2009

Results Of An Online Information Security Module In A Required Introductory MIS Course

Xin Luo
University of New Mexico, luo@mgt.unm.edu

Laurie Schatzberg
University of New Mexico, laurie@mgt.unm.edu

RESULTS OF AN ONLINE INFORMATION SECURITY MODULE IN A REQUIRED INTRODUCTORY MIS COURSE

Xin Luo
Center for Information Assurance Research and Education
Anderson School of Management
University of New Mexico
Luo@mgt.unm.edu

Laurie Schatzberg
Center for Information Assurance Research and Education
Anderson School of Management
University of New Mexico
laurie@mgt.unm.edu

Abstract

Information systems security is increasingly important to managers and employees from all disciplines, and in this work we go beyond studying MIS majors to study management students in general. In this research, we evaluate a Department of Homeland Security certified online mini-course used within a required undergraduate MIS course. We find that, for all but one of the seven modules, the training significantly improves students' mastery of the material.

Keywords: information security, learning impact, certificate, online training, MIS, information assurance

I. INTRODUCTION

Information security awareness and skills are increasingly important for graduates from a management degree program who are entering the workforce. While management students may not explicitly pursue an MIS career path, as employees and managers they share responsibility for ensuring that computing devices are free of malware, data are protected from unauthorized access or use, policies and training are up to date, and communication and Internet activities consistently reflect best practices. As the information security context continues to evolve, students will benefit from a balance of theory and practice in these topics. Clearly, the principles apply equally to one's personal and community involvement as they do to one's professional life.

Where, then, can and should business students develop their knowledge of information assurance concepts and practices? Such knowledge and skills can be taught within the context of an academic program, they can be learned by experience and personal reading, and they can be learned through on the job training once entering the workforce.

The current work examines the learning impact of teaching and illustrating the concepts within the context of an academic course. For this purpose, the authors used an ACT-Online (ACT-Online, 2009) cyber-security certificate mini-course for information security material. ACT-Online was developed by University of Memphis Center for Information Assurance in partnership with Vanderbilt University and Cobham Analytic Solutions. Individuals who successfully complete all modules of their mini-courses automatically earn FEMA certification for the content areas.

As part of the Center for Information Assurance Research and Education (CIARE) at the University of New Mexico, the current research is an initial step in evaluating the effectiveness of this cyber-security training. We chose the ACT-Online system because it was developed by academicians originally for classroom use, is easily accessible, and the associated certificate offers an additional incentive and credential for students entering the workforce.

In the following sections, we describe the CIARE research program and the introductory course within which the current work fits; we then present and discuss the results of the pre- and post-test using one ACT-Online mini-course, and outline future research.

II. BACKGROUND

For a number of years, there has been a growing emphasis placed on information security topics in MIS concentrations, including an entire issue of JISE which focused specifically on information security management education. In that issue, the editors [Surendran, et al., 2002] and authors focus on important graduate, undergraduate and curricular issues involved in bringing information security content to MIS students.

Cao, et al. [2002] show the benefits of a message encryption project for MIS students with little programming background. Grimaila & Kim [2002] report on a successful initial offering of a combined lab and lecture MIS course that covered 14 major information security topics.

Hazari, [2002] redesigned a traditional information systems course into a course for MBA-MIS students that focuses on issues within networked organizations. Cockcroft [2002] developed a graduate internet security course primarily for students in an e-commerce graduate program. Logan [2002] reports on an information security emphasis within an undergraduate MIS program that is part of an NSA Center of Academic Excellence in Information Assurance.

Hsu & Blackhouse [2002] found that a combination of lecture and colloquia format provided a solid balance of theory and practice for an elective graduate course, while Stevens and Jamison [2002] describe the content and methods used for an advanced elective IS security course for graduate students. Armstrong & Jayaratna [2002] describe a new graduate program in internet security management.

Focusing on the necessary intersection of academic preparation and industry practice, Kim & Surendran [2002] describe a collaborative effort by industry and academic partners who developed a comprehensive content area matrix for an information systems security curriculum using job analyses, interviews and academic review; while Kim & Choi [2002] use a Delphi technique to elicit professional knowledge requirements and then derive educational knowledge requirements for information security managers and for information security systems developers. More recently, Trimmer, et al. [2007] outline key information assurance topics in an undergraduate analysis and design course.

