WHISTLEBLOWING: AN ETHICAL DILEMMA

Joan K. Pierson,
Karen A. Forcht,
Ben M. Bauman

Information and Decision Sciences Department
James Madison University
Harrisonburg, Virginia, USA

ABSTRACT

Because most organizations depend on computer systems that electronically store important data to perform crucial business functions, the integrity of these information systems is paramount. Securing company systems, however, is not always an easy task. More sophisticated systems often provide widespread access to computer resources and increased user knowledge, which may lead to added difficulties in maintaining security. This paper explores whistleblowing--employees' exposing illegal or unethical computer practices taking place in the organization--as a method of computer security and the support for whistleblowing found in codes of ethical conduct formulated by professional societies.

INTRODUCTION

Whistleblowing is the term applied to the reporting by employees of illegal, immoral, or illegitimate practices under the control of their employers to parties who can take corrective action (Elliston 1985). Whistleblowing is a controversial organizational issue. On the positive side, whistleblowers can help organizations correct unsafe products or working conditions and curb fraudulent or wasteful practices. Whistleblowers may provide a previously underutilized source of information critical in maintaining the performance of large complex organizations (Ewing 1983, Miceli & Near 1985). Conversely, whistleblowers may threaten an organization's authority structure, cohesiveness, and public image (Weinstein 1979). Despite the problems, there is an increased interest on the part of managers in the issue of whistleblowing and how to handle such incidents (Barnett 1993, Ewing 1983, Keenan 1988a, Rowe & Baker 1984).

Codes of ethics provide guidance for professionals in such fields as accounting, law, engineering, medicine, and education, as well as in information systems. This paper examines support for whistleblowing found in codes of ethics formulated by computer-related professional societies.

ATTITUDES TOWARD WHISTLEBLOWING

Most studies on whistleblowing address the topic in a general manner--there are few published reports of research activities that concentrate on computer-related incidents. Research in the area of whistleblowing is difficult because the presence of organizational blocks aimed at thwarting whistleblowing also serve to block inquiry from outsiders (Parmerlee, Near, & Jensen 1982). Most managers and employees personally approve of the practice of whistleblowing, although managers appear to be slightly less empathetic on the issue than do employees. In a study conducted by Keenan, 96% of the employees and 87% of the managers indicated their personal approval of whistleblowing (Keenan 1988b). Those results are similar to earlier studies (United States Merit Systems Protection Board 1981). Most managers and employees also believe that whistleblowing is in the best interest of the company. Employees were again slightly more positive than the managers about the benefits to a company of whistleblowing in Keenan's study.

Deciding to Report Wrongdoing

It appears that the majority of personnel, regardless of whether they are managers or not, have witnessed some sort of wrongdoing in the workplace (Keenan 1988b). Most such incidents are not reported. A few research studies have examined factors affecting the decision of an observer to report wrongdoing. Ignoring wrongdoing is an expected response since ignoring observed organizational problems is the standard or norm.

Miceli and Near note that the observer's sense that he or she can be manipulated is another factor that reduces the likelihood that the incident will be reported--employees with a sense of powerlessness are not likely to jeopardize their careers. Inactive observers, those who choose not to blow the whistle, tend to be low paid, highly educated, supervisory "fast-trackers." They may be more likely than whistleblowers to have "lofty executive ambitions." Observers who have impressive evidence of serious wrongdoing are more likely to blow the whistle than those who do not. Observers are also more likely to blow the whistle if the observed wrongdoing has a direct effect on them personally than if it does not. Miceli and Near found no support for the hypothesis that whistleblowers who use internal communications channels for whistleblowing (rather than external channels) are members of organizations that use more extensive methods to communicate information about wrongdoing and whistleblowing than other organizations. It appears that employee decisions on whether to blow the whistle are not affected by their organizations' successful attempts at communication. The study did find, however, that whistleblowers were more knowledgeable of the presence of internal whistleblowing channels than were inactive observers (Miceli & Near 1985). Barnett found a relationship between the existence of formal disclosure policies or procedures and the number of whistleblowing actions (Barnett, Cochran, & Taylor 1993). Observers are more likely to blow the whistle if they believe that whistleblowing in general is ethical (Hauserman 1986).

