The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions[1,2]

By: Susan J. Harrington
Georgia College & State University
3690 Sussex Drive NE
Milledgeville, GA 31061-9337
U.S.A.
sharring@solar.gac.peachnet.edu

Abstract

This research asks whether codes of ethics affect computer abuse judgments and intentions of information systems (IS) employees. Codes of ethics examined include both company codes of ethics and those written specifically to deal with IS issues. In addition, since the intent of codes of ethics is to clarify responsibility and deter unethical behavior, both the psychological trait of responsibility denial and its moderating effect on codes was studied. While company codes did not affect the computer abuse judgments and intentions of all IS personnel, they did affect those IS personnel who tend to deny responsibility, thus suggesting that company codes may clarify responsibility and reduce rationalizations for some people. Unlike company codes, IS-specific codes of ethics had a direct effect on computer sabotage judgments and intentions, but had no differential effect on those high in responsibility denial. Finally, responsibility denial was directly related to all computer abuse judgments and intentions studied. Overall, codes had little effect on computer abuse judgments and intentions relative to the psychological trait of responsibility denial.

Keywords: Computer crime, IS security, abuse and crime, deterrence, management of security, responsibility, codes of ethics

ISRL Categories: EK09, EH0210, BB0103, BD0104, AF0404

Viruses, cracking (sometimes called "hacking"), computer fraud, illegal software copying, and corporate sabotage using a computer are familiar topics in the popular press. These well-publicized forms of computer abuse (i.e., the unauthorized, deliberate misuse of information systems) and the perception that American business is fraught with crime and corruption have led many organizations to adopt codes of ethics to try to avoid problems (Manley, 1991).

The fact that organizations are increasingly establishing codes of ethics is shown by a Conference Board survey in which nearly half of the responding companies had enacted their codes since 1987, with the result that 83-93% of U.S. firms now have a code of ethics (Berenbeim, 1992; Center for Business Ethics, 1992). These corporate codes of ethics are any written corporate statement of ethics, law, or policy that define standards, either by direct articulation or by articulating values or norms, for the work group's behavior (Stevens, 1994). They usually consist of a combination of directive statements for certain kinds of conduct, as well as general statements of corporate commitments to constituencies or a management philosophy (Berenbeim, 1992).

Many managers believe corporate codes can help deter improper actions of employees

[1] Gerry DeSanctis was the accepting senior editor for this paper.

[2] An earlier version of this paper was presented at the ACM Special Interest Group on Computer Personnel Research (SIGCPR) annual conference, March 26, 1994, Alexandria, VA.

(Manley, 1991). In addition, codes specific to the use of information systems, similar to or based on those of ACM, DPMA, or the British Computer Society (BCS), can provide even more specific guidance to information systems (IS) employees (Forcht, 1994). This guidance may be especially important for IS employees, who, by virtue of their computer knowledge, can perpetrate crimes of greater magnitude than employees without computer knowledge.

Yet, despite the prevalence of codes of ethics, their effectiveness is controversial (Stevens, 1994). Researchers from various fields have called for additional studies on the issues, including personality factors that may interact with codes (Ford and Richardson, 1994; Weaver, 1993). Thus, two important questions to ask are: (1) Do codes deter unethical behavior of IS employees; and (2) Is the effect of codes moderated by the psychological traits of the IS employee? This study examines these questions.

Corporate Codes of Ethics

The number of professional groups rushing to implement codes and the number of journal articles advocating codes indicate there is a widespread belief that codes of ethics can help resolve the ethical issues facing IS employees today. In fact, managers in general see codes as the most viable approach for dealing with ethics problems (Robin, et al., 1989), and codes are by far the most common way businesses address ethics concerns (Center for Business Ethics, 1986).

A major theory behind codes of ethics is that the codes clarify responsibility and so deter unethical behavior (Fimbel and Burstein, 1990; Oz, 1992). Generic codes of ethics (i.e., codes intended for all members of the organization) are believed to impact IS personnel behavior by clarifying certain responsibilities (Bequai, 1983; Johnson and Mulvey, 1995). A sample from such a generic code from an organization in this study is included in the Appendix.

Advocates of the view that generic codes clarify responsibilities include those (e.g., Johnson, 1989) who suggest that ethical issues in computer use are not new but merely a new "species" of ethical issue. For example, some generic codes remind personnel that theft and misuse of company property will not be tolerated; illegal software copying may be reduced by such reminders. Destructive viruses or corporate sabotage using a computer may be thwarted by statements concerning willful falsification and alteration or destruction of records. Unwanted sabotage of competitors or non-paying customers may be avoided by statements concerning fair treatment of suppliers, customers, and competitors.

Corporate Codes and Ethical Decision Making

Clearly codes are assumed to have an impact on the decision-making processes of the employee. Yet theory-based empirical investigations on IS personnel's decision-making processes involving computer abuse are scarce, perhaps because of the difficulty in identifying the many interacting individual and situational variables involved (Paradice and Dejoie, 1991; Rest, 1984).

Ethical decision-making models may aid in clarifying relevant variables (Rest, 1986). Ethical decision-making models have been proposed, but are not yet fully validated, that attempt to describe the decision-making processes related to ethical or unethical behavior. After reviewing ethical decision-making models, Jones (1991) integrated the models into one model, largely founded on the works of Rest (1986). This model consists of four main components: awareness, judgment, intention, and behavior (see Jones, 1991 for a full discussion). Codes of ethics may have the following effect on each component: (1) make the employee aware that an ethics issue exists and a potential computer abuse can occur; (2) aid the employee in making a judgment about right and wrong by clarifying right or wrong behavior regarding the abuse;

(3) courage employees to abide by their judgments, to place the value of doing right above other values, and to establish ethical intentions for behavior; and (4) behave ethically as a result of components 1 through 3.

Because of the difficulties in studying unethical behaviors (component 4), this study examines IS personnel's computer abuse judgments (component 2) and intentions (component 3). Research shows that attitudes and intentions are the best predictors of specific behaviors (e.g., Ajzen and Fishbein, 1980). Research into whether codes of ethics affect these components adds a new and important dimension to the study of IT ethics.

Corporate Codes and Deterrence

Codes are believed to deter computer abuse because they keep employees abreast of laws and regulations and clearly define unacceptable or illegal conduct, thereby influencing the employees' moral judgment (Bequai, 1983). Moreover, generic codes can be the basis for internal sanctions (i.e., punishments) that have a deterrent effect and can therefore affect the employee's intentions (Straub, 1990; Straub and Nance, 1990).

The effect of codes and sanctions on unethical judgments and intentions is consistent with the general deterrence theory of crime (Cressey and Moore, 1983; Straub, et al., 1993). General deterrence theory asserts that illegal behavior in the general population will vary inversely with more certain and severe punishment (Nagin, 1978). Laws and legal sanctions or sanction threats may lead to total prevention of a particular deviance, may change the flagrancy of its manifestations or may reduce the frequency with which such acts are done (Tittle, 1980). Thus, insofar as codes of ethics are like laws, codes may reduce unethical behavior.

There are several ways in which codes are like laws. First, like the laws and formal sanctions studied as part of deterrence research, some codes of ethics include sanctions or are the basis for litigation (Pitt and Groskaufmanis, 1990). Sanctions, according to deterrence theory, should reduce unethical behavior by providing knowledge to the population that unethical behavior produces a negative rather than a positive utility (Pearson and Weiner, 1985).

In addition, codes of ethics seem to use the same underlying mechanisms as laws and legal sanctions to deter unethical behavior. These mechanisms include creating fear and the desire to avoid unpleasant consequences, strengthening moral inhibitions and norms, clarifying rules, and creating habits of conformity (Pearson and Weiner, 1985; Tittle, 1980). For example, a study based on deterrence theory found that the threat of sanctions reduced the incidence of cheating on out-of-class programming assignments (Straub et al., 1993).

However, unlike laws, only 25–33 percent of codes have formal enforcement procedures (Mathews, 1987; Pitt and Groskaufmanis, 1990). Nevertheless, even without enforcement procedures, codes may act like laws as described by deterrence theory, for threats implied by laws may be explicit or may exist only in the vague potential of negative consequences (Tittle, 1980). The existence of a code of ethics and the affidavit of compliance often signed by the employee suggest sanctions will occur should the code be broken (Cressey and Moore, 1983). In fact, the corporation is like a private government that has enacted "laws" (codes of ethics) that emphasize the need for conformity to those laws in order to protect the corporate establishment (Cressey and Moore, 1983).

