CERIAS Tech Report 2004-43

CIVIC RESPONSIBILITY AND INFORMATION SECURITY: AN INFORMATION SECURITY MANAGEMENT, SERVICE LEARNING COURSE

by Melissa J. Dark

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Civic Responsibility and Information Security: An Information Security Management, Service Learning Course

Melissa J. Dark
Purdue University
401 N. Grant Street
West Lafayette, IN 47907
765-494-7661
mjdark@tech.purdue.edu

ABSTRACT
This paper describes a needed and innovative service learning Information Security Management class that was designed, developed, and offered at Purdue University in spring 2004. This paper overviews 1) the need for service learning, 2) the more specific need for service learning in information technology and educational technology programs, 3) the need for information security in K12 school corporations as these bodies of work pertain to this experimental course. For faculty interested in developing a similar course, the paper then 4) highlights the course description and objectives as a reference point, and 5) describes how this course evolved from past work with an emphasis on the type of capacity that was needed to make such a course possible.

Categories and Subject Descriptors
K.6 **[Management of Computing and Information Systems]:** Security and Protection – a*uthentication, insurance, invasive software (e.g., viruses, worms, Trojan horses), physical security*, u*nauthorized access (e.g., hacking, phreaking.*

General Terms
Information Security Education, Information Security Management, Information Security Risk Assessment.

INTRODUCTION
This course stems from three needs. The first is the development and integration of an Information Security service-learning course into IT/CS programs. The second need is adapting methods and models for information security risk assessment into curriculum for students so they graduate with needed knowledge and skills. The third need is service to the K12 schools by providing knowledge and skills needed to better secure their IT systems. Each need is discussed in greater detail below.

THE NEED FOR SERVICE LEARNING
Because there are many working definitions and examples of service learning in the literature and in practice, it was necessary to adopt a working definition and benchmark best practices to guide the development of the course. The definition that was adopted asserts that "service-learning is a method under which students learn and develop through active participation in thoughtfully organized service experiences that meet actual community needs, that are integrated into the students' academic curriculum or provide structured time for reflection, and that enhance what is taught in school by extending student learning beyond the classroom and into the community" [1]. With regard to the "learning" component of "service learning", a well-designed service learning course joins theory and practice, i.e., students experience the relevance of the subject to the real world. Students in service learning courses are empowered to make a difference with the skills they are learning in an environment where there is a need; furthermore, the learning experience and student learning outcomes are usually richer when there is a distinct and known need for the service. Student learning in service learning courses is enhanced because students are given more responsibility as well as a richer context as a classroom.

A primary outcome of service learning is to increase the civic responsibility and citizenship of students in the course; this occurs by exposing students to societal inadequacies where they can use the community service experience as a foundation for learning 1) about oneself, 2) the academic discipline, 3) real world skills and techniques, and 4) how the discipline, skills and techniques intersect with the social world around us. Research shows a strong correlation between student participation in a service learning course(s) and increased civic responsibility [3]. This course focuses on civic responsibility outcomes as relevant to the practice of system security design, development, and implementation. Ideally, the "service" piece of "service learning" will respond to a variety of social, environmental, and economic development needs [6]. A key goal for the service component of service learning is that it leads to long-term community changes

for the communities involved; in this course the community consists of the K12 school corporations involved.

It should be noted that in service learning pedagogy, there are a variety of experiential education programs that could fall under the service learning umbrella such as internships, externships, field experiences, volunteerism, etc. Each of these is slightly different from the other in the amount of service or learning that is intended and occurs. In the context of this course, service and learning were integrated and both were the goal. This service learning course was designed to 1) have academic relevance, 2) be curriculum and course bound, 3) be pedagogically driven, and 4) have students at the core. A key objective was to develop this service learning course according best practices for service learning to ensure that both the service enhances the learning and the learning enhances the service; in summary the course intends to benefit both the students who provide the service and the schools for whom the service is provided.

