Service Learning in Security

Susan J Lincke, *University of Wisconsin-Parkside*

Abstract *– Service learning enables students to provide real service to the community as part of their learning/educational experience. Service learning can take many forms in security, including maturity assessment, security planning, awareness training, product research, product evaluation, and facilities or procedural audit. These projects help students learn to communicate with non-technical staff, apply security training, obtain experience in a real world environment, develop professional documentation, and contribute to their neighborhood. This paper describes the benefits and challenges the author has experienced for each type, but also discusses tools that can help security instructors in implementing service learning in their security courses.*

Index terms – Service Learning, Security, Audit, Security planning, COBIT, CISA, CISM, Security Awareness training, Small business security.

I. Introduction

Service learning and security are an excellent combination, because together they generate student learning and practical experience, and service for the community. Small businesses make excellent community partners, because they offer smaller-scale problems. Small businesses are also more willing to work with students, since they often lack skill and money for security. This paper reviews different forms of service learning that University of Wisconsin-Parkside has tried relating to security.

The need for security in small business is very evident. Barlett and Fomen [1] report in their literature review that small and medium businesses have been found to lack security, often because they lack expertise and time. Less than 20% have a business continuity plan or disaster recovery plan. They lack internal IS expertise and security awareness. They therefore have problems performing effective risk management. They often need to outsource security competencies, which they cannot afford. They also are not aware of security regulation they must adhere to. Johnson and Koch [2] agree that small business security is very poor, in part due to lack of training and time. Baker and Wallace [3] developed a set of security questions based upon a number of standards and polled various businesses of different sizes and types. Businesses in general performed according to their size: large best, medium next best, and small worst. Our own research [4] also confirms the need for security help for small business.

Service learning can help both small businesses and students gain competence in security. With service learning, students are graded on authentic, real projects related to the program or course learning goals. Service learning is established in engineering projects and software engineering development [7-10]. In our security courses, community partners select projects from the following list of project types. They select one or more options, according to their needs. Students work in teams of 2-4 with the community organizations.

1. Security Maturity Assessment: An interview helps the organization determine their level of security maturity, and helps them to understand where they could improve.

2. Security Planning: Students work with an organization using the Small Business Security Workbook in planning for security policy, risk management, information security, network security, business continuity, etc.

3. Security Awareness Training: Students present to an audience to educate non-technical staff in security awareness.

4. Security Product Research: Students research and write a paper that evaluates multiple variants of a security tool. They recommend a product based on organizational needs.

5. Security Product Evaluation: Students evaluate one or more products that an organization is planning to adopt. Students prepare an audit plan and audit report.

6. IT Facilities Audit: A portion of the community partner's IT network is audited. This may include their wireless network, server, external border router,

ISBN 1-933510-96-X/$15.00

and/or social engineering. Students prepare an audit plan and audit report.

The first three projects are done as part of our Information Systems Security course, while the last three have been done as part of our Network Security course. These projects help to train undergraduate and graduate students to become security analysts or security architects. Each of these project types will be reviewed in more detail in Section II.

A. A Review of Service Learning

This section briefly describes the format and benefits of service learning as practiced in the information systems and engineering world. Service learning can take three forms:

- Service projects implemented as part of the university independent of course work: These often consist of short-term projects and may be associated with a separate organization on or off campus.
- Service required as an integral part of a course: These projects can be short or longer-term. The advantage is that teaching for the projects can occur during the semester. However less class time is spent on lecture and more on project, compared to other lecture-based courses.
- Service that is dedicated as part of a class: Courses such as capstone or project courses still earn credit and involve learning through group project work. These courses involve longer term projects, little lecture, and may be inter-disciplinary.

At our university, we have implemented service learning according to the second format [4-5]. However, the third format is also common for many universities, including Purdue University [8], Illinois Institute of Technology, and Point Loma Nazarene University [7].

Service learning has many benefits, of which the following references are simply examples. At Point Loma Nazarene University, Carter summarizes that in the technology areas, service learning has helped students gain valuable job experience and group and communication skills, and assisted students in clarifying career goals [7]. At Purdue University, service learning also has been useful in teaching ethics and standardized documentation techniques [8]. Mikelic and Boras found that not only do the students benefit, but service learning also provides skills for the instructor and trained help for the community partners, and establishes a better relationship between the university and community [9].

The author is not aware of many publications concerning service learning projects in security, except for [4-6], which are described later in this paper.