Even if employees are not completely aware of the contents of codes of ethics, deterrence theory suggests codes, like laws, may be effective, for the content may be communicated via distribution of the code, simple moral appeals, the visible presence of enforcers, or personal experience and observation of others' apprehension (Cook, 1980; Straub, et al., 1993). Moreover, such communication need not be perfect. For instance, limited rationality on the part of some potential criminals, combined with an information transmission mechanism that is not completely accurate, is sufficient to generate deterrent effects (Cook, 1980).

However, not all researchers would agree with the effectiveness of generic codes. One criticism is that much of what is in generic codes is unrelated to IS activities. For example, often generic codes include rules concerning conflict of interest or drug and alcohol abuse (Cressey and Moore, 1983). This criticism is supported by a study where it was found that codes had an unclear effect on Association for Systems Management (ASM) members and a small effect on non-ASM members (Fimbel and Burstein, 1990). Similarly, another IS study found that IS professionals believed the existence of codes had no significant impact upon their frequency of unethical behaviors (Vitell and Davis, 1990).

Another potential problem with generic codes is that much of what is in typical codes is only intended as a public relations gimmick or a means of protecting the corporation from legal liability (Laudon, 1995; Metzger, et al., 1993; Stevens, 1994). Moreover, many researchers feel that codes lack much impact—that other reasons, such as SEC directives, outside auditors, or public pressure for the enactment of laws account for any improvement in behavior (Cressey and Moore, 1983; Whiteside, 1978). Another criticism is that codes are nothing more than pseudo-ethics, for they merely codify existing rules or standards of behavior and do not encourage ethical reasoning when an individual is faced with new or difficult issues such as those that so often confront IS personnel (Ladd, 1985; Laudon, 1995).

Finally, companies usually do not report illegal activity to law enforcement authorities or impose severe sanctions on computer abusers (American Bar Association, 1984; Pitt and Groskaufmanis, 1990). Reporting of computer abuse is shunned, prosecution remains complex, detection is uncertain, conviction is rare, and even rewards such as golden parachutes and well-paid consulting jobs occur for convicted computer criminals (Bequai, 1983; Canning, 1986; Sokolik, 1980). The effect is that computer abusers are rarely caught or punished, a fact well-known to potential computer abusers (Hafner and Markoff, 1991; Whiteside, 1978). Such a situation suggests codes will have little, if any, impact on computer abuse, for certainty of sanctions is closely associated with deterrence (Paternoster, et al., 1982; Tittle, 1980).

Therefore, whether generic codes clarify correct behavior and have an effect on computer abuse judgments and/or intentions are important considerations. Because there is a serious question about the impact generic codes have on IS employees, it is important to test the hypotheses (in null form):

H1a: The presence of generic company codes of ethics will have no effect on IS personnel's judgments regarding computer abuse.

H1b: The presence of generic company codes of ethics will have no effect on IS personnel's intentions regarding computer abuse.

The Need for IS-Specific Codes of Ethics

A problem with generic company codes of ethics is that the topics often do not relate to IS situations. An IS employee may have difficulty relating generic codes to commonly encountered IS dilemmas. In fact, people are unable to draw analogies from general ethics issues to computer abuses (Conger, et al., 1995) , probably because of the depersonalized relationships, intangible property, and anonymity involved in computer abuse (BloomBecker, 1990; Krauss and MacGahan, 1979; Whiteside, 1978). In addition, computer abuse may be so different from white-collar crime that traditional laws are ineffective (Parker, 1989). It is for that reason, in fact, that IS-specific laws have had to be enacted.

Similarly, some would argue that IS-specific codes that address IS issues may be needed. An IS-specific code may aid in deterrence, for such a code may provide guidelines for judgments about appropriate behavior in technology use. Without such a code, it also may be easier to rationalize irresponsible action. Rationalizations are a way of neutralizing the norms generally embraced by an individual, allowing the individual to "drift" into unethical behavior (Pearson and Wiener, 1985). The amateur white-collar criminal and the computer abuser often go through a stage characterized by a decline in normative standards of conduct (i.e., a decline in judgments) and a rationalization process (i.e., enabling unethical intentions) (Conger, et al., 1995; Geis and Meier, 1979; Parker, 1981). Such a decline in standards and a rationalization process is believed to have led to Robert Morris' perpetration of the Internet worm (BloomBecker, 1990; Hafner and Markoff, 1991).

Thus, IS-specific codes are one way to relate norms to computing, to reinforce those norms, and to encourage individuals to live up to the norms. ACM and other corporations agree and have established IS-specific codes (see the Appendix for a sample of an IS-specific code from an organization in this study).

Yet, despite such arguments for an IS-specific code of ethics, nearly 90 percent of those organizations that have a code of ethics do not seem to have policies on particular ethics issues, other than conflicts of interest (Ethics Resource Center and the Behavior Research Center, 1990). As a result, there is a feeling by many organizations that IS—specific codes are not needed—that computer technology can be addressed under the organization's generic code of ethics. For this reason the Society for Information Management (SIM) has been reluctant to implement an code of ethics (Rifkin, 1991).

Again, deterrence theory has addressed a similar issue: i.e., whether a "precise" effect, one where a sanction or sanction threat is attached to a particular offense, is a better deterrent than a "diffuse" effect, where a particular offense is attached to other offenses or to a generalized sense of possible but imprecise sanctions (Tittle, 1980). Surprisingly, "precise" effects of formal sanctions have no advantage over generalized sanctions (Tittle, 1980), leading to the suggestion that IS-specific codes may have no advantage over generic codes of ethics. Precise effects seem more effective for informal sanctions such as peer or family disapproval, whereas diffuse effects are just as effective in formal sanctions.

Given the question of whether IS-specific codes lead to higher levels of ethicality, a second set of hypotheses is also tested in null form:

H2a: The presence of IS-specific codes of ethics will have no effect on IS personnel's judgments regarding computer abuse.

H2b: The presence of IS-specific codes of ethics will have no effect on IS personnel's intentions regarding computer abuse.

The criminological literature has been supportive of general deterrence theory overall. However, some conflicting results, weak main effects of sanctions, and other complexities identified by the research has led Tittle (1980) to call for additional research to identify specific conditions where deterrence works. This call for contingencies has not gone unanswered. Recently, for example, deterrence researchers have found that stable individual differences have a greater effect than legal sanctions (e.g., Bachman, et al., 1992; Grasmick and Bursik, 1990; Nagin and Farrington, 1992). Similarly, recent IS research supports the view that psychological traits and/or early parenting methods are related to computer abuse, particularly cracking (Shotton, 1989).

Denial of Responsibility

Regardless of codes of ethics, people vary significantly in the extent to which they accept responsibility for their actions. Individuals' lack of acceptance of responsibility for the consequences of their behavior has been linked to computer abuse (Johnson and Mulvey, 1995; Laudon, 1995). "Moral responsibility" (i.e., concern for the interpersonal consequences of acts) may be an enduring individual characteristic that provides consistency between what one says one should or would do and what one does; it is a concern for and acceptance of the consequences of one's actions (Kohlberg and Candee, 1984).

Peoples' tendency to ascribe responsibility to oneself or to diffuse and depersonalized others is related to rationalizing the consequences of one's behavior (Schwartz, 1977; Suedfeld, et al., 1985). This tendency is called denial of responsibility (RD) and is a relatively stable psychological trait. Those low in RD tend to accept responsibility and to be responsible for the welfare of others, live up to moral commitments, and follow either personal or societal rules and dictates (Staub, 1978). Alternately, those high in RD would tend to ignore standard norms and rationalize their unethical behavior by blaming depersonalized others, such as organizations.

As previously mentioned, rationalizations are often associated with computer abuse. Those who crack into computers argue that the weaknesses in the nation's computer networks and computer systems are pointed out (Conger, et al., 1995; Hafner and Markoff, 1991; Samuelson, 1989). In fact, some computer crimes take on the quality of'ideological acts to their perpetrators (Whiteside, 1978). Also common with computer crimes is the rationalization that no harm is done (Krauss and MacGahan; 1979; Parker, 1989). Similarly the "Robin Hood" syndrome, where the perpetrator differentiates strongly between harm done to an individual and harm done to an organization (which can be more easily rationalized), has been reported among computer abusers (Hafner and Markoff, 1991; Krauss and MacGahan, 1979; Parker, 1989). These rationalizations may be a symptom of high RD.

