Journal of International Information Management

Volume 3 | Issue 1 Article 9

1994

Computer abuse and computer ethics, a framework to guide research and practice^

Margret Anne Pierce
Georgia Southern University

John W. henry
Georgia Southern University

Computer abuse and computer ethics, a framework to guide research and practice[1]

Margaret Anne Pierce
John W. Henry
Georgia Southern University

ABSTRACT

The focus of the current research is to identify factors which can be used in constructing a theoretical framework to guide research and practice; those factors explored are categories of computer abuses, organizational factors, the application of professional and organizational codes, and the frequency of ethical decisions faced by practicing managers. A mailed survey of over 5000 Data Processing Management Association members revealed patterns of differences in the frequency with which various types of computer abuse (hardware, data, services, and programs) are observed by industry as well as by position within the organization. Knowledge of computer ethics codes were reported by about one-half of the respondents, and the use of professional codes of computer ethics was indicated by a majority of the respondents. The results of the research are discussed in terms of theoretical and managerial implications.

INTRODUCTION

Recently, computer abuse has received a great deal of attention, particularly since 50%-90% of U.S. firms report major dollar losses from computer abuse (Ernst & Whinney, 1989; Laplante, 1987, cited by Straub, Nance, & Carlson, 1990). For example, the Department of Justice reported annual dollar losses of $70 million to $100 million from automatic teller fraud alone. Even in the Los Angeles Police Department there were reports of "rampant unauthorized computer use" (Staff, 1993, p. 11). Thus, computer abuse, and more importantly how to curb abuses, assumes an ever-increasing importance as costs to organizations in both financial and human resources continues to rise. Moreover, the fields of computer science (CS) and management information systems (MIS) lack a substantial empirical base for theoretical guidance which demonstrates relationships of organizational, professional, and personal factors related to ethical decision making.

In this paper, computer abuse refers to the "unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information system by individuals" (Straub, Nance, & Carlson, 1990, p. 45). The abuse categories used in the Straub et al. study were: 1) hardware (and other physical assets associated with computers, theft or damage), 2) programs (theft or modification), 3) data (embezzlement or modification), and 4) computer service (unauthorized use of service or purposeful interruption of service). Based on their

[1] This research was partially funded by a Georgia Southern University Faculty Research Grant.

research Straub et al. (1990) made several recommendations regarding how information systems managers and computer security administrators should handle abuse incidents and the disciplining of perpetrators; these suggestions include 1) instructing employees regarding criminal acts, 2) establishing computer security policies, and 3) taking measures to protect information in the organization. Their point is that many employees who are not "computer professionals" are using computing resources; therefore, it is critical that managers establish clear statements of permitted and prohibited behavior related to these resources. Moreover it is important to know how many of the perpetrators violated known ethical standards for computer abuse.

In a study of ethical standards and computer crime laws, Gardner, Samuels, Render, and Coffinberger (1989) found that most people who use computers and computer resources have no clear understanding of the relevant ethical and legal issues, thus leaving the organization susceptible to computer abuse as well as vulnerable to legal prosecution. These authors assert that "Computer crime and unethical conduct are more likely if employees do not know what their organization considers unethical or criminal conduct" (Gardner, Samuels, Render & Coffinberger, 1989, p. 43).

How does the organization convey to employees expected standards of conduct? A formal company code or policy is seen as an option by many companies. In *Creating a Workable Company Code* (1990), it was reported that in a 1987 survey of American corporations 85% had codes of ethics or similar policy statements. This figure was up from 40% found in 1964 by a similar report. Formal company policy or code with sections related to computer technology is one means of transmitting the expectations of the organization to the employees.

