Journal of Information Systems Education

Volume 29
Issue 4
Fall 2018

Teaching Tip
Gaining Real-World Experience in Information Security: A Roadmap for a Service-Learning Course

Janine L. Spears

Recommended Citation: Spears, J. L. (2018). Teaching Tip: Gaining Real-World Experience in Information Security: A Roadmap for a Service-Learning Course. *Journal of Information Systems Education,* 29(4), pp. 183-202.

Article Link: http://jise.org/Volume29/n4/JISEv29n4p183.html

Initial Submission:	6 May 2017
Accepted:	22 February 2018
Abstract Posted Online:	18 September 2018
Published:	4 December 2018

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Teaching Tip
Gaining Real-World Experience in Information Security: A Roadmap for a Service-Learning Course

Janine L. Spears
Monte Ahuja College of Business
Cleveland State University
Cleveland, OH 44115, USA
j.l.spears@csuohio.edu

ABSTRACT

Students need real-world experience. Industry needs graduating students entering the workforce to be skilled in relevant subject matter, critical thinking, and communication skills. Community-based nonprofit organizations, as well as small businesses, need help in building organizational capacity. Instructors also benefit from periodic observation of organizational work in the instructor's area of teaching. A service-learning course that is focused on capacity building is a means to reach all of these goals. This article presents a roadmap for teaching a service-learning course in information security risk assessment. Students work in teams on a term-long project conducting an on-site risk assessment, making security recommendations, and producing and presenting a final security risk report to an organization's management. Teaching tips are offered on course planning, launch, materials, and execution.

Keywords: Service-learning, Security, Information assurance & security, Teaching tip, Soft skills, Team-oriented problem solving

1. INTRODUCTION

Service-learning "is a teaching and learning approach that integrates community service with academic study to enrich learning, teach civic responsibility, and strengthen communities" (NCSL, 2007, p. 3). Academic study, community engagement, and structured time for student reflection on the service experience are major cornerstones of this pedagogical approach. Service-learning is distinguished from community service in that the former integrates the service project into course materials and includes facets of career enhancement (McLaughlin, 2010). Service-learning has increasing theoretical and pedagogical guidance (e.g., Abrahams and Singh, 2010; Bamber and Hankin, 2011; Hrivnak and Sherman, 2010), including for Information Systems (IS) courses (Hall and Johnson, 2011; Lee, 2012; Wei, Siow, and Burley, 2007).

Service-learning courses have traditionally focused on community-building projects, based on a partnering, community-based organization's (CBO's) mission. For example, if students were partnering with Habitat for Humanity, they would likely participate in building affordable housing for low-income residents. Alternatively, in relatively more recent years, IS programs have begun offering service-learning courses that focus on capacity-building projects with partnering CBOs. Capacity building refers to "training and educational activities that aim to build the management skills of staff or focus on organizational processes that are necessary to promote growth and demonstrate effectiveness" (Sobeck, 2008, p. 50). Following the guidelines presented in Lending and Vician (2012) on teaching tips, this paper presents a service-learning course focused on building capacity in information security risk management within participating nonprofit CBOs.

IS service-learning courses examined in the literature focus on systems design and development projects (see Lee, 2012 for a review). In contrast, the present teaching tip makes a unique contribution by presenting a roadmap for an IS service-learning course aimed at improving an organization's information security while providing students with experiential learning in security risk assessment. Student teams work with a CBO during a term-long project to conduct an information security risk assessment. Students develop a formal report and present their findings, along with specific security recommendations, to the CBO. Given time constraints, only limited improvements can be made during the school term. However, for a subset of recommendations, students develop training materials on how a given security safeguard can be implemented. The training materials include step-by-step instructions or specific software configurations, as applicable, and a test plan on how CBO staff can periodically examine whether the security safeguard is functioning as designed.

The approach is innovative in that it exposes IS security students to the organizational and people aspects of managing security in the real world. Hall and Johnson (2011) reason that such exposure is important for IS students in general, given the common disconnect and lack of trust between information technology (IT) workers and end users, yet that relationship is crucial to success on IT projects. IS security students may face even greater challenges interacting with end users on security projects because security courses tend to focus primarily on technology to the exclusion of people and processes. Moreover, security is a sensitive topic that requires trust in order for end users to share security risk-related information with IT staff or buy into security policies. Yet, security students tend not to consider how security policies would impact the business or people of the organization. An instructor may try to describe this relationship, but in reality, it is "very difficult in a controlled classroom environment to prepare IT students to interact with end users in a real-world environment. The multi-dimensional aspects of the real-world cannot be duplicated in a traditional classroom setting" (Hall and Johnson, 2011, pp. 67-68).

The aim of the present article is to encourage and provide a roadmap for IS faculty in general, and IS security faculty in particular, on teaching a capacity building, service-learning course. The remainder of the paper presents the course structure, teaching suggestions, learning outcomes, and evidence of such outcomes, followed by a discussion and conclusion. Course materials are provided in Appendices.

2. COURSE LAUNCH

This section begins with the course description (Table 1) and objectives (Table 2) provided in the course syllabus (along with the Course Readings/Schedule and Course Assignments in Appendices 1 and 2, respectively), and then it describes how the course is structured and implemented. While the course subject matter is information security risk management, the course structure regarding the call for partners, pitch night, and assigning students to teams (as described in this section) have been applied in many other courses supported by the University Center that partnered with the instructor on this course.

Course Description
This course prepares students with real-world experience by partnering with a non-profit, community-based organization to identify information security vulnerabilities and propose recommendations that improve the organization's security and privacy practices. Within the context of an assigned community-based organization, students will work in teams to conduct a vulnerability assessment; identify and propose cost-effective security safeguards that may be administrative, technical, or physical; define a plan to test, monitor, and train system users on recommended security safeguards; and document project deliverables for the organization's management. The course emphasizes hands-on exercises and student reflection on an experiential term project.
Course Prerequisite
Introductory information security course

Table 1. Course Description in the Syllabus

Course Objectives	
Guiding objectives	Measurable objectives
1. Examine security in context 2. Develop problem-solving skills 3. Develop communication skills 4. Apply student education to the betterment of society	1. Perform an information security risk assessment in a real-world setting 2. Write an informative, value-added risk assessment report to a non-technical audience 3. Identify security safeguards that improve the client organization's security practices 4. Design a security safeguard that improves the client organization's security 5. Design a means to evaluate the effectiveness of proposed security solutions 6. Create an informative security training artifact for system users 7. Write a final security report

Table 2. Course Objectives in the Syllabus

2.1 Call for Partners

CBOs for the course are selected during the previous academic quarter. A university center for community-based service-learning (hereafter referred to as the University Center) that is responsible for matching service-learning courses with local CBOs distributes an online *Call for Partners* questionnaire to a list of prospective partners. The questionnaire, provided in Appendix 3, was developed by the instructor. Its purpose is to gauge a basic, relative understanding of each applicant's *need* for help with improving their security. The instructor then selects approximately four to five CBOs from the list of completed questionnaires.

Once the CBOs are selected for a given service-learning course, the instructor and, when possible, a representative from the University Center physically meet the CBO participants at their site. During the on-site meeting, the instructor describes the course structure and objectives to CBO representatives. Equally important, the instructor uses this meeting to get to know more about where the course can be value-added for the CBO. Thus, the instructor asks CBO staff general questions about the types of sensitive data they work with, a high-level description of their IT infrastructure, and areas of security concern the CBO would like students to include in their security assessments.