The prior research focuses on MIS majors with little attention paid to those pursuing other management studies. While MIS majors will undoubtedly shoulder major responsibilities for formulating information assurance policies, guidelines and training materials in the workplace, and will help implement technology-based security measures, students who are not MIS majors cannot be ignorant of the major concepts either. In their professional roles, they will be called upon to contribute to their organizations' information assurance frameworks and will need to mentor those they supervise. In everyday life, these individuals face the same challenges and threats as MIS majors.

Thus, we sought to investigate the usefulness of embedding information assurance training within the context of a required undergraduate MIS course. The intent is to begin to understand the extent to which such training impacts students' understanding and recognition of the importance of information assurance concepts.

Center for Information Assurance Research & Education

The Center for Information Assurance Research and Education (CIARE) at the University of New Mexico earned CAEIAE designation by the Department of Homeland Security in 2007 [CAE, 2007]. CIARE's mission is to advance the regional application, management, and knowledge of information assurance and information security through educational programs, business practice development, and scholarly research; and to assist with the emerging Information Assurance and

Information Security needs of local and regional constituents and the university community [IA, 2009].

CIARE is one of only 4 centers based in a management school. UNM Anderson faculty members developed a unique AACSB-accredited program that combines management of information security with fraud and forensic accounting. The program delivers an interdisciplinary focus on the human behavioral issues in protecting information. CIARE engages students and faculty in federal-level work with the FBI and its Regional Computer Forensics Lab (also housed at UNM) and provides access to DOE internships through the College Cyber Defenders program at Sandia National Lab. Locally, students participate in the Metro Law Enforcement Internship program with a focus on white collar crime units.

Through its education and training mission, CIARE primarily focuses on students who have chosen information assurance and/or MIS as their educational and career goals. However, a unique component of CIARE is to reach all of management, not only those who have self-selected to learn about the fields of MIS or IA. This broader perspective stems from research that people, rather than technology, are usually the weakest link in an organization's information infrastructure, and that security breaches often result from ignorance rather than malice [Loch et al., 1992; Sasse et al., 2001]. Faculty members associated with CIARE thus raise awareness, strengthen academic content, and provide skills-development opportunities. To bring this work to bear on all UNM Anderson students, content was added to the introductory MIS course, which is required of all management students.

Introduction to MIS Course at UNM Anderson School of Management

As described in Schatzberg [2005], the UNM capstone MIS course is taught to senior-level undergraduates with a focus on analyzing several IS-oriented business cases. The foundations of MIS are covered within this rich context of current, relevant case studies. Students are required to analyze both MIS and other management issues in each case, and to consider the interactions among them.

Because this course is required of all management students, backgrounds are quite varied and interest in MIS is widely varying, as well. However, information assurance is relevant for them all, when focused on individual risks and protections, as well as individual employees' emerging challenges and responsibilities. By combining our usual text and case coverage with intensive self-paced online material, we sought to maximize their exposure and retention of the key concepts. A sample syllabus is available here http://bit.ly/IAappendices.

In AY 2009, the faculty allocated several class sessions and independent work to the topics of information assurance. In addition to the text material, students undertook the ACT-Online mini-course in Information Security for Everyone [ACT-Online, 2009]. This online, self-paced mini-course covers topics such as malware, anti-malware programs and procedures, encryption, basic network security, and best practices in Internet usage, privacy protections, communication and file sharing.

University of Memphis Center for Information Assurance expanded its classroom program into one that's fully web-based, in collaboration with Vanderbilt University and Cobham Analytic Solutions. The resulting material is certified by US Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA). Thus, students who successfully complete any of the courses earn a nationally recognized certificate and can also apply for Continuing Education Units (CEU). While it's arguable that individual faculty members could develop equivalent local content, the prestige and portability associated with earning a recognized certification seemed to help motivate students to engage the material fully.