An additional source of ethical guidance in many professions has been the codes of ethics of the professional organizations (Frankel, 1989). Clearly professional organizations such as Computer Professionals for Social Responsibility, the Association for Computing Machinery (ACM) (Anderson, Johnson, Gotterbarn, & Perrolle, 1993), the Data Processing Managers Association (DPMA), the IEEE, and others have taken leadership positions by developing and disseminating codes of ethics related to computer use and professional behavior. However, many computer professionals who belong to DPMA, ACM, IEEE, and other professional organizations may not be aware of their organization's code of ethics, thus removing the impact of the code on the individual's ethical decision making.

PURPOSE OF THE CURRENT RESEARCH

The discussion above clearly suggests that a framework is needed to guide research on CS/MIS ethics and aid managers and professionals in making appropriate decisions related to the use of computer technology. The focus of the current research is to identify factors which can be used in constructing a theoretical framework to guide research and practice; those factors explored are categories of computer abuses, organizational factors, the application of professional and organizational codes, and the frequency of ethical decisions faced by practicing managers. In order to facilitate this process, one must know what types of situations might arise in a particular setting. Therefore, the first goal of the current research is to develop a profile of the ethical issues encountered in the "real world"; that is, the research is designed to identify areas in which computer professionals make ethical decisions and areas in which there are observed abuses. Since company codes are seen as one vehicle for conveying

ethical standards, the second goal of the research is to examine the prevalence of company codes of computer ethics. As mentioned previously, another source of ethical guidance is professional organizations; therefore, the third research goal is to examine the extent to which computer professionals have professional identity, are aware of the codes of ethics of their professional organizations, and apply the codes to guide behavior. Moreover, the research examines differences by industry and organizational level.

THE STUDY

A survey questionnaire was constructed by the authors. In addition to demographic information such as age, gender, education, position, and professional certification, respondents were asked if their company had a formal code of computer ethics. There were questions related to membership in professional organizations, professional identity, and the knowledge of and use of codes of professional ethics. Respondents were also asked to estimate the number of computer abuses during the last year in the categories of: hardware, software, data, and computer sevices. In addition the respondents were asked to indicate the frequency with which they make ethical decisions related to the following: privacy rights, liability, ownership/use of software, expertise, conflict of interest, unauthorized use, viruses/worms, responsibility to employers, copyright infringements, and unauthorized access.

A cover letter, questionnaire, and a metered return envelope were mailed to a random sample of 5102 Data Processing Management Association (DPMA) members. The random sample was stratified by industry represented in DPMA. The percentage of each industry type found in the DPMA and the sample is given in Table 1 along with the percentage of the returned questionnaires in each of the categories.

Table 1. Description of the Sample and the Returns by Industry Type

INDUSTRY TYPE	% SAMPLE	% RETURN
Manufacturing	18.9	18.7
DP Service/consult	16.0	18.9
Utilities	5.3	5.3
Wholesale/retail	5.0	5.7
Financial/real estate	11.9	12.9
Education/med/legal	27.7	14.9
Government	5.8	12.0
Printing/publishing	1.4	1.7
Other	8.1	9.7

A return rate of approximately 14% yielded 703 responses. The sample parallels the population closely except in the categories of government and education/medical/legal. It is possible that some of the respondents incorrectly classified themselves; for example, an instructor at a state college or university might indicate as industry type government rather than education. One very specialized industry which indicates how well the responses are distributed is the printing/publishing industry. Given the size of the return group, one would expect there to be 10 respondents (1.4% in DPMA; 1.7% in the return) in this category; there were 12. The profile by industry leads one to conclude that the sample obtained was representative of the population (DPMA members).

In the cover letter, respondents were invited to enclose a business card with their completed questionnaire if they wished to receive a copy of the results, and 193 business cards were received. In addition to these, several notes were enclosed indicating an immense interest in the research. Almost 10% of the questionnaires contained comments, and one person enclosed a newspaper editorial on the topic. A copy of the company "formal" code of computer ethics was requested from each respondent. Twenty-seven of these written codes were received. Although not all of the codes were specific to computer technology issues, all contained reference to the topic. The numbers of respondents, business cards, and company codes sent indicate a great interest and concern about computer ethics on the part of those surveyed.

