An Inquiry-based Learning Approach to Promote Cyber-ethics in Cybersecurity Education

Donna M. Schaeffer, PhD and Michelle Liu, PhD

Marymount University, Arlington VA
Donna.schaeffer@marymount.edu
michelle.liu@marymount.edu

Abstract

As cybersecurity becomes increasingly important in the public and private sectors, it is critical for educators to prepare future cybersecurity workforce in ethical decision making and behavior. Further, it is important for those preparing to work or working in the fields of health care, education, and finance, or providers of basic infrastructure such as the electrical grid, and consumer products / services to be aware of the legal and ethical implications of security breaches.

We seek to develop a cyber-ethics curriculum comprised of online learning modules to increase students' awareness of and sensitivity to various emerging cybersecurity breaches and controversies. The two major pillars of this project include inquiry-based learning and case method teaching (i.e., case studies). Through participating in scenarios, peer discussions, and reflective activities, students will discover the impacts of ethical decision-making and behavior in their lives, as well as the impacts their actions have on others. In addition to serving the students specializing in cybersecurity, part of the curriculum may be of interest to general education students or traditional STEM students as it adds an interdisciplinary and values-based dimension to the knowledge they learn in courses within their majors.

Introduction

A study by Burning Glass International Inc. (2013) declared cybersecurity to be one of the most highly sought-after fields in the country and demand for cybersecurity experts is growing at 12 times the overall job market. They report the demand for cybersecurity experts grew 73% during the five years from 2007 to 2012; the demand for all 'computer' jobs grew 20%, and the demand for all jobs grew just 6%. Thus, the demand for cybersecurity talents supersedes the overall IT job market (Rosenbush, 2013)

Certification is often needed to gain employment in the cybersecurity field. Popular certifications, such as Certified Information Systems Security Professionals (CISSP) include domains that cover ethics. The proposed cyber-ethics curriculum would help students prepare for certification. Working through the curriculum would reinforce ethical concepts that cyber-security professionals need to be good citizens in our global society and participate constructively in a community for the betterment of society.

As cybersecurity becomes increasingly important in the public and private sectors, it is critical that workers be prepared to think and act ethically and to be aware of the legal and ethical implications of security breaches. An organization's incident response plan should include answers to ethical implications. In this cyber-age, it is important that users have trust in systems. Laws and policies may protect users, but the cyber-age is global, thus varying norms and cultural mores exacerbate the issues. As workers become more specialized in fields such as health care, education, and finance as well as public utilities management, transportation, and infrastructure construction and maintenance, the ethical issues become more complex and difficult.

Every occupation as it aspires to become a profession assumes certain attributes as part of its professional standards and one of these invariably is a code of ethics. Cybersecurity is a new and evolving field. As it matures and stabilizes, it too will need to develop a Code of Ethics that is suited to its unique and dynamic role in modern society. The National Academies of Science report entitled "Professionalizing the Nation's Cybersecurity Workforce: Criteria for Decision-Making" included the need for an ethics code as one of its six conclusions (National Research Council, 2013). The conclusions are based on feedback from participants in three national workshops and many hours of studying and discussing the professionalization of cybersecurity by a cross section of stakeholders in the field. It recognizes the importance of critical thinking:

> "*Because cybersecurity is not solely a technical endeavor, a wide range of backgrounds and skills will be needed in an effective national cybersecurity workforce. For example: attackers target organizations and individuals as well as machines and networks, so cybersecurity is inherently concerned with human adversaries and behaviors of those in the organizations they target.*"

The report further counsels against developing a cybersecurity workforce that is educated and trained in technical knowledge "too narrowly" which risks overly concentrating on technical skills while ignoring vital non-technical skills and/or "…discouraging technically proficient people from developing nontechnical skills. The result would fall short of delivering the workforce the nation requires."

Project Background

The authors work in an independent Catholic university with a diverse student population of approximately 3,500 undergraduate and graduate students (68% female, and approximately 50% are ethnic minorities). Many students are working professionals, one-third of the students are first-generation college students, and transfer students from community colleges comprise almost one-half of the undergraduate population. Marymount is a student-centered learning community that has long placed a high priority on quality science, technology, and mathematics education, a commitment evidenced by the new state-of-the-art science building which substantially increases laboratory space and features state-of-the-art scientific and technology equipment.