Deterrence research has found that stable psychological traits similar to RD are related to a predisposition to engage in crimes as well as certain other kinds of irresponsible behavior (Grasmick, et al., 1993; Tittle, 1980). These traits—low moral commitment and low self-control—also involve lack of commitment to internalized norms and an insensitivity to the suffering and needs of others (Gottfredson and Hirschi, 1990; Tittle, 1980). In summary, deterrence research also suggests that computer crime may be more closely related to RD than to the threat of legal sanctions or codes.

Hence, whether codes exist or not, those high in RD would tend to form unethical judgments and intentions, whereas those low in RD would not:

H3a: Those IS personnel low in RD will exhibit a greater tendency to judge a computer abuse as wrong than those high in RD.

H3b: Those IS personnel high in RD will exhibit a greater tendency than low RD personnel to agree that they would perpetrate a computer abuse.

Because there is a stable tendency to either accept or deny responsibility, it would be expected that codes of ethics pinpointing responsibility would affect individuals differently. Those who tend to deny responsibility would be more likely to be influenced by clear guidelines that prevent them from easily rationalizing unethical behavior. Those who tend to accept responsibility may not need such guidelines, since they would tend to think through consequences and envision their role in any resulting consequences.

Based on interviews with numerous computer criminals, Parker (1981, pp. 46, 63) concludes, "Once motivated to penetrate and use a system to his own ends, a perpetrator plans, plots, gathers information, organizes, conspires, and finally rationalizes all of his intentional acts." When such perpetrators are in this stage of moral drift deterrence efforts are believed to be especially effective at reminding the perpetrator of responsibilities (Parker, 1981).

Parker's conclusions are similar to proposals by deterrence researchers (e.g., Bachman, et al., 1992; Tittle, 1980) who suggest that some individuals may be so effectively restrained by their moral beliefs that sanctions associated with unethical behavior are irrelevant. Schwartz and Orleans (1967) found differential effects of sanctions and appeals to conscience on different people in their study of tax evasion. Individuals who are not restrained by their moral beliefs may need restraint provided by sanction threats or appeals to conscience. Bachman, et al. (1992) found support for such an interaction effect between individual differences and sanctions.

For these reasons, the present study hypothesizes that codes of ethics will have more influence on those higher in RD, whereas those lower in RD will show consistently higher levels of ethical judgment and intention and be less influenced by codes. In essence, if codes of ethics have an impact, it will be on those IS employees who tend to deny responsibility. Those high-RD employees whose organizations advance codes of ethics will be less able to rationalize all forms of computer abuse:

H4a: Codes of ethics will heighten the ethicality of the computer abuse judgments of high-RD personnel more than of low-RD personnel.

H4b: Codes of ethics will heighten the ethicality of the computer abuse intentions of high-RD personnel more than of low-RD personnel.

In statistical terms, a significant interaction effect of codes of ethics with RD will influence IS personnel's judgments and intentions concerning computer abuse. In other words, codes operate conditionally: the relationship between codes and ethical judgments and intentions depends on whether a person is high or low in RD. Such a relationship is a moderating relationship, with RD acting as the moderating variable (cf. Baron and Kenny, 1986).

The overall research model of this study is depicted in Figure 1.

Method

Both criminological and organizational behavior studies suggest that ethical judgments and intentions are issue-contingent (see Jones, 1991, for a discussion). Thus, a questionnaire with different vignettes was used to measure

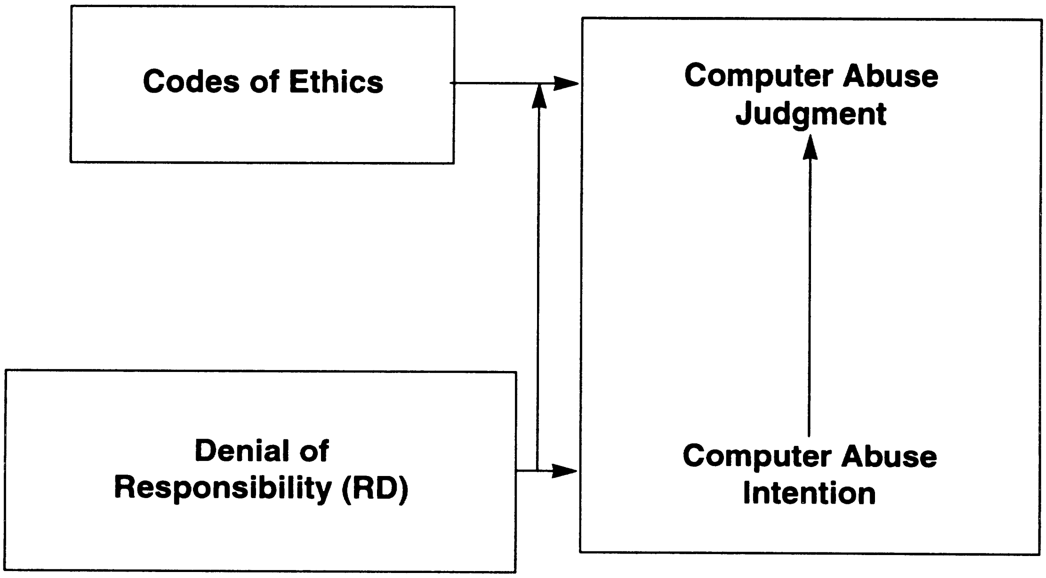

Figure 1. The Ethical Decision-Making Model Under Study

IS employees' judgments and intentions regarding different computer abuses.

Five vignettes were used: (1) cracking and using computer services by misidentification of self—adapted from Parker, et al. (1990, p. 57); (2) illegal software copying—adapted from Harrington (1989); (3) sabotaging a competitor's security system, identifying customers, and causing the system to "crash"—adapted from Parker (1980, p. 41); (4) writing and spreading viruses—adapted from Dejoie, et al. (1991, p. 164); and (5) fraud involving a programmer in a bank concealing an overdraft and "borrowing" funds temporarily by manipulating the computerized accounts—adapted from Parker (1980, p. 27.)[3] Vignettes have the advantage of providing a less-intimidating way to respond to sensitive issues and offering realistic scenarios that place the subject in a decision-making role. Moreover they avoid the subject's tendency to try to gain experimenter approval and so are commonly used in ethics and deterrence research (Alexander and Becker, 1978; Bachman, et al., 1992). In addition to the vignettes, the questionnaire consisted of potential rationalizations for the computer abuses, demographic data, and Schwartz's (1973) RD scale.

Sampling characteristics

After some initial testing on a convenience sample of students, the questionnaire was slightly revised and given to 219 IS employees in nine organizations in the northeastern Ohio area. MIS managers participating on a university advisory committee and MIS managers solicited through various contacts were encouraged to allow their employees to participate. Information on these companies and their codes of ethics is included in Table 1.

As shown in Table 1, some organizations communicate codes by having the employee sign the code, either upon employment or once per year. So it appears that the codes are being communicated to employees on a consistent basis. Analyses (not shown) were performed to study the effect of employee signing, sanctions in the code, whether sanctions were ever enforced, and the primary reason for the code. The result was that no effect of codes of ethics on computer abuse judgments and intentions was found. However, the lack of significance may be explained by the limited number of organizations in the sample having codes.

In this study, the nine organizations had, in total, 2077 IS employees, but a large time commitment per employee was involved. So after being instructed on the concept of random sampling, each MIS manager selected a small random sample of their IS employees. No statistically significant differences between companies with respect to the independent and dependent variables in this study were found.

The IS employees consisted of 80 programmer analysts, 78 analysts, 17 technical specialists, 15 managers or supervisors, 12 project managers, seven programmers, six security administrators, three not reported, and one information center specialist. Other characteristics of the employees are shown in Table 2.

The questionnaire was administered by the author so that the employees would be assured that the questionnaire was for research purposes only and not to be used by the employer. Moreover, the employees submitted the questionnaires anonymously and placed their questionnaires in a large box with a slot in the top, much like a ballot box.

Measures

RD Scale

The RD scale consisting of 28 items developed by Schwartz (1973) was used. The RD scale includes statements such as:

"You can't blame basically good people who are forced by their environment to be inconsiderate of others."

[3] Please contact the author for a copy of the questionnaire.

