UNIT V

- Computer crime, ethics and social issues
- Case studies about different live related problem.

MORALS, ETHICS, AND THE LAW

Morals

Morals are traditions of belief about right and wrong conduct. Morals are a social institution with a history and a list of rules.

Ethics

It is the branch of philosophy that deals with the determination of what is right or wrong. Suite of guiding beliefs, standards, or ideals that promotes an individual or community.

Laws

Laws are formal rules of conduct that a sovereign authority imposes on its citizens.

Laws Lag Behind

First computer crime

- In 1966, a programmer used computer code to keep his checking account from being flagged as overdrawn.
- When the bank discovered the crime the programmer could not be charged with a computer crime because no computer crime law existed.
- He was charged with making false bank records.

U.S. Computer Legislation

1. Freedom of Information Act of 1966
    a. Gave citizens and organizations the right to access data held by the federal government
2. Fair Credit Reporting Act of 1970
    a. Dealt with handling of credit data
3. Right to Federal Privacy Act of 1978
    a. Limited government's ability to search bank records
4. Small Business Computer Security and Education Act (1984)
    a. Advises Congress on matters relating to computer crime against small businesses
5. Counterfeit Access Device and Computer Fraud and Abuse Act
    a. Makes it a crime to gain unauthorized information pertaining to national security or foreign relations and provides other protection
6. In 1986, Electronic Communications Privacy Act was rewritten to cover digital, data, and video communications

   a. Included special section on email
7. Computer Matching and Privacy Act of 1988
   a. Restricts government's right to match computer files for the purpose of determining eligibility for government programs or identifying debtors

NEED FOR AN ETHICS CULTURE

If the firm is to be ethical, then top- level management must be ethical in everything that it does and says.

How the ethical culture is imposed

The executive's impost the ethics in three-tired fashion

1. Corporate credo
   a. Succinct statement of values a firm seeks to uphold
2. Ethics programs
   a. System of multiple activities designed to provide employees with direction in carrying out corporate credo
3. Tailored corporate codes
   a. Codes of ethics for a particular organization or industry