From this on-site discussion, the scope and focus of the upcoming student assessment is tentatively outlined between the instructor and CBO staff. Thus, the instructor uses the pre-course on-site meeting to form a plan with the CBO on how students will conduct a risk assessment at the CBO site. The planning discussion includes items such as the general approach students will follow in conducting the assessment, relevant organizational policies the CBO will provide to students, staff that students can interview, and any known scheduling constraints. Finally, at least one participant from each CBO agrees to attend the first night of class on campus

for "pitch night" (discussed in the next section) and the last night of class to hear student presentations.

Each CBO has a primary contact (hereafter referred to as the PC) who is the person the instructor and students interact most with throughout the project. The PC is typically the person who answered the Call for Partners questionnaire and is the liaison between the University Center and the CBO. As a result, the PC is typically someone working at the CBO in a non-technical, management or governance role. For example, CBO staff who work as office managers or who must report on regulatory compliance issues are often PCs. Consequently, effective communication with a non-technical audience becomes a critical success factor for students.

2.2 Pitch Night

The first night of class is referred to as pitch night, signaling the official launch of students' term-long project. Students enrolled in the course, the PC from each participating CBO, a staff person from the University Center (when possible), and the instructor attend pitch night in the assigned campus classroom. The session begins with a description of how service-learning courses differ from standard lecture-style courses, including student responsibilities. Next, the instructor briefly describes course objectives. Each PC then introduces his/her organization. The session concludes with students forming break-out sessions for informal group discussions where they meet their group members. PCs will often stay in class past their talk in order to informally meet and talk with students, as well as schedule students' initial on-site visit to the CBO.

The objectives of pitch night are three-fold: introducing each CBO to students, setting a level of expectation on student work, and providing the PC with greater insight into the course and its approach. After the course introduction, the PC from each participating organization gives an informal presentation, approximately 20 minutes in length, to the class (weekly class meetings are three hours). Each PC "pitches" the CBO's mission and security project needs to the students. That is, PCs describe the human or social services the CBO offers and the communities they serve. The PC further describes the organization to students, including the CBO's staff count, types and number of locations, extent of IT support, and a brief discussion on security topics of particular interest to the PC for the security risk assessment. Importantly, the PC concludes with a statement to students that the work they will do as part of the course is important to the CBO, i.e., is valued. Thus, the PC communicates to the class a sense of expectation, encouragement, and confidence in students as they begin the project.

In hearing the human and societal missions of these organizations during pitch night, students become aware that their work is for more than a course grade. That is, students get a sense that their work is needed to support this CBO's important mission (e.g., provide foster care, psychiatric counseling, back-to-work transition programs, etc.).

During pitch night, PCs also gain additional insight into what the course is about, its culture, the students, and the other types of projects that students throughout the course will work on during the academic term. Moreover, PCs hear the expectations being established for students along with the PCs role in enabling students to meet those expectations. In addition, each PC hears the security priorities of peer CBOs that may prompt the PC to consider additional security issues. Finally, an important aim of pitch night is to start student engagements with consensus among students, PCs, and the instructor on what the course is about, its objectives, and its approach.

2.3 Assigning Students to Organizations

Teams of three to four students are formed. Each team is assigned to a single CBO. Students may be pre-assigned to a participating CBO before or during pitch night. The goal is to begin student on-site visits for data collection by the second week of the academic quarter. Thus, teams must be formed quickly. The benefit of assigning students before pitch night is students can take advantage of the PCs class visit to begin discussing logistics, schedules, etc., in preparation for the students' initial on-site visit. Assigning students to teams before pitch night is particularly helpful when there are time constraints. For example, a 10-week academic quarter necessitates hitting the ground running so that student teams can quickly begin data collection for their risk assessments.

Instructor-defined student-CBO assignments are made based on the results of a short questionnaire emailed to students a week before the course start date after the instructor's initial meeting with each CBO. A brief list is compiled on security topics or skills (e.g., networks, mobile device security, regulatory compliance, policy, etc.) related to CBOs' interests for the course. A questionnaire is sent to students asking them to rank their interest and skill levels in each topic/skill. Students are also asked to list previous security and IS courses taken. Based on this information, the instructor matches students to CBO projects. Thus, the questionnaire is used to gauge each student's skill and interest, which is then matched to the security area planned for each CBO's risk assessment. However, students tend to generally be open to any assignment, enthusiastic to work on a real-world project.

3. STUDENT ACTIVITIES

The course primarily consists of two major activities. First, students work in teams on a term project to identify security risks at an assigned organization and to make security recommendations for reducing those risks. Second, each student writes reflection papers on their service experiences and insights gained during the course. Each of these major areas of activities is described in this section.

3.1 The Security Term Project

Students are tasked with conducting a security risk assessment, writing a formal report following industry standards, presenting their results to management, defining security safeguards, and providing training materials for managing a sample of security vulnerabilities.

3.1.1 Risk assessment scope: The focus of students' risk assessment is based, to the extent possible, on the particular security needs of their assigned CBO. For example, during the initial meeting with the instructor prior to the start of the course, multiple CBOs expressed a security concern about staff use of personal mobile devices to access organizational

information assets. Therefore, students worked with those CBOs on assessing risk and making recommendations for "bring your own device" (BYOD). Another CBO expressed concern about system access control for volunteers doing work for the CBO; therefore, students focused part of their assessment on access control policies and procedures. Yet another CBO expressed interest in students conducting a risk assessment on the security of public-facing computers (i.e., a computer lab accessible to clients). Thus, student risk assessments aim to add value to a CBO by focusing on security areas of particular concern, as explained by the PC.

Although the PC may express a desired area of focus for the security risk assessment, changes are sometimes needed after the start of the project, for example, when a PC realizes certain CBO staff will not be available to participate in the project. For example, one organization expressed interest in having students construct a compliance matrix containing a list of the CBO's required security controls per funding source. The students were to then use that compliance matrix to define the scope and priority areas of the risk assessment. However, after the first couple weeks of the course, it became clear that the manager working on compliance would not be available to meet with students or provide them input. Therefore, students had to revise the original risk assessment project focus.

In summary, each CBO may have differing areas of security need/interest. While two CBOs may have similar security interests (e.g., BYOD) and thus both request the same topic area to include in their risk assessments, there may be other CBOs with different, or more pressing concerns. Each student team typically examines multiple areas of security. Thus, the class is working on a variety of topical areas of security across the CBOs.

3.1.2 Risk assessment activities: Students conduct a risk assessment at the CBO by interviewing participants on-site, conducting facility walkthroughs to observe security strengths and weaknesses, and reviewing policies. Students use a questionnaire provided by the instructor, as well as a semi-structured interview script developed by students, as an initial guide on what to assess and discuss with CBO staff. The questionnaire evolves with each class based on observations of common security issues with CBOs. Using an industry standard for conducting risk assessments (NIST SP 800-30, 2012) as a framework, students analyze data collected and then write a detailed (~25-30 pages) risk assessment report. During week seven of the academic quarter, students present their risk assessment report to CBO participants, typically in person. Based on CBO preference, risk priority, and resource constraints, students develop designs and test plans for three to five low-cost, effective security safeguards. The original risk assessment report is appended with designs and test plans. Final reports are typically 50 pages or more, including tables, figures, step-by-step instructions, and references. Students visit their CBO client to discuss sensitive findings and to step CBO staff through recommendations and training materials contained in the final security report. During the final exam period, CBO participants attend class where student teams present generalized security recommendations to all attendees. The PCs often communicate to the instructor that they gained useful insight on security management during their visit.

