Winter 12-5-2004

Student Recognition and Awareness of Information Security in Course Learning from Management Information Systems and Computer Science Classes: An Empirical Investigation

Qinyu Liao

Xin Luo

Kirk P. Arnett

Student Recognition and Awareness of Information Security in Course Learning from Management Information Systems and Computer Science Classes: An Empirical Investigation

Qinyu Liao, Xin Luo, Kirk Arnett

Department of Management and Information Systems, College of Business and Industry,
Mississippi State University, Mississippi State, MS 39762, U.S.A
ql15@msstate.edu[1], xl96@msstate.edu [2], kpa1@msstate.edu[3]

ABSTRACT

A survey of college students from both IS and CS programs was undertaken to understand student recognition and awareness of information security issues in course learning. Comparisons will be made for students before and after taking the security class as well as between the two different majors. The results of the study will demonstrate possible differences in perceptions between students of two majors, and identify security issues which have not been identified so that students and institutions are able to improve academic achievements by better tailored security curriculum and training. The findings will also provide feedback to future employers of the students.

***Keywords*:** information security, assurance, awareness, perception, recognition

1. INTRODUCTION

Information security and assurance is becoming a mission-critical component of today's business enterprises, governments, and academic institutes. Notably, after the 9-11 tragedy, more people, such as government leaders, business managers, IT practitioners, and academic researchers, have realized the crucial importance of information security, which, without proper management and supervision, could trigger unforeseeable catastrophe. As a result, a variety of computer and information security training and courses have surfaced at torrent levels in both academia and industry in a bid to improve and revamp employees' and students' awareness, recognition, and assessment of information security. In industry, companies giving serious consideration to information security now yearn to hiring information security/assurance specialists who are able to help them underpin security control, management, supervision, and centralization.

Accordingly, major colleges or universities are endeavoring to open security-related courses, in either Management Information Systems (MIS) programs in Colleges of Business Administration or Computer Science (CS) programs in Colleges of Computer Science/Engineering or both, to spawn these desired information security specialists. And MIS and/or CS major students are enthusiastically interested in taking these courses in an effort to cater to the increasing market demand. The trend is expected to continue to grow in the years ahead as information security and assurance unveils its very importance in today's computing community.

According to literature, a number of researchers have already designed a variety of security frameworks and indicated and measured the importance of establishing security management and control [9, 10, 15, 16]. However, quite a few researches have shed light on assessment of students' information security awareness and recognition from both MIS and CS perspectives in course learning, despite the fact that both academic divisions offer security-related courses at major colleges or universities in the United States. In addition, employers are eager to discover the fitness between the sophisticated work requirements and college graduates' capabilities of handling security issues in the real world. This research, therefore, focuses on observing and identifying undergraduate and graduate MIS and CS major students' awareness, perception, and recognition with regard to information security in course learning.

This research project, funded by a major southern university's Center for Computer Security Research (CCSR) in the United States, intends to answer three questions:

1. What are the security issues recognized by student majors in CS vs. MIS?
2. Are there any differences in their security management skills after taking the security class?
3. Are there any differences in their security technology skills after taking the security class?

2. LITERATURE REVIEW

2.1 Technical Skills and Managerial Skills for IS Security

As more organizations become so dependent on

computer-based and telecommunications-intensive information systems, security has become a vital element for organizations of all types. The unlimited access by a large, knowledgeable community of end users from desktop, dial-in, and network facilities creates a new and extremely vulnerable environment [10]. Each year, billions of dollars worth of information resources are stolen, vandalized, and otherwise misused due to a growing number of industrial spies, computer "hackers," and even unwitting employees [7]. Additionally, Arce and Levy [2] found that the weakest link has shifted from the technology area to the physical area, the human resource area, the policy area, and even individual operating desktop operating systems.

