Managing Information Security Curriculum when Facing Course Scheduling Challenges: A Case Study

Marc J. Dupuis
marcjd@uw.edu

Barbara Endicott-Popovsky
endicott@uw.edu

University of Washington

I. Introduction

Universities are complex and multifaceted institutions. A single university often consists of numerous moving parts, all trying to align themselves in order to work effectively. Space is often limited. Scheduling can be difficult. Course offerings may change at the last minute.

It is this latter point that will be examined more closely here. In particular, what are some of the ways in which an instructor can teach an undergraduate course for an audience consisting largely of students generally not prepared for the content?

In this paper, we explore a case study in which an offering for one course was eliminated, which created a need for another course to open enrollment to those that had not taken the prior two courses in a three-course sequence. This third course would traditionally examine how to design and execute information security strategies in an organizational context. However, given that only two of the 43 enrolled students had taken both of the prior courses, flexibility and creativity were a must in making the course a success.

The remainder of this paper includes some background information, a discussion on the approach and overall structure of the course, some reflection from the authors with an analysis of some data, and finally some concluding remarks.

II. Background

Information security education in its various forms may include such topics as digital forensics, organizational risk management, software security, network security, and computer security, human factors, among others (Conklin, 2006; Dupuis, Crossler, & Endicott-Popovsky, 2012; Dupuis, Endicott-Popovsky, Wang, Subramaniam, & Du, 2010, 2011; Hentea, Dhillon, & Dhillon, 2006; Vaughn, Dampier, & Warkentin, 2004). Each one of these topics serves a different purpose, but all are important in the broader domain of information security. In other words, there is significant value in having courses that focus on specific components of information security, while also allowing the student to both understand and appreciate the larger information security domain.

The depth and breadth of any single one of these topics could require several courses that build upon one another throughout an academic year in order to provide adequate coverage (Whitman & Mattord, 2004). Given the complexity of any single one of the aforementioned topics, this makes sense and is warranted. In this case study, the organizational information assurance curriculum consists of a sequence of three courses: a general organizational information assurance course; a course on risk management, and finally a course that uses a case study approach to understand, design, and execute various information assurance strategies within an organizational setting.

However, in practice it may not always be feasible to limit the course only to students that had taken the prior course or courses in the sequence. In smaller programs with limited electives, at times the program and instructor have to make compromises so that there are adequate options during a term.

In the case study examined here, a new course was planned on being offered to junior-level students. In the final stages of approval, it met an administrative roadblock and was therefore not offered. As a result, there were not enough options for the junior-level students for that term. In order to accommodate the course shortfall, the instructor of the senior-level elective agreed to have it opened up to juniors as well.

In the next section, we discuss the overall approach taken and the structure of the course so as to meet some specific objectives.

III. Approach and Structure

From the beginning, there were two primary objectives that this course was designed to achieve. First, it should provide students with an ability to analyze complex information assurance situations so that they can provide thoughtful feedback on possible courses of action, including relevant recommendations. Second, students would continue to gain depth and breadth within the broader information security domain.

The first of these objectives posed a challenge in this particular offering of the course given the lack of prior relevant course content the junior-level students had had up to this point in time. The course is offered as a hybrid in which the students meet in class one day a week and supplement that with online content, including video lectures and readings. However, this first objective was still largely achieved through the use of these online video lectures and case study assignments that required thoughtful analysis of complex organizational information assurance problems. The use of online video lectures can be effective in providing content in a more flexible and convenient format, as well as allow for the students to be exposed to different viewpoints from industry experts, among others (Zhang, Zhou, Briggs, & Nunamaker Jr, 2006).

Likewise, the second objective posed unique challenges of its own, but also provided for the most opportunity to be creative in how it could be approached. Within this second primary objective, there were four secondary objectives: 1) Develop and/or improve professional communication skills, which is considered very important for information technology professionals (Heil, 1999); 2) Improve intrapersonal communication skills through team work; 3) Explore both the depth and breadth of the information security domain, and 4) Introduce academic research and relevant theories to the students.

In order to accomplish these four secondary objectives, students were given two different activities. In the first activity, students were tasked with researching an information security topic of interest to them and presenting it to the class. For the second activity, students collaborated in teams to work on a wide array of information security projects.

In the remainder of this section, we will discuss these two activities and how each of them met multiple components of these four secondary objectives.

Professional Presentation

The first activity consisted of having students present an information security research topic or article to the class. The instructor provided options each week for articles. Students could either choose one of the preselected articles or one of his or her choosing with instructor approval.

