Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Increasing Information Security Awareness in Non-security Courses: A Virtual Team Approach

Judith C. Simon, Aaron K. Smith, Charles J. Campbell, and Euntae Ted Lee, *University of Memphis*

Abstract – This paper describes a project to use a virtual team approach to add information security topics to two graduate courses where these topics are not the primary focus, using student teams from those two courses working with students enrolled in an information security management course. Students worked on development of an implementation plan involving security issues for a fictitious business case. Results indicated increased security awareness of students in all three courses by the end of the semester, based on pre-test and post-test results.

Index terms – virtual team, face-to-face team, information security awareness

I. Introduction

Information assurance/security concepts are taught in numerous courses designed for that topic. However, several courses focusing on other information systems and technology topics could be enhanced by specific content and activities that address information security issues related to the focus of those other courses.

The project described here involved three graduate-level Management Information Systems courses. One course involved information security management, while the other two were non-security courses into which information assurance topics could be added, primarily through the use of a project whose team members would be a mix of students from all three courses. A virtual team approach was determined to be the most practical approach for this project.

The courses used for this project are included in a graduate certificate program in Business Information Assurance that was recently approved by the University. Content used in this certificate program puts significant focus on topic guidelines for Committee on National Security Standards (CNSS) 4012 – Senior Systems Managers.

II. Use of Virtual Teams

The increasingly global nature of business activities has led many organizations to use virtual teams for some projects. Working in this virtual environment allows a team to be composed of those persons who are the best choice for the task, regardless of their physical location. This method is also effective in attracting and retaining employees who desire to work remotely [1].

Difficulties have been identified in various publications related to the use of virtual teams. For example, some reports have indicated that personal relationships and trust are difficult to build in this environment [2]. Other reports have indicated a reduction in team cohesion and an increase in conflict [3].

Working in a virtual environment was determined to be the best option for the project described here, which was designed in the format of a business case. The three classes involved met on different days, at different times and locations, and the students were enrolled in additional courses that resulted in further time conflicts. Scheduling times for team meetings would have been extremely difficult to accomplish in a face-to-face setting during the semester.

In addition, each team needed to be able to review the project presentations developed by the other teams as part of the final discussion activity, but oral presentations to the entire set of teams from this mix of courses were not feasible to schedule, a situation that is also common to global business teams.

Under these circumstances, it was decided to treat the use of virtual teams as part of the educational experience, with students expected to gain greater awareness of its advantages and disadvantages as well as greater knowledge of methods of providing a high-quality result. It was also felt that the use of virtual teams from multiple courses might provide a more business-like, realistic team experience than the traditional course team assignments where all the students on a team are in the same course, they often know all of the other students, and they focus only on issues relevant for that one course.

For purposes of this project, a virtual team was defined as one in which little or no face-to-face communication would be expected to occur for team activities. Because some teams would include more than one student from a particular course, complete elimination of any face-to-face contact was not possible.

ISBN 1-933510-99-4 ©2010 CISSE

Publications were reviewed that described experiences in using an online environment for educational projects and identified some of the difficulties. One publication noted the lack of nonverbal cues, resulting in a reduction in the richness of information sent by team members [4]. Another publication identified problems directly relevant to this project, including difficulties in working with multi-disciplinary teams in a virtual environment and the ability to transfer basic knowledge to real life scenarios [5].

Also included were suggestions for improving the experiences, such as allowing students to have some choice in the forms of communication used [6] and the need for teams to have frequent exchange of ideas and information [4].

III. Project Development

The development team included the three faculty members who were scheduled to teach the courses involved in this project, as well as a Ph.D. student who had a unique perspective by having taken all three courses. Team members had regular face-to-face meetings over four months prior to the beginning of the Fall 2009 semester when the project was to be implemented. Additional face-to-face meetings and electronic communications occurred throughout the semester.