In 1993, the university founded The Center for Ethical Concerns to support the University's commitment to providing a values-based education. Since its inception, the Center has sponsored a wide range of activities designed to increase awareness of ethical problems and to enable students and faculty to develop effective techniques to address these issues. The Center takes an interdisciplinary approach to ethics, and encourages discussion of ethical issues across the curriculum. In recent years, the Center has reached out to the wider community beyond the

campus through its speakers' program and its work with area high schools. A grant from the Virginia Foundation for the Humanities to the authors' university funded a project on the ethical use of the Internet for high school students (Refer more details from http://csic.marymount.edu/?page_id=7). This project was based on the premise that two factors are vitally important when training students to become computer security and information assurance (CSIA) professionals. The students must be well educated in the technical aspects of the field and, equally important, they must be aware of the social, legal, and ethical implications of deploying CSIA technologies. An awareness of the contextual (social, legal, and ethical) factors is necessary both to discourage harmful use of potentially dangerous knowledge and to encourage due care in the use of that knowledge even when intentions are honorable. This exploratory project created, implemented and evaluated innovative learning materials for CSIA exploratory project created, implemented and evaluated innovative learning materials for CSIA that integrated the technical aspects of CSIA with contextual elements and hands-on laboratory experiences. The materials were refined through ongoing formal evaluation in a classroom setting and findings were published on a dedicated website.

In fall 2012, a National Science Foundation grant funded our University's Cybercorps: Scholarship for Service (SFS) program providing four scholarships per year through 2017. In return for the scholarship, each recipient commits to a period of government service after graduation which is equal to the period of time during which scholarship support was received. In 2013, the university was designated a Center for Academic Excellence by The National Security Agency (NSA) and the Department of Homeland Security (DHS). During the same year, the Information Technology / Management Science Department of the University launched its Master of Science program in Cybersecurity.

Creating and Implementing an Inquiry-based Curriculum

Fit with Inquiry-based Learning at the University

The University adopted Inquiry-Based Learning (IBL) several years ago. In this pedagogy, learners are presented first with questions, problems, or scenarios rather than facts and content. Learners identify and research the issue to develop their knowledge or devise solutions. The role of the instructor is that of facilitator for such active learning.

Case studies are an appropriate methodology for IBL. Learning objectives for case studies include being able to obtain supporting evidence, explain the evidence, connect the knowledge gained from the evidence to general theories, and create arguments and justifications for explanations (Bell et al., 2010). While IBL is often used in the sciences, the authors believe that such pedagogy embodies the essence of active learning, which is appropriate for any discipline where we seek to develop critical thinking and investigative skills – important traits for working and living in the cyber-age. In addition, prior research has shown that active learning is more effective than solely lecturing for STEM ethics education (Loui, 2010; Pavlidis, 2013). However, there is no "one size fits all" solution or curriculum. One of the objectives of this study is to introduce a cased-based inquiry learning approach to cybersecurity curriculum and discuss its initial implementation in our program.

Fit with Framework of the National Initiative Cybersecurity Careers and Studies (NICCS)

The National Cybersecurity Workforce Framework (Refer more details from http://niccs.us-cert.gov/training/tc/framework) classifies the typical duties and skill requirements of cybersecurity workers. The Framework organizes cybersecurity into seven high-level Categories, i.e. *Securely Provision, Analyze, Operate and Maintain, Oversight and Development, Collect and Operate, Protect and Defend, and Investigate.* Each Category is comprised of several Specialty Areas. The proposed project will be designed to complement these Categories and Areas while recognizing the fluidity of the issues and challenges the cybersecurity field confronts daily and the various perspectives that must be considered when making ethical decisions in this field. The focus of the program will be to inform rather than codify the ethical decision making processes as they relate to the NICCS Categories and Areas.

Project Description

The purpose of the proposed project is to develop a cyberethics curriculum to increase students' awareness of and sensitivity to the importance of ethical decision-making and behavior in the technological world in which we live and to be consistent with the NICCS Framework cited above. However, it has been noticed that discussing ethics in the cybersecurity field without specific contexts and perspectives in mind may not capture the full dynamics of the problem, which will likely lead to an entrenched view and/or too narrow interpretation of the incident. As the National Research Council report (2013) pointed out, "*There are contexts, such as law enforcement and the military, where a careful distinction must be made between actions that may be duty in one context but prohibited, or even criminal, in another."* Therefore, we believe that it is important for our future cybersecurity workforce to obtain a more sophisticated understanding of various implications of the field's ethics framework and theories in order to respond to related problems effectively.

Though initially designed for cyber security students, the course materials including the case studies, will be posted on a dedicated website where they will be available to general education students who see themselves as consumers and users of technology. The exposure to such materials may spur their interest in pursuing a Science, Technology, Engineering, and Math (STEM) major. The materials will be accessible through the website to STEM faculty and STEM majors, adding an interdisciplinary and values-based dimension to the technical knowledge included in the STEM majors' courses.

In addition to the online curriculum, a seminar course on Cyberethics will be developed, implemented and evaluated. In the seminar, students will participate in scenarios, engage in peer discussions, and perform reflective activities where they will discover the impacts of ethical decision-making and behavior in their lives, as well as the impacts their actions have on others. By teaching students how to think ethically, critically, and from a values-based background, students will add value to society as they move into professional positions upon graduating. Selected Marymount faculty members will be trained to facilitate some sessions of the course, and to promote and encourage the incorporation of ethics in other courses.

