

Embedding Context: An Integrative Computer Security Course

Michael Clump, Janine Dewitt, and Cynthia Cicalese

Marymount University

Abstract

Computer security programs consistently segregate technical content and contextual information. This paper describes the results of an introductory graduate computer security course that embedded contextual content into the course. The students' thoughts on the amount and importance of these contextual components changed from the beginning of the course to the end of the course. In addition, students' ratings of the amount of course content that should be allocated to technical information decreased from the beginning to the end, as did their thoughts on technical content as the most important area for working in computer science. An examination of focus group responses indicated that the students now felt they needed to consider all concerns, not just technical ones, when implementing solutions.

Background

One approach to teaching ethical reasoning is to require a stand-alone course in the undergraduate program. This “segregated” pattern of curriculum delivery is common in the field of computer security—where students are fascinated by the technical measures that make it possible to thwart intruders and protect information assets. Teaching these students the skills necessary to defend against security breaches presents a conundrum because these same technical skills can be used to attack computers and networks. Students must gain experience weighing the social, legal, and ethical implications associated with technical security strategies. Computer security educators need to convince this potentially resistant audience, their students, that understanding how the social context affects selection of the most appropriate technical solution is both a relevant and necessary element of the computer security decision-making process. We proposed and tested an integrated approach that presents the contextual elements at the same time that technical content is introduced. (Clump, Dewitt, & Cicalese, 2007; DeWitt & Cicalese, 2006).

A typical computer security curriculum focuses on the course content that attracted students to this major—the technical aspects of computer security. Student exposure to the social, legal and ethical issues or contextual content occurs in these classes as an informal reference to a recent news event or more systematically in a single course that focuses primarily on computer science ethics or information policy. This traditional approach may not be the most effective preparation for facing complex situations on the job (DeWitt & Cicalese, 2006).

In response to the increasing complex situations at work, Bordogna, Fromm, and Ernst (1995) called for a transformation of undergraduate engineering programs by integrating knowledge and process across individual courses. The resulting holistic model of science education was an effort to align engineering students’ educational experience with the challenges that they face on the job, including their ability to account for the social context in which technical decisions are made. This integrative approach has gained favor in many other scientific disciplines, such as biology, but has yet to receive an empirical assessment in the field of computer science.

Computer science educators recognize the importance of developing students’ ability to reason ethically and take into account the social context of technical decision-making (Martin & Weltz, 1999). In

1996, the ImpactCS Project called for the integration of ethics and social responsibility across the computer science curriculum (Martin & Weltz, 1998). A recent survey of 251 computer science programs found that 88% of these programs provide students with some exposure to social and professional issues including ethics training, with 12% of the programs not teaching ethics at all (Spradling, Soh, & Anson, 2008). Although encouraging, this study does not describe how computer science programs provide ethics training—namely, the extent to which these programs sequentially develop a students' knowledge of the social, legal or ethical issues that are associated with the technical computer science content.

To examine this question of how engineering programs develop students' contextual knowledge, Colby and Sullivan (2008) reviewed accreditation self-studies of programs from engineering schools. From this pool of programs the researchers conducted seven site visits to undergraduate engineering programs—yielding a representative sample of how engineering programs teach ethics and professional responsibility. Researchers learned that case studies, both real and hypothetical, were commonly used to acquaint students with ethical decision-making. However, coverage of these contextual issues was uneven and often unplanned by faculty. Moreover, few programs assessed students' ability to recognize an ethical challenge or propose a solution that accounted for ethical concerns.

In the field of computer security and information assurance, conversations regarding how best to develop these analytical skills have been initiated, but not tested. For example, Dark, Harter, Morales, and Garcia (2008) suggest a four-dimensional approach to addressing ethics which could support the integration of social context (social, legal and ethical issues) across the curricula. The model proposed by these educators addresses some of the pedagogical challenges associated with teaching ethics that differ significantly from the challenges of teaching the technologies of computer security, but it is too soon to have data on the effectiveness of this approach.