During the course project, students are the primary (typically the sole) contact for CBO participants. Meanwhile, the instructor provides guidance and reviews students' weekly work-in-progress. Ongoing vetting of student reports and recommendations is conducted during informal class discussions and feedback on draft documents. In addition, prior to students' meeting with the PC to present their team report, each team presents their work in front of the class as a "sound check" to receive peer and instructor feedback, to ask the class any outstanding questions, and to hear the findings and recommendations of other teams.

3.2 Student Reflection Assignments

In addition to hands-on projects with an organization, service-learning also emphasizes employing student reflections as a sense-making technique for students (Gibson et al., 2011; NCSL, 2007). During the regular, 10-week quarter term, students are assigned 3 reflection papers to write approximately 3 weeks apart. Each reflection paper assignment contains three or four short-answer questions that are intended to prompt students to reflect and gain insight on some personal, interpersonal, or professional aspect of the project as experienced or perceived by the student to date. A sample of reflection questions assigned to students is provided in Appendix 4.

4. TEACHING SUGGESTIONS

4.1 Identifying Organizational Partners

Having a representative from the University Center distribute the Call for Partners questionnaire is very helpful. These representatives have a working relationship with pre-screened, prospective organizations. Those relationships between the University Center and the CBOs facilitate the instructor's access to partners. Moreover, the instructor is able to describe the type of preferred organizations (e.g., in terms of size, industry, etc.), so that the University Center can help identify specific CBOs that fit the description.

In absence of a University Center focused on service-learning or community outreach, an instructor can feasibly use his or her network (e.g., church, community CBOs, acquaintances with small businesses, etc.) to identify two CBO partners that can accommodate two student teams. The PCs at these organizations would engage in the activities previously described. In subsequent course offerings, prospective CBOs can be identified by referrals from the initial CBO partners.

Intuitively, in seeking CBOs with a greater need for security help, we target CBOs providing health or human services that require them to maintain sensitive data. The reasoning is that health and behavioral data (e.g., HIV testing results and psychiatric records, respectively) bring higher risk to clients if breached than would be the case for other types of organizations merely collecting contact or credit card data.

Final participant selection is based on a CBO's commitment to at least two people participating in the course project, including at least one business (i.e., non-IT) user, and to meeting the course timelines. Based on previous partnerships with eight CBOs, only two had an IT staff person as the PC; in both cases, the IT staff person could not convince business management to participate in the security risk

assessment. That is, business staff with information on organizational policy, regulatory requirements, and other needed information were not available. Given that business management buy-in is essential for any security funding and policy implementation, it is vital that a businessperson participate in the project. Otherwise, the project is more likely to be fruitless. Therefore, as part of the selection criteria, it is recommended that at least one business person be required to commit to participating per CBO partner.

4.2 Getting CBOs to Partner on a Security Project

While it is typically difficult to access organizations for academic research projects on security (Kotulic and Clark, 2004), we have found CBOs not only willing, but grateful, to have students help them with understanding their security risks and how to manage them. Why would CBOs allow access to their organizations for a security project that would expose their security vulnerabilities to unknown students? One explanation is that, from the start of the partnership, PCs are assured that students will not need to access the CBO's sensitive data or their network in order to conduct the analysis. Instead, students conduct their assessment by interviewing staff, reviewing documents, and by direct observation during a facility tour. Thus, a CBO's risk in participating in the course is greatly reduced since students do not come in contact with client data.

However, some system observation within the CBO enables students to identify basic, critical operating system and network configuration vulnerabilities. For example, viewing a CBO's router settings would reveal whether the default password is being used (a common vulnerability) or whether outdated network encryption is enabled (another vulnerability). The CBO decides both scope and access.

Finally, inform CBOs and students of inherent risk in the service-learning project (Saulnier, 2005), such as student inexperience and exposure to organizational security vulnerabilities. Consider having the PC and students sign a waiver accepting such risks. Students should also sign a non-disclosure agreement.

4.3 Course Prerequisites

The only prerequisite course requirement is an entry-level security course. Ideally, students would take the service-learning course after having taken several security courses so that they have more knowledge to contribute to the project. However, the course is taught as an elective. Therefore, only one prerequisite is required, thus enabling more students to take the course so that it will not be canceled due to low enrollment. As the course becomes better known, ideally additional course prerequisites can be added so that the course is taken later in a student's curriculum.

4.4 Undergraduate and Graduate Crosslisting

Both undergraduate and graduate students enroll in the same course, and they are often mixed within a given team. The purpose in crosslisting the course is to increase student enrollment so that the elective course will not be canceled due to low enrollment. Based on student reflection papers, both undergraduate and graduate students appear to benefit from working together. Moreover, all students benefit from gaining leadership and hands-on experience since none have previously worked on real-world security projects.

4.5 Student Absence on Pitch Night

It is very challenging for students to catch up in the course when they miss the first night of class. Given that this course only meets once per week and the first night is pitch night, students who are not present the first night tend not to fully catch up. Ideally, a student would have to be present the first night in order to maintain course enrollment. Since this may not be feasible, perhaps an instructor can request no late additions be allowed to the course roster. If this is also not feasible, the instructor may want to have a plan on how to handle bringing those students up to speed who miss the first class. There may only be one or two students who are absent the first class, but those students are then at risk and need special handling so that they are socialized into the course and project with the assigned CBO. On-site visits begin the second week of class; hence the need for students to be present the first week.

4.6 Instructor Mentoring and Student Ownership

After pitch night, signaling the project launch, the instructor fades into the background, enabling students to drive the team's interaction with the PC and other organizational members. In doing so, students naturally, or are otherwise forced, to take ownership in moving the project along. Credible security risk explanations and feasible security recommendations are required in student teams' final reports and presentations. It is a tall order for students to accomplish. The instructor coaches, mentors, encourages, reviews, and corrects as needed, while also requiring the students to lead, write, revise and resubmit, justify their recommendations, discuss with CBO staff, and present in front of all PCs and classmates.

4.7 Student Peer Exchange

During each class session, student teams informally present to the class their current status, experiences, questions, and concerns. These peer exchanges are an important aspect of the course for a variety of reasons. First, students gain experience articulating their ideas to others. Their peers will ask for clarification as needed and will provide feedback. The students providing feedback are often pleasantly surprised to see how much they have grown such that they are in a position to advise other students on security or organizational matters. Second, it is helpful for students to receive feedback from peers. If a student or team hears strong consensus from peers on a particular issue, they are more likely to take corrective action. Finally, students get the benefit of learning from other teams' experiences and approaches.

4.8 Domain Knowledge Expectations and Realities

When enrolling in the course, students tend to anticipate focusing on technical security. They quickly learn that communication and organizational issues take the bulk of their effort. For some teams where the CBO staff is not available as initially agreed, or some other unforeseen organizational issue arises, students may become frustrated or unsure how to respond. They learn quickly that the real world is not laid out as nicely as a typical lecture-based or lab-based course. People

are messy. Organizations have cultures that impact one's ability to get certain work done. Meanwhile, the clock is ticking and deliverables are due, especially in a 10-week quarter system. The hard skills students envisioned evolve to them learning far more soft skills than they previously realized were as necessary as they are. Nonetheless, quickly learning soft skills (i.e., communication, collaboration, leadership) in order to achieve their project deliverables is ultimately rewarding for students. In parallel, students' security knowledge is also further developed.