Information and system security has different meanings in the modern business environment. For some, the concept implies reliability (protection against accidental problems) and defensibility (protection against deliberate misuse). For others, IS security is placed into a people context and takes in to account culture, policies, organizational structures, and operating environments. Security technologies tend to address purely technical issues, such as the use of passwords for authentication, or cryptography to guard integrity, and largely ignore the human involvement [4].

Security experts have adopted security measures into four distinct, sequential activities: deterrence, prevention, detection, and recovery [5, 11, 12]. These four classes of sequential actions have a strong theoretical basis in deterrence theory. That is information security actions can deter potential computer abusers from committing acts that implicitly or explicitly violate organizational policy and lower systems risk [16].

In the corporate world, information security is generally seen as being of interest to the IT department, and so many professionals do not give adequate importance to the security concerns of an organization [3]. Straub [16] pointed out that managerial perception of the system security can influence organization security planning and strategies. To ensure the wholeness and soundness of information systems and organization, a security manager will have to take on the role of maintaining integrity of the organizational infrastructure, not just the technical information systems. Therefore, information system security is not a technical problem but a social and organizational problem because the technical systems have to be operated and used by people.

The theory of computer security offers a formal method for security engineering. It has three components: policy, mechanism, and assurance. The theory implies that to achieve a coherent security architecture, security must be considered from the outset, not as an afterthought. Competence in design for security policy enforcement, testing for security, and assessment of security must be part of the education of system implementers [8]. This agrees with Straub's model for effective system security management.

2.2 Importance of Security Awareness

Security awareness programs are a form of deterrent countermeasure which deserves special mention because educating users as well as their superiors about security yields major benefits [16]. In a survey about MIS management perceptions of the organization security threat, Loch et. al. [10] found out that there is a lack of awareness of the security risks and employee education regarding prevention measures. Managerial awareness is the key to successful security management [16]. To heightened security awareness on the part of managers, professionals, technicians, contractors, etc., all relevant groups should be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage information assets. There are needs to look to organizational theory, management science, and the developing field of information systems instead, for aid and succor in combating threats to security.

2.3 Need for Security Curriculum

Information security jobs in networking and databases will be hot in the next three to five years according to a IT workforce survey in 2004 by Information Technology Association of America [1]. Yet the number of skilled practitioners of computer security who are able to address the complexities of modern technology and are familiar with successful approaches to system security is very small [8]. The recent US Presidential Commission on Critical Infrastructure Protection recommends developing education on methods of "reducing vulnerabilities and responding to attacks on critical infrastructures." The commission recognizes the need to make the "required skills set much broader and deeper in educational level for computer scientists, network engineers, electronic engineers, and business process engineers." By moving to an educational system that cultivates an appropriate knowledge of security, we can increase the likelihood that our next generation of IT workers will have the background needed to design and develop systems that are engineered to be reliable and secure.

When talking about security in engineer education, Irvine [8] gave two important criteria for selecting outcomes for information security education: The education must result in graduates prepared for the security challenges they will encounter in their professional roles; the specific education outcomes for security in a given educational program must be consistent with those of the larger engineering context. Vaughn also considered that the computer science community has an obligation to train its graduates in known protection requirements, causes, vulnerabilities, current research, needed research, and to some extent,

computing ethics so that the graduates could be prepared to defend themselves and their employees from common threats that are known today and to help them understand the problem sufficiently such that they can contribute to discovery of the future solutions that are yet to be found [18].