Efforts to document the effectiveness of integrative approaches to computer science education are just getting underway, as educators begin to analyze data gleaned from the practice of outcomes-based assessment that is associated with accreditation (Rigby & Dark, 2006). Although we can locate efforts to measure students' understanding of information technology content by evaluating concept maps (Rigby, Dark, Ekstrom, & Rogers, 2008), it is more difficult to find assessments of integrative approaches in the field. We must instead extrapolate from the research in other scientific disciplines. When doing so

we find that some students in science and technical fields value an analysis of the social context more than others. Kilgore, Atman, Yasuhara, Barker, and Morozov (2007) examine the relative importance first year engineering students place on the technical details versus the context of the engineering design challenge. They found that women were more sensitive to these contextual factors. As a result, Kilgore et al. recommend that engineering programs incorporate context-oriented approaches to broaden the participation of women as well as to produce graduates who are better able to meet the challenges they will face on the job.

Case studies are one way of providing context with technical content. Instead of using a traditional lecture format, Venglar and Theall (2007) delivered ethics content to physical therapy students using the case-based method. Using focus groups, Venglar and Theall found that these physical therapy students expressed an increased appreciation for the importance of ethics content and felt more comfortable integrating the ethical content with clinical practice.

Based on research in higher education, we suggest that the process of integrating knowledge needs to be intentionally facilitated in the classroom because students do not automatically transfer knowledge or combine what they learn in different courses (Association of American Colleges and Universities and the Carnegie Foundation for the Advancement of Teaching, 2004; DeWitt & Cicalese, 2006). The case study materials evaluated in this paper were designed to provide multiple, sequential opportunities to examine the technical content, thereby increasing the students' abilities to assess relevant contextual issues and transfer knowledge from one situation to another (cf., DeWitt & Cicalese, 2006). Facilitated by a grant from the National Science Foundation¹ (NSF), a two-course sequence (Computer Security I and Computer Security II) served as the foundation. In these courses students developed the analytical skills necessary to integrate contextual analysis when developing computer security strategies. This paper will focus on the lessons learned from the implementation of the first course in this sequence, Computer Security I.

Description of the Course

Computer Security I (CS I) was initially developed and piloted in the Spring of 2005 (Hoffman, Cicalese, DeWitt, & Rosenberg, 2005). Based on the analysis of data gathered from the instructors and

students, the course was revised and offered a second time in the Spring of 2006. The faculty experience in CS I one was similar to that of other faculty who implement active learning strategies in traditional science classrooms. Student resistance can take many forms, including providing negative feedback regarding non-traditional instruction on the course evaluations (Thorn, 2003; as cited in Rhem, 2006). In addition, some computer security students were reluctant to discuss ethical issues. When CS I was offered the second time in the Spring 2006, the instructor emphasized the importance of using a systematic process of ethical reasoning and decision-making. This disciplined procedure, or “algorithm,” thereby enables students to make ethical judgments on the job that are sound and based on a solid rationale (DeWitt & Cicalese, 2006, p. 38).

CS I differed from traditional computer science courses in two ways. First, students were encouraged to take a more active role in the classroom. Second, the course content incorporated the discussion of the social, legal and ethical content. The class course schedule was developed using a specific scenario for a period of two to three weeks. These scenarios provided a basis for students to apply both critical and ethical reasoning. The initial scenarios were both general and open-ended. Students were prompted to ask questions, and as a result, fill-in the technical gaps concerning how a security breach occurs. As the semester progressed so did the complexity of the scenarios; they became more detailed and closer to actual incidents the students may encounter. These later scenarios required students to make specific technical assessments. The scenarios ranged in the determination of wrongdoing or blame, from being initially direct to complex and amorphous in the end (Clump et al., 2007; DeWitt & Cicalese, 2006).

Hands-on lab activities and discussions supplemented the technical course material which had to be presented in lecture format. For example, students discussed the advantages and limitations of installing a software application to disable illegal peer-to-peer file sharing after the different professional codes of ethics, legal statutes, and associated ethical dilemmas were covered. When learning about wireless vulnerabilities, students used different software programs to locate a hidden access point on campus. To prepare for these class activities and discussion of the scenarios, before class students were expected to complete the assigned readings and homework assignments which addressed the technical content of the scenario. To assess the students' progress, the students completed case analyses for

each scenario, which culminated in “The Final Challenge” (i.e., a final project) (Clump et al., 2007; DeWitt & Cicalese, 2006). “The Final Challenge” required students to create their own computer security scenario by extending analysis of a case introduced earlier in the semester (Bowyer, 2000). In addition to providing the relevant contextual information for the incident and their technical response to the incident, students provided a suggested action plan that considered the social, legal and ethical aspects associated with the case. The current study provides an assessment of this fully implemented integrative computer security course.