ANALYSIS AND RESULTS

Demographic Profile of Responses

The demographic profile of the returns provides further evidence that the sample was a representative one. Twenty-nine percent of the responses were from females and 71% from males. Ages ranged from 21 to 67 (M=41.8, sd=9.2, Med=43). Forty-three percent of the respondents had a four-year college degree, and 32% had a graduate degree (either Master's or Doctorate). A variety of positions/organizational levels were represented in the responses; Table 2 contains a description of this distribution.

Table 2. Distribution of Sample by Position

TITLE	% RETURNS
Senior Management	13.5
Middle Management	18.6
Programmer	8.5
Analyst	15.2
Software Engineer	3.8
System Supervisor	3.8
DP Manager	19.9
CS/MIS Educator	6.1
Other	10.8

The number of years in the profession ranged from less than 1 to 44 (M=16.4, sd=9.0, Med=15). Years employed by the current employer ranged from less than 1 to 37 (M=8.9, sd=7.3, Med=7). The company size ranged from 1 to 500,000 employees; in addition, one person indicated a company size of zero and another of over one million. The distribution was rather uniform over this range. The background and experience of the sample indicates a variety which parallels that of the population of computer professionals.

Types and Frequency of Ethical Decisions

Respondents were asked to rate on a scale from often (1) to never (5) the frequency with which they make ethical decisions in several categories. The mean, median, and mode are reported in Table 3.

Table 3. Responses to How Frequently You Make Ethical Decisions

	Distribution	Mean*	sd	Mode (n=)
Responsibility to Employer	right skew	1.9	1.1	1 (333)
Ownership/Use Software	right skew	2.1	1.2	1 (301)
Expertise	right skew	2.2	1.3	1 (266)
Liability	right skew	2.2	1.3	1 (270)
Unauthorized Access	right skew	2.5	1.41	1 (232)
Privacy Rights	right skew	2.5	1.4	1 (210)
Unauthorized Use	right skew	2.7	1.4	1 (186)
Copyright	uniform	2.9	1.5	1 (187)
Conflict of Interest	mound	3.1	1.4	3 (167)
Virus	u-shaped	3.2	1.6	5 (209)

* note: often = 1, never = 5

These responses suggest rather interesting patterns. Responsibility to one's employer emerges as an often addressed ethical issue; while the greatly publicized area of introduction of virus/worm into a system is not as frequently encountered. However, the statistics above do not present the entire picture of the response pattern; rather the distribution of the responses is also important. All of the distributions above were right-skewed except conflict, virus/worm, and copyright. Conflict of interest and virus/worm responses formed a "U" distribution; the copyright responses formed almost a uniform distribution. The modal response in all case except conflict of interest and virus/worm was "often" (1), the most extreme positive response.

Incidence of Company Codes of Computer Ethics

Respondents were asked if their company had a formal code of computer ethics. The results in Table 4 indicate that about 50% of those who returned the questionnaires were aware of formal company policies related to computer technology.

Table 4. Formal Company Code

	number	% total	% of answers
Yes	350	49.8	50.4
No	343	48.8	49.4
No answer	10	1.3	---

Incidence of Computer Abuse

In order to better understand trends in specific types of abuses the respondents were asked to estimate the number of abuses of each type which had occurred in their company during the last year. The categories used were those suggested by Straub et al. (1990): hardware (e.g., damage, theft, sabotage), programs (e.g., theft, modification of programs), data (e.g., embezzlement, modification of data), and computer services (unauthorized use, purposeful interruption of services). A summary of the responses is shown in Table 5. In addition the abuse categories in Table 5 were analyzed across industries and organizational position using one-way analysis of variance procedures and follow-up univariate least significant differences tests. Moreover the existence of formal company codes were recorded. The results are summarized in Table 6. The relationship of the frequency of abuse in each category to company size and frequency of ethical decisions was also examined using regression analysis.

