THE IMPACT OF PERCEIVED COMPUTING SECURITY ON ETHICAL BEHAVIOR: A UNIT OF STUDY FOR MIS STUDENTS

by

Randall S. Sexton
Computer Information Systems
Southwest Missouri State University
901 South National
Springfield, Missouri 65804
(417) 836-6453

Brian J. Reithel, Ph.D., CDP
Department of Management and Marketing
The University of Mississippi
University, MS 38677
(601) 232-7102

Ann L. Canty
Department of Management and Marketing
The University of Mississippi
University, MS 38677
(601) 232-5820

Address correspondence to: Randall S. Sexton, Ph.D.
Internet electronic mail: rss000f@mail.smsu.edu

The Impact of Perceived Computing Security on Ethical Behavior: A Unit of Study for MIS Students

ABSTRACT

Security in computing has been compared to the security of the Wild West days. This new frontier of technology has left some corporations vulnerable to attack because of a lack of understanding or employee education on the importance and value of the information resource. By using identified factors that affect ethical decision making and behavioral choices in the business setting, we can develop a curriculum to educate future users of the information resource. A module on ethics is proposed based upon two factors, perceived probability of detection without punishment and perceived probability of detection with punishment, that can influence behavior in four ethical dilemma areas identified by previous research. This unit of study is used as a method to improve students' awareness of the importance of the two factors as deterrents to unethical (and sometimes illegal) behavior. An instrument was developed to measure students' predictions of ethical behavior based on the extent of the two factors. In addition, another instrument was developed to measure the students' predictions of their colleagues' ethical behavior. These instruments were administered and tabulated in a junior-level MIS class at a major university in order to stimulate class discussion regarding the relationship between ethics, probability of detection, and punishment. At the end of the ethics module, an anonymous survey was conducted to measure the students' beliefs regarding the impact of the ethics module on their awareness of the role of perceived probabilities of detection without punishment. The results of the survey indicated that all participants believed that their awareness of the two factors had increased after completing the ethics unit.

KEYWORDS: Ethics, Security, CIS Education

The Impact of Perceived Computing Security on Ethical Behavior: A Unit of Study for MIS Students

INTRODUCTION

While the use of technology has increased rapidly, security measures for computer-based information systems have consistently lagged behind. Many corporations, in the race to beat the competition in capitalizing on this newfound resource, have neglected to incorporate basic security measures. During the last two decades, the increase in technology has been paralleled by financial losses by many of those companies that have openly embraced information technology [1]. Although these losses have increased with the increasing use of technology, this does not imply that technology causes unethical behavior. However, a lack of security, in any situation, could tempt unethical behavior. If a bank took no security measures, leaving its money right out on the counter, unattended during lunch hours, how many so-called ethical people would make an illegal withdrawal? Moreover, how many more would join in, if it were known that no punishment would be given? Common sense tells us that most people are not bank robbers, but given the above scenario, many would probably change their livelihood. Another example could be an employee alone in a room with valuable files of information and a copy machine at his or her disposal. How many would be tempted to copy the material for personal gain if they knew that nobody could possibly catch them? Now, look at our technological society, with its electronic funds transfers and computer accessible information. Without proper security, or at least perceived security, the above two scenarios can easily turn into reality.

Finances can be transferred, private files and data can be read, records changed, and valuable information stolen with ease from a trusted employee's desk. No corporation is immune; even the CIA has been victimized by unethical behavior. Aldrich "Rick" Ames was a CIA agent who successfully pilfered our nation's secrets for several years. What is ironic about his story is that Ames was caught because of his lack of security on his own notebook PC. Incredibly, Ames allowed his CIA boss to play a computer game on a personal computer that contained stolen data. Ames neglected to hide the directory that contained the information and

even had the temerity to name the directory after his Russian contact. As our society rapidly gains computer literacy, more information technology-related opportunities for unethical behavior will appear.

It is our contention that information systems educators can have a positive influence upon future ethical policies and practices in the business environment by introducing basic security concepts such as probability of detection, probability of detection with punishment, and the basic principles of ethics to the undergraduate student. Furthermore, these concepts need to be introduced in an applied exercise that engages the student's ability to arrive at reasoned choices and to personally consider the various factors that led to the student to his/her choice.