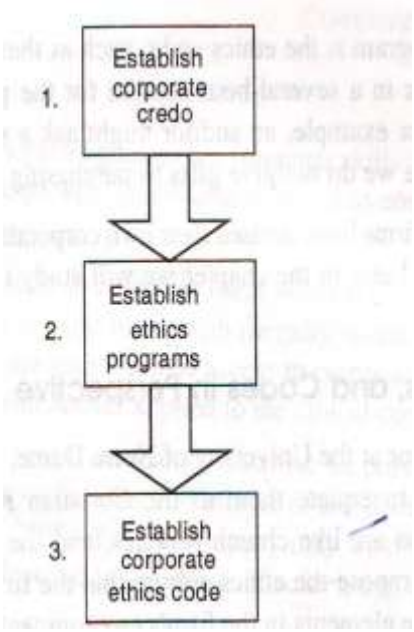
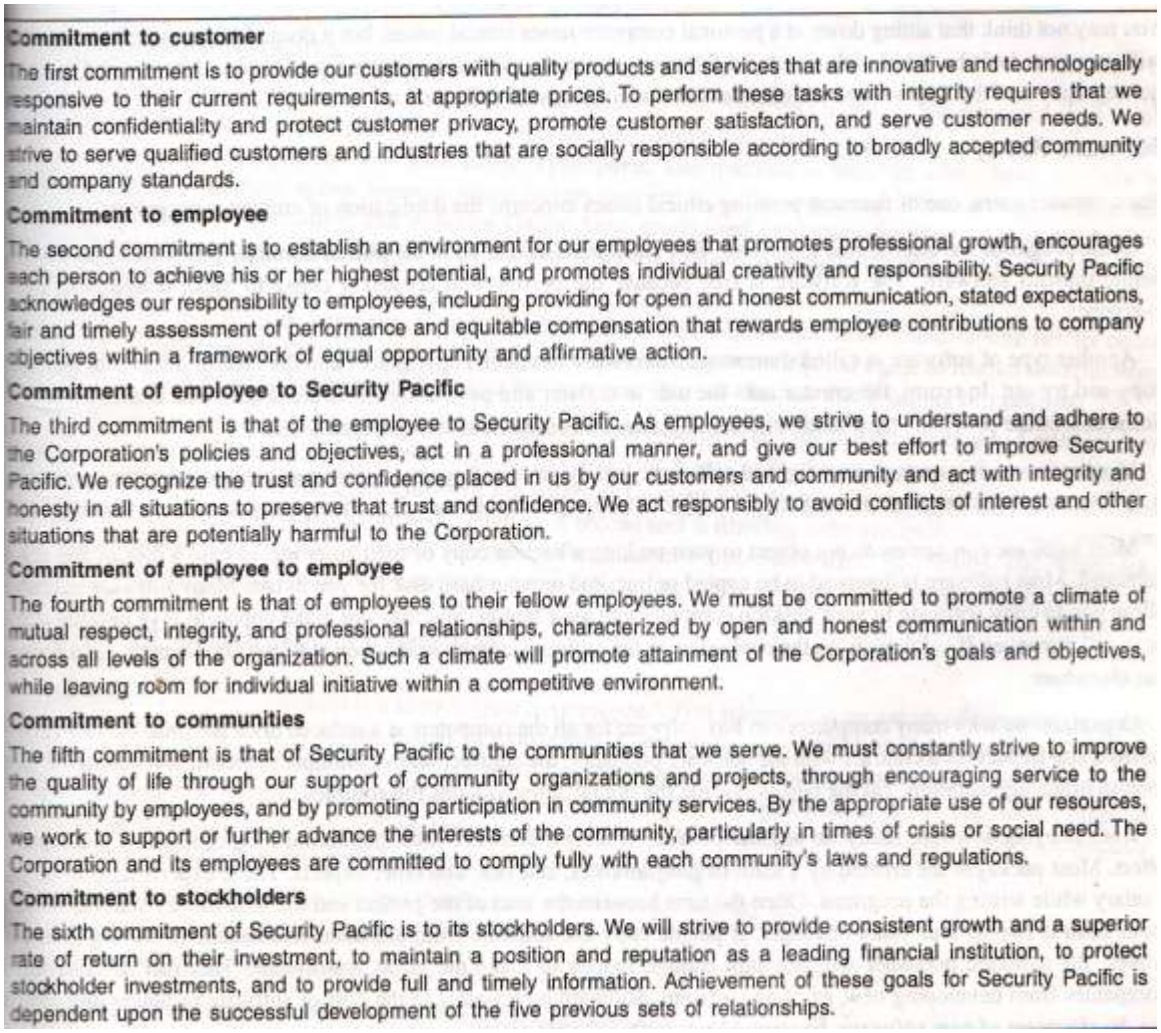


Fig.5.1 Ethics Culture

Example of a Corporate Credo



Commitment to customer

The first commitment is to provide our customers with quality products and services that are innovative and technologically responsive to their current requirements, at appropriate prices. To perform these tasks with integrity requires that we maintain confidentiality and protect customer privacy, promote customer satisfaction, and serve customer needs. We strive to serve qualified customers and industries that are socially responsible according to broadly accepted community and company standards.

Commitment to employee

The second commitment is to establish an environment for our employees that promotes professional growth, encourages each person to achieve his or her highest potential, and promotes individual creativity and responsibility. Security Pacific acknowledges our responsibility to employees, including providing for open and honest communication, stated expectations, fair and timely assessment of performance and equitable compensation that rewards employee contributions to company objectives within a framework of equal opportunity and affirmative action.

Commitment of employee to Security Pacific

The third commitment is that of the employee to Security Pacific. As employees, we strive to understand and adhere to the Corporation's policies and objectives, act in a professional manner, and give our best effort to improve Security Pacific. We recognize the trust and confidence placed in us by our customers and community and act with integrity and honesty in all situations to preserve that trust and confidence. We act responsibly to avoid conflicts of interest and other situations that are potentially harmful to the Corporation.

Commitment of employee to employee

The fourth commitment is that of employees to their fellow employees. We must be committed to promote a climate of mutual respect, integrity, and professional relationships, characterized by open and honest communication within and across all levels of the organization. Such a climate will promote attainment of the Corporation's goals and objectives, while leaving room for individual initiative within a competitive environment.

Commitment to communities

The fifth commitment is that of Security Pacific to the communities that we serve. We must constantly strive to improve the quality of life through our support of community organizations and projects, through encouraging service to the community by employees, and by promoting participation in community services. By the appropriate use of our resources, we work to support or further advance the interests of the community, particularly in times of crisis or social need. The Corporation and its employees are committed to comply fully with each community's laws and regulations.