NEED FOR SERVICE LEARNING IN COMPUTER INFORMATION SYSTEMS TECHNOLOGY (CIST) AND EDUCATIONAL TECHNOLOGY

A service learning course is a critical necessity in computer information systems technology and computer science curricula. Students in our programs become: systems analysts, application developers, consultants, database administrators, database developers, network administrators, network designers, programmers/analysts, sales representative, technical writers, Web managers, educators and trainers, and systems integrators. Our graduates are expected to possess strong technical computing skills, highly developed communication ability, excellent understanding of business needs, high professional standards, attention to the needs of the business user, and time-management skills to meet deadlines. Our graduates typically work for companies such as: Arthur Andersen, AT&T Global Solutions, Cargill, Inc., Eli Lilly and Company, Ernst and Young, Exxon, IBM, Intel, Microsoft, Price Waterhouse, Proctor and Gamble, USA Group, and so on. However, our program of study has a distinct and unmet need in the area of Information Security Management, Policy, and Response, specifically in the practice of information security risk assessment and risk management; a domain regarded as core to the information assurance and security curriculum [2].

Technology has a profound effect on mankind; it has the potential to be utilized to the benefit of mankind as well as to the detriment. Students who major in computer information systems technology need to have a solid understanding of the impact of these technologies and their potential for great harm. It is widely acknowledged in the information security community that there is a distinct need for teaching the social effects of information technology to engineering and technology students who are responsible for the design and development of new technologies. Today new technologies are designed, developed, and implemented without much consideration of security requirements; security is usually treated as an add-on solution, if at all. Technologies are developed based on what is possible, with little to no consideration of the 1) implementation issues, 2) lack of composability and integration, and the 3) social effects of these technologies on industry sectors, organizations, and individuals. Information security risk assessment and risk management principles are essential for our graduates regardless of whether they become systems analysts, application developers, consultants, database administrators, database developers, network administrators, network designers, programmers/analysts, etc., because information security risk assessment and risk management should underlie decision making across all of these job functions. This service learning course allows students to extend the theory to practice thereby exposing students to the true state of security 1) among an industry sector (K12 education), 2) at the organizational level (i.e., a school corporation), and 3) at the individual level (i.e., individuals within the school corporation). We employed active discussion and ongoing reflection of the nature and magnitude of these problems throughout the class with the intent of heightening the sense of civic responsibility among the students as it relates to security design, development, and implementation.

Deleted:

The purpose of an Educational Technology Program in general is to teach pre-service and/or in-service teachers how to effectively integrate technology into the curriculum using pedagogically sound models and materials. The Educational Technology program at Purdue prepares those not only aiming to become teachers, but also students who intend to become technology coordinators in school corporations. Technology coordinators are the individuals who are responsible for the information systems of the K12 schools. There are approximately 680 technology coordinators in the state of Indiana. However, a limitation of the current curriculum is that there is very little in the curriculum that examines 1) what can and does occur beyond the use of technology in the classroom, such as information assurance and security, 2) information technology from the standpoint of network architecture, development, and integration, and 3) information technology from the organizational perspective. For example, at Purdue University the topic is only covered in one course, EDCI 564 Integration and Management of Computers, and even then it is only for a brief period of time (perhaps 60 minutes total) and via a class discussion. It would appear that we are not sending our teachers nor our potential technology coordinators into the field prepared to deal with high priority issues. With this course, we can send better prepared teachers and technology coordinators into the schools with an understanding of the concerns and issues as well as the necessary knowledge and skills to protect themselves and their schools or school corporations. Moreover, having had hands-on experience in risk assessment and the development of an information assurance and security plan for the client involved in the K-12 service learning environment, our students will be considered a valuable asset to any school corporation, thereby becoming more marketable.

Deleted:

Deleted:

Employers are looking for educational technology graduates to be leaders in all areas and issues related to technology, including issues that they are currently not aware of, i.e., information security. Information security is not addressed in the International Society for Technology in Education (ISTE) standards for educational technology specialists. These are the standards that are used by most states in the country to guide the development of degree specializations in educational technology. The current standards are focused on integrating technology into the curriculum and skills development; however as technology is integrated and the skills are developed, we begin to see security

emerge as a critical issue. As technology is integrated school corporations will see (or fail to see due to a "lack of knowing what they don't know") information security threats, vulnerabilities, and risks. This collaboration among technology and educational technology will also be used to recommend the inclusion of security in the ISTE standards thereby extending the work done within Indiana to the national education technology community.