Reactions affecting decisions on whether to report problems in an organization include fear of reprisal, loyalty to the company, privacy and personal control, lack of skills in effective disputing, and a belief that it is pointless (Rowe & Baker 1984). Often, whistleblowing is viewed as a threat to hierarchical authority. Policymakers may want to discourage frivolous whistleblowing but not legitimate complaints (Parmerlee, Near, & Jensen 1982). In some organizations interested in exploring legitimate complaints, ombudsman systems have been set up in which a senior executive operating outside the normal chain of command is available to deal with employee grievances and concerns on a confidential basis (Brody 1986).

The fear of personal reprisal is a common thread running through the published reports of whistleblowing research. Whistleblowing statutes with the dual purpose of protecting whistleblowers and encouraging whistleblowing have been passed in many states. They do not appear to be having the desired effects; but they may be having an unanticipated, positive influence on some companies to change their policies, thereby reducing the incidence of cases brought by whistleblowers who make retaliation charges against their employers (Dworkin, Morehead, and Near 1987).

Whistleblowing in the Computer Environment

In one of the few research studies of whistleblowing in the computer environment, information systems professionals' attitudes toward whistleblowing were found to be similar to those referenced in research on whistleblowing that was not limited to computer environments. Ninety-six percent approved of whistleblowing and 92% agreed with the statement that whistleblowing is in the best interest of the organization. Other findings indicate that only 58% felt it is possible to protect a whistleblower from reprisal. Thirty-three percent responded that protection is probably or definitely not possible. Yet the majority of the information systems professionals believed that employees should be encouraged to act as whistleblowers (75%) but that monetary rewards should not be given (73%) (Pierson and Forcht 1990).

Nearly 40% of the information systems professionals in the study believe that their organizations do not provide as much encouragement for whistleblowing as is needed; 39% think that the level of encouragement is adequate; 21% stated that they are not sure whether the level of encouragement is appropriate. The respondents were much more confident of their own knowledge about when to blow the whistle on unethical or illegal computer use than they were of the abilities of other employees in their organization. About 66% of the respondents felt confident of their own knowledge about when to blow the whistle, whereas only 20% felt confident about other employees knowing when to blow the whistle. In addition, approximately 67% believe that their organizations do not disseminate enough information about when to blow the whistle on computer misuse (Pierson and Forcht 1990).

ETHICAL STANDARDS OF CONDUCT

One of the disturbing facts brought out in the study on whistleblowing in the computer environment is the evidence of lack of organizational policies or procedures outlining ethical and legal use of computers or the lack of awareness of such policies and procedures. Only 38% of the respondents in

the study were positive that their organizations had such guidelines; 42.6% were sure that there were none; the remainder were unsure (Pierson and Forcht 1990). The lack of guidance evidenced in the study leads to the question of whether the level of computer misuse might be decreased if employees knew what constitutes appropriate and inappropriate computer usage.

The need for statements outlining ethical and legal use of computers is two dimensional. First, there is a need for guidance for end users of computer technology. Information systems are organizational assets and must be protected in the same way as any other asset. Computer users have responsibilities to society and their employers to ensure that information system assets are safeguarded. Second, there is a need for guidance for information systems professionals that far surpasses that needed for end users. The responsibilities of information systems professionals include responsibilities to society, their employers, clients, colleagues, and profession.

Most people consider whistleblowing a last resort, an action to be taken only when all else fails. Although the majority of employees and managers approve of whistleblowing in general, they are hesitant to act as whistleblowers. They need guidance in determining for themselves whether or not unethical, illegal, or fraudulent actions have taken place. Codes of ethics often provide the needed guidance; some ethics codes contain support for whistleblowing actions.

Ethical Codes for End Users

Employees' decisions are governed by at least five sets of standards: general cultural, company, personal, situational, and industry. Each set of standards has an official form, such as that espoused in written documents, and an unofficial form that develops as people use the standards. It is little wonder that employees need guidance to determine what is ethical and unethical behavior with regard to computer usage. But no matter how many written policies and procedures are available for guidance, they will be worthless if the organization tolerates violations of stated ethical behavior (Fimbel and Burstein 1990).