It has been suggested that security insights must be integrated within the existing information systems programs, rather than be treated separately. There are two possible approaches: computer security could be the focus of the curriculum, which would investigate the foundations and technical approaches to security in considerable depth; a computer science or computer engineering curriculum could choose to use computer security as an important property to be addressed in all coursework [8]. Therefore, it is rare to find computer security course offerings at most academic institutions today. A comprehensive pedagogical approach would suggest that current CS course content be modified to include course specific discussion related to security in networks, database, operating systems, architectures, and software engineering followed by a capstone course learned at the end of the program that is specific to information security issues [18].Topics appropriate to security-oriented curriculum include security policy models; formal methods applied to system specification, development, and analysis; hardware and software protection mechanisms; security system design, implementation, and testing; database security; modern cryptography; cryptographic protocols; identification and authentication; and coherent network security architecture. Ideally, computer science and computer engineering texts, course materials, and laboratory exercises would have computer security completely integrated into appropriate topics and add a highly relevant dimension to the program- a feature prized by prospective employers [8]. Unfortunately, such materials do not yet exist. The coverage on techniques in security-related textbooks is moderate while other issues like security management have little in depth coverage. Therefore, the classroom coverage of security issue depends on the willingness of instructors to provide supplementary materials [13] because textbooks for courses in computer security provide only a good foundation for the student to learn the techniques that are used with computer systems and networks. In the interim, however, security-related supplements can be used.

Computer science and Information systems are two most common academic subdivisions in the computing field. While computer science examines topics related to computer concepts at technical levels of analysis by formulating processes/methods/algorithms largely using mathematically-based conceptual analysis, information science topics related largely to organizational concepts, especially usage/operation and technology transfer, although they also explore systems/software topics, all primarily at a behavioral level of analysis.

Glass et al. [6] conducted a study of representative and well-recognized journals from each field over the five-year period 1995-1999, and determined that system security and data security have been given minimal attention in the information systems arena. Reichgelt et al. [14] compared baccalaureate programs in IS, IT and CS. Their study shows that although data security ranked eighth of frequencies for topics offered by the surveyed universities, it is mostly integrated in the curriculum of computer science rather than a separate course. There are very few IS curriculum that cover the security topic.

The Center of Academic Excellence in Information Assurance Education Program was created to help academic institutions prepare security engineers for work in the government IT security area. Universities have respond to this call by setting up separate security course and offering security-oriented course in majors like information system. Students tend to naturally gravitate to this subject area as one of interest and one that offers good skills and knowledge that employers may find attractive [17]. It would be interesting to find out how the security courses are taught in different disciplines by comparing students recognition and awareness of information and system security before and after taking the class. The instructors and institutions can improve the program to fit student background and tailor the course content for future employer needs.

3. RESEARCH METHOD

An empirical investigation will be conducted in *Business Information Systems Security Management* class in the College of Business's MIS program (Course number BIS 6133 for both senior undergraduate and graduate MIS majors) this fall semester starting August 2004. Then data will be collected in the *Information and Computer Security* class in the College of Computer Science and Engineering's CS program (Course number 6243 for both senior undergraduate and graduate CS majors) the following spring semester in 2005 at a major southern university in the United States.

The security technologies and security management skills collected from prior security studies are listed in table 1. These skills are either currently in use or have been proposed by security researchers/practitioners for its importance in computer/system security.

Table 1. List of Issues in Security Technology and Security Management

Security technology	Security management
1. Anti-virus/Malware	1. Disaster recovery
2. Access-control	2. Data backup
3. Firewall	3. Security management policies
4. Password/Log-in	4. Employee education
5. Encryption	5. Patch management
6. Smart card	6. Identity management
7. Authentication	7. Vulnerability management
8. Intrusion detection	8. Procedure of log management
9. Virtual private network (VPN)	9. Procedure of incident report
10. Wireless security	10. Procedure of system maintenance
11. Contents filters	11. Procedure for approval of changes
12. Digital certificate	12. Documentation of changes
13. Network sniffers	13. Budget control
14. Biometric	

Survey questionnaires will be administered prior to and after these two security courses in order to measure any significant change on students' recognition and awareness of information security from both MIS and CS perspectives. Student demographic information such as gender, age, years of computer usage, ownership of computer and experience of other security courses will also be collected for analysis.

4. POSSIBLE FINDINGS

Since we only have data from one out of the four data collections designed for the study, there is no data analysis to report at this point.