One major challenge was to develop an information security-related project that would span three distinct yet interrelated courses. To adequately create an appropriate three-course virtual team project, documentation created by the National Institute of Standards and Technology (NIST) was used as a foundation for support material and objectives. NIST Special Publication 800-12 - An Introduction to Computer Security: The NIST Handbook and NIST Special Publication 800-30 - Risk Management Guide for Information Technology Systems contained excellent guidance for this project.

The NIST documentation was analyzed and adapted into multiple objectives and requirements to test the skills and knowledge developed in each course. The objectives were created in a way to promote an interdependent relationship among group members, i.e., to motivate group members to make decisions together.

The most extensive development aspect involved the creation of a case or scenario to use as a basis for this team project's assignments. This fictional situation was created to reduce the variability that could come from requiring each team to find a real organization to study.

The NIST documentation was used to develop pertinent questions that were specific to the fictitious organization. Organizational characteristics, such as the structure of the network, were designed by adapting similar descriptions from the NIST documentation. The project was designed so that all teams would assume that they were competing for a consulting contract to recommend the best design of a new network and related security needs, with the final team products being an electronic presentation of their proposal recommendations as well as an electronic executive summary of their work. Presentations were required to be done in PowerPoint or similar software, with extensive use of the Notes option to provide explanations and other details to the owner of the business.

A description of the business was developed, which was defined as a small retail enterprise that now has several stores. They want a new internal system and layout for each store and want a network for all stores to connect to the overall organization network. They also want a website that could be used for customers to place orders. They also want a set of corporate security policies.

Other details about the stores were developed so that teams would all base their primary efforts on the same situation. For example, the physical dimensions of all the stores were provided and all the stores would be expected to have the same layout. In addition, data regarding the average number of transactions per day was determined in advance along with information that considerable inventory is kept on the premises at each store. However, inventory management is desired to be handled through the network to the organization's inventory server rather than at each local store. Also related to the physical facility, another desire is to provide customers with in-store Internet access, so recommendations would be needed regarding equipment needs for that availability as well as possible wireless Internet access for customers.

Additional specific topics to consider as part of their design effort were included, such as:

1. Number of customer checkout areas needed
2. Frequency of updates from local sites to the organization's inventory server
3. Potential need for a designated customer service area within each store
4. Possible need for a separate connection for customer Internet access apart from the connection for inventory updates
5. Opportunities for additional uses of the website

Specific security considerations were identified for the teams, with an indication that the teams must consider confidentiality, integrity, and availability of the systems and information in making their recommendations. In addition to issues regarding the multiple stores being on the network and customers having Internet access in the retail stores, customer data such as credit card numbers would be traveling over the company's network and possibly stored within the overall system.

Another item provided for teams was a link to NIST Special Publication 800-30 - Risk Management Guide for Information Technology Systems, in order to provide further background assistance in their project development activities. In addition, a specific list of the risk management topics that needed to be considered in designing the system was developed. The detailed list is not shown here, but the major topics included:

1. Systems characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination
6. Impact analysis
7. Risk Determination
8. Control recommendation

Teams would also need to make recommendations regarding an employee training program related to the new company security policies being developed. These recommendations were to include suggestions for training methods and estimated cost. In addition, recommendations were to be made regarding ongoing training and awareness of employees, as well as a procedure for future updates to the security policies. One related recommendation was related to customer use of the in-store Internet access and any security awareness plans and policies that might be needed.

IV. Project Implementation

During the first week of the semester, students in all three courses took an information security awareness pretest. This 40-question objective test was developed after reviewing Committee on National Security Standards (CNSS) 4012 content as well as information assurance/security awareness textbooks and similar materials that were used to identify appropriate topics. A controlled environment was used. Tests were administered only within the course classrooms to regulate the amount of time allowed for the test (one class period) as well as to limit the possibility of using other resources to answer the questions.

Once the deadline had passed for new students to enroll in any of the three courses, the students were assigned to teams, which required considerable effort to ensure that each team had representatives from all three courses and that a student enrolled in two of the courses was assigned to only one team. The information security management course had the largest number of students, so each team had multiple students representing that course. The total number of different students involved was 46. Two courses had at least 20 students while one course had 9 students, so it was decided to have 9 teams. Eight of the teams had five students, and one team had six students. Students were assigned to be the primary person responsible for specified parts of the project depending on which course(s) they were taking. Some activities required students to collaborate and merge their efforts. Students getting credit for two courses were assigned an additional project involving an information security research report.

