ETHICAL PERSPECTIVES IN INFORMATION SECURITY EDUCATION

Dr. James K. Harris, Georgia Southern University, jkharris@georgiasouthern.edu

ABSTRACT

This paper relates the similarities between the deviations in moral behavior illustrated in the famous 1971 Zimbardo prison study with the behavior of deindividualized technologically savvy students in an anonymous environment such as the Internet. Suggestions are made to improve moral sensitivity and judgment through minimizing deindividualization, promoting moral argumentation using ethical scenarios, and establishing well defined ethical boundaries.

Keywords: Ethics, Deindividualization, Moral Argumentation, Moral Sensitivity, Information Technology

INTRODUCTION

Philip Zimbardo, a psychology professor at Stanford University, performed a groundbreaking and controversial study on moral behavior in his 1971 prisoner/guard study [3, 10]. Zimbardo recruited middle class college students as prisoners and prison guards for a "mock" prison. The students were arrested, handcuffed, booked and blindfolded. They were taken to a secure mock prison on the Stanford campus where the blindfolds came off. They were then assigned as either prison guards or prisoners. The guards were instructed to maintain control, but not to use violence. According to Zimbardo, the guards "steadily increased their coercive aggression tactics, humiliation and dehumanization of the prisoners" [9]. The guards' behavior continued to deviate as time progressed to the point where some of the prisoners needed to be released due to mental anxiety.

Zimbardo stated: "I had been conducting research for some years on deindividuation, vandalism and dehumanization that illustrated the ease with which ordinary people could be led to engage in anti-social acts by putting them in situations where they felt anonymous, or they could perceive of others in ways that made them less than human, as enemies or objects. I wondered, along with my research associates Craig Haney, Curtis Banks and Carlo Prescott, what would happen if we aggregated all of these processes, making some subjects feel deindividuated, others dehumanized within an anonymous environment in the same experimental setting, and where we could carefully document the process over time" [9]. It is a phenomenon in human behavior we have seen repeated at Abu Ghraib prison.

The question that this paper addresses is this: "Can the same scenario happen in a virtual setting?" In virtual settings students have "control" over computer systems. This control is the ability to compromise and control a computer system. These are the very skills taught in many information security related college and university programs. The computer system is viewed as the "enemy" (i.e., Zimbardo's prisoners). The computer system symbolizes "the administration" or "big business" in the mind of the student and is therefore viewed as an antagonist. The student has the ability to "humiliate" his "prisoner" by performing malicious acts to the system. Anonymity of the student is guaranteed by the Internet where there is no overlooking authority figure. This is a powerful inducement as illustrated in the Zimbardo experiment as even well-behaved middle class college students succumbed to this scenario. Zimbardo stated that any institution or agency can induce similarly dramatic transformations in behavior in a scenario where there is no authority figure dominating the scene [9].

THE EFFECTS OF DEINDIVIDUALIZATION

Deindividualization is the process of removing the identity of an individual, in other words, creating anonymity. It is used by groups to indoctrinate members into a larger "whole" where the group norms are redefined. This process strips away the identity of the individual allowing for the group identity to take its place, making it easier to behave in a deviant fashion, since the group norms can differ greatly from societal norms. This can cause relatively "normal" individuals to perform extreme acts, such as killing other humans when told to do so. As part of a large group, the individuals view their own actions as just a small part of the whole and therefore insignificant. Societal norms deteriorate into the norms of the group. According to Loch and Conger, "Deindividualization is not a well-researched topic and no accepted measure exists" [5]. It is however, fairly well defined and according to the definition, dependent on anonymity. Given this, one way to reduce deindividualization is to “individualize” students, in other words, give them each a unique identity. In a university environment this can be done through small class sizes, knowing students names, addressing students by name, taking a personal interest in students, allowing students to express their individual viewpoints in class, and grading and commenting on their work in an individual fashion. Unfortunately, this is the exact opposite of what is being done at most larger universities where the majority of information security related instruction occurs.

Deindividualization is the essence of "mob mentality” that allows for anonymity. Students can “hide” their actions within a group. The group itself then defines the norms under which ethical decisions are made. These norms can deviate significantly from societal norms. Individualizing students breaks up the group norms and allows each person to have a unique viewpoint. This can be promoted in a university environment by asking open ended questions that encourage students to think for themselves and involving students in classroom discussions by eliciting opinions. In stressing individualism, it is therefore important to emphasize tolerance for varying opinions. These are pedagogical methods woefully lacking in most technology related curricula where there are few, if any, open ended questions and little or no discussion between professor and students.

Tolerance for varied opinions is an example of moral sensitivity. According to James Rest’s model of morality theory [8], there are four components of morality:

- Intrepreting (moral sensitivity)—how our actions affect other people;
- Formulating (moral judgment)—which alternative is morally justifiable;
- Deciding (moral motivation)—pursuing moral values above non-moral values and
- Acting (moral character)—the will needed to carry out an action.

Clearly Zimbardo’s experiment showed that the prison scenario dramatically affected moral sensitivity and judgment. These two factors seem to be highly susceptible to an anonymous environment in which the penalties for improper behavior are ill-defined and there is no authority figure, such as on the Internet. The question becomes "how do we increase moral sensitivity and judgment?” Bebeau [1] provides evidence that moral argumentation and dilemma discussion develop moral sensitivity and judgment. McNeel [7] analyzed data from college students and found that a college education is effective in increasing scores on the Defining Issues Test (DIT). DIT is a well established benchmark that has been in use since the 1970s in more than 40 countries and in over 1,500 studies. Students are presented dilemmas and then asked to select a multiple-choice answer. Since it is a multiple choice test, the DIT does not require students to write down a reply in their own words and therefore this test measures recognition knowledge rather than verbal knowledge. McNeel’s study of the DIT scores shows that measured before and after a college education, moral judgment is the variable with the largest gains of all variables tested, which also included verbal aptitude, math aptitude, self-conceptualization, and attitudes. Bebeaus’ and McNeil’s studies indicate that it is important to discuss ethical scenarios, to perform moral arguments and to do these often enough to maintain a high moral sensitivity among students. Bebeau [1] also indicated that moral motivation and character are harder to affect.