Table 1. Organizational Use of Codes of Ethics

Organization	Industry Type	Sample Size	Generic Code?	IS-Specific Code?	Respondent Signs Code?	Respondent Signs Every Year?	Generic: Number of Exposures to Code Over Prior 3 Yrs	IS-Specific: Number of Exposures to Code Over Prior 3 Yrs	Sanctions in Code?	Sanctions Ever Enforced?	Primary Reason for Code*
#1	Manufacturing	27	X	X	X	X	3	1	X	–	3
#2	Service	10	–	–							
#3	Manufacturing	18	X	–	X	X	3		–	–	3
#4	Manufacturing	34	X	–	X	X	3		X	–	2
#5	Service	17	X	–	X	–	1		X	X	(see note 2)
#6	Manufacturing	8	–	–							
#7	Service	3	X	X	(see note 1)						
#8	Service	62	–	–							
#9	Service	40	X	X	X	X	3	1	X	–	–
		219	6	3	5	4			4	1	

Note 1: Organization #7 did not provide this information, claiming it was proprietary.

Note 2: Organization #5 marked category "6 = Other" for primary reason and stated, "because it is the right thing to do. People ought to understand what is expected of them."

***Primary reason for code:**

1 = is a deterrent to employee misconduct because it hints that the employee will be punished if the employee breaks the code.

2 = is a deterrent to employee misconduct because it stipulates the punishment the employee will receive if the employee breaks the code.

3 = used to educate employees on acceptable behavior in the workplace. It is not for enforcement of proper behavior.

4 = provides evidence in any court system to show that the company is making a concerted effort to prevent and detect corporate misconduct.

5 = is good public relations; it makes the company appear more ethical and concerned about social issues.

6 = Other: Please describe: ________

Table 2. Demographic Characteristics of the Sample

	N	Percent
Gender:		
Male	134	61.5
Female	84	38.5
Education:		
High school	6	2.8
Some college	49	22.6
Bachelor's degree	92	42.4
Some graduate work	31	14.3
Master's degree	36	16.6
Post-master work	3	1.4
Social Class:		
Lower class	8	3.7
Lower middle class	54	24.7
Middle class	134	61.2
Upper middle class	23	10.5
Company Code of Ethics:		
Yes	139	63.5
No	80	36.5
Specific Code of Ethics:		
Yes	70	32.0
No	149	68.0

	Mean	Std. Dev.	Minimum	Maximum
Age	37.10	7.92	22.00	62.00
Work tenure	15.96	8.27	0	41.00

"When you consider how hard it is for an honest person to get ahead, it is easier to forgive those who deceive others in business."

"I wouldn't feel that I had to do my part in a group project if everyone else was lazy."

Previous studies using RD support its validity and reliability. Schwartz (1973) reports the RD scale of 28 items has a Cronbach alpha of .78 to .81 and a test-retest reliability over a seven- to 10-month period, under different testing conditions, of .81. Additional validity of the original instrument was supported by a correlation of -.01 with social desirability. Schwartz and Clausen (1970) found that the median of RD was not directly at the neutral category, but instead was slightly toward the accept responsibility side of the scale. Schwartz and Clausen used median splits to divide respondents into high vs. low RD categories. Such a division appears reasonable, despite a non-neutral midpoint, since agreeing to nearly any of the questions suggests some level of responsibility denial.

In this study, a five-point Likert scale ranging from 1 ("strongly agree") to 5 ("strongly disagree") was used and coded such that the higher the total score, the higher the responsibility denial. Consistent with Schwartz, this study found a Cronbach alpha of .83 and a mean slightly toward the accept responsibility side of the scale. The scale has a skewness of 0.18, which suggests that the curve is slightly skewed but still very close to a normal curve in shape. As a result, it is believed that the distribution of RD is appropriate for the statistical tests used in this study.

RD's convergent validity was assessed by whether it correlated with rationalizations. Rationalizations were measured by agreement or disagreement to statements following some of the vignettes: "Computer users like this one (who cracks into a system) provide a service because they point out computer system weaknesses"; "The manager was using the services she paid for and so had a right to do what she did (identify a competitor's customers)"; and "Because of the vice president's orders (to beat the competitors any way she could), the manager is not responsible for her actions (i.e., crashing the system)." Together these three questions had a Cronbach alpha of .72.

Rationalization tendency was also measured by the subject's agreement/disagreement to four "Robin Hood" statements created specifically for this study: "Harming an individual is more wrong than harming a company"; "Stealing from companies is not as wrong as stealing from individuals"; "It is OK to steal from a large company if it benefits an individual"; and "It is OK to take advantage of a big company whenever possible, even if it means harming the company." These four Robin Hood statements loaded on one factor in a factor analysis and were found to have a Cronbach alpha of .80.

Since RD is associated with rationalizations, it was expected and found that RD is positively correlated with these two rationalization measures (see Table 3). In summary, this study found that the RD scale has good reliability and convergent validity.

Codes of Ethics

The manager of the IS department for each of the nine companies was asked whether the company had a code of ethics and/or an IS-specific code of ethics. Using the immediate manager's perceptions rather than employees' perceptions avoids a priming effect that would likely occur should the employees be asked about their awareness of codes of ethics.

Ethical Judgments and Intentions

It was the objective of the study to obtain judgment and intention scores for each person on each of the five computer abuses. Each person's agreement (1=strongly agree) or disagreement (5=strongly disagree) to statements such as whether the person in the vignette "was justified" or "did nothing wrong" and "I would do the same thing if I knew how" were averaged to obtain measures of judgment and intention, respectively. Therefore, the higher the judgment or intention score, the higher the presumed ethicality.

Construct validity of the dependent measures was checked by a factor analysis using varimax rotation of all statements related to computer abuse. Five computer abuse factors were found, but two unexpected factors mixed virus and fraud statements. These statements seemed to rotate into these two factors based on the level of impact to others, a finding confirmed by subjects' answers to open-ended statements included in the questionnaire. The first factor consisted of statements about viruses that erased files or ignored some of the user's commands, as well as two fraud statements about "borrowing money" by manipulating another person's computer account. The second factor included virus statements relating to creating a virus that wished the user to "have a nice day," and fraud statements on adjusting the bank's accounting system to avoid a service charge. Overall the first fraud/virus factor appears to include the more damaging aspects of fraud and viruses. The first factor also suggests greater impact to other individuals, rather than to organizations. Therefore this first factor was labelled "damaging fraud/viruses." The second factor was labelled "less damaging fraud/viruses."

The other factors clearly separated into sabotage, software copying, and cracking. The means, standard deviations, correlations, and reliabilities of the measures are shown in Table 3.

Results and Discussion

Hypotheses 1a through 2b were tested using ANOVA analyses of the main effects variables (see Table 4). A discouraging note for code of ethics advocates is that generic codes of ethics seem to have no direct, significant ($p < .05$) effect on computer abuse judgments and intentions. In other words, there is support for the null hypothesis 1: i.e., there is no main effect of generic codes of ethics. Although only a small effect size would be expected based on deterrence research (Cook, 1980), this study's lack of a main effect is probably not due to low power (the probability of accepting the null hypothesis when it is false), i.e., even assuming a low effect size, with a corresponding R2 of only 2–5%, the power of the test is between .56 and .90, suggesting a 56–90% chance that the test will find the relationship if it exists (cf. Cohen, 1988).

Similarly, IS-specific codes had little relationship to the computer abuses, with the exception of sabotage judgments and intentions ($F = 4.98$, $p < .05$ and $F = 4.06$, $p < .05$, respectively). Thus, there is mixed support for Hypothesis 2.

Because RD is conceptualized as a continuous variable (but measured using ordinal scales), simple Spearman correlation analyses shown in Table 3 were used to test Hypothesis 3. RD was strongly correlated with all computer abuse judgments and intentions. In summary, there is strong support for Hypothesis 3.

Finally, Hypothesis 4 of this research suggests that ethics codes will have a greater effect on those high in RD. This is known as an interaction or moderated effect, i.e., codes may be effective for those high in RD but ineffective for those low in RD.

In keeping with Baron and Kenny's (1986) suggestion that unstandardized (not betas) regression coefficients be used in moderated relationships, the hypothesized relationship was tested by least squares analysis using the general linear models (GLM) procedure of SAS. Such regression coefficients are not affected by differences in the variances in the independent variable or differences in measurement error in the dependent variable (Baron and Kenny, 1986). In addition, this study found no differential measurement error in the independent variable across levels of the moderator, a situation that could bias the results. Finally, rank-ordered tests, as suggested by Paternoster, et al. (1982) for use in deterrence research, showed no difference in the outcomes of the hypotheses tests. So continuous data was used in the regression and is the basis for the following discussion.

The multiple regression was run, first without the interaction effect, then with the interaction effect, as suggested by Cohen and Cohen (1975) and presented in Table 5. To reduce the threat of multicollinearity in the interactive model, RD was centered on zero, as suggested by Cronbach (1987) and supported by Jaccard, et al. (1990).