Commitment to stockholders

The sixth commitment of Security Pacific is to its stockholders. We will strive to provide consistent growth and a superior rate of return on their investment, to maintain a position and reputation as a leading financial institution, to protect stockholder investments, and to provide full and timely information. Achievement of these goals for Security Pacific is dependent upon the successful development of the five previous sets of relationships.

Fig.5.2 An example of a corporate credo

ETHICS FOR COMPUTER USER

Software piracy: involves making illegal copies of copyrighted software.

1. Public domain: some programs are offered free to any one. This software is said to be in the public domain.

2. Shareware: it has been copyrighted, and the creator offers it to any one to copy and try out.

3. Copyrighted: legally protected against copying or being used without paying for it

Unauthorized access

- A computer hobbyist is someone who enjoys pushing his or her computer skills to the limit.
- Sometimes that means trying to get past the security precaution that prevents unauthorized access to computer systems.
- The term **hacker** was originally coined to refer to computer users who experienced with computer programs to test their limits. Hacker attempts to gain unauthorized access to computer systems.
- The term **cracker** has been proposed to refer to this computer criminal, with hacker applied to the ethical computer user.

ETHICS FOR COMOUTER PROFESSONAL

Computer professional include:

- Programmers
- Systems analysts
- Computer designers
- Database administrator

Computer professionals have so many opportunities to misuse computer system that ultimately the only protection for the computer professional is to act ethically. The person who built your system knows its weakness. Computer professional organizations have developed codes of ethics for the professional.

The quality professional should have:

- A high standard of skills and knowledge.
- A confidential relationship with people served.
- Public reliance upon the standards of conduct established practice.
- The observance of an ethical code.

Professional standards

The codes establish several standards**:**
Competency: requires a professional to keep up with latest development in the industry. Because the computer industry encompasses so many areas and advancements are occurring constantly, no individual can be competent in all the areas. Therefore, the code requires professional to keep up with their areas of specialization to the best of their abilities and to seek help from other experts while encountering something unfamiliar.
Professional responsibility: involves doing the best possible job even though the user may not immediately recognize the difference between the best job and a worst job.
It also means informing the purchasing company if a program could have an advance effect on the public.
Third responsibility is honouring the privacy of the company while leaving a job.

Programmer liability

All experienced programmers know that all programs of any size have bugs. Programmer liability arises out of the need to determine whether the bugs were inevitable or the result of negligence on the part of the programmer.

ETHICS FOR BUSINESS

1. A business or organization must protect its data from:
    a. Loss or damage
    b. Misuse or error
    c. Unauthorized access
2. To protect data from loss, an organization must have proper backup procedures.
3. Type of misuse
    a. One type of misuse is not using the appropriate software or not using software properly.
    b. The second type of misuse of data occurs when an employee or company fails to keep data confidential.

ETHICS AND INFORMATION SERVICES

What is computer ethics?

Computer ethics is the analysis of the nature and social impact of computer technology, as well as the corresponding formulation and justification of policies, for the ethical use of such technology.

Reasons for the importance of ethics

- Logical malleability
    - Ability to program computer to do anything you want it to do
- The transformation factor
    - Computers can change the way things are done
- The invisibility factor
    - Invisible programming
    - Invisible complex calculations
    - Invisible abuse

SOCIAL RIGHTS AND THE COMPUTER

Society has certain rights when it comes to computer use. These rights can be viewed in terms of the computer or of the information that the computer generates.

Rights to the Computer

The computer is such a powerful tool that it cannot be kept from society. Deborah Johnson, a professor at Rensselaer Polytechnic Institute, believes that society has the right to computer access, computer skills, computer specialists, and computer decision making.

Right to Computer Access It is not necessary for everyone to own a computer, just as not everyone has to own a car. However, computer ownership, or access, might be the key to achieve certain other rights. For example, access to a computer might be the key to get a good education.

Ben Shneiderman, a professor at the University of Maryland at College Park, took a good look at the computing profession after the Los Angeles riots of 1992 and recognized that "software applications can easily be an aid to improve education, provide skills training, reduce adult illiteracy, improve community organizations, support entrepreneurs, and much more." A society that is viewed in this light has the right to computer access.

Right to Computer Skills When computers first came on the scene, there was widespread fear on the part of workers that the result would be mass layoffs. That did not happen. In fact, the computer has created more jobs than it has eliminated. Not all jobs require computer knowledge or computer use, but many do. In preparing students to work in a modern society, educators often regard computer literacy as a necessity.