Hypotheses

The development of an integrative approach to the CS I class involved embedding contextual information into the technical information: content related to ethics, such as ethical behavior of computer security professionals, and the legal implications of security strategies were necessary elements when presenting the technical foundation of the computer security course sequence. Three contextual elements impact the computer security decision-making process: the social standards of the organization and profession, the legal statutes, and ethical dimensions associated with the situation. All three must be taken into consideration when developing a security strategy.

As a result of the implementation of this integrative course, we hypothesized that the students' thoughts on:

1. the amount of course content that should be dedicated to technical content would decrease;
2. the amount of course content that should be dedicated to ethical content would increase;
3. the amount of course content that should be dedicated to legal content would increase;
4. and the amount of course content that should be dedicated to social content would increase.

Procedure

During the first class period of the Fall 2006 semester, each student was provided with an anonymous research packet which contained an informed consent form, a demographics questionnaire, and a 21-item questionnaire (here forth named the Student Perceptions Questionnaire, SPQ) that assessed the students' thoughts on how course content should be divided between technical aspects of

computer security, social implications of computer security, ethical aspects of computer security, and legal issues associated with computer security. The SPQ also assessed the students' beliefs about computer security and computer science in general. The students were given the research packets at the end of the first class period, and they were told to complete the packet at home during the intervening week. The students returned their research packets at the beginning of the class the following week. During the second to last week of the course, the students were again provided with the anonymous research packets. The students completed the research packets during the intervening week and returned them to the researcher at the beginning of the last class.

Complete pre-test and post-test data was obtained from 6 students. Since the course only met once per week and the university's deadline for students to add courses to their spring schedules occurred after the second class, and thus the second week, many of the students added the class after the initial (i.e., pre-test) research packets were distributed and collected. The distribution of the initial research packets occurred on the first day of class and the collection of these research packets occurred one week later, which was the second day of the class. As mentioned, the research packets were collected in the same manner at the end of the semester. The packets were distributed on the penultimate class, which was the second to last week of the semester; the students completed the research packets at home over the intervening week; the packets were then collected on the last day of class, which was held on the course's scheduled final exam day. Thus, the data provide an opportunity to analyze changes in the students' thoughts via a pre-test/post-test design, however, the low number of students leads to caution when interpreting the results.

At the end of the semester, all 13 of the students enrolled in the course were involved in focus groups. The students were divided into groups of three, asked to determine a recorder for the group, given sheets to answer 3 questions ("describe the strengths and weaknesses of using news stories of real computer security incidents as a basis for introducing you to computer security topics; describe how you now view the combination of the technical content of computer security with organizational, legal and ethical concerns; and now that we are finished, do you have suggestions for how to make the course a more effective learning experience"), and then given 30 minutes to complete the task.

Results

Quantitative Data Analysis

Since the focus of the course was to determine if embedding contextual information into a computer security course would alter the students' thoughts on the amount of course content devoted to these topics and technical content, we analyzed the data from the first question on the SPQ. This question asked, "For the following four areas, please indicate the percentage of a graduate course in Computer Security that should be devoted to these four topics. Make sure that you allocate a total of 100% to these four areas (the total cannot exceed 100%)," and the 4 options were: *Technical Aspects of Computer Security technologies*, *Social Implications of Deploying Computer Security technologies*, *Ethical Implications of Deploying Computer Security Technologies*, and *Legal Implications of Deploying Computer Security Technologies*.

For the students who took both the pre-test and the post-test version of this question, their desired amount of course content significantly increased for the Social Implications ($p < .05$)ⁱⁱ. The change in the students' prescribed amounts for Technical Aspects (decrease) and Legal Implications (increase) were marginally significant ($p < .10$). The students' prescribed amount did not significantly change for the Ethical Implications.