An encouraging finding for code of ethics advocates is that generic company codes do seem to improve some judgments and intentions of high-RD individuals. For "sabotage" and "damaging fraud/viruses" judgments and for "less damaging fraud/viruses" intentions, Hypothesis 4 is supported; for all other judgments and intentions, Hypothesis 4 was not supported. Where Hypothesis 4 is supported, the interaction of RD and the generic code add slightly to the variance explained (as shown by the improvement over the R^2 without the interaction). More likely to be a chance effect (at $p < .10$) were the interactions for the "less damaging fraud/viruses" judgment and the "damaging fraud/viruses" intention.

Although it is encouraging that RD and generic codes interact, less encouraging is the result of the test for interaction of RD with IS-specific codes. No interaction effects of IS-specific codes were significant, suggesting that IS codes do not clarify responsibility for high RD individuals. The non-significance may be partially due to low power, estimated at about

Table 3. Simple Statistics, Correlations, and Reliabilities of the Measures

			Std.															
	Variable	Mean	Dev.	Min.	Max.	1	2	3	4	5	6	7	8	9	10	11	12	13
1	RD	2.29	0.37	1.14	3.64	(.83)												
2	Robin Hood	1.94	0.61	1.00	4.25	0.44 0.000	(.80)											
3	Rationalization	1.61	0.59	1.00	4.00	0.35 0.000	0.38 0.000	(.72)										
4	Cracking Judgment	4.55	0.57	1.50	5.00	–0.347 0.000	–0.378 0.000	–0.565 0.000	(.68)									
5	Cracking Intention	4.38	0.66	1.75	5.00	–0.45 0.000	–0.47 0.000	–0.53 0.000	0.75 0.000	(.90)								
6	Copy S/W Judgment	4.02	0.73	1.00	5.00	–0.30 0.000	–0.37 0.000	–0.36 0.000	0.26 0.000	0.25 0.000	(.85)							
7	Copy S/W Intention	3.34	1.14	1.00	5.00	–0.29 0.000	–0.29 0.000	–0.22 0.001	0.20 0.003	0.33 0.000	0.53 0.000	(1.00)						
8	Damaging Judgment	4.79	0.37	3.75	5.00	–0.38 0.000	–0.44 0.000	–0.54 0.000	0.50 0.000	0.51 0.000	0.22 0.001	0.13 0.049	(.91)					
9	Damaging Intention	4.77	0.39	3.25	5.00	–0.37 0.000	–0.46 0.000	–0.53 0.000	0.48 0.000	0.51 0.000	0.20 0.003	0.17 0.011	0.89 0.000	(.89)				
10	Less Damaging Judgment	4.48	0.58	2.00	5.00	–0.34 0.000	–0.46 0.000	–0.56 0.000	0.41 0.000	0.49 0.000	0.23 0.001	0.14 0.046	0.67 0.000	0.68 0.000	(.70)			
11	Less Damaging Intention	4.52	0.62	2.50	5.00	–0.38 0.000	–0.46 0.000	–0.56 0.000	0.46 0.000	0.59 0.000	0.22 0.001	0.20 0.003	0.68 0.000	0.71 0.000	0.85 0.000	(.64)		
12	Sabotage Judgment	3.78	0.42	2.00	4.17	–0.38 0.000	–0.38 0.000	–0.73 0.000	0.53 0.000	0.50 0.000	0.31 0.000	0.24 0.000	0.58 0.000	0.54 0.000	0.58 0.000	0.60 0.000	(.85)	
13	Sabotage Intention	4.49	0.58	2.50	5.00	–0.35 0.000	–0.37 0.000	–0.75 0.000	0.52 0.000	0.52 0.000	0.32 0.000	0.26 0.000	0.55 0.000	0.55 0.000	0.61 0.000	0.61 0.000	0.84 0.000	(.79)

Numbers in parentheses on the diagonal are Cronbach alphas. The number under each Spearman correlation is the p-value.

Table 4. One-Way ANOVA of Main Effects Variables

Variables	Crack	Copy Software	Damaging Fraud/Viruses	Less Damaging Fraud/Viruses	Sabotage
Generic Code of Ethics:					
Judgment	0.04	0.34	1.61	2.15	1.59
Intention	0.67	0.02	0.25	3.66+	0.35
I.S.-Specific Code					
Judgment	0.18	0.06	1.34	0.90	4.98*
Intention	1.08	0.27	1.31	1.97	4.06*
df	218	216	215	214	218

Table values represent F values.
+p < .10; * p < .05.

0.60 for a small effect size (or R2 equal to two percent), but larger effect sizes would greatly improve the power of the test. At the minimum, then, the results of this study can be said to find no medium to large effects of IS-specific codes on high-RD individuals.

Although few statistical tests showed an effect of codes of ethics on computer abuse judgments or intentions, it is important that such findings be disseminated to the IS research community and to IS practitioners. Specifically, it is important for scientific purposes. One persuasive criticism of current published studies is that they are not representative of the population of studies conducted, since generally only studies with significant results are published (Rosenthal, 1979; 1991). Rosenthal suggests that ignoring studies with non-significant statistical tests can result in erroneous conclusions, since a p<.05 test will result in approximately five percent of the studies finding significant relationships when there really are none (type I error). In addition, an individual study with non-significant results does not have the power that meta-analytic procedures do, since meta-analytic procedures combine many individual studies, thereby lowering the incidence of type II errors (failing to reject the null hypotheses that are false). As a result, even non-significant results may lead to significant findings when combined into meta-analyses at a later date (cf. Rosenthal, 1979; 1991).

Limitations and Constraints

The above findings must be viewed with the limitations of the study in mind. For one, codes are just one aspect of an ethical corporate culture. Although they are typically the first ethics-oriented effort made by most companies, other influences may be at work.

Employee awareness and perceptions of the codes were not measured in order to avoid a priming effect. However, employees may be unaware of the codes despite their immediate manager's awareness. In particular, this may be the case with the IS-specific code, where the number of employee exposures to the code was limited.

Even if employees are aware of the code, employees may ignore the codes if they are disaffected at work or find the codes and admonitions in conflict with personal or subgroup norms (Badaracco and Webb, 1995; Donaldson and Dunfee, 1994). Although this may be viewed as a limitation of the study, it is also a strength—the fact that codes have any effect in the larger corporate environment is a significant finding.

Another limitation to the above research is the diversity of ethics codes now implemented across organizations. This problem occurs across generic codes (Cressey and Moore,

Table 5. Least Squares Analysis of Main Effects and Interactions With Denial of Responsibility

Variables	Cracking		Copy Software		Damaging Fraud/Viruses		Less Damaging Fraud/Viruses		Sabotage	
	Main Effects	Interaction	Main Effects	Interaction	Main Effects	Interaction	Main Effects	Interaction	Main Effects	Interaction
Generic Code of Ethics and Judgment										
Intercept	4.58	4.58	4.11	4.11	4.88	4.88	4.65	4.65	3.89	3.89
Generic code	–0.02	–0.06	–0.07	0.03	–0.07	0.64*	–0.12	0.71	–0.08	0.58+
Denial of responsibility	–0.58***	–0.60*	–0.57***	–0.51	–0.36***	0.05	–0.54***	–0.06	–0.47***	–0.08
Generic code * RD		0.02		–0.04		–0.31*		–0.37+		–0.29*
F-statistic	18.91***	12.55***	10.23***	6.80***	17.51***	13.78***	16.14***	11.87***	23.58***	17.22***
R-squared	0.15	0.15	0.09	0.09	0.14	0.16	0.13	0.14	0.18	0.19
Change in R-squared		–		–		0.02		0.01		0.01
Generic Code of Ethics and Intention										
Intercept	4.50	4.50	3.39	3.39	4.81	4.81	4.76	4.76	4.57	4.57
Generic code	–0.09	0.36	–0.04	0.70	–0.03	0.58 +	–0.17*	1.01*	–0.06	0.39
Denial of responsibility	–0.73***	–0.47	–0.88***	–0.46	–0.39***	–0.03	–0.63***	0.06	–0.57***	–0.31
Generic code * RD		–0.20		–0.32		–0.27+		–0.52*		–0.20
F-statistic	23.10***	15.61***	9.83***	6.73***	16.51***	12.34***	20.37***	15.72***	17.26***	11.79***
R-squared	0.18	0.18	0.09	0.09	0.13	0.15	0.16	0.18	0.14	0.14
Change in R-squared		–		–		0.02		0.02		–
Specific Code and Judgment										
Intercept	4.56	4.55	3.94	3.93	4.87	4.87	4.58	4.58	3.98	3.97
I.S.-specific Code	–0.01	–0.72	0.05	–0.12	–0.05	0.01	–0.06	–0.21	–0.12*	–0.42
Denial of Responsibility	–0.58***	–1.09**	–0.56***	–0.69	–0.36***	–0.32	–0.54***	–0.64+	–0.46***	–0.68***
I.S.-specific Code * RD		0.31		0.08		0.02		0.07		0.14
F-Statistic	18.85***	13.47***	10.10***	6.73***	16.89***	11.22***	14.98***	9.98***	24.86***	16.85***
R-squared	0.15	0.16	0.09	0.09	0.14	0.14	0.12	0.12	0.19	0.19
Change in R-squared		0.01		–		–		–		–
Specific Code and Intention										
Intercept	4.50	4.49	3.14	3.13	4.85	4.85	4.69	4.69	4.73	4.72
I.S.-specific code	–0.07	–0.37	0.12	–0.05	–0.05	–0.08	–0.10	–0.09	–0.14+	–1.01*
Denial of responsibility	–0.73***	–0.94*	–0.89***	–1.01	–0.38***	–0.40+	–0.62***	–0.61	–0.56***	–1.19***
I.S.-specific code * RD		0.13		0.08		0.01			–0.01	0.38+
F-statistic	22.85***	15.30***	10.13***	6.73***	16.84***	11.18***	18.55***	12.31***	18.93***	13.95***
R-squared	0.18	0.18	0.09	0.09	0.14	0.14	0.15	0.15	0.15	0.16
Change in R-squared		–		–		–		–		0.01
df	218		216		215		214		218	