The main purpose of a service learning project is to advance the learning that students receive. Therefore, the projects must be related to the subjects discussed in the course or program, and not simply be service projects. Grading is done on what the students have learned related to the course objectives, and not on how much time or effort they put into the project.

II. Security Service Learning Projects

This section discusses each of the security project types, including the benefits and complications that we have discovered from each.

A. Security Maturity Assessment

COBIT (Control Objectives for Information and Related Technology) is an IS/IT maturity model developed by ISACA for Sarbanes-Oxley legislation [11]. Working with this maturity model enables students to learn what best practices are, to see where organizations rank, and to practice communication skills, often with non-technical management.

We have created a questionnaire with a selected subset of COBIT questions, which were simplified for easier understanding. This questionnaire is included as an Appendix of the Small Business Security Workbook. The community partner is directed to answer each question with the status of their implementation: Do not do; do, undocumented; and do, documented; etc. Also an intention is recorded: would like to improve; fine as is. From these answers a maturity score is derived using the answers.

Most organizations that we have worked with were poor or woefully poor, raising the question whether our model, based on COBIT, is too advanced. However, our studies with schools or school systems have shown that for each question, some school (system) did find the implementation relevant, although higher maturity levels may not be as important [4]. Schneider and Wagner have used other surveys and service learning to contribute to the Findlay, Ohio community, by discovering the level of security maturity of area businesses [6].

Benefits: This questionnaire was beneficial to community organizations. They could see where they ranked relative to other organizations that semester, learn what the best practices were, and consider where they would like to improve.

ISBN 1-933510-96-X/$15.00

This project requires only one to two hours with the community partner. It can convince the partner to work with you on more extensive projects.

Challenges: The smallest businesses are often poor at security, so they tend to rate low with the questionnaire, and may be overwhelmed both by the questionnaire and their results.

These COBIT-level questions can be difficult for a new security instructor, students, and a small business manager to fully understand. In some cases there is a tradeoff between the question being general or specific. For example, "is authentication implemented" versus "do all persons have unique login with complex passwords of at least 8 characters"? The second is easier to understand if you are not a security professional, but may not address all authentication issues.

B. Security Planning

Security planning with students is possible using the Small Business Security Workbook. This Workbook leads the students through the security design process. It includes sections on policy, risk, business continuity, information security, network security, physical security, metrics, incident response, and audit. By working with the Workbook and a small business, students see how the different aspects of security planning fit together, build their understanding of security concepts, and practice communication with each other and non-technical management.

The Workbook was developed from the ISACA study guides for the Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and NISTIR 7621 [12-14]. Our experience is that partners choose to work with risk, information security, network security, and business continuity during a semester.

To prepare students to work with a section of the Workbook, the instructor gives a lecture on each topic. Next, students work with the associated case study section during the second half of the class, which enables students to become familiar with the topic and Workbook before encountering a real community partner. Then, the students are prepared to work with the partner.

An easy way to ease into this more extensive project is to use the Health First Case Study with the Workbook, before attempting service learning. In this case, students submit weekly case study chapters as homework. A solution manual is available for the case study. When the teacher is ready, the teacher can adopt the service learning component.

When attempting the service learning aspect, I attend the first couple of meetings with the community partner, and try to talk with the partner at the end of the semester to make sure the partner has benefited from the partnership.

Benefits: The Small Business Security Workbook and Health First Case Study are freely available, since the project was funded by NSF. Security planning helps organizations to define security policies, standards, and programs. It is difficult to audit an organization without a security framework. Our experience is that people are impressed in general with the Security Workbook. Customers who have participated with this have reported high satisfaction with the students' work. Students also benefit, since the Workbook and associated lecture materials are derived from the CISA and CISM materials [12-13]. Thus, these materials help to train students for professional certifications.

Challenges: Many small organizations have no time or see no need for security planning. Therefore, finding partners can be challenging. It may be challenging to find time in the small business manager's schedule for the 4-6 meetings that are required for the project (which assumes 1-2 hours per functional area). A release form is required in order to release students, professor, and university from liability, since security cannot be completely defended against, even for the most professional work. (After all, criminals are also professionals!)

C. Security Awareness Training

Security training can occur at three levels: security awareness with a procedural focus for general personnel; security awareness with a management focus for management, and security ideology and implementation training for IT. We have developed the first two types of security awareness presentations. These PowerPoint presentations are about 40 minutes to 1 hour each, and are freely available by contacting the author. Students must memorize the concepts within the presentation, and practice their presentation.

