A Framework for Information Security Ethics Education

by Melissa Dark, Rich Epstein, Linda Morales, Terry Countermine, Qing Yuan, Matt Rose and Nathan Harter
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

A Framework for Information Security Ethics Education

Melissa Dark, *Purdue University*[*], Richard Epstein, *West Chester University*, Linda Morales, *Texas A&M Univ-Commerce,*
Terry Countermine, *East Tennessee State University,* Qing Yuan, *East Tennessee State University,*
Muhammed Ali, *Tuskegee University,* Matt Rose, *Purdue University,* Nathan Harter, *Purdue University*

Abstract - This paper proposes a framework for teaching information security ethics at colleges and universities. The framework requires that students examine information security ethics from four dimensions: the ethical dimension, the security dimension, the solutions dimension and the personal moral development dimension. The intent is to use the framework to develop and/or select pedagogical resource materials for information security ethics education.

Index terms - Management, Security Legal Aspects, Curriculum Issues, Pedagogy, Ethical/societal Issues.

1. INTRODUCTION

The Internet has an enormous impact on society. The benefits are numerous and so is the potential for misuse and abuse. Hacking, spam, denial of service attacks, identity theft, digital rights infringement, and other abuses are now commonplace. Malice and criminal intent motivate some of these attacks, yet for others the motivation is not so clear.

An attacker may feel a need to prove a particular cleverness or technological skill. An attacker may view a particular vulnerability as a challenge that can't be resisted. An attacker may desire revenge against a corporation or private individual, or may view the downloading and sharing of copyrighted software, movies and music to be a personal "right". An attacker may be motivated by a dare from fellow hackers. Other motivations undoubtedly exist.

The ubiquity and openness of the Internet require self-governance; however, we see that the ethical maturity of Internet users is often put to the test. Instructors struggle to provide learning experiences that nurture ethical maturity. The Association for Computing Machinery (ACM) and the Institute of Electrical and Electronic Engineers (IEEE) have recognized the need to integrate ethics into computer science and information technology curricula [1,2,3] and have developed codes of ethics for computing and engineering professionals [3,4,5]. The National Science Foundation provides funding to improve ethics education in established and emerging science and engineering fields [6]. The problem has certainly been recognized in the information security community, where ethical judgments are needed on a regular basis. Information security programs are rapidly growing. Are these academic programs equipped to nurture the ethical development of information security students?

The authors of this paper have collectively participated in a series of workshops on ethics education in information security programs organized by the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. The ultimate goal of the authors is to have a positive influence on the ethical development of students in information security programs. The goal is a daunting one. The teaching of ethics is fundamentally different from the teaching of science and technology. Pedagogical approaches need to be purposefully selected to facilitate the creation of educational opportunities that allow students to examine their personal ethical beliefs. This needs to be done against the broader explicit context of right and wrong engendered by the existing technical, professional, legal and cultural environment.

2. THE FRAMEWORK

We have developed a framework for the development of pedagogical resource materials for teaching ethics to information security students. The discussion that follows assumes that pedagogical resources are organized by subject area of topic. Some examples of information security topics are: privacy, digital rights, and intellectual property. The framework examines information security ethics from four dimensions: the ethical dimension, the security dimension, the solutions dimension, and the personal moral development dimension. In addition, pedagogical approaches are explored to suggest effective ways to teach information security ethics to diverse audiences.

The ethical dimension considers the ethical implications of a given information security topic. Ethical implications are explored from various perspectives to have relevance for individuals, as well as groups of individuals and society at large. Examples of questions to guide the development of pedagogical resources include: What ethical dilemmas arise in discussions of this topic? How do evolving technologies impact the way that individuals, groups of individuals, and society perceive the ethical issues surrounding this topic?