Many businesses have formal policies that prohibit unethical conduct and prescribe punishment for it. These policies are typically found in operating and policy manuals and in supervisors' workplace statements (Bommer, Gratto, Gravander, Tuttle 1987). The relationship between the existence of company codes of ethics and reduced unethical practices is noted by several researchers (Bommer, Gratto, Gravander, Tuttle 1987, Fimbel & Burstein 1990, Vital & Davis 1990).

Lack of awareness of company standards of ethical conduct for computer usage may diminish the effectiveness of the standards. In one study of chief executive officers, over 80% responded that their company did have codes (Forcht 1991). Yet in another study of mostly lower-level managerial employees, 42% of the respondents were positive that their organization had not formulated conduct standards for employees for ethical computer behavior (Pierson and Forcht 1990). It may be that such codes do exist but that they are not advertised within the organization.

Widespread computer usage is a comparatively new phenomenon in private and public organizations. It is to be expected that without appropriate guidelines for and training in computer ethics some employees will unknowingly violate rules of ethics. In one large organization, an ethics program was developed that included both establishment of conduct standards and training. The results were favorable. After several years, employees were generally clear about the standards of conduct and their own responsibility in upholding the standards. Corrective action systems were developed and implemented to enforce compliance with the standards. Disciplinary and other corrective actions were taken as a result of the exposure of wrongdoing (Barker 1993).

There does not appear to be any standard code of conduct for employee usage of computers that specifies the employee's obligations for ethical behavior. It may be necessary for individual organizations to look to information systems professional societies for guidance in establishing reasonable usage standards and the obligations of the employee for proper use of computers.

Ethical Codes for Information Systems Professionals

Currently there are several professional information systems societies that have adopted codes of ethics for their members. It has been proposed that the differences among the codes be resolved and a single, coherent, international code of ethics for the information systems community be adopted. Oz (1993) points out that "Physicians, lawyers, and engineers have moral responsibilities and know to whom they are responsible. Professionals in the information systems field need similar guidance."

The three largest information systems professional organizations have ethical codes for their members that provide support for a potential whistleblower. The three organizations are the Data Processing Management Association, the Association for Computing Machinery, and the Institute for Certification of Computer Professionals. The pertinent guidelines in the three codes are noted below.

> The Data Processing Management Association (DPMA) is a worldwide organization. Its mission is "to advocate effective, responsible management of information to the benefit of its members, employers, and the business community." Two guidelines in its Code of Ethics and Standards of Conduct are of particular interest. One refers to the obligation of information systems professionals to their employers to "protect employer's interests at all times." A second cites a responsibility to the professional organization or its members to "take action against others' unethical conduct."
>
> The Association for Computing Machinery is the largest professional organization in the information systems industry. The standards of the organization are set forth in the ACM Code of Ethics and Professional Conduct in which is specified an obligation to the professional organization to "uphold and promote the Code" and to "agree to take action to remedy if the Code is violated."
>
> The Institute for Certification of Computer Professionals (ICCP) offers certification for information systems professionals. The certificates offered are Associate Computer Professional, Certified Computer Programmer, Certified Systems Professional, and Certified in Data Processing. As an obligation to the profession, the ICCP's Code of Conduct holds members responsible to "report violations of the Code; testify in ethical proceedings; and serve on panels to judge."

The responsibilities noted in the three ethical codes are clear in their intent: unethical and illegal actions should be reported.

CONCLUSION

Information systems are of increasing importance to organizations. Protection of these important assets becomes more difficult as the percentage of employees using information systems increases. In a perfect world, there would be no need for whistleblowers. For now, managers of information systems must utilize all methods available to control risks. Whistleblowing is one method.

It is unfortunate that the term "whistleblowing" is the one chosen to describe an action taken in good faith by an employee and in accordance with personal and professional codes of proper conduct. However, organizations should be aware of the circumstances in which it is appropriate to report wrongdoing and the long-term benefits of these actions.

Standards of ethical conduct established by professional computer-related societies can help employees in decisions of whether or not to blow the whistle on improper conduct. Public and private organizations should ensure that standards clearly setting forth employee obligations for computer usage are adopted and widely distributed. Not only do such ethical standards render guidance for determining ethical, moral, and legal behavior, they provide support in case whistleblowing is the only alternative.

