CHAPTER 12

COMPUTER ETHICS

Computer ethics has its roots in the work of Norbert Wiener during World War II. Wiener's book included

(1) An account of the purpose of a human life
(2) Four principles of justice
(3) A powerful method for doing applied ethics
(4) Discussions of the fundamental questions of computer ethics, and
(5) Examples of key computer ethics topics.

In the mid 1960s, Donn Parker of SRI International in Menlo Park, California began to examine unethical and illegal uses of computers by computer professionals. By the 1980s a number of social and ethical consequences of information technology were becoming public issues in America and Europe: issues like computer-enabled crime, disasters caused by computer failures, invasions of privacy via computer databases, and major law suits regarding software ownership.

During 1990s many universities introduced formal course in computer ethics. Many textbooks and other reading materials were developed. It triggered new research areas and introduction of journals.

Generally speaking, ethics is the set of rules for determining moral standards or what is considered as socially acceptable behaviors. Today, many computer users are raising questions on what is and is not ethical with regard to activities involving information technology. Obviously, some general guidelines on ethics are useful responsibly in their application of information technology.

General guidelines on computer ethics are needed for:

- Protection of personal data
- Computer Crime
- Cracking

12.1 Data Security

Personal data is protected by using an appropriate combination of the following methods.

Physical Security:

Physical security refers to the protection of hardware, facilities, magnetic disks, and other items that could be illegally accessed, stolen, damaged or destroyed. This is usually provided by restricting the people who can access the resources.

Personal Security:

Personal security refers to software setups that permit only authorized access to the system. User Ids and passwords are common tools for such purpose. Only those with a need to know have Ids and password for access.

Personnel Security:

Personnel security refers to protecting data and computer system against dishonesty or negligence of employees.

12.2 Computer Crime

A computer crime is any illegal activity using computer software, data or access as the object, subject or instrument of the crime.

Common crimes include:

- Crimes related to money transfer on the internet
- Making long distance calls illegally using computers
- Illegal access to confidential files
- Stealing hardware
- Selling or misusing personal
- Hardware and software piracy
- Virus
- Cracking
- Theft of computer time

It must be observed that 80% of all computer crimes happen from within the company. Over 60% of all crimes go unreported.

Making and using duplicate hardware and software is called piracy. We tend to pirate because:

- We like free things
- Why pay for something when we can get it for free?
- Our thinking and actions are self-serving
- If we have the opportunity to get away with something, benefit financially, and minimal risk is involved, the way in which we've been conditioned by our capitalist society to do it.

A virus is a self-replicating program that can cause damage to data and files stored on your computer. These are programs written by programmers with great programming skills who are motivated by the need for a challenge or to cause destruction. 57000 known virus programs are in existence. 6 new viruses are found each day.

Most of the computers in an organization have lot of free computer time to spare. In other words a lot of computer time is not used. Many solutions for using this spare time are being researched. However, this idle time of computers in an organization is being stolen illegally. Some other software runs on an idle computer without the knowledge of the organization. This is called theft of 'computer time'.

A commonly cited reference is the **Ten Commandments of Computer Ethics** written by the Computer Ethics Institute. This is given below.

- Thou shalt not use a computer to harm other people.
- Thou shalt not interfere with other people's computer work.
- Thou shalt not snoop around in other people's computer files.
- Thou shalt not use a computer to steal.
- Thou shalt not use a computer to bear false witness.
- Thou shalt not copy or use proprietary software for which you have not paid.

- Thou shalt not use other people's computer resources without authorization or proper compensation.
- Thou shalt not appropriate other people's intellectual output.
- Thou shalt think about the social consequences of the program you are writing or the system you are designing.
- Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans.

Computer crimes require special laws to be formed by the government. Different countries have different ways of making the laws and awarding punishment to those who commit the crimes. India has Cyber laws to prevent computer crimes.

12.3 Cracking

Cracking is the illegal access to the network or computer system. Illegal use of special resources in the system is the key reason for cracking. The resources may be hardware, software, files or system information. Revenge, business reasons and thrill are other common reasons for committing this crime.

12.4 Work, Family and Leisure

Portable computers and telecommuting have created the condition where people can take their work anywhere with them and do it any time. As a result, workers find their work is cutting into family time, vacations, leisure, weakening the traditional institutions of family and friends and blurring the line between public and private life. This is becoming an important issue in computer ethics.

Exercises

1. What is the need for a password to log into a computer system?
2. How does the Operating System enhance the Security ?