Table 1

Pre-test and Post-test Means and Standard Deviations for the Amount of Course Content

Content Area	Pre-test		Post-test		<i>t</i>	<i>p</i> -value	<i>r</i> ²	<i>d</i>
	<i>M</i> %	<i>SD</i>	<i>M</i> %	<i>SD</i>				
Technical	55.00	23.45	39.167	12.81	2.48	.06	.51	1.01
Social	11.25	4.40	18.33	5.16	-2.71	.04	.55	1.10
Ethical	16.25	10.69	17.50	7.58	-.264	.80	.01	0.11
Legal	17.25	9.87	25.00	11.83	-2.24	.08	.46	0.94

This data illustrate that the students' thoughts on the distribution of course content moved from being more focused on technical content to being more diverse by including a larger amount of contextual information. Along a similar line, question 20 on the SPQ had the students rank order the importance,

from 1 (*most important purpose*) to 4 (*least important purpose*), of “knowledge in that area is for working in computer science.” The students’ rank of technical content decreased from a mean rank of 1.00 (all students selected *most important*) at the beginning of the course to 2.50 at the end of the course (half of the students selected *least important* and half selected *most important*). The students’ ranking of the ethical and legal implications both increased from the beginning of the course (2.67 for ethical implications with 50% selecting *important*, 33.3% selecting *slightly important*, and 16.7% selecting *least important*; and 3.33 for legal implications with 16.7% selecting *important*, 33.3% selecting *slightly important*, and 50% selecting *least important*) to the end of the course (2.33 for ethical implications with 16.7% selecting *most important*, 33.3% selecting *important*, and 50% selecting *slightly important*; and 2.00 for legal implications with 33.3% selecting *most important*, 50% selecting *important*, and 16.7% selecting *least important*). The mean rank for social implications remained fairly stable changing from 3.00 (with 1/3 of students selecting each of *important*, *slightly important*, and *least important*) at the beginning to 3.17 (with 16.7% selecting *important*, 50% selecting *slightly important*, and 33.33% selecting *least important*) at the end of the course. The students now ranked both ethical and legal implications as more important than technical content.

Focus Group Qualitative Data Analysis

We used a grounded theory analysis (Patton, 2002) to assess the themes that emerged in the focus group data about the course and its scenarios. The themes of (1) helping the students learn potential threats and ways to prevent them and (2) students reading more compared to their other courses due to the engaging cases emerged as a result of the course using current information for course readings. The following are the statements from the focus groups to the question, “This course used news stories of real computer security incidents as a basis for introducing you to computer security topics. What were the strengths of this approach? For instance, did you read more of the course material compared to reading assignments in other courses? Did these incidents stimulate your thinking about potential computer security threats, risks and vulnerabilities?”:

- Theme 1: Provides current information allowing for better learning of potential threats and ways of preventing them:

- “Stories which were real and current give us the exposure about the things that attacks happen currently. Gives us clear ideas about defense and attacks on network and systems in a given prospective [*sic.*, *perspective*]. Reading in this class even though more is like reading a newspaper but not like reading a book.”
 - “Yes, these greatly helped us to learn about potential threats and building a secure network for an organization.”
 - “We learned current methods used by hackers today. Also, we learned of ways to prevent this.”
 - “Because of our projects and discussions we are able to analyze different security threats, risks, and vulnerabilities, and how they relate to each other.”
 - “We learned new and valuable resources from cases.”
 - “Real-life practical scenarios.”
 - “The course also stimulated our thinking about security issues and equally helped us make further research.”
- Theme 2: Increased, and engaging, reading:
 - “We read more here than we did in other courses.”
 - “The course material was sufficient enough that we didn’t need outside sources.”
 - “We learned more from cases than books.”

Additionally, the theme of increased respect and awareness for the organizational policies and consequences of different actions, such that they felt that they needed to consider all concerns, not just technical ones, when implementing a solution (which corresponds to the data from question #20 on the end of semester SPQ) emerged in the focus group data.

- “Gained respect for organizational and community policies.”
- “Better awareness for policies and even recommend the kind of policies an organization must follow.”
- “Legal and ethical cases should be a huge part of the course.”
- “Using a technical control is dependant on legal and ethical issues.”

- “We now think more actively about these three contextual issues. The legal and ethical concerns are specifically more aware.”
- “We need a policy that protects individuals from hackers legal action is needed to scare away any users thinking about violating someone’s right to privacy.”
- “Legal and ethical concerns are more on top of the list along with technical concerns. They all work together in having a more complete view of security issues.”
- “Raise awareness for consequences of hacking.”