MOTIVATION

Many corporations are reluctant to report computer crimes, which generally occur as a result of unethical decisions on the part of the perpetrators, because of fear of loss in customer confidence and escalations in insurance premiums. It seems logical that society's perception of possible detection and/or punishment would surely be affected by this lack of information. One conservative estimate of the loss from computer crime is $3 to $5 billion a year [2]. This estimate does not include those crimes that were not reported to an authority or kept secret from the public. A more recent estimate from the Software Publisher's Association places the loss to software vendors at $9.96 billion worldwide in 1993, and $8.08 billion in 1994 [3]. Another computer-oriented loss that is not so easily quantified is the loss of privacy. One example of this is the hacker who made his way into a national laboratory by using the Internet [4]. Our expanding technological society is quickly computerizing all of our personal, medical, and even criminal records. Lack of proper security, or the public's perception of lack of proper security, could mean an open invitation to attack the system. Greenwald estimated data losses of between $100 million and $300 million annually [1]. The increases in computer and software ease of use, accessibility, and computer literacy of the population have contributed to the outbreak of computer-related crimes [5]. It has been acknowledged for years that computer piracy has been rampant during the last two decades. One software industry estimate places the cost of software

piracy somewhere between $800 million and $1 billion [6].

One might think that these crimes are mainly committed by the career criminal, who has a natural disrespect for chances of being caught, but the National Center for Computer Crime Data (NCCCD) stated that former and current employees are more likely to breach a company's computer system than any other category of persons [5]. Estimates from the National Computer Security Association attribute 25% of all computer crimes to employees [7]. Computer crime will always be a problem because of the career criminal, no matter what security or perceived security is implemented in information systems. On the other hand, a target group that businesses and information systems educators should be concerned with is the group of employees or former employees that normally would not commit unethical acts against the company, but are so overwhelmed with unbalanced temptation that they cannot help themselves. In some instances, these unethical acts are "crimes" by legal definition, while in other instances the unethical acts are violations of trust, organizational rules, or other employment agreements.

The previously mentioned evidence provides a strong motivation for corporations, government, information systems educators, and society as a whole to find those factors that affect ethical decision-making in a technological environment. Research has found that detection alone as well as detection with punishment are two factors that are significantly correlated to ethical behavior [8,9]. These factors will provide tools that can be used to help curb current and future unethical decisions by educating students whose future responsibilities might include data security.

ETHICS MODULE

An instrument was developed around Mason's four ethical issues of privacy, accuracy, property, and accessibility (PAPA) [10]. Each topic area includes three questions, with the first asking the basic ethical question. The following two questions introduce different levels of perceived probability of being caught with no punishment and being caught with punishment, respectively. If detection alone, and detection with punishment have no effect on ethical decisions then the responses to the first question in each topic should correspond with the

responses to the following two questions. If detection and/or detection with punishment does influence ethical decision-making there will be a significant difference in how respondents answer the latter two questions, compared to the first. For example, if an individual answers NO to copying software on the first question but on the second question (where the chance of detection is known), this individual answers YES to any of the different levels of perceived detection, then the individual is telling us that perceived chance of detection does matter in ethical decision making.

UNIT OUTLINE: DATA SECURITY

I. The instrument developed for this research could be used as a tool to show the importance of perceived security in the business environment. After administering the survey in the MIS class, a quick analysis should show similar results to prior research, giving the facilitator the opportunity to demonstrate the importance of both perceived chance of detection and perceived chance of detection with punishment, while personally involving the student. The survey should precede any discussion of ethical behavior, and for tabulation convenience, should be administered toward the end of the class period in order to have time for calculating results. Because the survey contains sensitive questions regarding personal values, it should be administered anonymously in order to stimulate more accurate reporting of student perceptions. The survey, included below, can be administered within a 10 to 20 minute time period.

Property

1. Your place of work recently purchased an expensive software package that you greatly desire but can't afford. Would you copy this software for your own use? Circle your response: YES NO

2. In the same situation as question #1, if caught, you will NOT be punished and you have a (see below) percent chance of being detected. Would you copy the software in these situations?

Please circle YES or NO on all the choices below.

0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

3. In the same situation as question #1, if caught, you will be severely punished, and you have a (see below) percent chance of being detected. Would you copy the software in these situations?

Please circle YES or NO on all the choices below.

0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

Privacy

4. Currently, you greatly desire to know the contents of a fellow employee's private computer file. Would you read the file? Circle your response: YES NO.

5. In the same situation as question #4, if caught, you will NOT be punished, and you have a (see below) percent chance of being detected. Would you read the file in these situations?

Please circle YES or NO on all the choices below.

0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

6. In the same situation as question #4, if caught, you will be severely punished, and you have a (see below) percent chance of being detected. Would you read the file in these situations?

Please circle YES or NO on all the choices below.

