1988

DEVELOPING AWARENESS OF COMPUTER ETHICS

Karen A. Forcht
James Madison University

Joan K. Pierson
James Madison University

Ben M. Bauman
James Madison University

SESSION 3

DEVELOPING AWARENESS OF COMPUTER ETHICS

Panelists: Karen A. Forcht, James Madison University
              Joan K. Pierson, James Madison University
              Ben M. Bauman, James Madison University

ABSTRACT

The most important factor in effective computer security is people -- their attitudes, actions, and sense of right and wrong. This workshop will explore the ethical problems and issues raised in the computing environment. Topics to be discussed include misuse of computers, concepts of privacy, codes of conduct for computer professionals, disputed rights to products, defining ethical, moral, and legal parameters, and what security practitioners should do about ethics. Audience opinions will be welcome as they will aid in developing ethical standards for the information systems profession.

DEVELOPING COMPUTER SECURITY AWARENESS

The rapid increase in the use of sophisticated computers has proliferated in the past decade. Organizations' dependence on the reliability, security, and confidentiality of data is critical. Along with this mushrooming growth in dependence on computers, organizations are faced with the dilemma of numerous violations, intentional or unintentional, of their computer systems.

We are bound today with not halting the growing dependence of computer use; it is here to stay. We are, however, challenged by the necessity of controlling this use. Employees must be aware of the constant danger and vulnerability organizations face as they become increasingly automated.

The issue of computer security has fallen into the "gray" area that educators and industry alike have avoided for fear that too little knowledge could be hazardous and too much could be dangerous. Most organizations acknowledge the need for data security but approach security as a hardware, "nuts-bolts-alarms" solution. It may be more important, and far more successful, to address the issue of data security as an attitude rather than a technology. The technology may vary between companies and vendors, but the attitudinal parameters can remain constant. If individuals, through awareness and knowledge, develop an ethical, moral attitude toward computer security, the transition into the future will be smoother.

Companies are beginning to offer very well organized, sophisticated awareness programs for employees with the idea that the more employees know about security, the more likely they are to recognize danger points and possible breaches. Effective security programs must be a team effort by all employees.

TYPES OF PREVENTION

The current concept today in evaluating a computer security program is "prevention on the front end," not just "punishment on the backend." This concept represents a preventative maintenance attitude and should be practiced by all members of the organization.

To be fully effective and a part of life-long learning, ethical awareness should become a vital part of our educational system, starting in elementary schools and continuing through college classes. Once employees are in the business environment, their ethical education should not cease. Companies must constantly assess the "climate" of their technology and orient all employees on all facets of ethics and security.

By building a strong base in terms of ethics awareness and constantly reiterating the vital necessity to maintain this base, companies will be reasonably assured that they do, in act, have a "secure" system.

OBJECTIVES OF CODES OF PROFESSIONAL ETHICS

1. Inspirational -- it might be used to inspire members to be more "ethical" in their conduct.

2. Sensitivity -- to alert professionals to the moral aspects of their work.

3. Disciplinary -- to enforce certain rules of the profession on its members and defend integrity.

4. Advising -- to offer guidance in cases of moral perplexity about what to do.

5. Awareness -- to alert prospective clients and employers to what they may and may not expect by way of service from a member of the profession concerned. [Johnson and Snapper 1985]

SECONDARY OBJECTIVES OF CODES OF ETHICS

1. To enhance the image of the profession in the public eye.

2. To protect the monopoly of the profession in question.

3. To have the Code serve as a status symbol -- one of the credentials for the occupation.

SIDE-EFFECTS OF CODES OF ETHICS

1. A false sense of complacency to professionals about their conduct.

2. A sense of self-congratulation -- codes can be used as a cover-up for "unethical" or "irresponsible" conduct.

3. A tendency to divert attention from the macro-ethical problems to the micro-ethical problems -- do we scrutinize as a collective body?

4. To discourage, if not suppress, the dissenter, the innovator, the critic.

DEVELOPING AN ETHICS AWARENESS POLICY IN ORGANIZATIONS

If a company, organization, or agency decides to develop an ethics awareness program or rating system, numerous factors should be addressed. A number of terms are used to describe the various ways in which an individual's competence or standards may be measured. Parker's (1984) working definitions of these terms are:

Certification: An affirmation by a governmental or private organization that an individual has met certain qualifications.

Licensing: The administrative lifting of a legislative prohibition.

Accreditation: An affirmation by a governmental or private organization that an educational institution meets certain standards.

Ethics: A standard of conduct drawn up by an organization to protect the consumer and competition against "unfair" practices.

ACCEPTED CODES OF ETHICS FOR COMPUTER-RELATED PROFESSIONS

The following are excerpted from the entire text of Codes of Ethics from the following:

1. British Computer Society

2. Data Processing Management Association (DPMA)

3. Association for Computing Machinery

4. Institute of Electrical and Electronics Engineers (IEEE)

5. Institute for Certification of Computer Professionals (ICCP)

The text is provided as a handout. We will discuss these five codes in summation form.

REFERENCES

Johnson, D.G. and Snapper, J.W. *Ethical Issues in the Use of Computers.* Belmont, CA: Wadsworth Publishing Company, 1985, pp. 11-12.

Parker, D.B. *Ethical Conflict in Computer Science and Technology.* Reston, VA: AFIPS Press, 1984.