Course Evaluation Data

Two questions on the university’s end-of-course student evaluations provide important and relevant data. These questions are (1) “How would you rate this course as a learning experience?” and (2) “How much do you feel you have learned in this course compared to other courses you have taken at _____?”. The first question uses a 5-point Likert-scale with 1 (*very poor*) and 5 (*excellent*) as the end-points. All of the students chose the two highest options, indicating that the course was either an *excellent* or *good* learning experience (with 64.29% choosing the *excellent* option).ⁱⁱⁱ For the question, “How much do you feel you have learned in this course compared to other courses you have taken at _____?,” 75% of the students in course indicated that they learned either *much more* or *more* in the new CS I course than other courses they had taken at the university.^{iv} This question also used a 5-point Likert-scale with 1 (*much less*) and 5 (*much more*) as the end-points. Additionally, the option *this is my first course at the university* was provided.

Discussion

The quantitative and qualitative data analyses indicated that the students’ attitudes on the importance of contextual information (i.e., social, ethical, and legal issues) increased; this corresponded with a decrease in the students’ attitudes on the importance of technical aspects of a course. Teaching a course in which students are exposed to scenarios that depict the influence of contextual issues influences the students’ attitudes on these topics. The students stop seeing these as ideals that will be easy to apply and are outside of the realm of a class that teaches technical information, instead they start to see situations as more complex than “right or wrong,” or more specifically in computer science, as “0s

and 1s.” An interesting depiction of this arises from the second course in this introductory computer security sequence.

When Computer Security II (CS II) was taught for the first time, all of the students who took the first offering of CS II were those from the initial two times CS I was offered. At the end of the semester, we surveyed the students' thoughts on the combination of the two courses via focus groups. Using a grounded analysis to examine students' responses to the question, “Having completed both CS I and CS II, please describe how you now view the combination of the technical content of computer security with organizational, legal and ethical concerns,” the theme that surfaces from the data is that the technical content is important to students, but they now see that it does not exist in a vacuum. In their future/current jobs, these students know they must consider the implications of different technical solutions:

- Theme 1: Consider implications/ramifications:
 - “The technical content of computer security can be used in either malicious intent or with the objective to protect assets. In both cases, the impact of organizational, legal, and ethical ramifications always needs to be considered.”
 - “Ethical implications are ‘at least considered’ now versus before they were not.”
 - “The organizational, legal, and ethical concerns are now much more paramount in our thinking. The group agrees that this is most beneficial.”
 - “We are far more aware of the organizational, legal, and ethical concerns/viewpoints than before.”
 - “The technical attributes are always the initiators, but rarely ends there.”
- Theme 2: Increased knowledge of consequences:
 - “Appreciated the education on the consequences of the legal and ethical exploitations.”
 - “More educated now on FERPA.”
- Theme 3: Must balance of organization, legal and ethical concerns:
 - “Appreciate knowing that we have balance the pros and cons of the organization, legal, and ethical concerns.”

Conclusions

Integrative experiences and courses provide students with the opportunity to truly combine course information in manner that reflects the ways in which this information will be used outside of the classroom. Students often struggle in applying the course material, especially when it requires them to combine information from separate courses while in the work force. One manner that this course utilized which helps students to combine information is to embed the necessary social and contextual information into the technical information taught in a computer security course. By embedding the course material, an integrative course, and thus, an integrative learning experience was created. Changing students' expectations on a course is challenging and risky for an instructor. However, as the current course and evaluation of the student attitudes toward that course indicate altering course content, structure, focus, method of instruction and delivery, and assignments can positively alter student expectations, beliefs, and evaluations of that course.