The security dimension focuses on ways in which a topic manifests itself to information security professionals and others who have a vested interest in information security. The security dimension includes a discussion of weaknesses in the information infrastructure (e.g., holes and vulnerabilities) that are relevant to information security ethics. It includes discussions of specific exploits of these weaknesses and activities that allow individuals to behave in a manner that might be perceived as unethical. It

[*] *Center for Research and Education in Information Assurance and Security, Purdue University, West Lafayette, IN 47907. dark@purdue.edu*

ISBN 555555555/$15.00

includes discussions of significant historical exploits of relevant weaknesses. The goal of the security dimension is to communicate to the student the technical realities behind the security issues inherent in this particular topic.

The solutions dimension focuses on remedies that individuals, groups of individuals and society have created to address the ethical and security problems inherent in a topic. For example, suppose that the topic being discussed is software piracy. Then, the solutions dimension would include technical solutions (e.g., code obfuscation as a means of protecting proprietary software), legal solutions (e.g., the Digital Millennium Copyright Act), professional solutions (e.g., codes of ethics for software engineers and other computing professionals) and cultural solutions (e.g., how groups of individuals might decide to create a digital commons as a means of addressing the ethical issues related to intellectual property rights in cyberspace).

The personal moral development dimension includes introspection into one's personal beliefs in relation to this particular topic. How can students with different backgrounds in ethics and technology relate a particular topic (e.g., software piracy) to their own evolving moral values and development? How can their evolving moral values and development be informed by this exploration? And what basic values can students develop and nurture within themselves that will help them deal with the ethical issues and dilemmas that emerge in the realm of information security ethics?

The pedagogical approaches present methods and creative ideas for teaching diverse audiences. The framework's dimensions cover the basic content for lectures and classroom discussions relating to topics in information security ethics. The emphasis on the pedagogical approaches is to present creative and constructive learning experiences for students in various kinds of courses that address information security ethics issues. The authors place particular emphasis on projects and activities that will require students to construct, deconstruct, and reconstruct beliefs in various ways, in order to present learning experiences that foster the moral development of the students.

3. THE FOUR DIMENSIONS

3.1 The Ethical Dimension

The ethical dimension explores the ethical ramifications of a topic from a variety of perspectives. It entertains questions like: What are the implications of this topic for individuals, particular groups of individuals, and society at large? What ethical dilemmas arise in discussion of this topic? How do evolving technologies impact the way that individuals, groups, and society perceive the ethical issues surrounding this topic?

As students learn to analyze ethical problems and develop their personal ethics, they first must learn to examine topics from a variety of perspectives that sometimes conflict with each other. When asked to defend their views about what is right or wrong, many students are unable to successfully articulate the underlying reasons for their beliefs. They may justify their actions with superficial rationalizations such as "what is good for you may not be good for me" or "everybody else is doing it so it must be okay." Furthermore, existing and emerging security technologies add layers of complexity to issues, leading students to assume that, because they are dealing with an evolving technology, the underlying ethical norms have also changed. We want students to examine their current state of thinking and discover the inadequacy of intuitionist rationalization.

To foster a deeper, systematic understanding of ethical problems, the authors propose using three normative ethical theories as tools for examining the underlying ethical issues for any given information security topic. Normative ethical theories abound. For a detailed exploration of ethical theory, readers are referred to [7,8,9]. In this paper, we include a brief description of three broad ethical theories that are helpful in exposing ethical issues: virtue ethics, utilitarianism, and deontological ethics. Virtue ethics, an agent-centered approach, emphasizes the *motivation* for an action more than with the action itself. Virtue ethics emphasizes an individual's character; if an individual is virtuous, then his or her actions are thought to be ethical. Utilitarianism, a consequence-centered approach, emphasizes the ultimate outcome of an action whose worth is based upon the net total of "good" that it produces regardless of the motive. People are advised to maximize happiness and not just their own happiness. Finally, deontological ethics examine an agent's motives. They claim that, in order to act in an ethical manner, a person must take action for the sake of fulfilling an obligation. A person must do his or her duty. According to Kant [10], learning what is one's duty begins with the Categorical Imperative, to treat others as you would have them treat you. Students have heard versions of these theories before. They have been urged to cultivate virtue, as in "don't be stingy." They have been taught to anticipate how their actions will affect other people, to seek "the greatest good for the greatest number." And they have encountered some variation on the Golden Rule. They will have been acquainted with advice to develop virtue, maximize happiness, and perform their duties.