Right to Computer Specialists It is impossible for any one person to acquire all of the necessary computer knowledge and skills. Therefore, we should have access to those specialists who can provide what we need, in the same manner that we have access to doctors, lawyers, and plumbers.

Right to Computer Decision Making Although society does not participate to a great degree in the decisions that are made concerning how the computer is applied, it has that right. This is true when the computer can have a harmful effect on society. These rights are reflected in the computer laws that have been enacted to govern how computers are used.

In Johnson's view, social responsibility for ethical computer use can be achieved by satisfying society's rights in terms of the computer as a tool.

Rights to Information

The most widely publicized classification of human rights in the computer area is Richard O. Mason's PAPA. Mason, a professor at Southern Methodist University, coined the acronym **PAPA** to represent society's four basic rights in terms of information. The letters in PAPA stand for **p**rivacy, **a**ccuracy, **p**roperty, and **a**ccessibility.

Right to Privacy U.S. Supreme Court justice Louis Brandeis is credited with recognizing "the right to be let alone". Mason feels that this right is being threatened because of two forces. One is the increasing ability of the computer to be used for surveillance, and the other is the increasing value of information in decision making.

The federal government addressed a portion of this problem in the Privacy Act of 1974. However, that act only covers violations by the government.

According to Mason, decision makers place such a high value on information that they will often invade someone's privacy to get it. Marketing researchers have been known to go through people's garbage to learn what products they buy, and government officials have stationed monitors in restrooms to gather traffic statistics to be used in justifying expansion of the facilities.

These are examples of snooping that do not use the computer. The general public is aware that the computer can be used for this purpose, but it is probably not aware of the ease with which personal data can be accessed. If you know how to go about the search process, you can obtain practically any types of personal and financial information about private citizens.

Right to Accuracy The computer is given credit for making possible a level of accuracy that is unachievable in non-computer systems. The potential is certainly there, but it is not always reached. Some computer-based systems contain

more errors than would be tolerated in manual systems. In many cases, the damage is limited to only a temporary irritation, such as when you must call about the bill you have already paid. In other cases, the cost is much greater.

Right to Property Here we are talking about intellectual property, usually in the form of computer programs. We have seen that users who have purchased the rights to use prewritten software often copy it illegally, sometimes for resale. In other cases, one software vendor may clone a popular product of another vendor.

Software vendors can guard against theft of their intellectual property by means of copyrights, patents, and licence agreements. Until the 1980s, software was covered by neither copyright nor patent laws. Now, however, both can be used to provide some degree of protection. Patents provide especially strong protection in the countries where they are enforced because it is not necessary that a clone match the original version *exactly* in order for copyright protection to be obtained.

Software vendors try to plug up the loopholes in the laws by means of the licence agreements that their customers accept when they use the software. Violation of the agreements puts the customers in court.

Right to Access Prior to the introduction of computerized databases, much information was available to the general public in the form of printed documents or microform images stored in libraries. The information consisted of news stories, results of scientific experiments, government statistics, and so on. Today, much of this information has been converted to commercial databases, making it less accessible to the public. To have access to the information, one must possess the required computer hardware and software and pay the access fees. In light of the fact that a computer can access data from storage much more quickly and easily than any other technology, it is ironic that a right to access is a modern-day ethical issue.

Social Contract of Information Services

Mason believes that in order to solve the problems of computer ethics, information services should enter into a **social contract** that ensures the computer will be used for social good. Information services enters into the contract with individuals and groups that use its information output or are affected by it. The contract is not in writing but is implicit in everything that information services does.

The contract stipulates that:

- The computer will not be used to unduly invade a person's privacy.
- Every measure will be taken to ensure the accuracy of computer processing.
- The sanctity of intellectual property will be protected.
- The computer will be made accessible to society so that its members can avoid the indignities of information illiteracy and deprivation.

In summary, the information services community must assume responsibility for the social contract that emerges from the systems we design and implement.

CODES OF ETHICS

Because computers raise special ethical problems, people who work with computers tend to avoid the theoretical issues. Computer professionals prefer to set practical guidelines for ethical behaviour. Four U.S. professional computer societies have drafted codes of ethics to guide their members. These societies are the ACM (Association for Computing Machinery), DPMA (Data Processing Management Association), ICCP (Institute for Certification of Computer Professionals), and ITAA (Information Technology Association of America).