0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

Accuracy

7. You are currently working on a commission based salary that is figured automatically by a computerized system. If you received more commission than you deserved, would you keep the extra amount? Circle your response: YES NO

8. In the same situation as question #7, if caught, you will NOT be punished, and you have a (see below) percent chance of being detected. Would you keep the extra amount in these situations?

Please circle YES or NO on all the choices below.

0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

9. In the same situation as question #7, if caught, you will be severely punished, and you have a (see below) percent chance of being detected. Would you keep the extra amount in these situations?

Please circle YES or NO on all the choices below.

0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

Accessibility

10. By chance, you found the passwords that allow you to access several different restricted software applications and data. There is a software application that you greatly desire to use. Would you access this application? Circle your response: YES NO

11. In the same situation as question #10, if caught, you will NOT be punished, and you have a (see below) percent chance of being detected. Would you access the restricted software application in these situations?

Please circle YES or NO on all the choices below.

0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

12. In the same situation as question #10, if caught, you will be severely punished, and you have a (see below) percent chance of being detected. Would you access the restricted software application in these situations?

Please circle YES or NO on all the choices below.

0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

II. In order to compare this collective individual ethical perspective with students' perceptions of others' ethics, a second instrument should be administered after the first instrument, but before the results of the first instrument are presented to the students. The second instrument attempts to measure each student's

perception of others' ethics. By comparing the students' perceptions of their own ethics (from the first instrument) with their perceptions regarding those around them, a facilitator can demonstrate the importance of developing security practices that include raising the perception of detection and punishment in the working environment. The second instrument (shown below) can be administered in class and tabulated on the board. The facilitator can involve the class by collecting the instruments and randomly redistributing them to allow each student to call out responses that are tabulated on the board.

1. If ten employees had the opportunity to illegally copy a company owned software package, how many do you feel would copy the software? Circle your answer below.

1 2 3 4 5 6 7 8 9 10

2. If ten employees had the opportunity to read a fellow employee's private computer file, how many do you feel would read the file? Circle your answer below.

1 2 3 4 5 6 7 8 9 10

3. If ten employees had the opportunity to keep unearned income from a computerized mistake on their pay check, how many would keep the extra money? Circle your answer below.

1 2 3 4 5 6 7 8 9 10

4. If ten employees had the opportunity to access or use restricted software packages at work, how many do you feel would access the software? Circle your answer below.

1 2 3 4 5 6 7 8 9 10

III. Once the second form has been tabulated, these results can then be directly compared with the four main questions of the first instrument. These results should be similar and will stress that unethical behavior, if not controlled, can be a serious problem. After this comparison and appropriate discussion of how we basically see others as we see ourselves, a comparison of these results can then be conducted with the questions on the first instrument dealing with perceptions of detection and detection with punishment. The average responses for selecting unethical practices should go down as the chances of detection and detection with punishment rise. This pattern of response directly demonstrates the need for organizations to increase their employees' perceptions of detection and punishment.

IV. Next, outline Mason's paper on the four ethical issues (PAPA) of the information age [10]. Specific examples used in Mason's paper can give relevance to the role of these four issues in everyday society. The nature of morals, ethics, and ethical dilemmas can be explored. Furthermore, means of detecting unethical choices by members of a society can be discussed along with the role of societally-imposed

punishments for those who break the rules. The four major question areas of the survey should be discussed with regard to their alignment with Mason's four ethical issue groups.

V. Discussions could then be initiated to generate ways of increasing employees' perceived security.

Examples could be:

a. The publication of policy statements identifying appropriate behavior and punishment of unethical actions [11];

b. the enactment of security measures and the communication of these measures to employees to discourage unethical behaviors;

c. when an employee is caught engaged in an unethical activity, prosecute to the fullest extent of the company policy and criminal law (if appropriate);

d. show severe consequences for unethical behavior;

e. consistently follow through with stated punishments.

MODULE IMPLEMENTATION IN AN MIS COURSE AND RESULTS

The preceding module was implemented in the Fall of 1995 in an undergraduate Management Information Systems class at a major university. Fifty-one surveys were distributed and collected for tabulation, with one survey discarded for incompleteness. After the class ended, the responses were entered into SPSS and mean scores were calculated for each question. During the next class meeting, the second instrument was administered and tabulated in class. The results (shown below) were consistent with the expected results and were very useful in demonstrating the importance of perceived detection and punishment in deterring unethical practices. The columns labeled "Individual", "Detection" and "Punishment" came from the SPSS analysis of the first instrument while the column labeled "Others" came from the in-class tabulation of the responses to the second instrument.