One complication of using the ACT-Online material is that, at the time, only US citizens were permitted to access the site. Thus, we needed to identify an alternative training opportunity for international students. For this alternative, we chose a course from the Information Assurance Support Environment [IASE, 2009] called Federal Information Security Awareness, which is open

to everyone and also allows successful students to print a certificate of completion. In preparing this manuscript, we noted that course interface has undergone a major upgrade which makes the course even more inviting to students.

While we considered using the IASE training for all students, we decided that the ACT-Online benefits of providing us with pre- and post-test data, as well as individual performance data on each of the modules outweighed the potential awkwardness managing two certification processes.

To provide real-world context for the material, students also studied the TJX case [Haggerty & Chandrasekhar, 2008], which traces the security issues at the TJX, through the eyes of an information security officer on his first day on the job. While this work does not evaluate mastery of the case material as a function of the ACT-Online case, anecdotally it seemed to the instructors that students were applying concepts from the ACT-Online training in their TJX case analyses

III. METHODOLOGY

In Fall 2008, one faculty member tested the ACT-Online process in two sections of the MIS core course. In Spring 2009, ACT-Online was used in three sections. This research reports on combined results from three of the five total classes (two from Fall and one from Spring) because Department of Homeland Security permanently discontinued all instructor access to individual training results before we had downloaded all the UNM data for the spring.

About six weeks before the end of each term, students were assigned text reading on Information Security topics in their text [O'Brien & Marakas, 2008] and faculty explained the additional self-paced online work that would be required. Students were advised to bring laptops to class (UNM Anderson has a free loaner laptop for students who need) because class time would be allocated for the pre- and post-testing. Depending on students' incoming skills and knowledge, they would require several additional hours of homework to successfully complete the mini-course. Instructors also explained that while all students would receive comparable training, and that all successful students would earn a certificate of completion worthy of mention on their resumes in during interviews, US citizens would use the ACT-Online system while all others would use the IASE system.

In class, all students were given written instructions with screen shots to help them register for the proper training, and a sample of the instructions is http://bit.ly/IAappendices. The instructor was available during the entire class period for students who needed. Since no individual IASE performance data are provided for instructors, the remainder of this work focuses on the data generated by our students using the ACT-Online system.

Students were instructed to complete the pre-test of their knowledge in all seven modules. Table 1 shows the topics covered in each module. If a student's score was high enough in any module, he would receive a passing score and require no additional training or testing on that module. However, since the vast majority of students were neither MIS nor IA students, instructors set the expectation that most students should expect to require the ACT-Online training in order to pass the modules during subsequent post-tests.

In addition to the pre-test, students had five post-test opportunities. If, after five attempts the student did not pass all seven modules, the student could choose (1) to forego the certificate and earn partial credit in the course, or (2) to reset his training record and begin the training again. However, if the student chose to begin the training again, all prior training records were deleted and he had to complete the pre-test again.

Since some students would be required to complete significant amounts of training and additional reading, two class periods were allocated. During this class time, the instructor could also help explain concepts that individual students found difficult.

We were most interested in analyzing student success with the training, and defined success as students' ability to pass all seven modules. For students with IA backgrounds, the pre-test would reveal their mastery of material studied previously. For students without, we were interested in knowing how well the training enabled them to succeed on material they had initially struggled with. Secondarily, we were interested to know which topics incoming students knew the most and least about, so that we could focus our future attention on the least understood concepts and principles.

Table 1: Major Topics in ACT-Online Mini-course

Module	Content Summary
Module 1	Anti-virus, personal firewalls, OS
Module 2	Malware & P2P; facts & risk-minimizing strategies
Module 3	Encryption & physical security for computers
Module 4	Networking setup, standards, PW and keys
Module 5	Encrypting communications, best practices
Module 6	Privacy, cookies, social engineering attacks
Module 7	Safe browsing, penalties for misuse

IV. SAMPLE, RESULTS AND DISCUSSION

From the three classes with data available, we began with a sample of 78 records, and the overall performance is shown in Table 2 below. Seven students passed the pre-test and were certified without further training or the post-test. We believe that students in this group learned the material through prior academic study, on the job or through self study. Thirty-nine, or 50% of the participants, passed the training with one post-test, and over 20% passed on their second attempt, all of which suggests to us that the training materials prepare the students reasonably well to succeed on the post-test examination.