Applying these three ethical theories to a topic in information security allows students and instructors to investigate how the topic manifests itself to individuals and their belief systems, groups and their shared cultural values, and society at large with its social codes. Use of the theories also allows the underlying ethical dilemmas to be untangled from the confusion of detail that sometimes accompanies new technology. Ethical theories are beneficial for examining the impact that emerging technologies have on various populations because they help to separate technological features from their ethical implications, thereby preparing students to examine security issues.

3.2 The Security Dimension

The security dimension for a specific information security topic includes ways in which the topic manifests to information security professionals and others who have a vested interest in information security. The usefulness of information and communication technologies to society is challenged by the prevalence of vulnerabilities in these technologies. For example, vulnerabilities may allow unauthorized access and corruption of data without physical access, potentially from anywhere in the world. Recognized crimes are on the rise, as are other activities whose ethical impact is under debate. For example, in the past, intellectual property such as music was embedded in a physical medium which required some effort to reproduce, like a record or tape. Nowadays, the considerable amount of intellectual property available on the Internet is not bound to any physical medium. The benefits of easy access to information via Internet have to be balanced against violations of privacy and intellectual property enabled by the Internet.

Many questions arise. Take electronic mail as an example. Is it ethical to send unsolicited email? When is it ethical to send anonymous mail? What are the ethical guidelines and what is the etiquette for exchanging email? Is it ethical to distribute or use personal information that belongs to other people?

Servers on the Internet are vulnerable to denial of service (DOS) attacks. Some attackers justify DOS attacks as retaliation for opposing points of view or for business practices that are perceived as exploitative. Is Internet vigilantism justified under *any* ethical framework?

Personal information is spread across several databases, purportedly to improve service to ordinary citizens; but privacy is threatened because the information is potentially accessible over the Internet. Confidential information about several hundred thousand citizens has already been compromised [11]. Organizations generally try to minimize cost. Ethically speaking, what minimum level of privacy protection should an organization provide irrespective of cost?

Freedom of speech has received a boost from the Internet because any individual can make his or her opinions available globally on the Internet. However this freedom is accompanied by a considerable increase in intentional and unintentional disinformation. What steps can be taken to protect freedom of speech while discouraging disinformation?

It is easier to falsify one's identity by impersonating legitimate users, and more difficult to authenticate legitimate users of the Internet. Is it ethical to use someone else's password to gain access to Internet services?

These are a few examples of ethical issues that have been raised due to security vulnerabilities in IT systems and the open nature of the Internet. Pedagogical resources for the security dimension should clarify the responsibility of the security professional to recognize, prevent and avoid ethical misconduct in a world full of vulnerabilities.

3.3 The Solutions Dimension

The solutions dimension focuses on remedies that individuals, groups of individuals and society have created to address security problems and associated ethical dilemmas. We acknowledge that information security as a discipline is in its infancy. Ethical issues related to information security and motivations that give rise to unethical behavior tend to be ambiguous. There is a lack of consensus on solutions to many ethical dilemmas in information security. We feel that exposure to these ambiguities is beneficial to students' personal moral development. Students should be invited to explore and grapple with current imperfect solutions to ethical dilemmas and should be encouraged to examine the adequacy of solutions.

Components of the solutions dimension overlap with those in other dimensions discussed in this paper, however, the solutions dimension has a different focus. We now describe four perspectives to guide discussions in the solutions dimension: the technological, cultural, legal, and professional perspectives where students need to be guided in discussions to develop an understanding of the interaction and overlap among these perspectives.