NEED FOR IT SECURITY IN K12 SCHOOLS

Today, little hard data is available on information security incidents and threats within the K12 school sector. In a 2002 pilot study conducted by the Purdue University and five K12 school corporations in central Indiana, access to the entire system of all five school corporations was gained in an average of 30 minutes time. The pilot study, albeit small, was conducted in order to better understand the security posture of K12 school corporations in our geographic area. Once we had these data, we decided to try to find a way to work more closely with these school corporations to address the problem, which prompted the idea for the course and subsequently prompted school corporations to sign up to participate in the course.

Following are summary results from the penetration tests:

- 2 of the 5 schools tested were penetrated from the Internet.
- The remaining three had vulnerabilities that would have caused irreparable damage to systems if they were exploited and thus were not attempted.
- The testing team was able to easily obtain a complete list of all students and staff and some sensitive information from three of the five schools from the Internet, and from all schools once on the internal network.
- CIPA measures in place to prevent students from accessing inappropriate material could be easily circumvented in all of the schools using basic tools or techniques well within the grasp of the average student.
- Payroll and grade processing systems were relatively easily penetrated in four of five schools, although not actually penetrated due to their sensitive nature.
- The testing team's attacks and compromises were not detected by any schools IT staff without intentional disclosure where emergency changes were requested to protect the school's systems from immediate threats.

K12 schools, like any other organization, suffer from 1) threats to data, such as unauthorized use or disclosure of data, as well as destruction and/or alteration of data and 2) threats to systems, such as misappropriation of resources, denial of service, and destruction of systems or infrastructure. Like business and industry, K12 schools must be concerned with hackers, snoops, unaware and/or misinformed staff, and disgruntled staff. In fact, one Russian credit card ring case involved the storage of thousands of credit card numbers on a school corporation server in Michigan, unbeknownst to the school (personal interview, Richard Murray, Assistant United States Attorney). In addition to threats from typical outsider threats (hackers, snoops, vandals) and insider threats (employees), K12 schools must also be concerned with unaware, misinformed, and/or disgruntled students. Motives for attacking K12 IT systems vary widely and include:

- accessing data (e.g., credit cards, student records, staff records, personal data),
- modifying data (e.g., grades, attendance records),
- unauthorized resource utilization (e.g., Spam, WaReZ, i.e., pirated software, Pron, i.e., pornography, and Enslavement, i.e., zombie machines that execute other larger attacks), and
- vandalism (e.g., web defacement, destruction/modification of data).

Like business, K12 institutions must be concerned with a variety of attacks including viruses, worms, Trojan horses, reconnaissance scans, misuse of legitimate services, social engineering, and data interception and redirection. However, unlike business and industry, K12 schools have unique needs and constraints. First, schools have a unique security model. The standard security model is that of trusted and untrusted systems, where employees are considered trusted and everyone else is considered untrusted. In schools, employees are considered trusted, students are semi-trusted, and everyone else is untrusted. This difference presents a challenge to technology coordinators because they cannot adopt security architecture best practices from business and industry without modification. Second, technology coordinators in schools are busy, paid significantly less than their business/industry counterparts, and are at varying skill/experience levels. Ongoing funding challenges in public education leaves a shortage of IT staff in K12 schools and often results in the more skilled system administrators seeking employment in the private sector; in fact K12 schools often redeploy teachers with little to no technical education to manage their IT systems. Third, funding fluctuates with the economy and politics. In a strong economy, schools might have sufficient funds to provide needed professional development opportunities to their technical staff. However, in a down economy, funding to professional development is cut; unfortunately new threats and vulnerabilities to IT security do not recede simultaneously. Fourth, K12 schools are also subject to a higher level of public and community governance. Schools are expected to serve the role of "guardian" to our students and when they fail to fulfill this role, they are subject to intense public scrutiny. With regard to IT security, this becomes a "Catch 22" for our K12 schools; they can't get funding without admitting a problem, yet if they admit a problem, they are subject to public judgment for failing to sufficiently serve their role as a "guardian".