ACM Code of Professional Conduct

The ACM was formed in 1947 and is the oldest of the U.S. professional computing societies. In an attempt to formulate a set of ethical principles for computer professionals, the ACM developed a statement of the ethical values of its members. Its Code of Professional Conduct consists of five *canons:*

1. An ACM member shall act at all times with integrity.
2. An ACM member should strive to increase the member's competence and prestige of the profession.
3. An ACM member shall accept responsibility for the member's work.

4. An ACM member shall act with professional responsibility.
5. An ACM member should use the member's special knowledge and skills for the advancement of human welfare.

The ACM code recognizes the responsibility of the ACM member to himself or herself, to the profession, and to human welfare.

DPMA Code of Ethics

The DPMA was founded in 1951 and has about 35,000 members worldwide. Its mission is to "advocate effective, responsible management of information to the benefit of its members, employers, and the business community." Its code consists of *standards of conduct* that spell out the obligations of the data processing manager to (1) the firm's management, (2) fellow DPMA members and the profession, (3) society, and (4) his or her employer.

ICCP Code of Ethics

The ICCP was founded in 1973 for the purpose of certifying computer professionals. Its certifications include the Certified Computer Programmer (CCP) and the Certified in Data Processing (CDP). In order to become certified the applicant must pass an examination and agree to abide by the ICCP's code of ethics.

The ICCP ethics code recognizes the obligations of its members to the profession, the members' employers, and the members' clients. Its code is embodied in a *Code of Conduct*, one meant to be relatively permanent, that deals with such issues as social responsibility and conflict of interest. The ethics code also includes a *Code of Good Practice*, which is intended to be updated periodically. One of the good practice codes specifies that violations can result in a revocation of certification. The ICCP ethics code is the only one with real teeth in it.

ITAA Code of Ethics

Whereas the memberships of the ACM, DPMA, and ICCP consist of individuals, the ITAA was founded in 1961 as an association for organizations that market software and computer-related services. Its code consists of *basic principles* that address judgement, communication, and quality service in dealing with clients. The companies and employees are also expected to uphold the professional integrity of the computer industry.

ETHICS AND INFORMATION SPECIALISTS

Many researchers have studied the ethical beliefs of information specialists. A number of studies have been conducted on both practising information specialists and college students majoring in information systems. These studies typically employ **conflict of ethics scenarios**, which are descriptions of certain acts that the subject evaluates as being either ethical or unethical. The scenarios, therefore, provide a way to measure the subject's ethical beliefs.

The SRI Studies

Two studies during the 1970s and 1980s provide most of the data that describes the ethical beliefs of practising information specialists. The first study came in 1977 and consisted of a computer science and technology ethics workshop, which was sponsored by SRI International and utilized conflict of ethics scenarios. Ten years later, the study was repeated to incorporate new technology in a revamped set of scenarios.

The Study Participants Participants in the 1987 workshop included twenty-seven persons from industry, government, and academia. Because of their practical experience, these participants were regarded as information specialists.

The Conflict of Ethics Scenarios The 1987 workshop used fifty-four scenarios; an example appears in Fig. 5.3.

A university student used the campus computer network as an authorized user. The service director announced that students would receive public recognition if they successfully compromised the computer system from their terminals. Students were urged to report weaknesses they found. This created an atmosphere of casual game playing and one-upmanship in attacking the system.

The student found a means of compromising the system and reported it to the director. However, nothing was done to correct the vulnerability, and the student continued to use her advantage to obtain more computer time than she was otherwise allowed. She used this time to play games and continue her attacks to find more vulnerabilities.

Fig.5.3 A conflict of ethics scenario

Table 5.1 shows the tabulation of responses by the experts to three ethics questions relating to the scenario. Twenty experts thought the student's behaviour was unethical, one thought it not unethical, and four thought that no ethics issues were involved. In terms of the service director, the feelings were more mixed. Nine thought that by encouraging the student to compromise the system, the director had acted unethically. Seven said he had not acted unethically, and nine felt that ethics was not an issue. Eighteen thought that by not correcting the vulnerability, the director had acted unethically, three said he had not acted unethically, and four saw no ethics issue.

Table 5.1 How the workshop participants Responded to the scenario

Category	No. of Responses
Student using computer services by taking advantage of a vulnerability	
Unethical	20
Not unethical	1
No ethics issue involved	4
Service director encouraging compromise of the computer system	
Unethical	9
Not unethical	7
No ethics issue involved	9
Service director not correcting the vulnerability	
Unethical	18
Not unethical	3
No ethics issue involved	4

The 1987 SRI study provides an ethics benchmark against which the beliefs of information specialists and IS students can be compared. How do the beliefs of a programmer or a student compare to those of experts who have given the issues much thought—as viewed from the perspective of society?