Students were provided with the list of members of each team and assigned a short assignment that required them to communicate with other team members, followed by a brief report sent to the instructors. Students were told that they could use any form(s) of communication that fit the team members' needs throughout the project. In other words, they could choose to have face-to-face meetings or work entirely virtually, or choose a combination of the two. All of the teams decided to focus on a virtual team approach, considering the schedule difficulties described above.

To initiate the actual team project, the students were provided with the business case, including a description of a fictitious organization, its sites, and the owner's request for proposals to implement a new network with adequate security. Student teams had several milestones during the project, at which time they were required to submit progress reports.

Teams were instructed to decide among themselves how they would accomplish the tasks during the semester, who would be responsible for different aspects of the project, who would submit reports, etc. To provide a little emphasis on the information security direction of the project, each class viewed a small number of brief security-related videos as part of the course content during the semester.

Final project results (recommended solutions for the business case) were due a week prior to the end of the semester, allowing time during the last week for all teams to evaluate the other teams' products and submit their reviews. Each team had to work together in its review and agree on a ranking of the other teams' work, which was designed to end the course with a team activity that required collaboration. The activity also provided each team with examples of other solutions to the same project that they could compare with their own results, as well as other methods of providing effective virtual presentations.

During the last week of the semester, a security awareness posttest was given, containing the same questions as the pretest. Resulting comparisons are described in the next section.

V. Project Results

Pretest and posttest scores were compared to determine any increase in awareness of information security topics.

A. Pretest Results

Pretest results showed that students were not very knowledgeable about the test topics at the beginning of the course.

On the pretest the overall number of questions that were missed by a majority (over 50%) of students:

19 out of 40 (47.5%) missed by majority

Students' overall scores on the pretest were also reviewed, indicating a similar result:

Pretest overall average: 54%

Pretest averages were also compared by course:

Computer hardware/system software: 54%

Data communications systems/networks: 57%

Information security management: 52%

B. Posttest Results

Posttest results showed considerable improvement when compared with pretest results. An important note is that during the semester none of the three instructors had been provided with any information as to which topics on the pretest were missed most often by their students or the actual scores for each of their students. Since the research-related purpose of the project was to study the possible increase in students' security awareness through the use of these multiple-course teams to work on a security-related business case, any knowledge of test results might have influenced instruction, so the results were not provided to instructors until after the end of the project.

Posttest overall number of questions that were missed by a majority (over 50%) of students:

7 out of 40 (17.5%) missed by majority

Students' overall scores on the posttest were also reviewed, as follows:

Posttest overall average: 73%

Posttest averages by course were reviewed:

Computer hardware/system software: 58%

Data communications systems/networks: 68%

Information security management: 76%

C. Pretest/Posttest Comparison

As shown above, the number of test questions missed by over half of the students dropped significantly from the pretest (47.5%) to the posttest (17.5%). Based on that result, it is not surprising that the overall averages increased significantly from the pretest (54%) to the posttest (73%).

The comparison of change from pretest to posttest by specific course was interesting in that it confirmed the importance of direct instruction. The students in the information security management course spent the entire semester discussing information security issues and solutions, and those students had the greatest improvement in their test averages between the pretest (52%) and the posttest (76%). The course involving data communications systems and networks had the second largest improvement from pretest (57%) to posttest (68%). The data communications and networks course had a separate unit on network security during the semester. The third course on computer hardware and

system software had the lowest level of improvement from pretest (54%) to posttest (58%). This course had no additional security content as part of the course beyond the small set of videos viewed in all three classes. These results suggest that direct instruction accompanied by the implemented team project created a greater improvement in security awareness than the team project alone.

It is expected that the posttest scores would improve even more if this project were repeated and content were included in each course that is directly related to the topics most often missed.