As future information security professionals, it is important for students to understand the legal solutions to ethical issues in the field. Students need ample opportunities to discuss many questions including: What is legal? What is ethical? Where do legal solutions address ethical issues and where do they fall short? What is unique about legal issues and ethics in information security?

From a legal perspective, relevant laws and regulations must be studied. The deployment of network security solutions is required by regulations. Three examples are Sarbanes Oxley, Gramm Leach Bliley, and the Health Information Portability and Accountability Act (HIPAA). Information security students have to understand the legal and technological ramifications of compliance. They need to be cognizant of their professional responsibilities and liabilities. They need to be cognizant of and able to analyze how we as a society encode our ethical choices through law.

The professional solutions perspective explores professional expectations and codes of ethics for information security. Again, students must understand how professional codes of ethics attempt to provide solutions to ethical issues in the information security profession, where they succeed and where they fall short.

The cultural solutions perspective addresses how cultural factors can shape ethical behavior. This is explored in the context of societies, as well as formal and informal groups. Students are exposed to practices that reflect accepted norms in these social groupings and explore the effectiveness of such solutions.

The technological solutions perspective addresses how technology is used as a means of addressing information security ethical issues and enforcing solutions. Students will learn to analyze how technology enables ethical and unethical behavior. Students investigate how technology can be used to prevent misuse of intellectual property, and how technology at the same time can create new vulnerabilities. As students consider each perspective of the solution dimensions, they will also consider how the perspectives interact with each other. Questions include: What is the interplay of the various solutions? How do legal, professional, cultural and technological solutions address ethical issues in information security? Do they fall short in any way? If so, how and why?

3.4 The Moral Development Dimension

Unlike the previous dimensions where knowledge is *object*, this dimension is qualitatively different in that *subject* is explored in relation to *object*. In other words, we seek to have students explore, explain, defend, question, deconstruct, and redefine their personal beliefs of right and wrong against the backdrop of the first three dimensions. Therefore, the personal ethical framework that we are interested in is not a description of what is accepted as right and wrong by groups of people. This is known as descriptive ethics; while useful in some areas, descriptive ethics does not offer enough insight into who or where our students are ethically and how we, as mentors, can create opportunities for them to grow. Nor are we interested in normative ethics, which are ethical frameworks for deciding what should be right and wrong. We use normative ethics as a tool for students to explore, question, reframe, defend, tear down, and hopefully rebuild their personal ethical code, but we are not formally interested in whether or not utilitarian perspectives are better than deontological perspectives.

Instead, the moral development dimension describes the stages and transitions that humans experience as they develop morally, as they develop their own *personal* beliefs and behaviors about right and wrong. These stages and transitions have been widely researched by several developmental psychologists, including Piaget, Kohlberg, Perry and Kegan, who are all regarded as experts in this field. Developmental psychologists tend to agree that ethical development is epochal, meaning that the changes we experience in our personal beliefs about right and wrong occur in distinct phases or stages. Furthermore, the growth is cumulative with each stage building on the previous stage. The growth is characterized not by the need for the next stage, but rather by the need to abandon the current stage as the individual awakens to and comes to accept (which some do not) that one's current belief system is no longer sufficient. For the most part, the sequence of stages is invariant, one progresses from stage A to stage B and then from B to C, but will not pass directly from A to C. Ethical changes in an individual also take place in the context of one's relationship to the environment, not just as a result of the demands of relationship or in the context of a web of relationships, but rather in the context of changes in the nature of a person's relationship with his or her environment. These types of changes are described as constructivist approaches to development where the focus of inquiry is "who am I" (subject), "what is the world" (object), and "what is the relationship between subject and object"? The answers to these questions change over time.

This is at the heart of our interest in the moral development dimension. In our model, we want to create educational opportunities that allow students to examine their existing beliefs regarding ethical and technical issues and in relation to existing technical, professional, legal, and cultural solutions as depicted in figure 1. In an earlier section, we described how students examine these solutions with an external, objective point of view. Now, the student is positioned at the center of the intersecting circles. We wish to create educational opportunities that allow and encourage students to explore "who am I now" in relation to technical, professional, cultural, and legal solutions to these ethical and security issues, and asks questions such as "what is the relationship between who I am, who I want to be, and these issues and solutions"?