Note: Numbers in the table represent B coefficients. + p<.10; * p<.05; ** p<.01; *** p< .001.

1983) and so may be especially problematic for IS-specific codes. IS-specific codes are likely to be inconsistent in their attention to issues such as viruses, copyrights, cracking, etc., since even codes of IS professional organizations such as ACM and DPMA are inconsistent (Oz, 1992; 1994a). Further content analysis of both generic and IS-specific codes of ethics is needed to see what computer abuses are covered by the codes.

Lack of findings for the effect of codes may also be due to a number of factors: sampling problems, such as the sample being taken from one area of the country; low variability in judgments and intentions concerning computer abuse; and slightly lower power in some of the statistical tests. Future researchers may wish to keep such factors in mind for future studies.

Implications and Conclusions

Although inexpensive and relatively widespread, codes of ethics seem to have some effect, albeit a small one, on computer abuse judgments and intentions. IS-specific codes have a direct effect on sabotage judgments and intentions. Generic codes affect those high in responsibility denial and so improve some computer abuse judgments and intentions. The computer abuses affected by generic codes' interaction with RD include both damaging and less damaging fraud/viruses as well as sabotage. In summary, codes of ethics do have an effect, but they are related to only certain abuses.

Developers of codes of ethics can find some comfort in the finding that codes have any influence at all. Often a code is viewed as a form or procedure that is looked at once and then "filed." This research did find a relationship between codes and certain forms of computer abuse, and if that relationship should result in the avoidance of even a single occurrence of computer abuse, then the code must be considered a success.

Future research is needed to clarify why the effect of codes is sporadic. It may be that the codes to which the IS employees were exposed include clarifications and sanctions for only some of the abuses studied here. Moreover, there may not be consensus on what is proper behavior for some computer acts (cf. Conger, et al., 1995). Future research should compare the content of codes of ethics with specific IS issues in order to analyze whether sanctions are included as part of the codes and to determine whether IS personnel are aware of the code contents and sanctions.

The direct effect of IS-specific codes on sabotage judgments and intentions is also a relationship that warrants further study. That IS-specific codes had no impact on other forms of abuse is in line with the findings of deterrence researchers that a "precise" effect—one where a sanction or sanction threat is attached to a particular offense—has no advantage over generalized sanctions. That the "diffuse effect" of generic codes has more effect overall suggests that generic codes may be sufficient for deterring computer abuse. However, IS-specific codes' effect on sabotage suggests further study is needed to see if the IS-specific codes' main effect is repeatable, and, if so, why its effect in this case is specific to computer sabotage.

Because codes have been found to have some effect in this study, managers may wish to implement codes but strengthen the codes' effect, where possible. General deterrence theory, which has effectively guided this study, suggests that one reason for the sporadic effect of codes may be the perception that there is low probability of being caught. Yet publicizing and prosecuting computer abuse has been found to be a rare event (Loch, et al., 1992; Sokolik, 1980; Straub and Nance, 1990). Managers may do well to reinforce their codes of ethics by making ad hoc reminders of policy whenever an event, such as a scandal or computer abuse, brings a particular policy into the forefront (Krauss and MacGahan, 1979; Straub, et al., 1993). Alternatively, annual security briefings may have deterrent value, particularly if they emphasize consequences of losses for the organization and for the employees, including sanctions described or implied by the codes (Parker, 1981). Thus, management's challenge may be the application of the codes of ethics rather than the creation of the codes (Bequai, 1983).

The need for such management support is in keeping with recommendations of other ethics researchers who have suggested that codes are effective only where they gain the day-to-day support of top management (Fimbel and Burstein, 1990; Oz, 1994b; Parker, 1981). Moreover, top management support may be more effective than codes of ethics because the effect of legal sanctions is not as great as the effects of other sources of control, such as future employment chances and opportunities (Grasmick and Bursik, 1990; Williams and Hawkins, 1986). Management sets the moral climate of the company, and employees take their cues from management on how to get ahead (Badaracco and Webb, 1995; Krauss and MacGahan, 1979). In general, employees will find it expedient to attend to the admonitions of top management.

Another management tactic is also suggested by recent deterrence research that has found that social and personal costs, such as conscience, shame, and significant others, can act as stronger deterrents against crime than formal penalties (e.g., Grasmick and Bursik, 1990; Nagin and Paternoster, 1993). Similarly, most computer criminals are bothered by the shame, loss of respect, and anguish in confrontations with their friends, associates, victims, and family (Parker, 1981). Therefore, management may wish to encourage the informal sanctions of peers and significant others where possible, and researchers may wish to measure perceptions and effects of both formal and informal sanctions in future research on codes of ethics.

Nevertheless, use of formal and informal sanctions is not fool-proof. The sporadic impact of codes in this study is consistent with recent deterrence research that has found that respondents' moral beliefs and commitment are more important sources of social control than formal or informal sanction threats (Bachman, et al., 1992). Deterrence theory and computer security researchers (e.g., Baskerville, 1988; Parker, 1983; Sokolik, 1980; Tittle, 1980) likewise have suggested that deterrent controls such as codes of ethics may only serve to reinforce other controls, for codes by themselves may not have a major effect on behavior. Such a suggestion is supported by this study, which found that codes interact with responsibility denial (rather than act as a main effect themselves) when affecting computer abuse judgments and intentions.

The interaction effect of generic codes with denial of responsibility may suggest why studies on codes of ethics have heretofore had mixed results: i.e., codes of ethics appear to have different effects on different people, depending on an individual's personality. In this case, ANOVA analysis suggested that generic company codes had no effect on ethical judgments and intentions; yet there was a significant effect when the interaction with responsibility denial was taken into account. Researchers on the impact of codes of ethics are encouraged to examine interaction effects in the future. Managers should be aware that codes and other forms of management control will have different results, depending on an individual's sense of responsibility. Managers will need to focus on those who tend to deny responsibility. Those individuals are less likely to form ethical judgments and intentions and are more likely to be deterred by clear guidelines.

In conclusion, a major finding of this study is the effect of the enduring psychological trait of denial of responsibility and how management controls may deter unethical judgments and intentions through denial of responsibility. The effect of codes of ethics is sporadic and weak in comparison to this enduring psychological trait, but codes do have some effect on high-RD individuals. As a result, management can expect codes to have some impact but cannot expect to control employee behavior solely through codes of ethics.

In addition to codes, management should implement carefully planned security measures that focus on aspects of responsibility, such as clear job descriptions and expectations; careful hiring and placement practices;

job rotation; separation of responsibility in input, operation, programming, and output; audit logs and periodic audits; system access controls; and employee morale monitoring (cf. Baskerville, 1993; Fisher, 1984; Krauss and MacGahan, 1979; Parker, 1981). Management should identify, by name, individuals who will be held personally responsible for each and every specified asset (Carroll, 1987). Holding individuals personally responsible should reduce the rationalizations available to those who tend to use them to deny responsibility.