4.9 Improved Information Security at CBO

A guiding service-learning objective is for students to contribute their education to the betterment of society. Students accomplish this by helping client CBOs improve security, indirectly by raising awareness of security risks found within the CBOs environment and directly when CBO management adopts students' security recommendations. Student interviews with multiple CBO staff, students' discussing their findings with the PC, and related internal CBO discussions raise organizational awareness of security risks. Moreover, security awareness has been found to be an important antecedent to effective organizational security performance (Spears and Barki, 2010).

The time constraint of a 10-week course curtails the number of security improvements that a CBO can adopt by the end of the course. Nonetheless, students make a positive impact. For example, simple yet important parameter settings for multiple CBOs' existing software were recommended in order to encrypt the hard disk of a critical computer or to manage email server security. At least two CBOs made important physical security improvements, including moving critical paper records from under the ceiling water sprinklers, moving from the public's open view the keys to file cabinets containing sensitive client information, and moving unsecure boxes of sensitive client records to a locked storage space. Students also developed policy documents requested by their CBO client, such as a BYOD policy, an incidence response plan with a graphical decision tree, and a security compliance requirements matrix across government funding sources. Students defined security-related questions for staff at three CBOs to ask their external IT vendors. That is, PCs knew that a discussion was needed on security with their external IT vendors but did not know what to ask; students helped with this. In other CBOs, students acted as the internal IT staff person's "wingman" by raising security awareness within the CBO while interviewing staff, and in advocating security practices be implemented. Two other CBOs created a new staff position that students believed were largely attributed to their recommendations and reasoning of why additional IT support was needed to manage security risks. As appropriate, students also made more complex security recommendations, such as implementing MDM (mobile device management) software, thus planting a seed for the CBO of possible solutions.

Finally, security vulnerabilities commonly observed across multiple CBOs informed a security risk assessment checklist constructed by a team of one PC, a graduate student, and the instructor. The checklist will be made freely available to small organizations for security self-assessment and improvement. Thus, the course has the potential to reach beyond participating CBOs to help other small organizations improve their security practices.

4.10 Student Team Management

The first time the course was taught, no formal team management approach was used aside from requiring each group to designate a leader. Students were also required to submit team peer evaluations at the end of the term. Only one of the four teams worked well together; the remaining three teams had conflict throughout the project. Although the course had a mixture of undergraduate and graduate students, that did not appear to be a factor in group dynamics, nor was work experience or age. The one team that excelled contained one undergraduate and two graduate students. One of the challenged teams had all graduate students, while the other two challenged teams were all undergraduate students. Two teams had one team member causing most of the anxiety within the team. These team members would either miss meetings or were uncompromising in their views and recommendations. A third team was challenged because multiple team members were missing meetings, not submitting work, and ignoring the group leader's pleas to do the work. Three of the four teams raised their frustrations repeatedly with the instructor.

To address team challenges during the first course offering, the instructor did an intervention. The online tool polleverywhere.com was used to conduct an anonymous, open questionnaire and discussion on teams. Students were asked to rate themselves and team members on contribution. Importantly, students were asked short answer questions on the one thing they would like to improve about their team, at least one thing they liked about their team, and one thing they could individually do to improve the team. As the anonymous kind words of what they liked poured on the overhead screen, the tension was broken, and the teams appeared to work better together, though some challenges remained.

The second time the course was offered, three techniques were added to the course as a means to improve team interaction. First, at the beginning of the course, students were asked to sign a service level agreement stating they essentially agreed to do the work and communicate with their teams. The purpose here is to further raise awareness that both the CBO and team are counting on each student to do his/her part. Second, portions of the Affinity Group Research Model (Saulnier, 2005) were adopted, whereby students rotate the roles of Task Master, Time Keeper, and Record Keeper. Roles rotated per deliverable, approximately every two to three weeks. By using this approach, each student must lead the team. It prompts shy students to rise to a leadership role, and it discourages students from sitting back and letting others do the heavy lifting. Third, students were required to maintain team time sheets whereby each team member logs his/her time spent on the project. All team members can see and contribute to the team's time sheet, thus encouraging honest input. Time sheets are submitted periodically throughout the school term.

4.11 Scholarly Research

A capacity building service-learning course can provide a means to collect data, test a design science artifact, or conduct other research activities. For example, the instructor of the present course was awarded a research fellowship for the

course. From that fellowship, a security questionnaire was developed for CBOs based on observations of common security issues uncovered the first time the course was taught. The questionnaire is tested and evolves each time the course is taught with an end goal of making it freely available to CBOs and small businesses. As a second example, a theoretical model on information security knowledge transfer was developed and examined with qualitative data (Spears and San Nicolas-Rocca, 2015). In yet another example, the previous research on risk modeling was integrated into one team's project (Spears and Parrish, 2013). Thus, a service-learning course can be used to identify new research ideas or examine existing models and artifacts.

4.12 Teaching in an Unstructured, Real-World Setting

As described in Hrivnak and Sherman (2010), teaching a service-learning course is no panacea given the unstructured nature of the approach coupled with faculty time pressures and commitments. However, despite its challenges, a capacity building service-learning course can be transformative for students. Observing that transformation at the end of the course is rewarding and comparatively impossible to achieve in a traditional class setting because the real-world cannot be duplicated in the classroom. Second, teaching a capacity building service-learning course in information security risk assessment enables the instructor to validate that security topics taught in the college's security curriculum are relevant and current. Moreover, the instructor is able to integrate security risk trends observed during the service-learning course into prerequisite security courses as learning material. Finally, through students' community engagement, instructors also participate in community engagement in a service-learning course. Similar to students, an instructor can also be inspired and further motivated by knowing the course is helping a CBO that provides valuable community services.

5. EVIDENCE OF LEARNING OUTCOMES

Successful course completion requires that students achieve the course objectives listed in Table 2 by performing the activities described in Section 3. However, the literature was consulted to further assess the cognitive effects of the service-learning experience for students.

Research has found that student participation in a service-learning course increases the student's academic learning, personal development, and interpersonal development (Calvert and Kurji, 2012; Lee, 2012; Yorio and Ye, 2012). In the remainder of this section, a theoretical model on learning outcomes is presented, followed by a description of a sample of students and participating CBOs from which these learning outcomes were examined. Finally, evidence of learning outcomes being achieved is presented.

5.1 Learning Outcomes

Learning outcomes were analyzed using the theoretical framework presented in Figure 1. Each outcome is defined in Table 3 as described in Lee (2012).

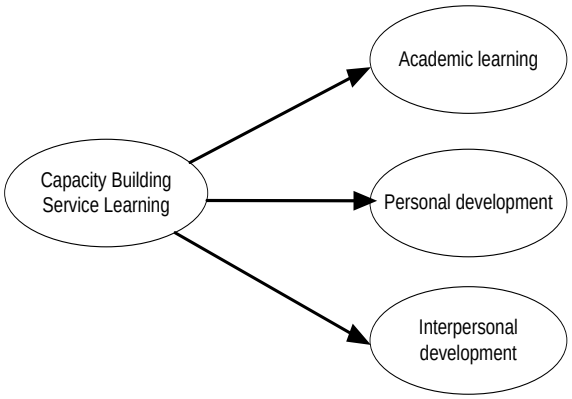

Figure 1. Student Learning Outcomes

Learning Outcomes	Definition
Academic Learning	
Domain-specific knowledge	Refers to student's broader understanding and application of the interdisciplinary theoretical knowledge of the information sciences
General knowledge	Refers to critical thinking and lifelong learning skills. Critical thinking skills are developed as students apply and adapt various problem-solving strategies. Lifelong learning occurs by self-teaching.
Personal Development	
Personal efficacy	Develops when students realize that their skills and knowledge can make a difference in the community
Self-knowledge	Occurs when students understand themselves better by gaining an understanding of their strengths and weaknesses
Career development	The service experience provides skills and experience students now find valuable in their careers.
Interpersonal Development	
Communication Collaboration Leadership	Includes effective communication (verbal and written), the ability to work effectively with others (e.g., teammates and CBO staff), and leadership skills

Table 3. Measures for Conceptual Coding (Lee, 2012)

5.2 Sample of Student and CBO Participants

Lee's (2012) theoretical model on service-learning outcomes (see Figure 1) was examined after the course had been taught twice. Twenty nine students collectively participated in these two course offerings, with approximately half graduate and half undergraduate. Students majored in information security

or in IS. All students had previously taken an introductory security course, while approximately half had taken multiple security courses.