Five students required three or more iterations through the material, and ten ended the testing process after passing some, but not all, modules. Of the 78 student records, 13 were removed before further analysis because of duplicate IDs assigned to a given student. Thus, our working sample was 65 unique students and records.

Due to constraints in the data, we did not have demographic data available for analysis. Thus, we were unable to compare IA majors with others, MIS and non-MIS majors, gender or other useful comparisons.

Table 2: Summary of Participants' Performance

Category	Qty	%
Total Students	78	100.00%
Students passing with pre-test	7	8.97%
Students passing with 1 post-test	39	50.00%
Students passing with 2 post-test	17	21.79%
Students passing with 3 post-test	2	2.56%
Students passing after> 3 post-test	3	3.85%
Students ending without passing	10	12.82%

Aggregate Results

We then performed a series of paired-samples t-test to gauge the differences between pre-test and post-test knowledge. We first looked at the aggregate results of all seven modules. As shown in Tables 3.1 and 3.2, t-value is 10.757 and p-value is 0, both of which demonstrate statistically significant differences existing in the pre-test and post-test sessions. This implies that, from a general perspective, students' training results improved considerably after the students completed the training

Table 3.1: Aggregate Differences using Paired Samples Test

	Paired Differences					t	df	Sig. (2-tailed)
	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
				Lower	Upper			
Post_Test – Pre_Test	269.594	200.4984	25.0623	219.5107	319.6768	10.757	63	.000

Table 3.2: Aggregate Paired Samples Statistics

	Mean	N	Std. Deviation	Std. Error Mean
Post_Test	518.86	64	106.1646	13.27057
Pre_Test	249.27	64	172.0164	21.50204

Figure 1 illustrates the change in students' performance more. For each student, the lower (blue) point is their pre-test total score, summed across all seven modules. The corresponding higher point indicates their post-test score. The magnitude of the difference between these points illustrates the relative knowledge gain for each student. It is notable that quite a few students had very little incoming knowledge on the information assurance topics and yet most of them learned enough in the training to score above 600 points (passing) on the post-test.

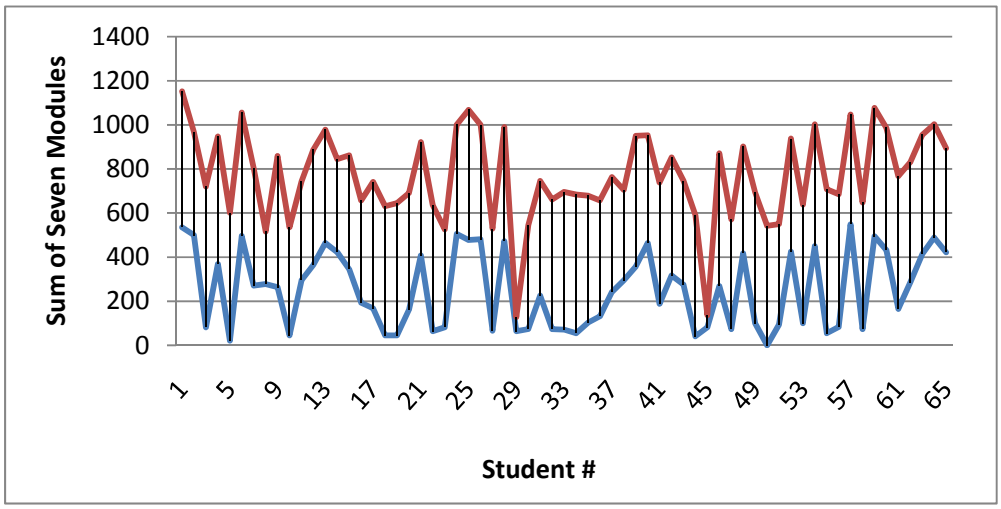

Figure 1: Seven-Module Sum Change

Module-level Results

We then disaggregated the results to study the differences in each module using a paired samples t-test. Since the content areas vary widely from behavioral to technical, we wanted to analyze the results for each module. The module results are summarized in Figure 2.0, which reports the t-tests results for each module. Modules 1-6 reflect significant differences in pre- and post-test results, while Module 7 does not. Table 4 provides the corresponding paired sample t-test results