Table 5. Computer Abuse Incidents During the Last Year

Type	none	90%	mean	st. dev.
Hardware	62.9%	< =6	2.9	9.7
Programs	57.9%	< =24	9.5	23.4
Data	82.1%	< =2	2.0	10.8
Services	63.2%	< =15	7.9	22.4
Total abuses	38%	< =76	20.9	47.6

Hardware. The mean number of *hardware* abuses was 2.9 (sd=9.7) and 90% of the respondents indicated six or fewer incidents within the last year. No abuses of this type were observed by 62.9% of the respondents. Moreover, the number of hardware abuses did not differ by industry or company type. There were, however, significant differences in number of abuses by position of the respondent ($F=2.00$, $p=.045$). Post hoc comparisons of the individual categories revealed significant differences between several categories of positions. CS/MIS educators reported a higher (M=7.6) number of abuses than senior management, programmers, software engineers, system supervisors, DP managers, and those in the other position category. Middle management (M=4.2) and DP managers (M=1.4) also differed significantly from each other in the number of hardware abuses that they reported in the survey.

Employees of companies which had formal company codes of computer ethics reported significantly ($F=5.76$, $p=.017$) more hardware abuses (M=3.9) than those from companies without such codes (M=1.9). The regression showed that the number of hardware abuses was not correlated to company size or to the frequency (often to never) of ethical decisions made related to any of the issues reported in Table 3.

Table 6. Computer Abuse by Industry and Organizational Position

	Hardware	Programs	Data	Services	Total
Industry					
Manufacturing	4.5	9.4	1.6	8.24	22.4
DP Service/Consult	2.3	11.9	2.1	7.21	21.9
Utilities	4.1	22.1	5.7	12.91	40.6
Wholesale/Retail	2.9	6.6	.5	8.95	18.2
Financial/Real Estate	1.0	5.1	.3	7.49	13.4
Education/Med/Legal	1.2	7.5	1.0	8.00	16.6
Government	1.1	4.4	.3	3.32	8.9
Printing/Publishing	3.6	7.7	1.9	13.42	26.1
Other	2.8	7.1	2.4	6.29	17.5
F-value	1.10	3.35***	1.52	1.05	2.46*
Position					
Senior Management	1.3	3.8	.8	3.71	9.2
Middle Management	4.2	12.9	2.8	7.49	25.2
Programmer	2.3	8.0	1.3	11.60	22.4
Analyst	3.8	7.8	2.1	8.30	21.5
Software Engineer	1.1	8.5	.6	9.00	16.3
System Supervisor	2.0	10.4	.5	6.50	18.4
DP Manager	1.4	6.9	1.6	5.93	15.1
CS/MIS Educator	7.6	32.9	5.3	26.33*	69.5
Other	3.2	8.4	2.5	5.27	17.9
F-value	2.00*	5.17***	.70	3.58***	5.57***
Company Code					
Yes	3.9	9.7	2.2	10.1	24.26
No	1.9	9.3	1.8	6.0	18.08
F-value	5.76*	.035	.149	4.53*	2.45

***p < .001, ** p < .01, *p < .05

Programs. Respondents reported that the number of abuses related to *programs* were higher than those related to other categories of abuses (M=9.5, sd=23.4) with 90% of them reporting 24 or fewer cases: 57.9% reported no program type abuses during the preceding year. The number of program type abuses differed significantly by the respondent's company type (F=3.35, p=.001). Those in education reported the highest number (M=22.1) of abuses, and this number differed from the number reported by manufacturing, DP service/consultants, utilities, wholesale/retail, financial/real estate, government, printing/publishing, and those in the "other" industry type. The number of reported program type abuses differed by the position of the respondent (F=5.17, p=.000) with CS/MIS educators reporting the highest number of abuses (M=32.9), and this number differed from the number reported by senior management, middle management, programmers, analysts, software engineers, system supervisors,

DP managers, and those in the other position category. Senior management had the lowest number (M=3.9), and differed significantly from middle management (M=12.92). Analysis of variance showed that the number of program type abuses was not related to whether or not the company had a code. Regression analysis showed that the number of hardware abuses was not correlated to company size, or frequency of ethical decisions (Table 3).