Eight CBOs partnered with the course. Participating CBOs provided health and human services for their clients. In performing their respective missions, these agencies handled sensitive information, such as:

- Psychiatric records of parents with children living in a children's home
- Felony records of clients transitioning back into the work force
- Financial and mortgage records of clients at risk of home foreclosure
- Alcohol and substance abuse and other mental health records

While these agencies handled *very* sensitive information and intuitively realized the need for data protection, they generally lacked resources (i.e., staff, technical expertise, funding) to assess security risk within their environments. For example, the eight CBOs we worked with had an average of one IT staff person. CBOs generally work with small, off-site IT contractors. With total annual revenue per organization ranging from $1.5 to $15 million, these CBOs do not have the financial resources to hire security consultants to conduct a risk assessment and identify needed improvements. Consequently, CBOs partnered with the college course for students to assess information security risks and recommend affordable security safeguards.

5.3 Data Collected

Students were assigned three reflection papers throughout the academic quarter, resulting in one assignment every three weeks. Each reflection paper assigned asked students three or four questions that prompted them to reflect on various aspects and milestones associated with their service experience. For example, students were asked questions on their perception of their domain-specific knowledge, such as what they observed on identifying security risk within a CBO, what skills they felt they needed to improve, and their plan for doing so. Students were also asked to reflect on their communication style, successes, and areas of limitation with their "client" and with fellow team members, as well as how they might improve communication effectiveness. Students were asked to what extent they felt organizational decision-makers at the assigned CBO understood the risks students were trying to communicate, and whether student recommendations would ultimately be implemented. Finally, students were asked to imagine they were on a job interview and were asked by the interviewer to describe an example of a challenge they faced while working on a team project and what they did to overcome the challenge. Similarly, students were asked to describe, as if on a job interview, an example of when they demonstrated leadership to get team work done and how their experience with conducting a risk assessment for a small CBO could be applied to working on risk assessments for larger organizations. Student responses to these questions formed the data corpus used to examine learning outcomes presented in Figure 1. A sample of reflection questions is provided in Appendix 4.

5.4 Evidence of Learning Outcomes

Qualitative data from student reflection papers were analyzed using qualitative research methods (Cassell and Symon, 2011; Miles and Huberman, 1994; Urquhart, 2001). Each student's answer to each reflection question was segmented into conceptual codes (i.e., the learning outcomes in Table 2) when a student's reflection presented evidence of a concept. For example, if a student stated in a reflection paper that he or she gained insight on the security discipline as a result of performing particular activities, that portion of the student's response was coded as domain-specific knowledge. If a student described, for example, "problem-solving on the fly," that was coded as critical thinking. "At its core, qualitative research is about the analysis of language" (Conboy, Fitzgerald, and Mathiassen, 2012, p. 117). Approximately 250-300 pages of student reflections were coded using Table 2 as a theoretical lens. Salient, recurring descriptions per code across student reflections were summarized and are presented in Appendix 5 as evidence of learning outcomes. There was evidence of each learning outcome presented in Table 2.

6. DISCUSSION

Service-learning courses provide a unique opportunity for both students and the instructor to interact with the real-world as part of the academic curriculum. In turn, participating organizations increase IS-related capacity. Salient observations and challenges with this pedagogical approach are discussed next.

6.1 Some Observations on a Service-Learning Course

Teaching a service-learning course in information security is quite unique from teaching a lecture or lab-based security course. First, course preparation is different. Organizational participants are identified the academic term prior to the course being taught. Once organizations agree to participate in the course, the instructor works on defining interesting student projects that match stated organizational needs.

Second, considerable effort goes into launching the course. For example, at the start of the course, project teams form; by the second week, on-site data collection begins. At the start of the course, it is critical to set the expectation for student work ethic, provide guidance on team management, and coach students on communicating security topics to non-technical end users. From an instructor's perspective, the bulk of the course workload is in launching the course and then in coaching students throughout the process. Meanwhile, student projects form the basis of course material and discussions during class time. While the course must be planned and organized, the execution of student projects is organic.

A third distinction of a capacity building service-learning course is that the goal of student projects is to help their client organization improve some aspect of their operations. However, students are themselves novices in the field, and this is typically their first real-world engagement – often times in an organizational workplace in general, but certainly in a security work capacity. The student trainee is tasked with being an organization's trainer; thus, the student cannot be a passive learner.

Fourth, peer-learning across teams is an important aspect of service-learning to integrate into the course structure. That

is, the instructor integrates activities during class time that facilitate peer-learning. For example, each student team works with a different organization. As a means to share each team's experiences and learn from each other, peer exchanges are conducted each week whereby each team informally presents before the class their service experiences and plans for next steps. In addition, prior to presenting team findings and recommendations to their assigned organizations, each team conducts a "sound check" in class as a dry run of the team's findings and the logic behind their recommendations. Similarly to the weekly peer exchanges, "sound checks" provide a forum for class feedback. Thus, students not only learn from the work done in their individual teams, they also learn from the experiences, techniques, and solutions presented by student peers.

Finally, experiential learning in a service-learning course provides students with rich experiences to discuss on job interviews. From an instructor's perspective, it is rewarding to hear from students that the knowledge gained from the course was instrumental in helping them land their first security job. Similarly, it is rewarding to witness students evolve and mature during the course. They often begin the course unsure about how to assess and communicate risk in a real organization. Yet, by the end of the course, students are visibly more confident in their communication skills and their ability to find feasible solutions to problems in a real-world setting. Based on class discussions and reflection papers, students demonstrably have more insight on the business aspect of managing security within an organization. Students grow to understand the value of security recommendations must be understood by decision-makers who are typically not IT staff. Moreover, students gain insight on how security risk management and organizational change are affected by organizational culture. Finally, students can describe on job interviews specific project challenges they overcame, including effective problem-solving and leadership skills.

6.2 Some Challenges of a Service-Learning Course

While teaching a service-learning course is mostly rewarding and value-added, there are nonetheless various challenges confronting the instructor (Hrivnak and Sherman, 2010). One key challenge is that information security students are often surprised by the amount of effort (time) it takes to collect the data, analyze the results, and write a detailed and reasonably polished risk assessment report with specific security recommendations. Most students (~90%) rise to the occasion as best they can. However, a small number of students do not rise to the occasion and are frustrated as they fall behind or are pushed by team members and the instructor to perform better. Thus, the course tends to accentuate most students' strengths and a few students' weaknesses.