Deleted:

In summary, the problem is that we know the IT systems of K12 schools are vulnerable; these vulnerabilities have potential downstream implications for misuse of data, misuse of systems, personal safety, crimes against children, public embarrassment to schools and so on. These systems are not going to become less vulnerable without significant and deliberate efforts to secure them. It is highly unlikely that schools are going to be able to afford outsourcing IT security given budget constraints and the relatively high costs of security consultants. In addition, the IT workforce in schools are currently lacking in security knowledge and expertise, while at the same time, security threats, vulnerabilities, and countermeasures are changing daily. What is needed is a mechanism to provide ongoing educational opportunities to technology coordinators in schools that provides

Deleted:

them with needed and current knowledge and skills to better secure their systems. This service learning course provides this public service on an ongoing basis.

INFORMATION SECURITY RISK ASSESSMENT CLASS

Our students worked in teams to provide information security risk assessment consultation to school corporations. There were six teams with 3-5 students per team. Each team was assigned to a school corporation; larger teams were assigned to larger school corporation in an attempt to allocate resources proportionately.

The course used existing quantitative and qualitative risk assessment methodologies [4], [5], [7]. Students in the course were required to conduct a comprehensive information security risk assessment using the risk assessment model to assess information security practices as they relate to technology, policy, and people.

Each student group brought specific and necessary skills to the process. The educational technology students brought primary background knowledge related to the K12 environment in terms of organizational mission, policy making, culture, and knowledge and skills of teachers and administrators. The IT/CS students bring primary background knowledge in information systems technology (design, development, and integration) and information security policy. The interdisciplinary teams that were formed complemented each other to conduct the risk assessment in a comprehensive manner customized to the needs of K12 school corporations. In addition, the students learned from each other, i.e., educational technology students learned how to conduct risk assessments in their own current/future schools and technology students learned how to apply a generic risk assessment process to the unique needs to K12 schools where assets, threats, and vulnerabilities differ from those common to the private sector.

Course Description and Objectives

The course description and objectives are described below. They have been paraphrased for the purposes of this paper.

Course Description: Students spend the first 7 weeks of the class learning through more traditional methods, i.e., lecture and reading. However, for the next 7 weeks of the class, students are assigned to a team tasked with performing an information security risk assessment for a client, which will be a K12 school corporation in the west central area of Indiana.

A service learning course intends to provide an education experience:

- whereby students learn and develop through active participation in thoughtfully organized service experiences that meet actual community needs, that are integrated into the students' academic curriculum or provide structured time for reflection, and that enhance what is taught in school by extending student learning beyond the classroom and into the community.
- that increases the civic responsibility and citizenship of students in the course; this occurs by exposing students to societal inadequacies where they can use the community service experience as a foundation for learning 1) about oneself, 2) the academic discipline, 3) real world skills and techniques, and 4) how the discipline, skills and techniques intersect with the social world around us.
- that joins theory and practice, i.e., students experience the relevance of the subject to the real world. Students in service learning courses are empowered to make a difference with the skills they are learning in an environment where there is a need; furthermore, the learning experience and student learning outcomes are usually richer when there is a distinct and known need for the service.

Objectives:
After completing the course, students were able to:

- Conduct an information security risk assessment.
  - Perform asset identification and classification
  - Perform threat identification
  - Perform vulnerability identification
  - Perform control analysis
  - Perform likelihood determination
  - Conduct impact analysis
  - Conduct risk determination
  - Identify control recommendations
  - Document results
- Identify pertinent standards and regulations and their relevance to information security management.
- Describe legal and public relations implications of security and privacy issues.
- Present a disaster recovery plan for recovery of information assets after an incident.