The curriculum could be made available to rising juniors and seniors in local high schools and to community college students who enroll in Marymount's existing summer institutes. Throughout

the course, student familiarity with ethical theories and their ability to critically reflect upon the ethical impacts of current cybersecurity issues will be formally assessed and the course materials and presentations will be adapted accordingly.

As the project proceeds, the authors will create a series of learning modules, each representing one of the NCCIS categories. Each module will be related to cybersecurity and ethics as seen from various perspectives, e.g., how ethics codes might (in the short run) affect the hiring of "black hats" (those who have violated computer security laws or rules in the past but may be a valuable source of talent in protecting computer security) for "white hat" jobs. When desiging the curriculum, the project authors will:

1. gather participants' (students, faculty, other community members) reactions to the case studies, either through video interviews or written questions.
2. identify which levels of skill acquisition (Dreyfus and Dreyfus, 1980) the participants exhibit in the topic of ethics.
3. create an online learning module that links the topics of cybersecurity and ethics for learners.

Expected Outcomes:

The online learning module in cybersecurity and ethics will be designed to:

- Provide an opportunity for learners to develop a deeper understanding of themselves, the people with whom they interact, and the challenges of living and working in the cyber-age.
- Help learners discover the impacts their decisions, made in various situations and unfamiliar circumstances, have on themselves and others

Project Details

The ultimate goal of the project is to research, develop, and recommend ways to improve the ethical decision making competencies of graduates who enter the cybersecurity field. The project will study the learning gains and confidence levels of students who complete the Cyberethics Learning Module over a two-year period and the impact it has on student's understanding of the Categories and Areas of NICCS. Initially, the module will be offered to students in the Networking and Security specialization in the Bachelor of Science in Information Technology program; however, the materials will be published online and accessible to faculty and students in other disciplines. Over time the module could be offered to general education students to provide foundational elements of cyber-ethics. Special attention will be paid to underrepresented groups in the cybersecurity and information technology fields including women, minorities, Veterans, and students with barriers to learning.

The following student populations will be targeted over a two-year time frame:

- Students in the Networking and Security major within the Bachelor of Science of Science in Information Technology program.
- Students in the Cybersecurity Master's degree program.

- Students from other disciplines/programs (such as criminal justices, forensic computing, psychology and legal studies, etc.) can take different modules and apply to their classes.

A web site that will provide the Cyber-ethics Learning Module content and provide links to existing resources will be developed. The site will include descriptions of assignments for those who may want to incorporate ethical decision making into their teaching, and case studies. A comments feature will be added to the Web site that will allow the community to ask questions, get tips, and give ideas for incorporating cyber-ethics via a variety of pedagogy. The comments feature will create a "community of interest" around the project to give feedback on the methodology and its ability to inspire students in ethical decision making and awareness of living in the cyber-age.

Evaluation of the project

The success of the proposed pedagogy will be assessed by several means. First, we will design and distribute pre- and post-surveys to assess student mastery of the major ethics theories and critical thinking capabilities. We will also evaluate student satisfaction with the IBL approach and the course design in general. Based on these results, a detailed assessment report will be generated.

Conclusion

The IBL curriculum in cyber-ethics can address the practical ethical dilemmas that cyber-security professionals and individuals face in their daily lives. Its implementation will provide rich and meaningful resources to students, and as a result of being exposed to the curriculum, we hope there are positive impacts. The IBL approach provides students and cyber-security professionals with time and space for personal reflection and sharing information. This is especially important in the diversity of the global age. Students are enabled to explore different situations that they will face, both as computer security professionals and as users of systems.

Ethical dilemmas will be unavoidable in the cyber-age. Students need a framework within which to make decisions. Cyber-security professionals also need a framework for ethical decision making.

References

Bell, T., Urhahne, D., Schanze, S., & Ploetzner, R. (2010). Collaborative inquiry learning: Models, tools, and challenges. *International Journal of Science Education, 3*(1).

Burning Glass International Inc. (2013). Report on the Growth of Cybersecurty Jobs Retrieved from http://www.burning-glass.com/media/4187/Burning%20Glass%20Report%20on%20Cybersecurity%20Jobs.pdf

Loui, M. C. (2010). EESE: Role-Play Scenarios for Teaching Responsible Conduct of Research. Final Report. NSF SES Award 0628814.

National Research Council. (2013). *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*. Washington, DC: The National Academies Press.

Pavlidis, I. (2013). EESE: Experiencing Ethics. Annual Report. NSF SES Award 1135357.

Rosenbush, S. (2013). Demand for CyberSecurity Jobs is Soaring. *Wall Street Journal, March 04, 2013*. Retrieved from http://blogs.wsj.com/cio/2013/03/04/demand-for-cyber-security-jobs-is-soaring/