References

- Association of American Colleges and Universities and the Carnegie Foundation for the Advancement of Teaching, (2004). *Statement on integrative learning*. Retrieved on January 31, 2007, from http://www.aacu.org/integrative_learning/pdfs/ILP_Statement.pdf
- Bordogna, J., Fromm, E., & Ernst, E. (1995). An integrative and holistic engineering education. *Journal of Science Education and Technology*, 4, 191-198.
- Bowyer, K. W. (2000). Pornography on the dean's pc: An ethics and computing case study. *Journal of Information Systems Education*, 3-4, 121-126.
- Clump, M. A., DeWitt, J., & Cicalese, C. (2007). Assessment required: An interdisciplinary computer security team's creative SOTL experiences. *Proceedings of Improving University Teaching Conference*, 32. Retrieved July 3, 2007, from <http://www.iutconference.org/>
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Hillsdale, NJ: Lawrence Erlbaum Associates.
- Colby, A., & Sullivan, W. M. (2008). Ethics teaching in undergraduate engineering education. *Journal of Engineering Education*, 97, 327 – 338.
- Dark, M., Harter, N., Morales, L., & Garcia, M. (2008). An information security ethics education model. *Journal of Computing in Small Colleges*, 23(6), 82-88.
- DeWitt, J., & Cicalese, C. (2006). Contextual integration: A framework for presenting social, legal and ethical content across the Computer Science and Information Assurance Curriculum. *Proceedings of the Conference on Information Security Curriculum Development*, 3, 30-40. Retrieved July 3, 2007, from <http://doi.acm.org/10.1145/1231047.1231054>
- Hoffman, L., Cicalese, C., DeWitt, J., & Rosenberg, T. (2005). *An integrated approach to computer security instruction using case study modules and a portable network laboratory*. Presentation at the 4th World Conference on Information Security Education, Moscow, Russia.
- Kilgore, D., Atman, C., Yasuhara, K., Barker, T., & Morozov, A. (2007). Considering context: A study of first-year engineering students. *Journal of Engineering Education*, 96, 321-334.

- Martin, C. D., & Wertz, E. Y. (Eds.) (1998). *From awareness to action: Integrating ethics and social responsibility across the computer science curriculum: Third report from the Project ImpactCS steering committee*. Washington, DC: George Washington University, School of Engineering and Applied Science. Retrieved on January 24, 2009 from <http://www.seas.gwu.edu/~impactcs/paper3/pg1.html>
- Martin, C. D., & Wertz, E. Y. (1999). From awareness to action: integrating ethics and social responsibility into the computer science curriculum. *ACM SIGCAS Computers and Society*, 29(2), 6-14.
- Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). London: Sage Publications.
- Rhem, J. (2006). The high risks of improving teaching. *The National Teaching and Learning Forum*, 15(6). Retrieved on January 28, 2007 from <http://www.ntlf.com/html/ti/risks.htm>
- Rigby, S., & Dark, M. (2006). Using outcomes-based assessment data to improve assessment and instruction: A Case Study. *ACM SIGITE Newsletter*, 3(1), 10-15.
- Rigby, S., Dark, M., Ekstrom, J., & Rogers, M. (2008). Measuring conceptual understanding: A case study. *Proceedings of the ACM SIGITE conference on Information Technology Education*, 9, 11–16. Retrieved January 24, 2009, from <http://doi.acm.org/10.1145/1414558.1414563>
- Spradling, C. L., Soh, L.-K., & Ansorge, C. (2008). Ethics training and decision-making: Do computer science programs need help?. *Proceedings of the SIGCSE Technical Symposium on Computer Science Education*, 39, 153–157. Retrieved January 24, 2009, from <http://doi.acm.org/10.1145/1352135.1352188>
- Venglar, M., & Theall, M. (2007). Case-based ethics education in physical therapy. *The Journal of Scholarship of Teaching and Learning*, 7, 64-76.

Notes

i This work has been supported by grants DUE-0313792 and DUE-0536630 from the National Science Foundation, by the Clare Boothe Luce Program of the Henry Luce Foundation, and by an equipment donation from Cisco Systems.

ii Even though the number of students enrolled in the course was small, and the number who completed the pre-test and post-test surveys is even smaller, the questions to which the students responded were continuous in nature, and thus, reporting the mean percentage or the mean rank seems to provide most informative measure of the students' responses. We also used *t*-tests to compare the students' responses, which with the small number of students this can be perceived as problematic, but given the very large and substantial effect sizes (based on Cohen, 1988), it seems informative to report these statistical comparisons.

iii It should be noted that there was a significant increase in student evaluations from when this version of the course was offered the first time in the Spring 2005 ($M = 3.58$, $SD = 1.06$) to the second time in the Fall 2006 ($M = 4.64$, $SD = .50$), $t(36) = -3.51$, $p = .001$.

iv For the students who responded to the question and the course was not their first course at the university, there was a significant increase in student evaluations from when this version of the course was offered the first time in the Spring 2005 ($M = 2.91$, $SD = .92$) to the second time in the Fall 2006 ($M = 3.92$, $SD = .67$), $t(32) = -3.33$, $p = .002$.