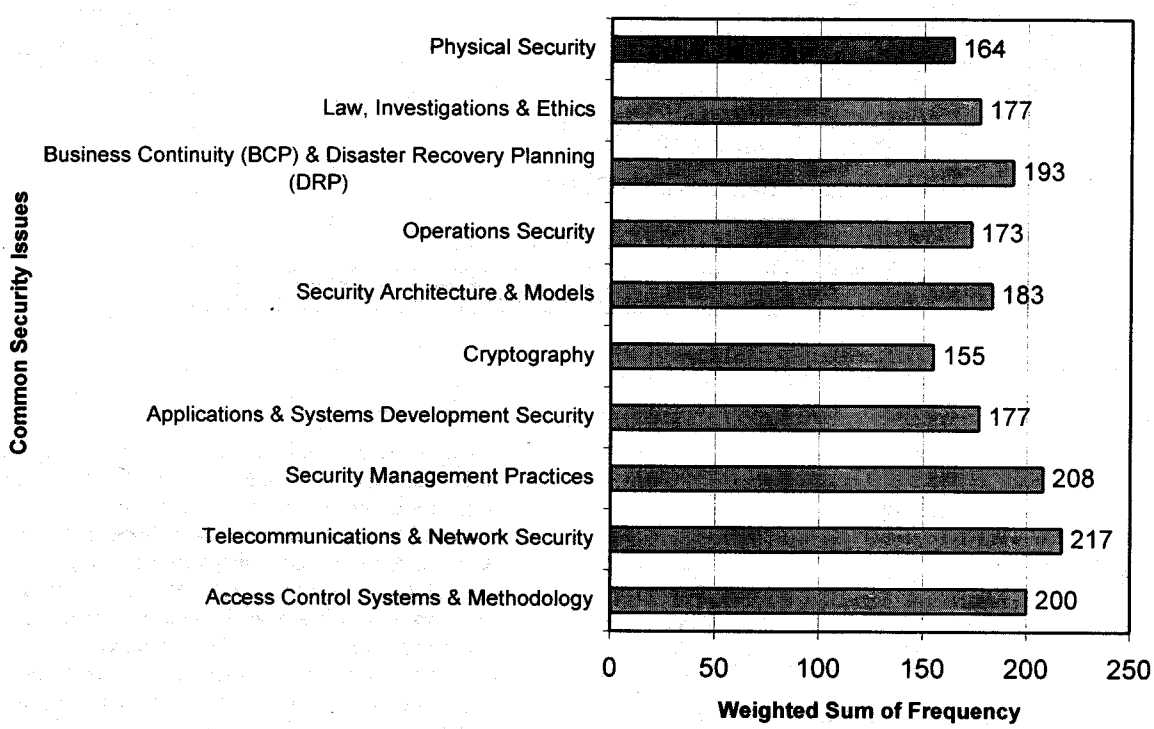
The web-based survey allowed for the collection of open comments from respondents in a memo field. The complete responses are shown in Table 8. The comments show an emphasis on security processes over technology. They also show the divide over whether security should be taught in a single

dedicated course or integrated into other IS courses. One interesting comment was also made concerning the possible political incorrectness of teaching an IS security course and the potential for legal action taken against a school for teaching hacking skills.

TABLE 6
Frequencies and Percentages of the Relative Relevance of Common Security Issues to an Undergraduate IS Security Course

	Relative Relevance									
	Low				Moderate				High	
	1		2		3		4		5	
Common Security Issues	F	%	f	%	f	%	f	%	f	%
Access Control Systems & Methodology	0	0%	4	8%	9	18%	15	31%	21	43%
Telecommunications & Network Security	0	0%	2	4%	7	14%	13	26%	28	56%
Security Management Practices	0	0%	2	4%	9	18%	18	36%	21	42%
Applications & Systems Development Security	0	0%	8	16%	15	31%	14	29%	12	24%
Cryptography	4	8%	9	18%	17	34%	18	36%	2	4%
Security Architecture & Models	0	0%	7	14%	15	30%	16	32%	12	24%
Operations Security	0	0%	5	10%	23	46%	16	32%	6	12%
Business Continuity (BCP) & Disaster Recovery Planning (DRP)	1	2%	4	8%	7	14%	22	45%	15	31%
Law, Investigations & Ethics	0	0%	7	14%	18	36%	16	32%	9	18/%
Physical Security	2	4%	6	12%	24	48%	12	24%	6	12%

FIGURE 5
Weighted Sum of Frequency



CONCLUSION

The present study was an exploratory study concerning security issues in the IS curriculum. The study yields trends and hints of the landscape of the problem and some guidance for further studies. From this study we can conclude that security issues are not covered in great depth in current IS curricula. The majority of faculty would like to see a single IS security course taught as an elective. At the same time, however, the majority of faculty would also like to see security issues integrated into all IS courses. Lastly, this study gives some guidance as to the major security topics and subtopics considered most relevant to be covered in an IS security course or in the IS curricula.