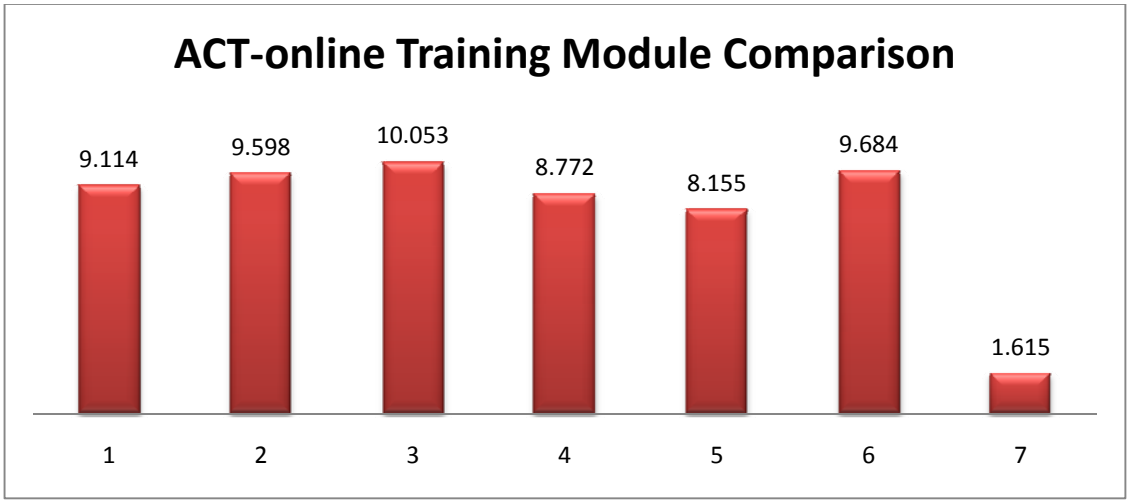

Figure 2: T-test Results for Module-by-module Comparison

Table 4: Paired Samples Test

	Paired Differences					t	df	Sig. (2-tailed)
	Mean	Std. Dev.	Std. Error Mean	95% Confidence Interval of the Difference				
				Lower	Upper			
Module 1 (Post – Pre)	36.8154	32.5653	4.0392	28.7461	44.8847	**9.114**	64	.000
Module 2 (Post – Pre)	45.5077	38.2259	4.7413	36.0358	54.9796	**9.598**	64	.000
Module 3 (Post – Pre)	46.9231	37.6330	4.6677	37.5983	56.2478	**10.053**	64	.000
Module 4 (Post – Pre)	40.9231	37.6133	4.6654	31.6030	50.2432	**8.772**	64	.000
Module 5 (Post – Pre)	40.6154	40.1512	4.9801	30.6664	50.5644	**8.155**	64	.000
Module 6 (Post – Pre)	47.0154	39.1438	4.8552	37.3160	56.7147	**9.684**	64	.000
Module 7 (Post – Pre)	8.4154	42.0193	5.2119	-1.9965	18.8273	1.615	64	.111

According to the measured significance of the t-scores in Table 4, we can conclude that Modules 1 through 6 did significantly improve students' recognition of the information security topics covered in those modules. Module 3, which focuses on encryption and physical security, shows the greatest development of knowledge and recognition. This finding was interesting because

students were also preparing their analyses of the TJX case study, which highlights encryption and physical security issues.

While the first six training modules all provided significant learning improvement, performance improvement in Module 7 was not significant, based on the t- and p-values in the table. This module focuses on safe browsing practices and also penalties for misuse of the Internet. The results indicate that the training for this module failed to enable students to materially enhance their understanding of these topics.