A second challenge is the instructor must closely vet (i.e., validate) the accuracy and reasonableness of each student team's detailed report, including explanations of the threat level, the reasonableness of their security recommendations, control designs, and control tests. Students are often prompted to explain "why" for the decisions they make (e.g., why are these particular threats or vulnerabilities most important; why choose this technology to mitigate that risk). Students' critical thinking skills are engaged during this process, though it is not an easy process for some students. Given the goal that an external organization may use the students' report as guidance, a reasonable degree of accuracy and quality is important.

Vetting is a challenge because the instructor bears some responsibility for what information gets communicated to the CBO. Occasionally, a student is resistant to the instructor's veto of an unreasonable recommendation. For example, one student was developing recommendations for a BYOD (bring your own device) policy. He wanted to suggest wiping (i.e., permanently erasing the entire contents of) a user's personal smartphone after (only!) four failed login attempts. He was very adamant that this was the best security policy and was quite resistant to both the instructor's and classmates' explanation of why such a policy was too harsh and would likely result in user uproar and organizational chaos if carried out. He could not imagine why a user's personal device may legitimately encounter more than four failed login attempts (e.g., the user forgot the passcode, the user's child was playing with the device, etc.). He also did not understand the practical implications for a user if an organization automatically erased all of the user's photos, contact lists, calendars, and other important data on one's personal smartphone. Eventually, after significant class discussion, and finally an overruling, the student agreed to change this recommendation in his team's report.

A third challenge for the instructor of a capacity building service-learning course is mentoring students on professional etiquette in real-time. That is, aside from the security aspect of students' experiential learning, students are also learning professional etiquette. For example, who to copy on certain types of emails and the inclusion or use of CBO and staff persons' names or organizational logos in a formal report. Thus, in addition to students being challenged to learn domain knowledge in real time from limited on-site visits, they are simultaneously learning business etiquette, thus adding an additional level of student anxiety, at least for some students. This challenge is also a key opportunity of a service-learning course.

While so important and rewarding for an instructor to witness, it is nonetheless a challenge to teach *communication in context* to students – coaching students on how to effectively communicate risk and security to non-technical or non-security staff. Students learn through trial and error that they must be able to describe risk and security in laymen's terms in order to be understood and to achieve the desired outcome of implementing security improvements. This very valuable lesson has long-term career effects and cannot be taught as well in a traditional lecture-based course.

Finally, another challenge is laying an effective structure for team cohesion and shared workload. Some teams thrive, while some teams may have one member who is grossly under-performing or is resistant to the team's direction. Team leaders get frustrated when their team members ignore their leadership (e.g., work delegation). The approach taken in this course is to follow aspects of the Affinity Research Group Model approach (Saulnier, 2005) whereby team members rotate roles for each key deliverable. Students are also required to record how much time each team member spent on the project. Finally, students complete an online peer review using the CATME peer evaluation questionnaire (http://info.catme.org/catme-tools/).

6.3 Future Directions

Now that a basic structure for the course has been established, additional enhancements or expansions can be made in future course offerings. First, although each CBO demonstrated at least one improved security practice based on student recommendations, students wondered which and to what extent other recommendations would be adopted. A survey will be developed and administered to the PC of each CBO at the end of the subsequent academic term. CBO adoption of students' recommended security practices will be assessed along with PC course satisfaction. In doing so, the course can evolve with continuous improvements.

Second, making the course inter-disciplinary could provide input from legal policy and more detailed technical students. Therefore, future course offerings will aim to cross-list the course with the law and engineering colleges so that students across security-related disciplines can engage in strategy, policy, technology implementation, etc.

Finally, service-learning courses provide an opportunity to conduct research, such as examining relevant theory or designing artifacts. For example, a security risk assessment tool for small organizations has been constructed based on course observations and is being piloted.

7. CONCLUSION

A service-learning course on security risk assessment provides students the ability to apply theoretical concepts learned in the classroom to the real-world. Previous research has found, and the present article finds further evidence, that students gain academic learning, personal development, and interpersonal development from their service experiences. Of particular value to security students is they learn how to communicate and collaborate with end users in order to identify security risks and make security recommendations that are both understandable and feasible. Simultaneous to learning *what* to communicate, students are learning *how* to communicate as they gain domain knowledge in a business environment. In turn, organizational awareness of specific security risks is raised within participating CBOs, and security improvements are made.

8. ACKNOWLEDGEMENTS

The author thanks Howard Rosing and Jeff Howard for their guidance and encouragement in developing a security risk assessment service-learning course and for the faculty research fellowship from the Irwin W. Steans Center at DePaul University that provided financial support for integrating research into the course. The author would also like to thank the anonymous reviewers for providing insightful feedback that contributed to improvements in the paper.

9. REFERENCES

Abrahams, A. S. & Singh, T. (2010). An Active, Reflective Learning Cycle for E-Commerce Classes: Learning about E-commerce by Doing and Teaching. *Journal of Information Systems Education*, 21(4), 383-390.

Bamber, P. & Hankin, L. (2011). Transformative Learning through Service-Learning: No Passport Required. *Education & Training*, 53(2/3), 190-206.

Calvert, V. & Kurji, R. (2012). Service-Learning in a Managerial Accounting Course: Developing the 'Soft' Skills. *American Journal of Economics and Business Administration*, 4(1), 5-12.

Cassell, C. & Symon, G. (2011). Assessing 'Good' Qualitative Research in the Work Psychology Field: A Narrative Analysis. *Journal of Occupational and Organizational Psychology*, 84, 633–650.

Conboy, K., Fitzgerald, G., & Mathiassen, L. (2012). Qualitative Methods Research in Information Systems: Motivations, Themes, and Contributions. *European Journal of Information Systems*, 21(2), 113.

Gibson, M., Hauf, P., Long, B. S., & Sampson, G. (2011). Reflective Practice in Service Learning: Possibilities and Limitations. *Education & Training*, 53(4), 284-296.

Hall, L. L. & Johnson, R. D. (2011). Preparing IS Students for Real-World Interaction with End Users Through Service Learning: A Proposed Organizational Model. *Journal of Organizational and End User Computing*, 23(3), 67-80.

Hrivnak, G. A. & Sherman, C. L. (2010). The Power of Nascency: Realizing the Potential of Service-Learning in an Unscripted Future. *International Journal of Organizational Analysis*, 18(2), 198-215.

Kotulic, A. & Clark, J. G. (2004). Why There aren't More Information Security Research Studies. *Information & Management*, 41, 597-607.

Lee, R. L. (2012). Experience is a Good Teacher: Integrating Service and Learning in Information Systems Education. *Journal of Information Systems Education*, 23(2), 165-176.

Lending, D. & Vician, C. (2012). Writing IS Teaching Tips: Guidelines for JISE Submission. *Journal of Information Systems Education*, 23(1), 11-18.

McLaughlin, E. (2010). The "Real-World" Experience: Students' Perspectives on Service-Learning Projects. *American Journal of Business Education*, 3(7), 109-118.

Miles, M. B. & Huberman, A. M. (1994). *Qualitative Data Analysis* (2nd ed.). Sage.

NCSL. (2007). Learning in Deed: The Power of Service-Learning for American Schools: 1-58: National Commission on Service-Learning.

NIST. (2012). Special Publication 800-30 Guide for Conducting Risk Assessments: National Institute of Standards and Technology: U.S. Department of Commerce.

Saulnier, B. M. (2005). Service Learning in Computer Information Systems: "Significant" Learning for Tomorrow's Computer Professionals *Information Systems Education Journal* 3(10), 1-12.

Sobeck, J. L. (2008). How Cost-Effective is Capacity Building in Grassroots Organizations? *Administration in Social Work*, 32(2), 49-68.