Both presentation materials review common attacks and security definitions (viruses, phishing, social engineering), and security techniques recommended by *NISTIR 7621 Small Business Information Security: The Fundamentals* [14]. Questionnaires can be given before and after the training, to determine how much attendees have learned.

ISBN 1-933510-96-X/$15.00

Since the PowerPoint presentation and questionnaires are already available, students need only learn the material and give the presentations. Notes under the PowerPoint slides help to prepare students for presenting each slide.

Benefits: This is a popular option with community partners, including the university. End-users are often interested in learning security, not only for business use, but also for home use.

Challenges: To turn this presentation into organization-specific training (not security-generic), it is required that the organization have risk analysis, information security, and physical security policies, and that the trainers have access to this information. In addition, potentially business continuity and/or incident response policies could be added for extended training, if available.

D. Security Product Research

Students learn from the community partner about the security concerns that they have, or which security products they are considering implementing. Students then research the different products and write a report on what they find. Students practice continuous learning and research skills, as well as writing and organizing skills.

Benefits: Students perform research off the Web and write a paper and/or present on the topic.

Challenges: Often students cut and paste marketing information for various security tools. It is not a valid analysis, and often involves plagiarism. A Security Product Evaluation is much preferred!

E. Security Product Evaluation or Facility Audit

Audits involve students working with real equipment and security tools to execute an audit plan (formatted similar to a test plan). They must research more about the product(s) they are testing, evaluate audit results, and prepare/organize audit plans and audit reports.

There are different types of audits: audits of existing infrastructure [5], procedural audits, and evaluations of security products. An evaluation of a security product is not really an audit, but works similarly in that students create a test plan (or audit plan), do the evaluation, and then write an audit report. Procedural audits can involve one student surveying users to ask how they do their jobs, while another student actually tests the security actions of the employees, by phone, e-mail, and/or in person. Audits can include social engineering attacks, when written into the audit plan. For all types of audits, the students work according to the needs of the community partner.

Facility or equipment types of audit projects work well when the class trains students in the use of security tools and audit. Students test first in a classroom lab environment, and then implement testing in a real live environment. Auditing existing infrastructure is a challenge for students because they must set the test up in a foreign environment, and interpret results, which is often half of the total work. Evaluating a security product requires researching the respective tool(s) and being creative in writing the audit plan.

It is helpful if the instructor has a working relationship with the community partner, to mitigate communication problems. The audit plan must be signed by the community partner. This ensures that students have discussed testing with the partner, and the community partner is in accord with the audit plan. If the audit is to be done on site, the partner's signature gives permission for the students to actually perform the audit. Students must also understand that regardless of the signed release, they can only do what is defined in their audit plan. The signed release should contain a provision that the community partners always have a knowledgeable representative with the student, if the student works on the organization's computers.

Professional audit plans and reports must be provided to the community partner, and this can be achieved via the grading policy. This instructor gives feedback to students before the document is delivered to the customer. Students have a week to correct the document based on the feedback. These corrections help to improve student grades, in addition to achieving a professional level of documentation.

All three types of audits can be assigned the same semester and with the same audit plan/report outline, so students can choose which type to perform. For security product evaluations, student can give very interesting presentations to the class at the end of the semester – the other types of audits may be restricted by non-disclosure.

Benefits: Product evaluations can be performed in the university lab or student's personal lab, and does not threaten the community partner's infrastructure or security privacy.

Challenges: Larger companies are not interested in having students audit their infrastructure, but may be willing to have students review security products for them in the school's security lab. Smaller organizations with no security expertise, and often no IT staff, are more often

willing to allow students to audit their facilities. However, these organizations rarely have security policies or plans to test against.

F. Other Projects

Security projects can involve requirements/design, implementation, test/audit, and support. We have not performed projects relating to implementation and support. Implementation could include configuring security tools (firewalls, wireless LANs, servers). Support could include recovery or forensic work, including rebuilding a computer. Since the author's courses do not emphasize these skills, these types of projects are not described.

From our experience, new types of projects arise with every new community partner.

III. Logistics and Special Concerns

Since our computer science program is fairly small, these elective security courses are offered to both undergraduate and graduate students. Projects will likely succeed when more mature students are paired with less experienced students in teams of 2-4 people. Mature students generally include those with work experience, graduate students, or better-performing students. Alternatively, weaker student teams can be assigned easier projects. The author usually attends the first community partner meeting, and possibly additional meetings, depending on the team maturity. Therefore, it is infeasible to manage more than 5 projects in a semester, unless some projects are associated with the student's workplace and require less attention.