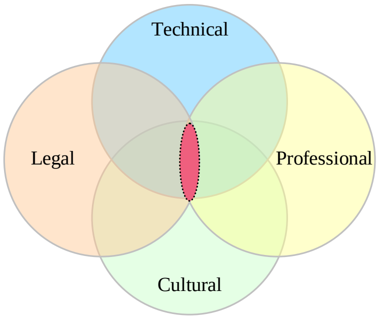

Figure 1:

In addition, we are interested in creating educational opportunities that encourage moral sensitivity [12], allow students to engage in moral reasoning [12,13], and continually question and evolve their moral beliefs, as they become more aware of the subtle complexities involved in this dimension. We envision students moving through a cyclic process where at times they view an issue or their beliefs about the issue from an opposing perspective, which creates the need to move out of that plane (where plane is analogous to developmental stage) in order to evolve a new and more sufficient personal outlook of right and wrong (figure 2).

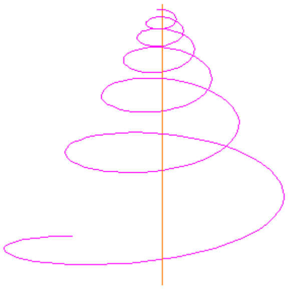

Figure 2. Spiral of Development

4. PEDAGOGICAL APPROACHES

Often teaching involves the dissemination of facts, concepts and principles; when this is the case, then the role of the teacher is to teach students a body of existing knowledge and that knowledge is primarily cognitive in nature. However, ethics, when viewed from the moral development perspective, is not primarily cognitive in nature. Rather the development of ethical and moral beliefs includes cognitive, affective and social components. The important point here is that teaching/learning theories grounded in cognitivism are insufficient in this domain. So, individuals who are challenged with teaching information security ethics will find themselves faced with needing to teach differently. In this section, we provide a list of suggested learning activities that could be particularly useful when teaching information security ethics. Each of these approaches is grounded in a learning theory called constructivism. We start with a brief discussion of constructivism.

The central tenet of constructivist philosophy is that "knowledge is not transmitted, it is constructed" [14]. Constructivists believe that learning is a search for meaning, where meaning is derived from experience, and experience is the result of continuous active agency by the individual. Furthermore, meaning requires understanding wholes and their constituent parts. The learning process focuses on primary concepts and not isolated facts. Learners should build organizational patterns (mental models) of association between primary concepts and affiliated parts through experience. Learning should start with the issues around which students are actively trying to construct meaning and then provide enough significant opportunities for students to gain experience in a reflective and iterative manner. When this happens, then the learning becomes meaningful in that it is derived from experience making it fundamentally self-referent; that is to say it is deeply rooted in personal identity and viewing life from the inside out in the context of social systems. This implies long-term retention.

ISBN 555555555/$15.00 © 2

Constructivist beliefs about learning have implications for teaching. In order to teach well, we must understand the mental models that students use to perceive the world and the assumptions they make to support those models. Meaning-making is dynamic and full of continuous tension; in fact tension is a necessary part of the process. When an individual must choose between beliefs, ideas, attitudes and behaviors that are contradictory—as is the case in ethical analysis, then the learner will embark on meaningful learning. As teachers we must provide opportunities for students to experience, interact, reflect and construct their internal principles and to regulate their behavior voluntarily and through their own conviction. This kind of autonomous moral character cannot be coerced.

Next we present a variety of learning activities that might be appropriate for teaching information security ethics using a constructivist approach.