Spears, J. L. & Barki, H. (2010). User Participation in IS Security. *MIS Quarterly*, 34(3), 503-522.

Spears, J. L. & Parrish, J. L. (2013). Security Requirements Identification from Conceptual Models in Systems Analysis and Design: The Fun & Fitness, Inc. Case. *Journal of Information Systems Education*, 24(1), 17-29.

Spears, J. L. & San Nicolas-Rocca, T. (2015). Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations. *International Journal of Knowledge Management*, 11(4), 52-69.

Urquhart, C. (2001). An Encounter with Grounded Theory: Tackling the Practical and Philosophical Issues. In E. M. Trauth (Ed.), *Qualitative Research in IS: Issues and Trends*, 104-140. Hershey, PA: IDEA Group Publishing.

Wei, K., Siow, J., & Burley, D. L. (2007). Implementing Service-learning to the Information Systems and Technology Management Program: A Study of an Undergraduate Capstone Course. *Journal of Information Systems Education*, 18(1), 125-136.

Yorio, P. L. & Ye, F. (2012). A Meta-Analysis on the Effects of Service-Learning on the Social, Personal, and Cognitive Outcomes of Learning. *Academy of Management Learning & Education*, 11(1), 9-27.

AUTHOR BIOGRAPHY

Janine L. Spears is an Associate Professor in Cleveland State University's Monte Ahuja College of Business. Her research and teaching focus on information security risk management and online privacy. Her research has been published in *MIS Quarterly*, *Information & Management*, *Journal of Information Systems Education*, *International Journal of Knowledge Management*, and in IEEE and AIS conference proceedings. She holds a Ph.D. from Pennsylvania State University, an M.B.A. from Case Western Reserve University, and a B.S. in Computer Information Systems from California State University – Los Angeles.

APPENDIX 1. Syllabus Components

The course syllabus and objectives were provided in Section 2 of this teaching tip. This Appendix provides the reading materials and course schedule, as listed in the syllabus.

A3.1 Reading Materials

No textbook is required for purchase. Instead, freely available industry security standards will be used throughout the course. Some articles will also be provided. In addition to the provided materials, students will need to locate additional relevant resources, given specific project and learning needs. Industry security standards include:

- NIST SP 800-30, Guide for Conducting Risk Assessments, Rev. 1, 2012 (available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Rev. 4, 2013, updated as of 01/22/2015 (available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)
- NIST SP 800-66, An Introductory Resource Guide to Implementing the HIPAA Security Rule, Rev.1, 2008 (available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf)

All NIST SP 800-series standards can be found at http://csrc.nist.gov/publications/PubsSPs.html.

- CIS Critical Security Controls (commonly referred to as the SANS Top 20 Security Controls), version 6.1, 2016 (available at https://learn.cisecurity.org/20-controls-download)
- HIPAA Security Rule Guidance, (available at https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html)
- PCI DSS version 3.2, 2016 (available at https://www.pcisecuritystandards.org/document_library)
- Cloud Security Alliance suite of tools in their GRC Stack (available at https://cloudsecurityalliance.org/download/grc-stack/)

A3.2 Tentative Course Schedule

Week	Lecture
1	Pitch Night
2	Information Gathering
3	Risk Identification
4	Security and Privacy Safeguard Selection
5	Risk Assessment Report
6	Designing Security Safeguards
7	Assessing Design Effectiveness of Security Safeguards
8	Implementing Security Safeguards
9	Testing Security Safeguards
10	Security Awareness and Training
	Group Presentations on Project Results

APPENDIX 2. Major Course Assignments

The first six assignments listed below are performed per team, while the last is performed per student.

1. Construct a risk assessment report
2. Create a risk-control matrix
3. Design a sample of security controls (safeguards)
4. Define test plans for a sample of controls
5. Create security training material
6. Compile a final information security report
7. Reflection papers

In addition, student teams develop semi-structured interview scripts for conducting on-site risk assessments. Instructions for the risk assessment report and risk-control matrix are provided in this Appendix.

Team deliverables to client include:

1. Risk assessment report, written within the framework of NIST SP 800-30
2. Training artifacts
3. Group presentation slides

Team deliverables to instructor include:

1. Same deliverables as to client, plus:
2. Initial drafts of interview script(s); security risk table (following NIST SP 800-30); visual aid (e.g., diagram) for security risk identification; risk-control matrix; and security test plans
3. Table containing which students performed (or took the lead on) which portions of the report and other deliverables.
4. Team time sheets
5. Student peer evaluations for team members

Learning Objectives:

1. Research the area of risk you and your team are focused on
2. Identify and estimate overall risk within your team's risk assessment scope
3. Identify existing controls for each risk identified
4. Identify control recommendations for one or a set of risks with an estimated moderate, high, or very high risk level
5. Develop the core body of your risk assessment report

Instructions:

A4.1 Risk-Control Matrix Group Assignment

I. Identify risks to include in your Risk Assessment Report

1. Consult **NIST SP 800-30, Appendices F, G, H, and I for guidance and sample table formats** for the following items

    - Assume the tables created for threats and vulnerabilities will be included as an Appendix in your risk assessment report

2. For a specific asset (e.g., computing device(s), specific network component(s), operating system, business process, policy):

    a. Identify threats that are relevant to your client's organization
    b. Identify relevant vulnerabilities
    c. Estimate the severity of each vulnerability
    d. Estimate the likelihood of occurrence for each threat
    e. Estimate the magnitude of impact for each threat
    f. Estimate the overall risk level, based on the likelihood that one, or an aggregated set of risks will occur and result in an adverse impact

II. Risk-Control Matrix Template

1. For each threat identified in #I above that has an estimated overall risk level of moderate, high, or very high, include them as risks within the following risk-control matrix

Category	**Risk (concise, informative description)**	**Overall Likelihood of Adverse Impact**	**Existing Control**	**Existing Control Type** (administrative, operational, technical, or physical)[e]	**On a scale of 1-5, does the existing control appear to be effective** (1=not at all effective; 5=very effective)

A4.2 Risk Assessment Report Group Assignment

Learning Objectives:

1. Compile the components of your risk assessment into a professional, reader-friendly report for your client
2. Clearly explain the work you have done
3. Clearly explain why something is a threat or vulnerability, and why it matters
4. Clearly justify your recommendations

Instructions:

I. Gather each team member's notes and work-to-date on your client's risk assessment:

1. Interview scripts
2. Interview notes
3. Diagrams and visual aids
4. Threat and vulnerability tables
5. Risk-control matrices

II. Create an outline of the structure of your group's risk assessment report

1. Using NIST SP 800-30, Appendix K as a guide, decide the core sections of your report
2. Decide which tables and figures will be included in the body of the report, and which will be used as supporting documentation in an Appendix
3. Include an Executive Summary in your report that is a maximum of 3 pages

    a. As a group, decide what content should be included in the Executive Summary
    b. Within the Executive Summary, summarize the most important information in the report, including the key takeaways from the risk assessment
    c. Write the Executive Summary as if the Director at your client site will only ready the Executive Summary, and flip through the remaining sections to gain more detail where he/she is most interested