REFERENCES

Barker, Richard A. (1993), "An Evaluation of the Ethics Program at General Dynamics," **Journal of Business Ethics,** Vol 12, No 3, pp 165-177.

Barnett, Tim, Cochran, Daniel S., and Taylor, G. Stephen (1993) "The Internal Disclosure Policies of Private Sector Employees: An Initial Look at Their Relationship to Employee Whistleblowing," **Journal of Business Ethics**, Vol 12, No 2, pp 127-136.

Bommer, Michael, Gratto, Clarence, Gravander, Jerry, and Tuttle, Mark (1987) "A Behavior Model of Ethical and Unethical Decision Making," **Journal of Business Ethics,** Vol 6, pp 265-280.
Brody, Michael (1986) "Listen to your Whistleblower," **Fortune,** Vol 114, pp 77-78.
Charney, Scott (1992) "The Justice Department Responds to the Growing Threat of Computer Crime," **Computer Security Journal,** Vol VIII, No 2, pp 1-12.
Dworkin, Terry Morehead, and Near, Janet P. (1987) "Whistleblowing Statutes: Are They Working," **American Business Law Journal,** Vol 25, pp 241-264.
Elliston, F. A., (1982) "Civil Disobedience and Whistleblowing: A Comparative Appraisal of Two Forms of Dissent," **Journal of Business Ethics,** Vol 1, pp 167-177.
Ewing, D. W. (1983) **Do It My Way--Or You're Fired,** New York: John Wiley and Sons.
Fimbel, Nancie and Burstein, Jerome S. (1990) "Defining the Ethical Standards of the High-Technology Industry," **Journal of Business Ethics,** Vol 9, pp 929-948.
Gordon, Richard (1992) "The Long Road to Responsible Computing," **Computer Security Journal,** Vol VIII, No 1, pp 69-80.
Hauserman, John L. (1986) "Whistleblowing: Individual Morality in a Corporate Society," **Business Horizons,** Vol 29, No 4, pp 28-38.
Keenan, John P. (1988a) "Communication Climate, Whistleblowing, and the First-Level Manager: A Preliminary Study," **Academy of Management Best Papers Proceedings,** pp 247-251.
Keenan, John P., (1988b) "Comparing Employee and Managerial Whistleblowing: A Preliminary Study and Evaluation," **Proceedings, Annual National Conference of the Council on Employee Responsibilities and Rights,** October, Virginia Beach, Virginia.
Malone, David (1993) "The Ethical Issues of Automated Information Processing," **Journal of Computer Information Systems,** Vol XXXIII, No 3, pp 82-84.
Miceli, M. P. and Near, J. P. (1985) "Characteristics of Organizational Climate and Perceived Wrongdoing Associated with Whistleblowing Decisions," **Personnel Psychology,** Vol 38, No 3, pp 525-544.
Oz, Effy (1992), "Ethical Standards for Information Systems Professionals: A Case for a Unified Code," **MIS Quarterly,** Vol 16, No 4, pp 423-433.
Parmerlee, Marcia A., Near, Janet P., and Jensen, Tamila C. (1982), "Correlates of Whistleblowers' Perceptions of Organizational Retaliation," **Administrative Science Quarterly,** Vol 27, pp 17-34.
Pierson, J. K., and Forcht, Karen (1990) "Whistleblowing as a Computer Abuse Countermeasure," **Data Security Management,** New York: Auerbach Publishers.
Rowe, M. P. and Baker, M. (1984) "Are You Hearing Enough Employee Concerns?" **Harvard Business Review,** May-June, pp 27-35.
United States Merit Systems Protection Board (1981) **Whistleblowing and the Federal Employee,** Washington: Government Printing Office.
Vitell, Scott J. and Davis, Donald L. (1990) "Ethical Beliefs of MIS Professionals: The Frequency and Opportunity for Unethical Behavior," **Journal of Business Ethics,** Vol 9, pp 63-70.
Weinstein, D. (1979) **Bureaucratic Opposition,** New York: Pergamon Press.