The Susan Athey Study of High-Tech Students

In 1993 Susan Athey, a professor of computer information systems at Colorado State University, conducted an experiment that compared the ethical beliefs of sixty-five IS and computer science majors with those of the SRI experts. Athey used seven of the SRI scenarios and found that the students disagreed with ten of the experts' decisions. Where the experts viewed a scenario as describing unethical behaviour, the students saw it as not unethical. Professor Athey hypothesized that the differences were due to the greater experience of the experts, combined with the fact that the students observed much of the unethical behaviour on a daily basis in the form of misuse of computer time, software piracy, and so on—thus, perhaps accepting it as the norm.

ETHICS AND THE CIO

Perceptions of the CIO's Ethics

- Do not take advantage of opportunities to act unethically
- Ethics breeds success
- Firms and managers have social responsibilities
- Managers back up their ethics beliefs with action

Taking Advantage of Opportunities to Act Unethically Table 5.2 shows that opportunities exist in some firms for CIOs to engage in unethical behaviour. However, there is a strong feeling that the CIOs do not behave unethically. This means that many CIOs do not act unethically even when the opportunity presents itself. The figures from this table and also Tables 5.3 and 5.4 do not always add up to 100% for a variety of reasons, including missing data and rounding.

Table 5.2 CIOs usually do not act unethically, even though the opportunity exist

Question	Agree (%)	Disagree (%)
There are many opportunities for MIS managers in my company to engage in unethical behaviour.	47.5	37.7
MIS managers in my company engage in behaviours that I consider to be unethical.	19.7	80.3

Ethics Breeds Success Table 5.3 relates ethics to success. It shows that successful CIOs are ethical and that success does not require one to compromise ones's ethics. The table also shows that successful managers do not withhold information, make rivals look bad, look for scapegoats, or take credit that they do not deserve. These responses indicate that the CIO and other managers create an ethics culture.

Ethics Breeds Success Table 5.3 relates ethics to success. It shows that successful CIOs are ethical and that success does not require one to compromise ones's ethics. The table also shows that successful managers do not withhold information, make rivals look bad, look for scapegoats, or take credit that they do not deserve. These responses indicate that the CIO and other managers create an ethics culture.

Table 5.3 ethics and success

Question	Agree (%)	Disagree (%)
Successful MIS managers in my company are generally more ethical than unsuccessful managers.	73.8	13.1
In order to succeed in my company, it is often necessary to compromise one's ethics.	18.0	75.4
Successful managers in my company withhold information that is detrimental to their self-interest.	21.3	50.8
Successful managers in my company make rivals look bad in the eyes of important people in my company.	23.0	59.0
Successful managers in my company look for a scapegoat when they feel they may be associated with failure.	23.0	67.2
Successful managers in my company take credit for the ideas and accomplishments of others.	16.4	75.4

Firms and Managers Have Social Responsibilities Table 5.4 shows that managers must often put their responsibility to society before their responsibility to the firm and that both firms and managers have social responsibilities that go beyond their responsibilities to the stockholders.

Managers Back Up Their Ethics Beliefs with Action The information specialists believed that top management in their firms had communicated their lack of tolerance for unethical behaviour and would take action against anyone violating those standards.

Using the Vitell-Davis study as the basis, we can conclude that a supportive ethics culture exists in most firms and that the CIO is seen as a good role model.

Table 5.4 corporate social responsibility

Question	Agree (%)	Disagree (%)
The socially responsible manager must occasionally place the interests of society over the interests of the company.	68.9	21.3
The fact that corporations have great economic power in our society means that they have a social responsibility beyond the interests of the shareholders.	96.7	3.3
As long as corporations generate acceptable shareholder returns, managers have a social responsibility beyond the interest of shareholders.	70.5	16.4