AVERAGE LIKELIHOOD THAT UNETHICAL BEHAVIOR WILL OCCUR				
Mason's PAPA	Individual	Others	Detection	Punishment
Property	60%	52%	37%	14%
Accuracy	60%	69%	50%	15%
Privacy	38%	52%	24%	6%
Accessibility	44%	44%	37%	10%

After discussing the results of the module, the students were asked to complete another

anonymous survey, consisting of only one question (see below) to determine whether the awareness of the effects of detection and punishment on ethical behavior had been heightened for the students as a result of the ethics module.

> *The module on ethics _____ my awareness of the importance of detection and detection with punishment concerning security issues in computing.*
>
> *A. increased*
> *B. did not increase*

Out of the forty-nine students in attendance, all forty-nine responded that their perceptions had been "increased" by the unit. This was a 100% positive response to the ethics module, leading us to believe that it was fairly successful in implementation. To measure for a lasting affect of heightened awareness this same measure could be implemented upon the completion of the course.

CONCLUSIONS AND RECOMMENDATIONS

By involving the students in the survey exercise, an instructor will have a better chance of getting the students to actively consider and to actually realize the importance of data security as a whole, and specifically, to realize the importance of perceptions about detection and/or perceived detection with punishment. Ethical issues will be introduced to the students and possible problems with inadequate security in information systems will be personally demonstrated to the students. This article is not the first to suggest the need for studying the ethical issues faced by information systems users [12]. However, this article does suggest a method by which an information systems educator could actively involve a student in the ethical decision-making process.

This type of unit of study could fit virtually any undergraduate or graduate level MIS class. Most introductory MIS courses already contain a module on ethics, which would be an appropriate place to implement this module. The hands-on effect of the survey will hopefully, bring home to these students the important role that perceived detection and punishment play in ethical behavior. This module is also appropriate for upper level classes that deal with managing

the IS function. By becoming more aware how people react to perceived detection and detection with punishment, these students will have additional tools that will help them control the ethical practices of employees they manage. Since the unit is short, it could be added into existing curriculums without much effort, leaving the exact placement of the unit up to the instructor. Since the dependency of information is ever increasing in society, the need for educators to address ethical issues also increases. This unit of study is one way to appropriately address this need.

REFERENCES

1. Greenwald, J. (June 6, 1994). Breaking into the system; the cost of computer crime is on the rise. *Business Insurance*, 28(23), pp. 3-6.

2. Rosenblatt, K. "Deterring Computer Crime", *Technology Review*, Feb/March 1990, pp. 35-40.

3. Software Publishers Association (July 5, 1995). Software piracy poses global threat. *SPA News Release, pp.* 1-4.

4. Stoll C. (May 1988). Stalking the wily hacker. *Communications of the ACM*, 31(5) pp. 484-497.

5. Alexander, M., (1989). Hacker stereotypes changing. *Computerworld*, 23(14), pp. 101.

6. Eining, M. M. & Christensen, A. L. (1991). A psycho-social model of software piracy: The development and test of a model. *Ethical Issues in Information Systems*, Boyd & Fraser Publishing Company.

7. Harper, D. (February 1994). Computer crime may be close to home; most illegal activity is performed by employees. *Industrial Distribution*, 83(2), pp. 41.

8. Dickson, J.W. (1978). Perceptions of risk as related to choice in a two-dimensional risk situation. *Psychological Reports,* 44, pp. 1059-1062.

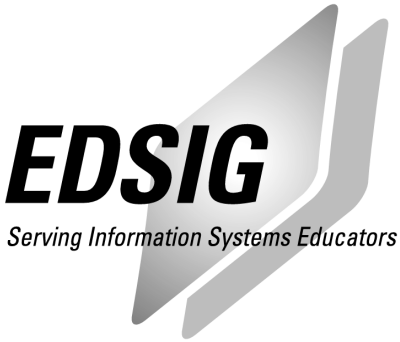
9. Neumann, P. G. (August 1992). Fraud by computer. *Communications of the ACM*, 35(8), pp. 154.

10. Mason, R. O. (March 1986). Four ethical issues of the information age. *MIS Quarterly,* pp. 4-12.

11. Pfleeger, C. P. (1989). *Security In Computing*. PTR Prentice Hall, Englewood Cliffs, New Jersey, 1989.

12. Paradice, D. B. & Dejoie, R. M. (1991). The ethical decision-making processes of information systems workers. *Journal of Business Ethics*, 10, pp. 1-22.

Information Systems & Computing
Academic Professionals



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096