We provide two possible explanations for post-test scores that are not materially different from pre-test scores. First, students' incoming knowledge may be so complete that there is little room for improvement through training [Liao and Luo, 2007]. Second, students may not fully grasp the concepts and the training materials and so they gain little from the training

To further explore the results from Module 7 noted above, we then calculated the mean pre-test and post-test scores for each module. While we knew from the results in Table 4, that all other modules showed significant improvement in the post-test, we wanted to explore the students' incoming knowledge as a possible explanation for the results in Module 7. In Figure 3, we show the mean scores.

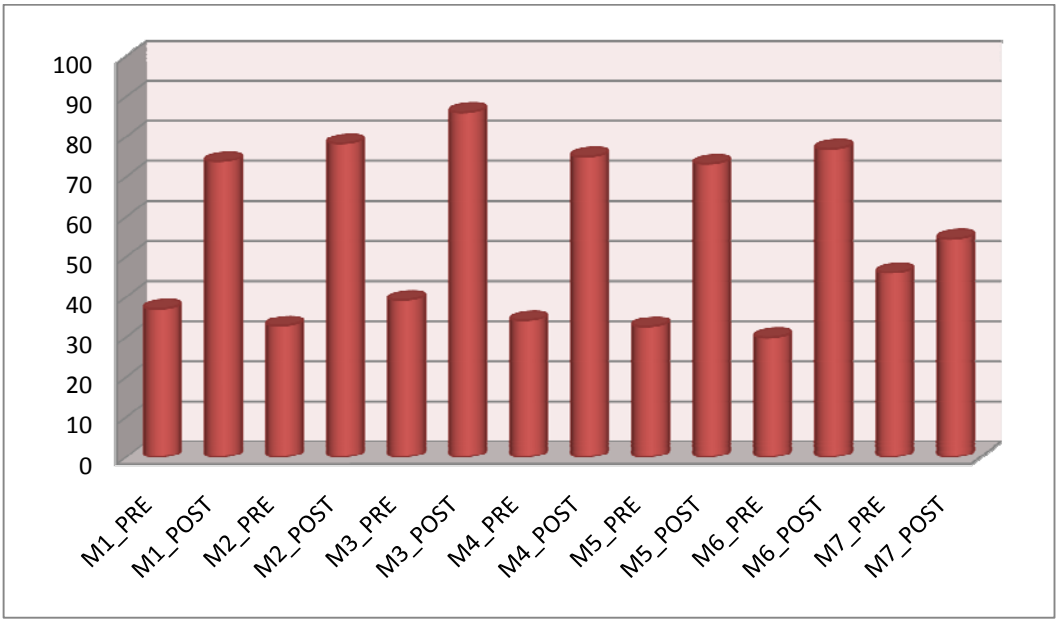

Figure 3: Mean Comparison for Each Module's Pre-Test and Post-Test Scores

These results show that, for Modules 1-6, the students' pre-test scores averaged 29-39%, while students averaged 46% in Module 7. The students achieved the greatest gains in Module 3 and, as noted, they augmented their knowledge least in Module 7.

We note that for Modules 1-6, students doubled their knowledge between pre- and post-test, a far more pronounced result than for Module 7. By the end of the training, participants significantly improved their knowledge of a broad array of important information security issues. These include malware, anti-virus protection (i.e., firewall), safe operating systems, minimizing risks, encryption, passwords and networking communications, and human-factor-driven attacks and breaches. They also gained deeper understanding about personal privacy and social engineering attacks that are generally rooted in misperceptions and weak comprehension of human factors in information systems security.

These data invite additional possible explanations for the students' performance on Module 7. Perhaps they focused on their weakest areas (Modules 1-6), or as the deadline drew near, they had little energy to devote to Module 7. Anecdotally, we observed that students did work through the modules in sequence (1, 2, 3, etc.).

We conjecture that our finding for Module 7 stems from a general lack of attention to the risks inherent in Internet browsing, the main topic of that module. Perhaps the university and the students' places of employment lack well defined, widely acknowledged, and fully implemented information security policies and practices. Further, the students who were accustomed to using their browser's default settings also demonstrated a preference for their own convenience over security concerns. Nonetheless, this gap calls for further empirical studies investigating the psychological and mental drivers that enable individual students to consider security issues while they are browsing.