1) Have the students write an ethical cyberwill. In contrast to a code of ethics, a cyberwill invites the student to express his or her vision of how cyberspace can be used to improve the human condition.
2) Have the students write a code of ethics. Using existing codes of ethics as a model (e.g., the ACM Code of Ethics), the students can develop a code of ethics that specifically relates to the information security ethics topics covered in the course.
3) Use improvisation and role playing. Role playing and theatrical improvisations are tools that enable students to explore the perspectives that might conflict in an ethical dilemma. What is the malicious hacker thinking? What is the impact upon the victim of identity theft?
4) Create video enactments of ethical situations. Taking the idea of using theatrical improvisations a step further, students can be encouraged to create a video of an ethical situation that relates to information security.
5) Explore the use of defensive tools. For a particular topic, students might be encouraged to explore the use of specific tools. For example, students who are studying privacy issues can explore the technical issues in using a tool like Pretty Good Privacy or anonymizers on the Web.
6) Set up a trial by jury situation. One way to get students to explore ethical issues is to set up a situation in which an individual is charged with some crime in cyberspace. Present the case to the class and have the students deliberate as a jury that must decide whether the defendant is guilty.
7) Develop a criminal code for particular security offenses. Another creative activity would be to have students write up their own criminal code for a particular security offense. For example, what should the guidelines be for guilt in cases of identity theft? What should decide the severity of the penalties applied in cases such as this?
8) Have students write and present a speech to be presented before a Congressional committee. Speech-writing is another means of getting students to explore ethical issues in information security. For example, students can be told to pretend that they are an information security expert that has been asked to testify before a Congressional committee on some issue in information security ethics.
9) Fill (or fix) a policy vacuum. Similar to the previous activity, students can pretend that they are to develop policy reflecting the government's stance on a particular information security issue. This is especially useful for getting students to think critically about policies that they disagree with (e.g. a timely example is the Digital Millenium Copyright Act).

5. A DETAILED EXAMPLE

We now illustrate the use of the framework by identifying each of the four dimensions in a case study. We will use Case 6.3 A Harmless Prank [15] as an example. Readers should know that the point of this example is to illustrate the four dimensions. We are not trying to suggest that the following is a prescription for using this case study.

In this case a student hacker has broken into a university computer system that contains confidential personnel records and financial data. He claims that he did this to prove that the system was not hacker-proof, and that it was "just a prank". We have augmented the case with the following twists. In investigating the case, we find out that Steven gained access to confidential personnel records and financial data by hacking into the Provost's computer. Also during the investigation, it was determined that the Provost failed to comply with the university computer security policy that requires logging off every night.

5.1 The Ethical Dimension

Steven appears to be a serious student with a good academic record, and is highly regarded by the department and its faculty. From a utilitarian point of view, we examine the consequences of hacking. In this particular example, there are no apparent direct consequences for university employees since the personnel records were not actually breached. However, in general, hacking does have consequences for the victims, since it can result in breaches of confidentiality, financial loss, and violations of data integrity. Utilitarianism opens an avenue to guide students in exploration of why hacking may be ethically wrong. The consequences for victims could be severe. Utilitarianism also provides an opportunity to discuss the rationalization used by Steven, in claiming that he provided a service to the university by exposing a vulnerability in the security of the computer system. As a consequence, the security flaw can be fixed, and future intrusions may be prevented. Does this argument have ethical merit, or is it simply a self-serving rationalization?

Deontological ethics requires us to examine whether hacking is intrinsically right or wrong, by asking whether or not the activity would be harmful if it were practiced by everyone. Students can be asked to discuss the reactions that Steven might have if his own computer had been broken into by a hacker. Students can also be asked the reactions they would have regarding the 'rightness' or 'wrongness' of the issue if Steve had hacked into a child pornography site or into the site of a spammer.

Finally, virtue ethics will require that students analyze whether Steven's motives have merit in the sense that he claims that this was simply a prank. If Steven were a white hat hacker and his motives were to purposefully identify vulnerabilities in systems, would the act be ethical? As a white hat hacker, should he have sought the consent of the university administration first?