A significant limitation of this study is the sample used. Both classes that will be investigated are from the same university and are comparatively small in size because of the availability of separately offered security courses. Also, both are single section courses and are taught on different terms at different times. Future studies should also include students in other universities and courses which has security as an integrated part of the course.

The final result of the study will identify how students' skills and/or perceptions of information security management and technology change after finishing the class. The research findings will be used to help students and instructors achieve further academic excellence in both colleges by fine tuning security curriculums and training and by providing business employers with more instrumental feedbacks with respect to efficient hiring of MIS and CS graduates in the job market.

ACKNOWLEDGEMENT

A number of people have generously given valuable time and effort towards this article. The authors appreciate Dr. Ray Vaughn, Professor of Computer Science and Engineering, for the support of The Mississippi State University Center for Computer Security Research (CCSR), and Dr. Merrill Warkentin and Dr. J. P. Shim, Professors of Management Information Systems at Mississippi State University, for their research directions and suggestions.

REFERENCES

[1] The annual IT workforce study by ITAA, 2004.
[2] Arce, I., and Levy, E., "The weakest link revisited", *IEEE Security & Privacy*, Vol. 1, No. 2, pp. 72-76, 2003.
[3] Dhillon, G., "Information system security management in the new millennium", *Communications of the ACM*, Vol. 43, No. 7, pp. 125-129, 2000.
[4] Fink, D., "IS security issues for the1990s", *Journal of Systems Management*, Vol. 46, No. 2, pp. 46-50, 1995.
[5] Forcht, L., *Computer Security Management*, Danvers, MA: Boyd & Fraser, 1994.
[6] Glass, R. L., Ramesh, V., and Vessey, I., "An analysis of research in computing discipline", *Communications of the ACM*, Vol. 47, No. 6, pp. 89-94, 2004.
[7] Hill, L. B., and Pemberton, J. M., "Information security: an overview and resource guide for information managers", *Records Management Quarterly*, Vol. 29, No. 1, pp. 14-25, 1995.
[8] Irvine, C. E., Chin, S. K., and Frincke, D., "Integrating security into the curriculum", *Computer*, Vol. 31, No. 12, pp. 25-30, 1998.
[9] Lee, S. M., Lee, S. -G., and Yoo, S., "An integrative model of computer abuse based on social control and general deterrence theories", *Information & Management*, Vol. 41, No. 6, pp. 707-718, 2004.
[10] Loch, K. D., Carr, H. H., and Warkentin, M. E., "Threats to information systems: today's reality, yesterday's understanding", *MIS Quarterly*, Vol. 16, No. 2, pp. 173-186, 1992.
[11] Martin, J., *Security, Accuracy, and Privacy in Computer Systems*, Englewood Cliffs, NJ: Prentice-Hall, 1973.
[12] Parker, D. B., *Computer Security Management*, Reston, VA: Reston Publishing, 1981.

[13] Prichard, J. J., and Macdonald, L. E., "Cyber terrorism: a study of the extent of coverage in computer security textbooks", *Journal of Information Technology Education*, Vol. 3, pp. 279-289, 2004.
[14] Reichgelt, H., et al., "A comparison of baccalaureate Program in information technology with baccalaureate programs in computer science and information systems", *Journal of Information Technology Education*, Vol. 3, 2004.
[15] Straub, D. W., "Effective IS security: an empirical study", *Information Systems Research*, Vol. 1, No. 2, pp. 255-276, 1990.
[16] Straub, D. W., and Welke, R. J., "Coping with systems risk: security planning models for management decision making", *MIS Quarterly*, Vol. 22, No. 4, pp. 441-469, 1998.
[17] Vaughn, R. B., Dampier, D. A., and Warkentin, M., "Building an information security education program", *2004 Information Security Curriculum Development Conference, at Kennesaw State University, Kennesaw, GA*, 2004.
[18] Vaughn, R. B., and Boggess, J., "Integration of computer security into the software engineering and computer science programs", *The Journal of Systems and Software*, Vol. 49, pp. 149-153, 1999.