Threats and Countermeasures	204	1
Violations, Breaches, and Reporting	197	2
Business Continuity (BCP) & Disaster Recovery Planning (DRP)		
Business Continuity Planning	187	2
Disaster Recovery Planning	192	1
Law, Investigations & Ethics		
Laws	182	3
Investigations	176	4
Major Categories of Computer Crime	182	3
Incident Handling	188	2
Ethics	192	1
Physical Security		
Facility Requirements	162	3
Technical Controls	153	4
Environment/Life Safety	151	5
Physical Security Threats	173	1
Elements of Physical Security	167	2

TABLE 8
Open Comments from the Respondents

I would suggest a security curriculum focused on Managerial Strategies and Policies. Technical Solutions should be covered as part of these strategies.

Many issues relating to IS security are beyond the experience of undergraduate students. You have to work first with things they can relate to, like hacking, viruses and disaster recovery plans, and then get on to more subtle issues later. That means you can't have just one course, you need some of this material very early on, but the rest can only be taught after the students have some real experience, say from an internship.

At general undergraduate level, it is most important that students understand concepts, threats, basic countermeasures and management rather than technical details and legal issues.

Security processes are more important than covering a specific technical threat or solution: the threats/solutions change but the basic processes remain fairly constant.

In a perfect world, security would be integrated across the curriculum. However, this requires a level of coordination that is very difficult to achieve. In addition, many professors do not have the background to present the security aspects of an area in addition to their expertise in that area. Therefore, while sub-optimal, it is probably better to have a single course where security can be added to existing knowledge rather than being taught in an integrated fashion.

I try to bring security issues into my database class and my system design class. I would make a security class required if there was room in the curriculum (there is not). However, bringing in issues with the relevant course is also appropriate and often a break from the "technical" issues.

I attempted to introduce a special topics Security course for undergraduate IS majors. The department [chair & other IS faculty] felt that undergraduates might take the course simply to learn "Hacker/Cracker" skills. The stated reason was a fear of potential legal action against the school if former students were ever arrested for computer-related criminal activity.

I missed the discussion on why security is needed; that security requirements stem from different (business) interests of the involved parties and that the motivation for attacks is important in any risk analysis. I recommend you take a look at Kai Rannenberg: Multilateral Security – A concept and examples for balanced security. Proceedings of the 9th ACM New Security Paradigms Workshop 2000. 19-21 September 2000, Cork, Ireland. ACM Press. An earlier version can be found in the CD-Proceedings of the 23rd National Information System Security Conference, 16-19 October 2000, Baltimore, Maryland via http://research.microsoft.com/security/

This is an evolving issue. We are changing how we do things to take security into account. Students are hearing more about this issue.

REFERENCES

1. "2001 CSI/FBI Computer Crime and Security Survey," **Computer Issues & Trends,** 8:1, Computer Security Institute, Spring 2001.
2. "Certified Information Systems Security Professional Common Body of Knowledge Study Guide," **ISC2,** Boston, MA, 2000.
3. Vaas, L. "The Cobbler's Children Have Neither Shoes Nor a Firewall," **eSecuring the Enterprise,** 1:14, Ziff Davis, September 25, 2001.
4. Verton, D. "Microsoft MCSE Training Faulted, "**Computerworld,** 35:33, August 13, 2001, p. 1.
5. Weippl, E. "The Transition from E-commerce to

M-commerce: Why Security Should be the Enabling Technology," **Journal of Information Technology Theory and Application** 3:4, 2001, pp. 17-19.

6. Wilcox, J. "Microsoft Confronts Security Fears," http://www.zdnet.com/zdnn/stories/nesw/0,4586,00.html?chkpt+zdnnp1tp01, October 3, 2001.

IACIS
International Association for Computer Information Systems

Join one of the fastest growing professional computer-related organizations and receive the following benefits:

Receive the *Journal of Computer Information Systems* (a refereed magazine published quarterly).

Participate in the Certified Data Educator (CDE) Program (a program, monitored by a board of computer experts, that allows participants to receive CDE certification by demonstrating their computer knowledge).

Attend the National IACIS convention and other special conferences.

The Association honors an outstanding educator from the computer field (annually the membership identifies and selects a "Computer Educator of the Year").

To become a member, complete the Application for Membership form and send to:

G. Daryl Nord
International Association for Computer Information Systems
College of Business Administration
Oklahoma State University
Stillwater, OK 74078 .

Detach and Mail

THE INTERNATIONAL ASSOCIATION FOR COMPUTER INFORMATION SYSTEMS
APPLICATION FOR MEMBERSHIP

Last Name _____ First Name _____

Institution or Firm _____

Address _____

City _____ State _____ Zip _____

Title _____

Home Address _____

City _____ State _____ Zip _____

For Mailing

☐ Use Business Address ☐ Use Home Address

Member's name, if any, who sponsored you _____

TO JOIN IACIS OR TO RENEW YOUR MEMBERSHIP

( ) **Individual membership,** Foreign and Domestic, $50.00/year.

( ) **Students and retired membership,** open to retired members and bona fide students. $25.00/year.

For subscription to our *Journal* (no membership):

( ) **Institutional membership,** Foreign and Domestic, $125.00/year

( ) Back issues of *Journal*, $20 per issue

(Please include check payable to IACIS with application)

The Association is a non-profit California corporation governed by an Executive Council. It was founded in 1960.