5.2 The Security Dimension

This dimension explores hacking from the perspective of an information security professional. The goal is to create a discussion environment in which students are able to understand and internalize the ethical responsibilities of the network security administrator. Here are some questions to facilitate the discussion. If the university administration decides to takes a lenient approach to Steven's violation, does the network security administrator have an obligation to educate the administration about potential consequences of hacker attacks? To what degree is the network security administrator obliged to educate them about threats to confidentiality, integrity, availability, authenticity, non-repudiation, etc.? If efforts to raise awareness about security are poorly received by the university administration, how much of an ethical responsibility does the network security administrator have to persist (even if there may be a political price to pay?) The network security administrator is responsible for several systems and is very busy. Should he or she spend time trying to remove the vulnerability since Steven's exploit did not result in a breach of confidentiality? Should Steven's suggestions for improving the security of the system be accepted and implemented, or are they suspect? Perhaps Steven's recommendations are not trustworthy. What, if anything, should be done to see if the system has other vulnerabilities? Should a company be hired to do a penetration test of all of the school's computer systems? What are the pros and cons of asking students like Steven to discover other system vulnerabilities?

The discussion should then loop back to discuss the ethical nature of the response of the network security administrator. Students can be asked to identify a course of action that the network security administrator should take and justify the course of action using one of the ethical theories. In doing so, students are also asked to examine conflicts in their beliefs about right and wrong. Is their supporting argument for the network security administrator's course of action in conflict with their beliefs about the 'rightness' or 'wrongness' of Steven's actions?

5.3 The Solutions Dimension

We examine the remedies for hacking and ethical dilemmas associated with the remedies. Let's suppose that the university's budget for security tools is limited. Choices have to be made. Does the network security administrator have the obligation to perform a risk assessment and use the results to prioritize spending? Can he or she be held liable for future intrusions? What legal issues might arise in this case if the network security administrator chooses to do nothing or chooses to do something? If the network security administrator chooses to take action, must he/she do it in any certain way to demonstrate due diligence?

Did Steven break any laws? Is this a computer intrusion? If Steven had broken into confidential records, would he have broken any laws? Did Steven violate any university policies? If so, what are the policies and what are the repercussions? If not, should the university create a policy on hacking? Should Steven's university computer privileges be suspended? What purpose would this serve? Did the computer science department require Steven to sign a White Hat agreement? If so, should a university administrator discuss the meaning of the White Hat agreement with Steven? What purpose would this serve? Does the ACM Code of Ethics and Professional Conduct give any guidance about the ethics of hacking? If Steven had not broken a law, a policy, or a code of conduct, is his action ethical?

The Provost has broken a policy. Students should be encouraged to examine if her actions are ethical. Should the Provost be reprimanded for her actions? What should the repercussions be for her violation? How should the repercussions for the Provost and Steven be compared? Students should be challenged to distinguish between when policies and laws support social norms regarding right and wrong, and when the need for right and wrong extends beyond laws and policies.

5.4 The Moral Development Dimension

This scenario is intended to provide an environment for students to examine 1) their existing beliefs about whether or not hacking is an ethical activity, 2) their beliefs about a ethical course of action for a network security administrator to take, and 3) their beliefs about the ethics of the Provost who violated university policy.

Students will be encouraged to analyze the actions of the different actors and discuss their beliefs about rightness and wrongness. They will be asked to formulate a course of action and defend it based upon their beliefs about what is right and wrong. They should be provided opportunities to examine conflicts in their own ways of thinking. For example, a rich moment of discovery might be for students to explore if their justifications of right and wrong are internally consistent. Another rich moment of discovery could stem from the discussion if the instructor tells students to assume that Steven did not break any policies or laws. If this is the case, then are Steven's actions acceptable and should there be any repercussions? Why or why not? The hope is that students will engage in a dialog about the existence (or non-existence) of an ethical principle regardless of whether or not there is a policy or law.