Therefore, at minimum, managers must use a multifaceted approach to deterring computer abuse and not depend upon the simple solution of codes of ethics. The use of tactics, such as codes of ethics, for purposes of general deterrence should not be overstated but should not be discarded either. The strong effect of denial of responsibility, its associated rationalizations, and the effect of generic codes on those high in denial of responsibility suggest that "it also seems necessary that the rationalizations of the offender be penetrated and that offenders be made to confront less palatable interpretations of what they have done" (Geis and Meier, 1979, p. 440). Finally, researchers and management alike may find it fruitful to discover how clear guidelines, sanction threats, and knowledge of sanctions can be communicated to IS personnel, via codes of ethics and other mechanisms.

Acknowledgements

The author would like to thank Gerardine DeSanctis, the associate editor and three anonymous reviewers for their many helpful suggestions. A "thank you" is also extended to Tor Guimaraes, who made suggestions on a semifinal version of the paper.

References

Ajzen, I. and Fishbein, M. *Understanding Attitudes and Predicting Social Behavior*, Prentice-Hall, Englewood Cliffs, NJ, 1980.

Alexander, C.S. and Becker, H.J. "The Use of Vignettes in Survey Research," *Public Opinion Quarterly* (42:1), 1978, pp. 93–104.

American Bar Association (ABA). *Report on Computer Crime*, Task Force on Computer Crime Section of Criminal Justice, 1800 M Street, Washington, D.C., 1984.

Bachman, R., Paternoster, R., and Ward, S. "The Rationality of Sexual Offending: Testing a Deterrence/Rational Choice Conception of Sexual Assault," *Law & Society Review* (26:2), 1992, pp. 343–372.

Badaracco, J.L. and Webb, A. "Business Ethics: A View From the Trenches," *California Management Review* (37:2), 1995, pp. 8–28.

Baron, R.M. and Kenny, D.A. "The Moderator–Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations," *Journal of Personality and Social Psychology* (51:6), 1986, pp. 1173–1182.

Baskerville, R. *Designing Information Systems Security*, John Wiley & Sons Ltd, Chichester, U.K., 1988.

Baskerville, R. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys* (25:4), 1993, pp. 375–414.

Bequai, A. *How to Prevent Computer Crime: A Guide for Managers*, John Wiley & Sons, New York, 1983.

Berenbeim, R.E. *Corporate Ethics Practices*, The Conference Board, New York, 1992, pp. 7–10.

BloomBecker, B. *Spectacular Computer Crimes*, Dow Jones-Irwin, Homewood, IL, 1990.

Canning, R.G. "Information Security and Privacy," *EDP Analyzer* (24:2), 1986, pp. 1–11.

Carroll, J.M. *Computer Security* (2nd ed.), Butterworths, Boston, MA, 1987.

Center for Business Ethics. "Are Corporations Institutionalizing Ethics?" *Journal of Business Ethics* (5:2), April 1986, pp. 85–91.

Center for Business Ethics. "Instilling Ethical Values in Large Corporations," *Journal of*

Business Ethics (11:11), November 1992, pp. 863–867.

Cohen, J. *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.), Lawrence Erlbaum Associates, Hillsdale, NJ, 1988.

Cohen, J. and Cohen, P. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*, Erlbaum, Hillsdale, NJ, 1975.

Conger, S., Loch, K.D., and Helft, B.L. "Ethics and Information Technology Use: A Factor Analysis of Attitudes to Computer Use," *Information Systems Journal* (5:3), July 1995, pp.161–184.

Cook, P.J. "Research in Criminal Deterrence: Laying the Groundwork for the Second Decade," in *Crime and Justice: An Annual Review of Research* (2), N. Morris and M. Tonry (eds.), The University of Chicago Press, Chicago, 1980.

Cressey, D.R. and Moore, C.A. "Managerial Values and Corporate Codes of Ethics," *California Management Review* (25:4), 1983, pp. 53–77.

Cronbach, L.J. "Statistical Tests for Moderator Variables: Flaws in Analysis Recently Proposed," *Psychological Bulletin* (102:3), 1987, pp. 414–417.

Dejoie, R., Fowler, G., and Paradice, D. *Ethical Issues in Information Systems*, Boyd & Fraser Publishing Company, Boston, 1991.

Donaldson, T. and Dunfee, T.W. "Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory," *Academy of Management Review* (19:2), 1994, pp. 252–284.

Ethics Resource Center and the Behavior Research Center. *Ethics Policies and Programs in American Business*, Ethics Resource Center, Washington, D. C., 1990.

Fimbel, N. and Burstein, J.S. "Defining the Ethical Standards of the High-Technology Industry," *Journal of Business Ethics* (9), 1990, pp. 929–948.

Fisher, R.P. *Information Systems Security*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1984.

Forcht, K.A. *Computer Security Management*, Boyd & Fraser Publishing Company, Danvers, MA, 1994.

Ford, R.D. and Richardson, W.D. "Ethical Decision Making: A Review of the Empirical Literature," *Journal of Business Ethics* (13:3), March 1994, pp. 205–221.

Geis, G. and Meier, R.F. "The White-Collar Offender," in *Psychology of Crime and Criminal Justice*, H. Toch (ed.), Holt, Rinehart and Winston, New York, 1979, pp. 427–443.

Gottfredson, M.R. and Hirschi, T. *A General Theory of Crime*, Stanford University Press, Stanford, CA, 1990.

Grasmick, H.G. and Bursik, R.J. "Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model," *Law & Society Review* (24:3), 1990, pp. 837–861.

Grasmick, H.G., Tittle, C.R., Bursik, R.J., and Arneklev, B.J. "Testing the Core Empirical Implications of Gottfredson and Hirschi's General Theory of Crime," *Journal of Research in Crime and Delinquency* (31:1), February 1993, pp. 5–29.

Hafner, K. and Markoff, J. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon & Schuster, New York, 1991.

Harrington, S.J. "Why People Copy Software and Create Computer Viruses: Individual Characteristics or Situational Factors," *Information Resources Management Journal* (2:3), 1989, pp. 28–37.

Jaccard, J., Turrisi, R., and Wan, C.K. *Interaction Effects in Multiple Regression*, SAGE Publications, Inc., Newbury Park, CA, 1990.

Johnson, D.G. "The Public-Private Status of Transactions in Computer Networks," in *The Information Web: Ethical and Social Implications of Computer Networking*, C.C. Gould (ed.), Westview Press, Boulder, CO, 1989, pp. 37–55.

Johnson, D.G. and Mulvey, J.M. "Accountability and Computer Decision Systems," *Communications of the ACM* (38:12), 1995, pp. 58–64.

Jones, T.M. "Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model," *Academy of Management Review* (16:2), 1991, pp. 366–395.

Kohlberg, L. and Candee, D. "The Relationship of Moral Judgment to Moral Action," in *Morality, Moral Behavior, and Moral*

Development, W.M. Kurtines and J.L. Gewirtz (eds.), John Wiley & Sons, New York, 1984, pp. 52–73.

Krauss, L. and MacGahan, A. *Computer Fraud and Countermeasures*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1979, pp. xi–xii.

Ladd, J. "The Quest for a Code of Professional Ethics: An Intellectual and Moral Confusion," in *Ethical Issues in the Use of Computers*, D.G. Johnson and J.W. Snapper (eds.), Wadsworth Publishing Company, Belmont, CA, 1985, pp. 8–13.

Laudon, K.C. "Ethical Concepts and Information Technology," *Communications of the ACM* (38:12), 1995, pp. 33–39.

Loch, K.D., Carr, H.H., and Warkentin, M.E. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), June 1992, pp. 173–186.

Manley, W.J. *Executive's Handbook of Model Business Conduct Codes*, Prentice-Hall, Englewood Cliffs, NJ, 1991, pp. 3–10.

Mathews, M.C. "Codes of Ethics: Organizational Behavior and Misbehavior," in *Research in Corporate Social Performance and Policy*, W.C. Frederick and L.E. Preston (eds.), JAI Press, Inc., Greenwich, CT, 1987, pp. 107–130.

Metzger, M., Dalton D.R., and Hill, J.W. "The Organization of Ethics and the Ethics of Organizations: The Case for Expanded Organizational Ethics Audits," *Business Ethics Quarterly* (3:1), January, 1993, pp. 27–43.