4. Decide which team member is completing which section(s) of the report

III. Write the paper sections

1. Include an executive summary at the beginning of your report that summarizes report, including key findings
2. Within the body of your written report, provide clear descriptions -- and examples where helpful -- of the risks included in your report, and why the ones you have rated high (and very high) are important
3. Within the body of your written report, provide a clear justification of why you recommend each key safeguard (i.e., those that will counter the risks you have identified as most important)
4. Within your report, briefly explain each table and Figure included within the body of the report
5. While your report is structured and professional, write and organize the report such that you are telling a story (it has a beginning, a middle, and conclusion that flows in a logical order that is informative to the reader)

6. Write in a voice that your target audience will understand

IV. Use Appendices in your report

1. The purpose of an Appendix is to provide supporting/additional detail

    a. This helps you have a more streamlined body of the report so that the report is easier for the reader to digest

2. Include your interview scripts as a separate Appendix

    a. Revise your "draft interview scripts" previously submitted [on Blackboard] so that the interview script(s) contained in the Appendix reflect the questions actually answered by your client
    b. Including your interview scripts helps toward repeatability of this risk assessment

3. Consider which figures (visual aids) would be best to include as an Appendix instead of within the body of paper
4. Reference each Appendix within the body of the text so that the reader knows to see the Appendix for specific types of more detailed or supporting information

APPENDIX 3. Call for Partners Questionnaire

The online survey tool Qualtrics is used to distribute the following questionnaire online to prospective community-based organizations (CBOs). The first page of the questionnaire describes the course to the respondent. If the person wishes to continue with the questionnaire and apply for the course, he or she answers questions on the second page of the survey.

[The College] is offering a course aimed at helping partnering non-profit organizations assess and improve information security within their organizations. Working with [the University Center], the course targets non-profit organizations providing health and human services. These organizations tend to handle sensitive client information, yet typically do not have the expertise or other resources to identify ways to protect information.

Students will help organizations identify areas of weakness in current data protection measures, propose cost-effective measures to improve data protection, and provide training materials on how to implement their recommendations. Throughout the 10-week term-long project, students will use as guidance reputable industry standards that are widely adopted by government agencies and the private sector.

As a means of ensuring the project is value-added, partnering organizations may choose an area of particular concern for students to focus on during their information security risk assessment. Examples include, but are not limited to access control; asset management (an inventory of your IT assets to protect); Bring Your Own Device (BYOD) policies; data breach incidence response planning; desktop security; network security; physical security (of information); and security program development.

Note: Students can achieve these course objectives without directly accessing personal client information. If you are interested in becoming a prospective partner, please answer the following questions by [date].

We will notify you whether your project has been selected. For selected projects, we will request to meet site representatives. Meanwhile, should you have any questions, you are welcomed to contact the instructor teaching the course, [instructor's name and email address]

[Press the Next button if you would like to continue]

What is the name of your organization?

Does your organization store sensitive client information electronically? Yes/No

Is there a particular area of concern that you would like students to focus their assessment? (Check all that apply.)

- Access control
- Asset management (an inventory of your IT assets to protect)
- Bring Your Own Device (BYOD) policies
- Data breach incidence response planning
- Desktop security
- Network security
- Physical security (of information)
- Security program development
- Other - there is another area of concern for information security
- There is no particular area of concern

Briefly describe any particular areas of concern your organization has related to protecting data security that you would like this course to help address.

Are the computers in your organization connected to a computer network? Yes/No

Do you exchange client data with external organizations (e.g., government agencies; IT service providers, etc.)? Yes/No

Does your organization currently have a security policy? Yes/No

Within the past 2 years, has your organization undergone a risk assessment for data protection (as far as you know)? Yes/No

Approximately how many employees work at your facility? _____

How many, if any, information technology staff work for your organization? _____

Do you have any comments or questions?

Please provide your contact info, including name, role, work address, email, and phone number.

Thank you for your interest in this course.

APPENDIX 4. Sample of Student Reflection Questions

Students are asked an average of three reflection questions at various times during the academic term. Since the course was taught over a 10-week quarter, reflection questions were assigned three times during the quarter. The questions are intended to prompt students to reflect on some aspect of the service-learning experience at that point in time. Questions cover topics such as the student's perspective on teamwork, his/her leadership skills, interviewing end users on security risk, likelihood that recommendations will be adopted, etc. A sample of reflection questions is provided below.

1. To what extent do you think the decision-makers in your client's organization will understand the security risks and recommended solutions presented by your team? How can your team get the client to understand why the recommendations you deem most important are in fact important, necessary, and feasible? In other words, how can the client be convinced? Provide an example to illustrate your answer.

2. Imagine that you are on a job interview and are asked a common question such as, "Provide an example of a project you worked on where you faced a challenge. Describe the challenge and what you did to overcome the challenge. What was the outcome of your effort?" Use the risk assessment project you have worked on in this course to answer this interview question.

3. What have you learned about working in teams on a project with a client and tight deadlines? Describe the type of team member you have been so far on this project. In what ways have you helped your team members advance the project? How can you be an even better team member?

4. Imagine that you are on a job interview for a position as a security analyst for a large, well-known security consulting firm. The interviewer is the security manager you would be reporting to should you get the job. The interviewer noticed on your resume that you took a course that involved conducting a risk assessment for a nonprofit organization. The interviewer asks you to describe any insight you gained in that course on conducting a risk assessment in an organization. Furthermore, you are asked how knowledge that you gained from the course can help you to be effective at conducting risk assessments for this consulting firm's clients. (In other words, how can you apply knowledge gained to the work of a larger security consulting firm?) How would you answer these questions posed by the interviewer?

APPENDIX 5. Qualitative Coding of Student Learning Outcomes

Student reflection papers from 29 students across two course offerings were coded using as a theoretical framework concepts defined in Lee (2012) on service-learning outcomes. The following table contains summarized examples of learning outcomes that were cited in student reflection papers.

Learning Outcome	**Dimension**	**Student Reflections**
Academic Learning	Domain Specific	• Observed specific security vulnerabilities in practice • Learned to apply industry standards (NIST) to real-world environment • Learned framework that will be useful for any future risk assessments • Realized security must be designed as a sustainable process • Learned multiple ways to identify and manage security risk
Academic Learning	Critical thinking	• Problem-solving on the fly • Improved writing for a specific audience (e.g., non-technical end users)
	Lifelong learning	• Searched credible sources and strengthened knowledge • Found that breaking down tech terms to simplest explanation for end users actually strengthens the tech person's knowledge
Personal Development	Self-knowledge	• Became self-aware of own non-verbal communication • Observed self being too formulaic; relying on checklists; later improved
Personal Development	Personal efficacy	• Became motivated and was able to make a difference for CBO • Confident that he/she can now do bigger projects • Realized that shortcomings in one area are offset by strengths in another
Personal Development	Career	• Hired for first security job; described service experience during interview • Course helps security students build credibility for employment • First time applying curriculum knowledge outside of class
Interpersonal Development	User communication and collaboration	• Observed the importance of user-friendly language • Must gain user perspective and mgmt. perspective when presenting a case • Users are worker bees; gatekeepers; initially guarded • Must gain user's trust for any real information exchange • Kept grounded reality in forefront of mind when making recommendations • Recommendations must be feasible for approval • Student team acted as CBO's IT dept's "wingman" • Translating tech to non-tech was like learning a new language
Interpersonal Development	Team communication and collaboration	• Aimed to prevent anger, confusion, or mixed guidance on team • During team's tough times, reminded self that workplace conflict is normal • Learned it is important to mitigate team problems; do not ignore • Used as guiding principle, effective comm among team is critical to success
Interpersonal Development	Leadership	• Students rotated taking lead as Task Master, Scribe, Recorder • Developed strategies for handling non-responsive clients

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 2574-3872