To increase students' sensitivity to the moral issues in the case, it might be effective to have students explore their beliefs from a personal perspective. This could be accomplished by asking students to make an exhaustive inventory of the files on their own computers, and then discuss the problems they might encounter if they themselves were victims of benign hacking, malicious (destructive) hacking or data theft. It could be interesting to have this discussion with students when the case study is initially introduced (before delving into the three other dimensions), and then to revisit with a second discussion after the other three dimensions have been explored. If the personal case is placed first, students may enter the case empathizing with potential victims and ready to crucify Steven…no matter what. If the personal case is placed later, students might empathize with Steven as a peer and be more inclined to defend him….after all it was a harmless prank. Either could be instructive in getting students to explore the questions of "who am I" (subject), "what is the world" (object), and "what is the relationship between subject and object"?

6. CONCLUSION

This paper presents a detailed framework for teaching information security ethics. The authors believe the model has several advantages. This approach explores ethical issues in information security first from the perspective of normative ethics. This provides students with a foundation in ethical theory that helps students move beyond superficial rationalizations to explore the nature of right and wrong from a reasoned perspective. Our approach then explores the sufficiency of existing solutions from multiple perspectives. This is critical as we seek to have our students understand that ethics are complex social constructs, and as such, one dimensional, static solutions are simplistic and naïve. Our approach includes a moral development component, which challenges students to understand and advance their level of moral development with regard to information security ethics. Finally, this paper attempts to provide educators with ideas and resources to help them use this framework to teach information security ethics.

7. ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 0113725. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

8. REFERENCES

[1] Association for Computing Machinery and the Computer Society of the Institute of Electrical and Electronics Engineers. Computing Curricula 2001. New York: ACM Press, 2001.

[2] Association for Computing Machinery and the Computer Society of the Institute of Electrical and Electronics Engineers. Computing Curricula Information Technology Volume. New York: ACM Press, 2004.

[3] IEEE-CS/ACM Joint Task Force on Software Engineering Ethics and Professional Practices (SEEPP). Software engineering code of ethics and professional practice (Version 5.2). http://www.acm.org/serving/se/code.htm.

[4] Association for Computing Machinery. ACM code of ethics and professional conduct. New York: The Association for Computing Machinery, May 2001. http://www.acm.org/constitution/code.html.

[5] Institute for Electrical and Electronic Engineers. IEEE code of ethics. Piscataway, NJ: IEEE, May 2001. http://www.ieee.org/about/whatis/code.html.

[6] National Science Foundation. Ethics Education in Science and Engineering (EESE), Arlington, VA: National Science Foundation, 2005.

[7 Johnson, D. (2001). Computer Ethics (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

[8] Spinello, R. (2003). Cyber Ethics: Morality and Law in Cyberspace (2nd ed.). Sudbury, MA: Jones and Bartlett.

[9] Popkin, R.H., & Stroll, A. (1993). Philosophy Made Simple (2nd Rev edition). New York: Doubleday.

[10] Kant, I. (1964). Groundwork of the Metaphysic of Morals (H. J. Paton, Trans.). NY: Harper & Row.

[11] UNESCO Press, “UNESCO promotes 'knowledge societies' to maximize the impact of communication technology”, Oct 2003.

[12] Rest, J. (1984). The Major Components of Morality. In Morality, Moral Behavior, and Moral Development by W. Kurtines and J. Gewirtz. John Wiley & Sons.

[13] Pritchard, M. (1999). Kohlbergian Contributions to Educational Programs for the Moral Development of Professionals. Educational Psychology, 11 (4), pp. 395-409.

[14] Smith, P. & Ragan, T. (1999). Instructional Design. John Wiley & Sons, Inc.

[15] Spinello, R (2003). Case Studies in Information Technology Ethics (2nd ed.). Upper Saddle River, NJ: Pearson Education.

[14] Popkin, R.H., & Stroll, A. (1993). Philosophy Made Simple (2nd Rev edition). New York: Doubleday.