A release form is important, which releases students, faculty, and university, from responsibility if the organization's security is attacked. This release form should include a confidentiality clause specifying that when students go on interviews, it is most important that the students do not describe the security details of their project work. However, they may use their community partners as references. If the instructor includes findings as part of his or her research, then human subjects review is also a concern.

IV. Acknowledgements

The development of the Workbook and Health First Case Study was funded by the National Science Foundation (NSF) Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning. We would like to thank NSF for making this work possible. We thank also the students who participated in the courses, thereby helping to improve it! Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author, and do not necessarily reflect the views of the NSF.

V. Conclusion

Service learning benefits students by helping them to gain experience actually implementing security with community partners. Students learn to apply their security skills toward a specific environment – and interpret results. Students also learn communication skills by communicating with non-technical partners and in developing professional documentation. Service learning also helps community partners who cannot afford professional help or who are insufficiently aware of the need. Security service learning has helped the author/instructor to actively practice security, thereby offering experience, confidence, and research material.

We have developed a number of tools to assist security courses in implementing service learning projects. These include the Small Business Security Workbook, the Health First Case Study, a COBIT maturity model evaluation, lecture materials, and two security awareness training presentations. We would be willing to not only share these materials, but work with other universities to enhance these materials. Please contact lincke@uwp.edu for more information.

VI. References

[1] Barlette, Y., Fomin, V. V. (2008) 'Exploring the suitability of IS security management standards for SMEs', *Proc. 41st Hawaii International Conf. on System Sciences*, Jan. 2008, Waikoloa, Big Island, Hawaii.

[2] Baker, W. H. and Wallace, L. (2007) 'Is Information Security under Control? Investigating Quality in Information Security Management', *IEEE Security & Privacy*, Jan/Feb, 5 (1): 36-44.

[3] Johnson, D. W. and Koch, H., (2006), "Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive?" *Proc. 39th Hawaii International Conf. on System Sciences*, Jan. 2006, Waikoloa, Big Island, Hawaii.

[4] Lincke, S., Kumar, R. & Tiwari, V. (2010). Security of Information Systems in Schools: An Evaluation using Audit and COBIT Interviews. *Journal of Information Systems Security (JISSEC)*, Dec. 30, Vol. 6 (3).

[5] Lincke, S.J. (2007). Network Security Auditing as a Community-Based Learning Project. *Proc. 38th SIGCSE Tech. Symp. on Computer Science Education*, March 7-10, 2007, pp. 476-480.

[6] Schnieder, H. & Wagner, L. (2009). Information Assurance Awareness: Partnership between Students and Community. *Proc. 13th Colloquium for Information Systems Security Education,* Seattle WA, June 1-3, 2009.

[7] Carter, L. (2009). "The Business of Service Learning", *39th ASEE/IEEE Frontiers in Education Conf.*, Oct 18-21, pp. T3G-1-T3G-6.

[8] DeRego, F. R., Zoltowski, C., Jamieson, L. & Oakes, W. (2005). "Teaching Ethics and the Social Impact of Engineering within a Capstone Course", *35th ASEE/IEEE Frontiers in Education Conf.*, Oct. 19-22, pp. S3D-1-S3D-5.

[9] Mikelic, N. & Boras, D. (2006). "Service Learning: Can our students learn how to become successful student?" *28th International Conf. on Information Technology Interfaces* June 10, 2006, pp. 289-294.

[10] Alkadi, G., Beaubouef, T., & Schroeder, R. (2010). "The Sometimes Harsh Reality of Real World Computer Science Projects," *ACM Inroads*, Dec. 2010, vol. 1, no. 4, pp. 59-65.

[11] IT Governance Institute, (2007). *COBIT® 4.1*, Arlington Heights IL, DOI=http://www.itgovernance.co.uk/cobit.aspx.

[12] ISACA. (2009). *CISM Review Manual 2010*, Arlington Heights IL. DOI=http://www.itgovernance.co.uk/products/1402.

[13] ISACA. (2009). *CISA Review Manual 2010*, Arlington Heights IL. DOI=http://www.itgovernance.co.uk/products/1403.

[14] Kissel R., (2009). "NISTIR 7621 Small Business Information Security: The Fundamentals (Draft)", National Institute of Standards and Technology, U.S. Dept. of Commerce, May 2009.