Data. The number of reported *data* type abuses was lower than the number of abuses in the other categories (M=2.0, sd=10.8), and 82% of the respondents reported no knowledge of this type of abuse within the last year. Ninety percent of the respondents reported two or fewer incidents of abuse. The number of data abuses was not related to company type, position of the respondent, the presence of a company code of computer ethics, or to company size. It was found that less frequent ethical liability decisions related to the number of reported data type abuses ($r=11$, $p <= .05$).

Services. The mean number of abuses related to *services* was 7.9 (sd=22.4), and 63.2% reported no such abuses. Fifteen or fewer abuses were reported by 90% of the respondents. The analysis showed no significant differences in number of service type abuses by industry type. There were, however, significant differences in number of reported abuses by position of the respondent ($F=3.58$, $p=.000$) with MS/MIS Education reporting the highest number (M=26.3), and this group differed from senior management, middle management, programmers, analysts, software engineers, system supervisors, DP managers, and those in the other position category. Senior management had the lowest (M=3.7) number of observed service abuses. Significant differences in the number of abuses ($F=4.53$, $p=.034$) were found between those who have a computer ethics code (M=10.1) and those who do not (M=6.0). Company size correlated with the number of service type abuses reported ($r=.09$, $p < .05$). The frequency of ethical liability decisions was related to abuses to computer services ($r=-.16$, $p <= .01$).

Total abuses. The number of *total abuses*, found by summing the number of abuses reported in the four categories, had a mean of 20.9 (sd=47.6) with 38% reporting no abuses of any type and 90% reporting less than 76. This number of total abuses differs by company type ($F=2.46$, $p=.013$). Education with the highest (M=40.6) number of total reported abuses differed significantly from manufacturing, DP service/consultants, utilities, wholesale/retail, financial/real estate, government, and those in the "other" industry type. Those in DP services and consulting reported the lowest (M=8.9) total number of abuses. Significant differences in the number of abuses by position ($F=5.57$, $p=.000$) were found with CS/MIS educators highest (M=69.5), and this differed from the number reported by all other groups (senior management, middle management, programmers, analysts, software engineers, system supervisors, DP managers, and those in the other position category). Senior management, with the lowest number (M=9.3) of total obseved abuses, differed significantly from middle management (M=25.2). There were no significant differences in the total number of abuses by the presence of a company code of computer ethics or by company size. The frequency of ethical liability decisions was related to the total number of reported abuses to computer services ($r=.09$, $p <= .05$).

Professional Orientation, Professional Codes and Licenses

The results of questions related to professional orientation, licenses, and professional codes are found in Table 7.

Table 7. Professional Orientation, Licenses, and Professional Codes

Perception: Do you think of yourself as a computer professional or employee?

	number	% tot	% of answer
Comp Pro	543	77.2	79.5
Employee	140	19.9	20.5
No answer	20	2.8	---

License: Do you hold any professional certification or license?

	number	% tot	% of answer
Yes	206	29.3	30.0
No	281	68.4	70.0
No Answer	16	2.3	---

Codea: Are you familiar with computer ethics codes of organizations?

	number	% tot	% of answers
Yes	411	58.5	83.4
No	82	11.7	16.6
No Answer	210	29.9	---

Codec: If yes, do you use them to guide your behavior?

	number	% tot	% of answers
Yes	454	64.6	79.9
No	113	16.1	19.9
No Answer	136	19.3	---

Professional orientation was operationalized in two ways. The first was a perception of one's self as a professional rather than an employee (Do you think of yourself as a computer professional or employee?). The second indication of professional orientation was the holding of a professional license (Do you hold any professional certification or license?). Of those who answered the perception question, 79.5% indicated that they thought of themselves as professionals rather than employees. Only 30% (206) of the respondents hold one or more professional licenses, and of these 122 hold CDP credentials (many also hold other licenses). A Chi-Square analysis of the responses to these two questions revealed significant differences in response rates ($X^2 = 3.9$, l.s. $< .05$); i.e., more of those who hold licenses think of themselves as professionals.