Nagin, D. "General Deterrence: A Review of the Empirical Evidence," in *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*, A. Blumstein, J. Cohen, and D. Nagin (eds.), National Academy of Sciences, Washington, D.C., 1978, pp. 95–139.

Nagin, D.S. and Farrington, D.P. "The Stability of Criminal Potential from Childhood to Adulthood," *Criminology* (30:2), 1992, pp. 235–259.

Nagin, D.S. and Paternoster, R. "Enduring Individual Differences and Rational Choice Theories of Crime," *Law & Society Review* (27:3), 1993, pp. 467–496.

Oz, E. "Ethical Standards for Information Systems Professionals: A Case for a Unified Code," *MIS Quarterly* (16:4), December 1992, pp. 423–433.

Oz, E. *Ethics for the Information Age*, Wm. C. Brown Communications, Inc., Dubuque, IA, 1994a.

Oz, E. "When Professional Standards Are Lax: The CONFIRM Failure and Its Lessons," *Communications of the ACM* (37:10), October, 1994b, pp. 29–36.

Paradice, D.B. and Dejoie, R.M. "The Ethical Decision-Making Processes of Information Systems Workers," *Journal of Business Ethics* (10), 1991, pp. 1–21.

Parker, D.B. *Ethical Conflicts in Computer Science and Technology*, American Federation of Information Processing Societies (AFIPS) Press, Reston, VA, 1980.

Parker, D.B. *Computer Security Management*, Reston Publishing Co., Inc., Prentice-Hall Co., Reston, VA, 1981.

Parker, D.B. *Fighting Computer Crime*, Charles Scribner's Sons, New York, 1983, p. 304.

Parker, D.B. *Computer Crime: Criminal Justice Resource Manual* (2nd ed.), National Institute of Justice, U.S. Department of Justice, 1989, pp. 7–9.

Parker, D.B., Swope, S., and Baker, B.N. *Ethical Conflicts in Information and Computer Science, Technology, and Business*, QED Information Sciences, Inc., Wellesley, MA, 1990.

Paternoster, R., Saltzman, L.E., Chiricos, T.G., and Waldo, G.P. "Criminology: Perceived Risk and Deterrence: Methodological Artifacts in Perceptual Deterrence Research," *The Journal of Criminal Law & Criminology* (73:3), 1982, pp. 1238–1258.

Pearson, F.S. and Weiner, N.A. "Criminology: Toward an Integration of Criminological Theories," *The Journal of Criminal Law & Criminology* (76:1), 1985, pp. 116–150.

Pitt, H.L. and Groskaufmanis, K.A. "Minimizing Corporate Civil and Criminal Liability: A Second Look at Corporate Codes of Conduct," *The Georgetown Law Journal* (78), 1990, p. 1559–1654.

Rest, J.R. "The Major Components of Morality," in *Morality, Moral Behavior, and Moral Development*, W.M. Kurtines and J.L. Gerwitz (eds.), Wiley, New York, 1984.

Rest, J.R. *Moral Development: Advances in Research and Theory*, Praeger Publishers, New York, 1986.

Rifkin, G. "Are Corporate Codes Enough? Maybe Not," *Computerworld*, October 14, 1991, pp. 87.

Robin, D., Giallourakis, M., David, F.R., and Moritz, T.E. "A Different Look at Codes of Ethics," *Business Horizons* (32:1), January–February 1989, pp. 66–73.

Rosenthal, R. "The 'File Drawer Problem' and Tolerance for Null Results," *Psychological Bulletin* (86:3), 1979, pp. 638–641.

Rosenthal, R. *Meta-Analytic Procedures for Social Research* (revised edition), Sage Publishing, Newbury Park, CA, 1991.

Samuelson, P. "Can Hackers Be Sued for Damages Caused by Computer Viruses?" *Communications of the ACM* (32:6), June 1989, pp. 666–669.

Schwartz, R.D. and Orleans, S. "On Legal Sanctions," *University of Chicago Law Review* (34:2) Winter 1967, pp. 274–300.

Schwartz, S.H. "Normative Explanations of Helping Behavior: A Critique, Proposal, and Empirical Test," *Journal of Experimental Social Psychology* (9:4), July 1973, pp. 49–364.

Schwartz, S.H. "Normative Influences on Altruism," in *Advances in Experimental Social Psychology* (10), L. Berkowitz (ed.), Academic Press, New York, 1977, pp. 221–279.

Schwartz, S.H. and Clausen, G.T. "Responsibility, Norms, and Helping in an Emergency," *Journal of Personality and Social Psychology* (16:2), 1970, pp. 299–310.

Shotton, M.A. *Computer Addiction? A Study of Computer Dependency*, Taylor & Francis, London, 1989.

Sokolik, S.L. "Computer Crime—The Need for Deterrent Legislation," *Computer/Law Journal* (2:2), 1980, pp. 353–383.

Staub, E. *Positive Social Behavior and Morality: Social and Personal Influences*, Academic Press, New York, 1978.

Stevens, B. "An Analysis of Corporate Ethical Code Studies: 'Where Do We Go From Here?'" *Journal of Business Ethics* (13:1), January 1994, pp. 63–69.

Straub, D.W. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), 1990, pp. 255–276.

Straub, D.W. and Nance, W.D. "Discovering and Disciplining Computer Abuse in Organizations," *MIS Quarterly* (14:1), March 1990, pp. 45–55.

Straub, D.W., Carlson, P.J., and Jones, E.H. "Deterring Cheating by Student Programmers: A Field Experiment in Computer Security," *Journal of Management Systems* (5:1), 1993, pp. 33–48.

Suedfeld, P., Hakstian, A.R., Rank, D.S., and Ballard, E.J. "Ascription of Responsibility as a Personality Variable," *Journal of Applied Social Psychology* (15:3), 1985, pp. 285–311.

Tittle, C.R. *Sanctions and Social Deviance: The Question of Deterrence*, Praeger Publishers, New York, 1980.

Vitell, S.J. and Davis, D.L. "Ethical Beliefs of MIS Professionals: The Frequency and Opportunity for Unethical Behavior," *Journal of Business Ethics* (9:1), January 1990, pp. 63–70.

Weaver, G.R. "Corporate Codes of Ethics: Purpose, Process and Content Issues," *Business & Society* (32:1), 1993, pp. 44–58.

Whiteside, T. *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud*, Thomas Y. Crowell Company, New York, 1978.

Williams, K.R. and Hawkins, R. "Perceptual Research on General Deterrence: A Critical Review," *Law and Society Review* (20:4), 1986, pp. 545–572.

About the Author

Susan J. Harrington is an associate professor of information systems at Georgia College & State University in Milledgeville, Georgia. She previously worked in information systems for 12 years at several large companies in northeastern Ohio and later became a tenured faculty member at Kent State University Stark Campus. Her Ph.D. is in MIS from Kent State University. She has published articles in the *Training & Development Yearbook*, *Academy*

of Management Executive, *Data Base*, *Computer Personnel*, *Information Resources Management Journal*, *Security, Audit & Control Review*, *Journal of Fixed Income*, *Review of Business*, and *Journal of Systems Management*. Among her current interests are computer crime, ethical decision making, and the role of corporate culture in the implementation of IT innovations.

Appendix

Samples of Codes of Ethics[4]

Part of a Generic Code of Ethics that applies to IS employees:

> During and after employment, employees shall not, without proper authority, give or release to anyone not employed by <Company Name> any confidential information of <Company Name>, including confidential information regarding its business or financial affairs, ... or investments, products, processes, technical data, or other projects or any confidential information.
>
> Access to assets is permitted only in accordance with management's authorization. In this regard, no false or misleading entries shall be authorized, approved, or made in the books and records for any reason, and no employee shall engage in any arrangement that results in such an entry.

Part of an IS-Specific Code of Ethics:

> The <Company Name> licenses the use of computer software from outside companies. Copying this software is a violation of U.S. copyright laws, which carry both civil and criminal penalties. Unauthorized copying of software by <Company Name> employees may result in disciplinary action.
>
> Below you will find a list of guidelines defining your responsibilities:
>
> ☐ Read and follow the policies established in the license agreement that accompanies every software package. Pay special attention to policies pertaining to making backup copies, installing and transferring ownership.
>
> ☐ A copy of the license agreement and original media should always be retained and labeled with the asset number to which it belongs and be immediately available for audit.
>
> ☐ When transferring software package(s) from one employee to another, all copies of the original media must accompany the software package or be erased. In addition, all copies of the software package must be erased from the previous system unless otherwise stated in the license agreement.

[4] These samples are from the companies who participated in this study.