The topics included such things as social engineering, the insider threat, cryptography, network security, human factors, and organizational support issues, among others. Additionally, several of the articles included one or more theories, models, and/or frameworks common to the discipline. Students in an undergraduate information technology program are rarely exposed to social science and behavioral theories related to the use of technology, but it was valuable in helping them understand why individuals behave in often counterintuitive ways.

In preparation for the presentation, the student had to research the topic and understand the specific article assigned or chosen. Prior to class commencing, the student was required to provide the instructor with three questions related to the article that was being presented. Given the enrollment for the course, four to five presentations were given by students each week. The instructor combined the questions from each of the students presenting that week and handed them out at the beginning of class. The students were expected to make a good faith effort to answer the questions. At the end of the class period, they handed them in for credit.

Having students answer questions related to the presentation helped keep them engaged in listening to the presentations and asking questions of the presenter. Likewise, having students develop questions based on what they read and were set to present, helped them think about the material in a different light.

The presentations themselves were meant to be relatively short at no more than five to 10 minutes for each presentation. The presenters then led a discussion afterward.

This activity addressed three of the four secondary objectives. The only secondary objective not covered was the improvement of intrapersonal communication skills through team work. Engaging undergraduate students in research has several benefits (Healey & Jenkins, 2009; Hu, Kuh, & Gayles, 2007; Ozay, 2013). Next, we will discuss the other activity, information security team projects.

Team Projects

The second activity consisted of team projects, which have generally shown to be effective in information retention and critical thinking (Felder & Brent, 2001; McInerney & Fink, 2003). Several project options were provided to the students and the students were allowed to sign up for the project that appeared most interesting to them. The team projects were focused on developing depth and breadth within the information security domain, while also developing intrapersonal communication skills. They allowed the students to become engaged in meaningful projects that were generally interesting to them. If there was not an option available that met garnered their interest, they could propose a project to the instructor.

The projects included the following: 1) Developing an information security dashboard website; 2) Analyzing the use of digital forensics in the federal court system; 3) Examine how individuals choose their Facebook friends; 4) Develop digital forensics labs to be used by future students; 5) Develop hacking labs to be used by future students; 6) Create videos to help educate consumers about the dangers of malware; 7) Examine how individuals use passwords through interviews and questionnaires, and 8) Create videos to help educate consumers about effective password usage.

There were four stages to the project. In the first stage, the teams were tasked with conducting research relevant to their topic. They had to find peer-reviewed journal articles and both analyze and summarize the existing research on their topic.

In the second stage, the teams were required to develop a tri-fold brochure presenting the information they had found thus far. The brochure was meant to be informative and/or helpful, depending on the project.

The third stage consisted of the teams finalizing a draft version of their final deliverable. This was important in ensuring that the teams continued working toward their final deliverable. If any issues were uncovered, it would also give the teams time to adjust their approach for the final deliverable.

Finally, the teams presented their final deliverable to the class on the last day of the term. The format of how the final deliverable was presented varied, but included showing a video, discussing what they learned, demonstrating a website that was developed, etc.

This activity addressed all four secondary objectives. Next, we will discuss some thoughts on the approach used and analyze some data from student evaluations.

IV. Discussion and Analysis

In this section, we will discuss the overall experience with the approach used in this particular offering of a course. This will include both anecdotal evidence, as well as some observations from the course evaluation that students completed.

Professional Presentation

The professional presentation activity was effective in engaging students in material that they generally would not have engaged themselves in. Likewise, throughout the term they became exposed to a very broad range of information security topics.

The presentations themselves generally consisted of short PowerPoint presentations. However, some students chose to use alternate means to present the material. This included one student that engaged his fellow classmates with a brief lecture and demonstration of cryptography by using the dry erase board. Interestingly enough, this particular presentation was given by a student that has not been particularly fond or comfortable with presentations in prior courses. However, his presentation was arguably the most well-received of the term as he engaged his fellow classmates in a complex topic by using an interactive approach that included student participation, a demonstration, and a brief lecture on the history of cryptography.

While this student was effective in making a complex topic interesting and approachable to the other students, some of the other presentations were not as strong. As is typical with students, some excel at public speaking and giving presentations, while others struggle. Several students became frustrated and disengaged with the individuals that struggled, whether through reading the slides rather than presenting the information, or simply having great difficulties with the subject matter.

Comments in the course evaluation with respect to the professional presentations were somewhat mixed. About 90% of the comments related to this were positive, including the following: “Doing personal presentations helped stretch my thinking because it generated discussion and questions.” Several other comments expressed similar sentiments. However, some of the students felt as though the professional presentations used too much class time that could have been better spent through lectures from the instructor.

Next, we will discuss the results from the team projects.