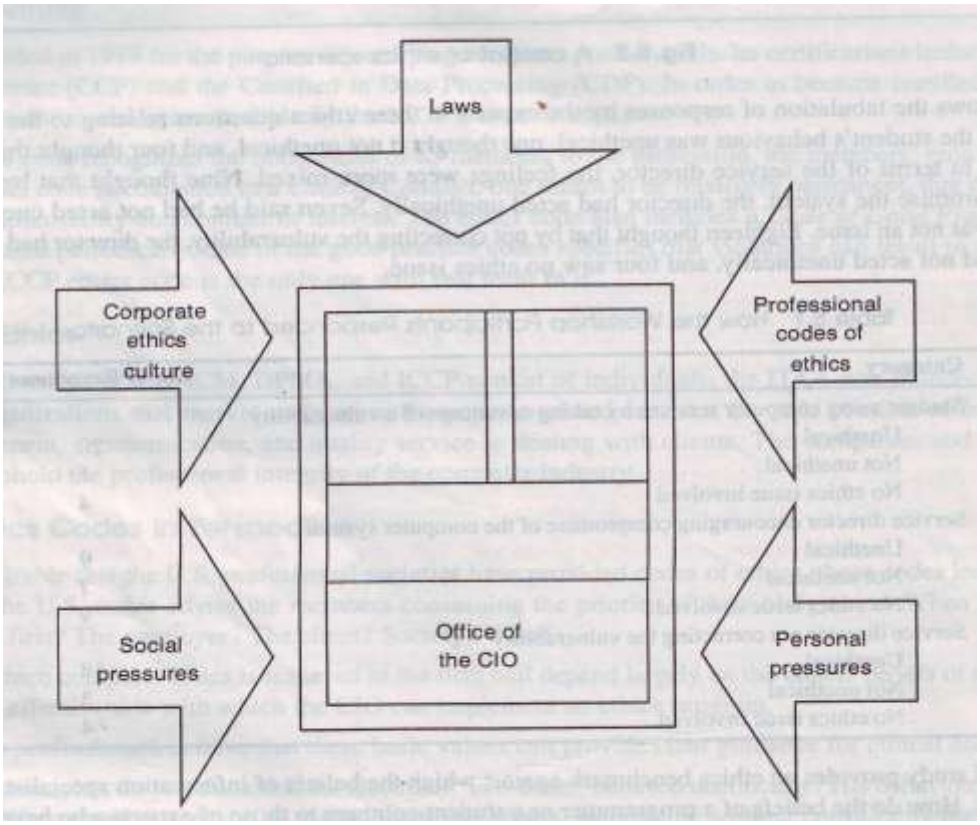


Fig.5.4 the CIO is influenced by a hierarchy of factors

Achieving an Ethical Computer Operation

1. Formulate a code of conduct.
2. Establish rules of procedure relating to such issues as personal use of computer services and proprietary rights to computer programs and data.
3. Make clear the sanctions that will be taken against offenders-such as reprimands, termination, and civil action.
4. Recognize ethical behavior.

Focus attention on ethics by means of such programs as training sessions and required reading.

6. Promote computer crime laws by keeping employees informed.
7. Keep a formal record that establishes accountability of each information specialist for her or his actions, and also minimizes the temptations for violations by means of such programs as ethics audits.
8. Encourage the use of rehabilitation programs that treat ethics violators in the same way that corporations show concern for the recovery of alcoholics or drug offenders.
9. Encourage participation in professional societies.
10. Set an example.

An Information Services Code of Conduct

- Conduct all activities in a manner that precludes any form of dishonesty
- Avoid any act that compromises integrity
- Avoid any act that might create a dangerous situation
- Not use alcohol or drugs while at work
- Maintain courteous and professional relations with users, associates, and supervisors
- Adhere to the no-solicitation rule and any other employment policy
- Protect confidentiality of sensitive information about the organization's competitive position, trade secrets, or assets
- Exercise sound business practice in the management of such company resources such as personnel, computer use, outside services, travel, and entertainment

CONTROLLING PREWRITTEN SOFTWARE

When a firm is serious about controlling its prewritten software, it can take the following steps:

1. Announce to the employees that the company has decided to embark on a software management policy and explain why. The announcement should come from someone high in the organization—the president or a vice-president. The announcement should make it clear that the company is serious about the project and expects everyone to co-operate.
2. Hire a software manager—someone who is technically competent in the areas of networks and databases.
3. Provide the software manager with an adequate budget to support the operation, which will include the hiring of a staff and making software purchases in quantity in order to receive discounts.
4. Establish a software committee of top-level managers to establish policy concerning such things as acceptable vendors for particular types of software.
5. Conduct an audit to find out what software is on each computer and server. Auditing software is available to perform this task for networked systems. Ask users if they use all of the software on their systems. Go ahead and remove any unused software and archive licensed software for possible future use by other users.
6. Assemble proof of licences. Original copies of the licence, purchase orders, or check requests are acceptable proof; so too are serially numbered diskettes and the original page of the user manual. Catalogue this documentation by department rather than on the basis of the company as a whole. Departmental control is much easier to enforce.
7. Remove unlicensed software. The authorization for the removal should come from the same executive, or executives, who announced the software management policy. While removing the software, be careful about data files. Have users archive all of their data before the software removal is performed.