D. Student Perceptions of Virtual Teams

One voluntary activity at the end of the course was for students to indicate their preference as to virtual teams or face-to-face teams. Nearly 50% of the students participated. Students were asked to indicate any previous experiences they had with virtual and face-to-face teams. A few students had taken an online course that included a virtual team activity within that course. One student had full-time work experience where virtual teams were used because they had global teams. No students had previous experience with virtual teams involving multiple courses.

Students were asked to identify advantages of using virtual teams versus face-to-face teams. All the participating students were able to identify several advantages and disadvantages of each method. Most often, students mentioned convenience for students with conflicting schedules as an advantage of virtual teams. The most often identified advantage of face-to-face teams involved the value of human interaction and trust-building. Students were asked to indicate a specific preference for one method, and their choices favored virtual teams slightly (57%). However, many students also commented that the decision would usually depend on the circumstances.

VI. COMMENTS/RECOMMENDATIONS

Although all three instructors indicated that some students complained initially about the multi-course project and its virtual team environment, they agreed that student comments were much more positive at the end of the experience. One student, for example, indicated that his virtual team seemed to be more actively involved throughout the project than was true of his experiences in other classes where the teams were working face-to-face within one course and knew each other.

Some of the recommendations identified by the instructors are based on suggestions found in the literature, and others are based on the experiences of implementing this project. The recommendations include:

1. More extensive team-building activities should be used at the beginning of the semester, which have been found to be effective in reducing negative biases and providing opportunities for relationship building [2].

2. Specific group organizational activities should be provided at the beginning of the project, such as setting up an online mechanism for team communications. The use of tools such as Google Groups and Google Docs might be considered.

3. More security content should be provided before implementing the team project.

4. Security content added to each course should include items that were determined to need more emphasis, based on posttest results.

5. The project itself should be provided to students in smaller blocks at a time rather than providing the entire set of business case materials at once.

6. Instructors should expect the implementation of a project of this type to require a greater time investment than traditional course projects. Initial development activities are extensive, and frequent communication with teams is critical to the success.

7. Additional research on this methodology of using a virtual team approach for implementing information security content should be considered using courses where no students are currently taking an information-security related course. This replication would assist in determining what effect the students enrolled in security related courses may have had on the final project results.

8. Further research is needed on effective methods of implementing a virtual environment for multiple-course team projects in educational environments.

9. Further research should be conducted to compare virtual team results with face-to-face team results in solving business cases where security needs to be implemented.

10. Additional research related to virtual teams versus face-to-face teams in student environments might focus more on differences that might occur in levels of commitment to the project depending on the team format. For example, a project of this type could be subdivided so that half of the teams use a face-to-face environment and half use a virtual environment, assuming that a face-to-face environment would be feasible.

VII. References

[1] L. Martins, L. Gilson, M. Maynard, "Virtual teams: What do we know and where do we go from here?", Journal of Management, Vol. 30, No. 6, pp. 805-835, 2004.

[2] L. Robert, A. Dennis, Y Hung, "Individual swift trust and knowledge-based trust in face-to-face and virtual team members," *Journal of Management Information Systems*, Vol. 26, No. 2, pp. 241-279, 2009.

[3] A. Kankanhalli, B. Tan, K. Wei, "Conflict and performance in global virtual teams," *Journal of Management Information Systems* (forthcoming).

[4] E. Williams, R. Duray, V. Reddy, "Teamwork orientation, group cohesiveness, and student learning: A study of the use of teams in online distance education," *Journal of Management Education*, Vol. 30, No. 4, pp. 592-616, 2006.

[5] A. Rutkowski, D. Vogel, M. Genuchten, C. Saunders, "Communication in virtual teams: Ten years of experience in education, *IEEE Transactions on Professional Communication*, Vol. 51, No. 3, , pp. 302-312, 2008.

[6] P. Gibbings, J. Lidstone, C. Bruce, "Using student experience of problem-based learning in virtual space to drive engineering educational pedagogy," *Proceedings of the 2008 AaeE Conference*, 2008.