Team Projects

The team projects appeared to engage most of the students in very creative ways. It allowed them to use other information technology type skills for specific projects related to information security. Likewise, the four-staged approach was effective in keeping the teams on task throughout the term. Each of the deliverables were important as standalone items, while at the same time helping them move toward a final deliverable.

One of the students noted: “…this class was very interactive and presented a lot of topics that were challenging.” Similar comments were made by others. As with any team project some students become disengaged, which causes problems amongst team members. Nonetheless, this component seemed to be quite well received by the students. The videos presented were entertaining and well done. The website looked professional with important content that was updated automatically. And finally, the other team projects engaged students in performing research on important topics related to information security.

Finally, in the next section we will offer some concluding remarks on this experience.

V. Conclusion

Instructors often have to be flexible in the content they deliver and how it is delivered so as to provide the best learning experience for as many students as possible. The problem posed in this case study is not necessarily unique. While we approached it in a particular manner that yielded some positive results, we do not believe there is a one size fits all solution to such challenges.

For example, the enrollment in the course consisted primary of junior-level students (75% or so), while the rest were seniors. The junior-level students appeared to be the most satisfied with their experience in the course, while some of the seniors did not appreciate the breadth of the topics covered. For example, one student presumed to be a senior commented: “We did not go into very advanced topics like I would have expected from a 400 level class.” The course was modified to be as effective as possible for the majority of enrolled students, but in the process it disenfranchised some of the students the course was originally intended for.

Quantitative measures on the course evaluation were high with a median value of 4.4/5 (5=excellent; 0=very poor) for the question of how the course as a whole was. The instructor’s contribution was likewise high with a median value of 4.7/5. Comments were generally encouraging as it related to the four secondary objectives. For example, one student noted: “Yes it helped me to build on my writing and communications skills.”

Overall, creativity and flexibility were required for this course to be successful. On the whole, we believe it was a success. Although it is never ideal to have to adjust the curriculum last minute as we had to here, there were some positive takeaways that can be reflected upon for future course offerings.

References

Conklin, A. (2006). Cyber defense competitions and information security education: An active learning solution for a capstone course. *System Sciences, 2006. HICSS’06. Proceedings of the 39th Annual Hawaii International Conference On*, *9*, 220b–220b. IEEE.

Dupuis, M., Crossler, R., & Endicott-Popovsky, B. (2012). *The Information Security Behavior of Home Users: Exploring a User’s Risk Tolerance and Past Experiences in the Context of Backing Up Information*. Presented at the The Dewald Roode Information Security Workshop, Provo, Utah.

Dupuis, M., Endicott-Popovsky, B., Wang, H., Subramaniam, I., & Du, Y. (2010). *Top-Down Mandates and the Need for Organizational Governance, Risk Management, and Compliance in China: A Discussion*. Presented at the Asia Pacific Economic Association Conference, Hong Kong, China.

Dupuis, M., Endicott-Popovsky, B., Wang, H., Subramaniam, I., & Du, Y. (2011). Top-Down Mandates and the Need for Organizational Governance, Risk Management, and Compliance in China: A Discussion. *China-USA Business Review*, 319.

Felder, R. M., & Brent, R. (2001). Effective strategies for cooperative learning. *Journal of Cooperation & Collaboration in College Teaching*, *10*(2), 69–75.

Healey, M., & Jenkins, A. (2009). *Developing undergraduate research and inquiry*. Higher Education Academy York.

Heil, M. R. (1999). Preparing technical communicators for future workplaces: a model that integrates teaming, professional communication skills, and a software development process. *Proceedings of the 17th Annual International Conference on Computer Documentation*, 110–119. New Orleans, Louisiana, USA: ACM.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education*, *5*.

Hu, S., Kuh, G. D., & Gayles, J. G. (2007). Engaging undergraduate students in research activities: Are research universities doing a better job? *Innovative Higher Education*, *32*(3), 167–177.

McInerney, M. J., & Fink, L. D. (2003). Team-based learning enhances long-term retention and critical thinking in an undergraduate microbial physiology course. *Microbiology Education*, *4*, 3.

Ozay, S. B. (2013). Engaging Undergraduates in Research. *Journal of Educational and Instructional Studies in the World*, 5.

Vaughn, R. B., Dampier, D. A., & Warkentin, M. B. (2004). Building an information security education program. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, 41–45. ACM.

Whitman, M. E., & Mattord, H. J. (2004). Designing and teaching information security curriculum. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, 1–7. Kennesaw, Georgia: ACM.

Zhang, D., Zhou, L., Briggs, R. O., & Nunamaker Jr, J. F. (2006). Instructional video in e-learning: Assessing the impact of interactive video on learning effectiveness. *Information & Management*, *43*(1), 15–27.