In an attempt to investigate the impact of codes of computer efthics drafted by professional organizations, the respondents were asked the following questions:

a. Are you familiar with codes of organizations?
b. If so, which ones? (choices were DPMA, ACM, IEEE)
c. Do you use them to guide your behavior?

The responses to the first and last question are shown in Table 7. Of the total respondents, 58.9% (411) indicated that they were familiar with one or more of the codes (remember that all respondents were DPMA members). This appears to be inconsistent with the response of 454 (64.6%) who stated that they use the codes to guide their behavior. Perhaps some respondents use the codes for decision making but do not consider themselves thoroughly "familiar" with them. In response to question (b) above, 72% indicated only familiarity with the DPMA code of ethical conduct. Another 8.7% were familiar with both the DPMA and ACM codes. There was no significant difference in the indicated use of a professional code between those who held a license and those who did not.

The responses to perception of self as professional were significantly different by respondent's familiarity with professional codes ($X^2 = 11.14$, l.s. $< .001$) with more of those thinking of themselves as professionals knowing of the codes. Likewise significantly ($X^2 = 10.38$, l.s. $< .002$) more individuals who hold licenses are also familiar with the professional codes of ethics.

DISCUSSION

In this study of computer professionals (a sample of DPMA members), most respondents indicated they often had to make ethical decisions related to privacy rights, liability, ownership, expertise, unauthorized use, responsibility to employer, copyright, and unauthorized access. Less frequent ethical decisions were found in the areas of conflict of interest and viruses/worms. One explanation for this might be that in a business setting, conflict of interest is generally a well defined concept; in fact, sometimes one's contract or at least verbal agreement involves an explicit discussion of the appropriate behavior in this area. The implication is that expected behavior in the other areas, e.g., privacy rights, etc., needs to be communicated to employees and computer professionals in a more explicit manner thus perhaps illuminating some ethical dilemmas in these areas.

About one-half of the respondents in the current study indicated that their company had a formal code of computer ethics. The question remains whether codes actually exist in more companies and the employees simply have not been made aware of them. It is interesting to note that in a 1987 study, 85% of the American corporations surveyed had general ethics policy statements (*Creating . . .*, 1990), but only 55% distributed the code to their employees. Since computer ethical codes are more specialized than general codes of ethics, perhaps computer codes of ethics are more widely circulated and enforced than more general ethics/goal statements.

More computer abuses related to hardware and services were reported in companies with a formal code. Perhaps those companies who have codes have greater sensitivity to abuses; therefore, more abuses are reported. It also could be that those environments which have had problems with abuse in the past have introduced codes of ethics in an effort to deter inappropriate behavior and have not been entirely effective.

The numbers and types of abuses reported varied by type of industry and position. It was disappointing to find that the CS/MIS educators reported the largest number of abuses. The academic setting should "practice what it preaches" and take a leadership role in the study and teaching of computer ethics. It is essential that this setting reflect the "high road"

with regard to setting a standard of conduct both in terms of those employed by the institutions and the students enrolled in them. In the latest curriculum recommendations for Computer Science undergraduate programs, *Computing Curriculum 1991* written by the ACM/IEEE Computer Society Joint Curriculum Task Force (1991), specific recommendations are made regarding the need to teach social issues. In fact, the social and professional context of computing is considered one of the three general principles which should encompass the entire course of study (Turner, 1991). These represent attempts by the profession to address the problem of students and entry-level professionals who are unprepared to make informed ethical decisions.