By establishing a formal system for controlling its prewritten software, a firm can achieve and maintain control. Anything less is likely to be unsuccessful.

Despite statistics supporting widespread ethics violations, however, the general feeling is that firms and their managers are not only aware of their ethical responsibilities but make honest efforts to abide by them.

This is not to say that there is little room for improvement. Parker's ten-step action plan seems very reasonable for any CIO to follow. However, only 13 per cent of the information specialists in the Vitell-Davis study indicated that their firms had formal, written ethics codes. There is considerable opportunity for CIOs to formalize their ethical beliefs in the manner that Parker suggests.

PLAGIARISM

Plagiarism is the unauthorized use of another person's original words or ideas. You may have heard discussions at your college about plagiarism, for it has been around a long time. People sometimes plagiarize by copying another's writing from a book or a term paper. Plagiarism is not only unethical behaviour; it is also a violation of copyright law—a form of intellectual theft. Unfortunately, the Information Age and word processing have made plagiarism much easier.

For example, a college student loaned a fellow student the disk containing her bibliography for the class term paper. He used it for his term paper and then passed it along to ten other students. The professor saw identical bibliographies in their papers, and all received a reprimand for their actions. This accessibility means that each student must take more stringent measures to avoid plagiarizing, even unintentionally.

All kinds of information are distributed on floppy disks and optical disks these days. This information includes magazine articles, the works of William Shakespeare, book excerpts, works from the Internet—the list goes on and on. In addition, it is not uncommon to obtain information from electronic sources over the telephone lines. While using this information responsibly and ethically, you must cite the source whether your work is a paraphrase or a direct quotation—in a reference or citation, providing the author's name, the article title, where it was published, the date, and so on.

Most information can easily be plagiarized simply by copying portions of text into a word processor and creating a file. The plagiarist may simply put his or her name on the document. Some try to obscure the plagiarism by changing a few words, modifying some sentences, adding or deleting a paragraph here and there, and calling the result an original work. But the plagiarist knows that he or she has committed an unethical act. And although a short-term goal may have been met—that of getting a term paper in on time—the long-term goal of acquiring knowledge through the learning process and disseminating it through the effective use of language has not. Plagiarism, like other unethical acts, really hurts the plagiarist most of all.

A recent college graduate was hired as a staff writer of a well-known investment advice newsletter. Key to the newsletter's success were its original insights into the market and its unique perspective on investments. This young woman worked hard but often ran late on her deadlines. Fearful that she would not have an article done in time, she plagiarized an article from a magazine published by an investment services company, typing it into her word processor and submitting it as her own work. The editor immediately sensed the lack of insight in the work and challenged its originality. The woman confessed that she had plagiarized the work, and although her editor understood the reason, the plagiarism was the ground for dismissal. The writer could not be trusted to report and write ethically and responsibly again, and thus her career as a writer and journalist came to an abrupt and unfortunate conclusion.

THE COMMANDMENTS OF COMPUTING

The computer Ethics in Washington, D.C., has attempted to codify these principles into a set of 'commandments' for computer users and computer professionals. The institute has formulated the following guidelines:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which thou hast not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program thou art writing or the system thou art designing.
10. Thou shalt always use a computer in ways that show consideration and respect for thy fellow humans.

A PERSONAL ETHICS GUIDE

1. Is it honourable?
   Is there anyone from whom you would like to hide the action?
2. Is it honest?
   Does it violate any agreement, actual or implied, or otherwise betray a trust?
3. Does it avoid the possibility of a conflict of interest?
   Are there other considerations that might bias your judgement?
4. Is it within your area of competence?
   Is it possible that your best effort will not be adequate?
5. Is it fair?
   Is it detrimental to the legitimate interests of others?
6. Is it considerate?
   Will it violate confidentiality or privacy, or otherwise harm anyone or anything?
7. Is it conservative?
   Does it unnecessarily squander time or other valuable resources?

Fig.5.4 questions that determine the ethics of an action