Additional Observations

Figure 3 shows that students advanced their knowledge most in Module 3, which focuses on human-factor breaches, such as social engineering attacks (i.e., an intruder masqueraded as a legitimate IT staff asking a novice user for his system access information). This suggests that the topic should continue to be emphasized in information security education or awareness programs since the coverage yields strong results.

The comparatively low increase in Module 7 is difficult to interpret completely from this small study. However, it implies that students still encountered difficulties understanding safe browsing and the penalties for misuse in organizations. Further study of the training and the testing materials, and sequencing, might yield additional insights. Nonetheless, the topic is key for all networked computer users. Organizational policies dealing with punishment for misuse and unsafe browsing need to be further elucidated and elaborated in information security education and in daily workplace practices.

V. CONCLUSIONS, LIMITATIONS & FUTURE WORK

Information systems security is an increasingly relevant aspect of general management education. In an effort to meet the increasing demand for qualified students who have a satisfactory command of information security in today's market, the faculty in UNM's Anderson School of Management Center for Information Assurance Research and Education (CIARE) began to disseminate information security knowledge as part of the required undergraduate MIS course.

This study examines the learning impact of teaching and illustrating information systems security concepts within the context of this general MIS course. The authors used an ACT-Online cyber-security certificate mini-course as information security materials to gauge individual students' pre-test and post-test training scores. By reviewing the results, we identified the topics participants knew the most and least about, so that we could focus future attention on the least understood concepts and principles thereby enabling incoming students to master the needed knowledge.

Results of the study strongly suggest that differences in understanding about the first six modules of the ACT-Online training persist between the pre-test and post-test sessions. It is worth mentioning that participants show an abundant increase in understanding human-factor-driven attacks, which are sometimes overlooked by general computer users who tend to focus on technological countermeasure, The statistical insignificance of Module 7, which relates to organizational policies coping with misuse and browsing safety, indicates that students need additional guidance in the arena of how to design, establish, and comply with various organizational polices to regulate users' behavior toward a hardened and secure computing environment.

Although the findings of the study provide useful suggestions for design and delivery of information security content within a general MIS course, inevitably the study has limitations.

First, because of the impossibilities of selecting a random sample of students throughout the student population of UNM, the study used a convenience sample from the Anderson School of Management. With this limited external validity, this research only focuses on investigating the learning impact of business majors. Therefore, it is possible that the findings are not generalizable to courses in other academic areas. The authors therefore suppose that the findings of this research might vary across different disciplines (i.e., computer sciences/engineering, education, foreign languages) and that the certificate training's modules may need to be tested among these groups.

Second, because of the small sample size, the authors cannot definitely presume that these results accurately reflect all participants' learning outcomes. As such, future research is desired to analyze subjects' responses from additional populations. Finally, future studies are suggested to employ measures of learning, such as measuring behaviors and knowledge over time and in varying contexts.

Finally, because of data limitations, we were unable to make comparisons of subgroup performance, and to analyze any revealed differences that might exist for MIS majors vs. non-majors, students who had (not) completed IA courses, gender and work experiences. To be actionable, future studies will need to account for such demographic characteristics.

ACKNOWLEDGEMENTS

The authors would like to thank the IAIM 2009 anonymous reviewers for their helpful comments on this work and our future work in this area.

REFERENCES

ACT-Online [2009], Cyber Security Training site: Course Catalog – Information Security for Everyone, https://www.act-online.net

Armstrong, H. and N. Jayaratna [2002], "Internet Security Management: A Joint Postgraduate Curriculum Design," *Journal of Information Systems Education*, Vol. 13(3), pp. 249 – 258. http://www.jise.appstate.edu/Issues/13/249.pdf

Cao, Q. J. David, X. Bai and O. Katter [2002], "Using ASP-Based Message Encryption Project to Teach Information Security Concepts," *Journal of Information Systems Education*, Vol. 13(3), pp. 183 – 186. http://www.jise.appstate.edu/Issues/13/183.pdf