All of the respondents in the current study were members of DPMA; thus, when asked if they were familiar with professional codes of computer ethics, one would expect them to at least be aware of the DPMA code. Disappointingly, less than 60% indicated that they were familiar with any professional code of computer ethics. This suggests that the professional organizations need to make a concerted effort to inform their membership of the professional codes and their interpretation (see Anderson et al., 1993, for an example of this type of article in the *Communications of the ACM*). ACM has done this in recent years with full length articles in the journals as well as almost monthly articles on some aspect of computer ethics and legal obligations. In order to have an impact, the professional organizations need to get their message before the membership.

The research indicates that those who perceive themselves as "professionals" know of the codes with more frequency. Moreover, a more relevant question than who knows of the codes is who actually applies the codes to guide behavior. About 65% of the respondents indicated that they applied the codes to help make ethical decisions. Thus, this suggests that less abuse might occur if more of those who work with computers had a sense of professionalism and were informed of and instructed on the use of computer codes of ethics.

MANAGERIAL IMPLICATIONS

The research indicates that there are many ethical decisions related to computer technology being made each day in a variety of business settings. Abuses involving hardware, programs, data, and services are being observed in all types of business settings, although the frequency varies by industry type. Guidance for those faced with ethical decisions is clearly needed. Sources of guidance which have not been fully tapped are company codes of computer ethics and professional codes of computer ethics. Companies need to take a close look at the types of decisions their employees are facing as well as the types of abuses encountered most frequently and tailor or append existing codes to provide a thorough discussion of considerations which should be addressed as action decisions are made. The codes must be distributed, discussed, and enforced. They must be a part of the ethical corporate culture in order to be effective (Schlegelmilch & Houston, 1990). Further, the professional organizations need to foster professional identity, build codes of ethics which address the types of issues faced by their membership (see Martin & Martin, 1990, for a discussion of a content comparison of several codes including DPMA and ACM), and broadly publicize the professional codes. The aim is to minimize the frequency with which a person using computer technology must make an uninformed decision regarding the appropriate action to be taken. As much as possible it should be clear what action the company and the profession would expect in the situation, and these two positions should be congruent.

REFERENCES

ACM/IEEE Joint Curriculum Task Force. (1991). *Computing curriculum 1991.* New York: ACM Press

Anderson, R. E., Johnson, D. G., Gotterbarn, D., & Perrolle, J. (1993). Using the new ACM Code of Ethics in decision making. *Communications of the ACM, 36*(2), 98-107.

Creating a workable company code of ethics. (1990). Washington, DC: Ethics Resource Center.

DPMA. (1989, January). *DPMA position statement handbook.* Park Ridge, IL: DPMA.

Ernst & Whinney. (1989). *The 1989 computer abuse survey: A report.* (Available from authors, 2000 National City Center, Cleveland, OH 44114.)

Frankel, M. S. (1989). Professional codes: Why, how, and with what impact? *Journal of Business Ethics, 8*(2 & 3), 109-116.

Gardner, E. P., Samuels, L. B., Render, B. & Coffinberger, R. L. (1989, Fall). The importance of ethical standards and computer crime laws for data security. *Journal of Information Systems Management,* 42-50.

IEEE. (1987). *Ethics source sheet.* New York: IEEE.

Laplante, A. (1987, May). Computer fraud threat increasing, study says. *Infoworld, 18,* 47.

Martin, C. D. & Martin, D. H. (1990). Professional codes of conduct and computer ethics education. *Social Science Computer Review, 8*(1), 96-108.

Schlegelmilch, B. B. & Houston, J. E. (1990). Corporate codes of ethics. *Management Decisions, 28*(7), 38-43.

Staff. (1993). Newstrack: He'll be back. *Communications of ACM, 36,* 11.

Straub, D. W., Jr., Nance, W. D. & Carlson, C. L. (1990). Discovering and discipline computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

Turner, A. J. (1991). Summary of the ACM/IEEE joint curriculum task force report: Computing curriculum 1991. *Communications of the ACM, 34*(6), 69-84.