Past Work and Capacity

For other educators interested in developing a similar course, it should be noted that this course is an extension of work that has already been started by the author, the School of Technology, the Center for Education and Research in Information Assurance and Security (CERIAS), the Wabash Valley Educational Cooperative (WVEC) and school corporations in central Indiana. Based on experience, the long-term partnership is an essential ingredient in finding school corporations willing to participate in a class where students will be conducting vulnerability assessments on relationships the school corporation's information system. While there would be several ways to build such a partnership, the following activities demonstrate how the partnership formed that laid the groundwork for this class.

For over a year, these partners worked together to 1) provide professional development workshops in Information Security to technology coordinators, 2) provide seminars and workshops for K12 school administrators, and 3) conduct pro bono vulnerability assessment to provide a list of system specific vulnerabilities to each school corporation and suggest remediation plans. The workshops conducted included:

- Information Security Risk Assessment
- Information Security Regulations for K12 Schools
- Creating and Auditing Information Security Policies

- Information Security Training and Awareness for K12 Schools
- Intrusion Detection
- Email Forensics

In addition to leveraging past work with the K12 schools, several existing service learning resources at Purdue University were leveraged to execute this course. These included working with other faculty members with more experience in service learning; working with the Service Engagement Advisory Board, and attending on campus workshops on service learning.

In addition to leveraging the resources of the University, we leveraged the resources and infrastructure of the Wabash Valley Education Center (WVEC) to work with K12 schools. The WVEC provides technology leadership to K12 school corporations in west central Indiana. WVEC is one of nine educational service centers (ESC) that serve approximately 92% of the school districts in Indiana. Wabash Valley opened in 1967 and was of the first centers in Indiana. WVEC serves 16 counties and 36 school corporations that surround Tippecanoe County. WVEC has over 70,000 students and nearly 7,000 teachers in 177 buildings with whom they communicate.

Future Work

The work described in this paper has really just begun. There are several next steps to be taken to advance the work started here. The first step will be to modify and improve the class before it is offered again. In addition to offering the class again on the Purdue University West Lafayette campus, we anticipate offering the class throughout the state of Indiana. Previously, the partnership with Wabash Valley Education Center was described.

The author is currently in the process of developing similar relationships with other educational service centers in the State of Indiana. At the same time, the author is partnering with faculty at other Purdue campuses including: Calumet, Westville, Indianapolis, Columbus, Kokomo, Richmond, and South Bend. Once these partnerships are in place, the course will be replicated throughout the State of Indiana, thereby serving more students and more schools. In addition to expanding the work throughout the State of Indiana, the author has developed partnerships with faculty in Maine, Tennessee, and Texas to export the class to these states. In addition to refining and disseminating the course, future work will also include research with regard to the influence of the course on students' civic responsibility.

In addition to expanding this work with the K12 sector, the author was invited to make a presentation about the class to the Indiana Department of Education. Through that presentation, information about the class was shared with the Indiana Cybersecurity Officer, who is responsible for cyber security coordination across Indiana governmental agencies. At this time, discussion is underway to have various state agencies as clients in the course in the spring, 2005.

REFERENCES

[1] Corporation for National and Community Service (1990). *National and Community Service Act of 1990.*

[2] Davis, J. & Dark, M. (2003). *Defining a curriculum framework in information assurance and security.* American Society of Engineering Education Annual Conference Proceedings, 2003.

[3] Gray, M., Ondaatje, E., & Zakara, L. (1999). *Combining service and learning in higher education.* Rand Education. ISBN: 0-8330-2757-3.

[4] NIST (2001). *Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology.* Available at: http://csrc.nist.gov/publications/nistpubs/index.html

[5] Peltier, T. (2001). *Information security risk analysis.* Auerbach: Boca Raton, FL.

[6] Service Engagement Committee (2002). *Report to the vice provost for engagement* (unpublished). Purdue University.

[7] Tipton, H. & Krause, M. (Eds.). (2000). *Information security management handbook, 4th edition.* Auerbach: Boca Raton, FL.