CAE [2007], Centers of Academic Excellence, http://www.nsa.gov/ia/

Cockcroft, S. [2002], "Securing the Commercial Internet: Lessons Learned in Developing a Postgraduate Course in Information Systems Security," *Journal of Information Systems Education*, Vol. 13(3), pp. 205 – 210. http://www.jise.appstate.edu/Issues/13/205.pdf

Grimaila, M and K. Kim [2002], "An Undergraduate Business Information Security Course and Laboratory," *Journal of Information Systems Education*, Vol. 13(3), pp. 189 – 196. http://www.jise.appstate.edu/Issues/13/189.pdf

Haggerty, N and Ramasastry Chandrasekhar [2008] "Security Breach at TJX," Ivey case 9B08E003. http://cases.ivey.uwo.ca

Hazari, S. [2002], "Reengineering an Information Security Course for Business Management Focus," *Journal of Information Systems Education*, Vol. 13(3), pp. 197 – 204. http://www.jise.appstate.edu/Issues/13/197.pdf

Hsu, C. and J. Blackhouse [2002], "Information Systems Security Education: Redressing the Balance of Theory and Practice," *Journal of Information Systems Education*, Vol. 13(3), pp. 211 – 218. http://www.jise.appstate.edu/Issues/13/211.pdf

IA [2009] Information Assurance Program at University of New Mexico Anderson School of Management (http://ia.unm.edu)

IASE [2009] Information Assurance Support Environment; Federal IS Security Awareness for non-DOD employees http://iase.disa.mil/eta/issa/Federal_ISS_V1/index.html

Kim, K and K. Surendran [2002], "Information Security Management Curriculum Design: A Joint Industry and Academic Effort," *Journal of Information Systems Education*, Vol. 13(3), pp. 227 – 236. http://www.jise.appstate.edu/Issues/13/227.pdf

Kim, S. and M. Choi [2002], "Educational Requirements Analysis for Information Security Professionals in Korea," *Journal of Information Systems Education*, Vol. 13(3), pp. 237 – 248. http://www.jise.appstate.edu/Issues/13/237.pdf

Liao, Q & X. Luo [2007], "Studying Computer Security in a MIS Degree Program." *Proceedings of SW Decision Sciences Institute*, pp.226 – 235. Online at http://www.swdsi.org/swdsi07/2007_proceedings/

Loch, K. D., H. H. Carr, and M. E. Warkentin [1992], "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly, Vol.16 (2), pp. 173-186.

Logan, P. [2002], "Crafting an Undergraduate Information Security Emphasis within Information Technology," *Journal of Information Systems Education*, Vol. 13(3), pp. 177 – 182. http://www.jise.appstate.edu/Issues/13/177.pdf

O'Brien, J. and G. Marakas [2008]*, Introduction to Information Systems*, 13/e Custom Published with Perle MIS Cases. McGraw-Hill: 2008. ISBN-13 978-0-390-75659-6

Sasse, M.A., Brostoff, S., and Weirich, D [2001], "Transforming the 'Weakest Link' -- a Human/computer Interaction Approach to Usable and Effective Security," *BT Technology Journal*, Vol.19 (3), pp 122 - 131.

Schatzberg, L. & D. Harris [2005], "Initial Experiences with a Capstone Approach to an Introductory IS Course (IS 2002.1)." *Information Systems Education Journal* 3 (8), pp 1-10. Online at http://isedj.org/3/8/

Stevens, K. and R. Jamison [2002], "A Popular Postgraduate Information Systems Security Course," *Journal of Information Systems Education*, Vol. 13(3), pp. 219 – 226. http://www.jise.appstate.edu/Issues/13/219.pdf

Surendran, K., K-Y. Kim, and A. Harris [2002], "Accommodating Information Security in our Curricula," *Journal of Information Systems Education*, Vol. 13(3), pp. 173 – 176. http://www.jise.appstate.edu/Issues/13/173.pdf

Trimmer, K., C. Schou, and K. Parker [2007], "Enforcing Early Implementation of Information Assurance Precepts throughout the Design Phase," Journal of Information Systems Education, Vol. 9(1), pp. 95-120. http://www.sig-ed.org/jier/v9n1/JIERv9n1_article5.pdf