LAWS, RULES, AND REGULATIONS

Many programs do not emphasize existing laws, rules and regulations. Logan and Clarkson [6] performed a survey of a graduate computer security class at Marshall University and found that no students had read the university's Acceptable Use Policy. This contributes to Zimbardo’s scenario in which bounds on acceptable behaviors are ill-defined. Having well-defined boundaries is especially important in male dominated computer related programs,since men and women seem to have distinctly different ethical mindsets. Kreie and Cronan [4] found "men and women were distinctly different in their assessment of what is ethical and unethical behavior. For all scenarios, men were less likely to consider a behavior as unethical. Moreover, their judgment was most often influenced by their personal values and one environmental cue—whether the action was legal. Women were more conservative in their judgments and considered more environmental cues, as well as their own personal values." This indicates that ethics education is absolutely necessary to establish legal and regulatory boundaries for students, especially male students. Legal and regulatory topics should be covered whenever a related technology is introduced. For example, if port scanning is introduced as a topic in a computer security class, it should be pointed out that there is a campus policy that prohibits port scanning (if there is one). If not, appealing to one’s moral judgment that "port scanning for fun" is not appropriate might not work in a male dominated computer security class where the attitude is likely to be "no harm, no foul."

THE IMPLICATIONS OF ETHICS EDUCATION

The stakes are high. Consider the case of "Mafiaboy" (Canadian law prohibits revealing his real name), at the time a 14-year-old high school student from an affluent suburb in Montreal who in February of 2000 used distributed denial of service (DDS) attacks to bring down some of the top Internet websites including Amazon.com, Buy.com, Dell.com, CNN.com, Etrade.com and Yahoo.com According to *Confessions of Teenage Hackers* [11], "To many who knew him, there was nothing odd about him. He was a normal kid." The facts led some people to believe that he knew his activities were criminal. His use of a denial of service toolkit in which the toolkit's author had given this warning to all the hackers who downloaded it: "WARNING: Using this program on public networks is HIGHLY illegal and they WILL find you and put you in jail" indicated his awareness. However, it is believed that Mafiaboys' older brothers installed the DDS attack software on the 75 or so zombie computers used in the attacks and that Mafiaboy only knew how to initiate the attacks. The older brothers were aware of the legal implications of attacking major websites and only used the zombies to attack smaller targets, but investigators believe that their younger brother probably did not. The Internet provided anonymity. Lack of supervision certainly played a role. According to Dan Verton [11], "Mafiaboy's mother responded to her son's prosecution by telling the judge that his father was not strict enough in supervising and guiding him." Clearly in this case, there was a lack of moral sensitivity and poor moral judgment. It is no wonder considering in later interviews Mafiaboy's father said he found his sons accomplishments "impressive" [11]. This case had all the elements of Zimbardo's experiment, unsupervised control, anonymity, and indoctrination. The attacks caused an estimated 1.7 billion dollars in damages [11].

CONCLUSIONS

Our current state of ethics research indicates that reducing deindividualization, promoting moral argumentation by using computing related ethical scenarios, and defining legal and regulatory boundaries increase moral sensitivity and judgment among college and university IT students. Increasing moral sensitivity and judgment makes it easier to behave in an ethical manner, reduces the situational effects leading to abusive behavior and are important and necessary components of ethics education in information security related programs.

REFERENCES

1. Bebeau M.J. (1994). Can ethics be taught? a look at the evidence revisited. *The New York State Dental Journal*, *60*(1), 51-57.
2. Dittman, M. (2004) What makes good people do bad things. *Monitor on Psychology, 35,*(9), 68.
3. Haney C., Banks C., & Zimbardo P. (1973). Interpersonal dynamics in a simulated prison. *international Journal of Criminology and Penology,* 1, 69-97.
4. Kreie J., & Cronan T. (1998). How men and women view ethics. *Communications of the ACM, 41*(9), 70-76.
5. Loch K., & Conger S. (1996). Evaluating ethical decision making and computer use. *Communications of the ACM, 39*(7), 74-83.
6. Logan P., & Clarkson A. (2005). Teaching students to hack: Curriculum issues in information security. *2005 SIGCSE Conference Proceedings, 37*(1), 157-161.
7. McNeel, S. P. (1994). College teaching and student moral development. In J.R. Rest & D. Narvarez, *Moral development in the professions: Psychology and applied ethics*. 27-49. Hillsdale, NJ: Erlbaum.
8. Rest, J.R. (1984). The Major Components of Morality. In W.M. Kurtines & J.L. Gewitz *Morality, moral behavior, and moral development*, 24-37, New York: Wiley.
9. Stanford University News (1997). Prison experiment: Still powerful after all these years. http://www.stanford.edu/dept/news/pr/97/970108 prisonexp.html.
10. The Stanford Prison Experiment related links http://www.prisonexp.org/links.htm.
11. Verton, D. (2002) *The Hacker Diaries: Confessions of Teenage Hackers*, 55-89, New York: McGraw-Hill.
12. Wikipedia http://en.wikipedia.org/wiki/Mafiaboy.
13. Zimbardo P. (1999). Recollections of a social psychologist's career: An interview with Dr. Philip Zimbardo. *Journal of Social Behavior & Personality*, *14*(1), 1-23.