UNIT 4 SOCIAL, ETHICAL AND LEGAL ASPECTS

Structure **Page No.**

4.0 INTRODUCTION

The information systems, Internet and the World Wide Web have grown rapidly and are now used by millions of people worldwide. Their importance in every day life is well known, however, it is also important to realise that the information systems and Web are what we make them and the code of ethics and morals we apply on these. The Objective of this unit is to make all students familiar with the negative aspects of information systems.

The issues related to morals, ethics and privacy of information and action and the security of information systems are, increasingly, a focus of concern for the business community and the public at large. Accordingly, ethics, morals, privacy and security are active topics of discussion from a wide range of perspectives. We will be bringing in these concerns for deliberation in this unit.

4.1 OBJECTIVES

After going through this unit, you should be able to:

- appreciate the impact of information systems (IS) on society;
- recognise the effect of the changes in Information Technology on moral dimensions and ethical issues;
- appreciate the ethical principles and dilemma on account of information system;
- discuss responsibility, accountability and liability in the use and application of information system, and
- become familiar with information rights and intellectual property rights.

4.2 SOCIETY IN THE INFORMATION AGE

The commercialisation of information communication technologies has been widely recognised as an important tool for economic growth. Strategies to utilise information technology for development priorities and prospects vary from sector to sector, and from country to country.

Development Opportunities and the Information Age

There is an established consensus that the information age offers significant potential for growth in all countries. The benefits of communications networks, principally reduced transaction costs and the ability to overcome impediments to productivity are especially important in considerations of how developing countries might more fully participate in the global economy.

Despite the acknowledged potential of the information age for economic growth, most developing countries have yet to significantly benefit from the vast resources and opportunities made possible by information technology. There remains considerable uncertainty about the specific ways information technology can be applied to development goals and to promote identified objectives. Determining critical elements of a regulatory environment conducive for growth and development is particularly challenging, given the context- specific nature of the benefits of information technologies for productive economic and social activity. Importantly, the pervasive role of intellectual property rights in regulating almost all aspects of the digital economy has been insufficiently analysed as part of a broad development agenda for the digital economy. Patents, particularly pharmaceutical patents, have long been the subject of concern in and discussion of the role of intellectual property in development. This has occasioned neglect of other intellectual property rights such as copyright and trademarks. Yet, copyright law is essential to the viability of the Internet as a development tool. Virtually all aspects of the digital economy are affected by copyright or recent quasi-copyright systems that provide rights for technological protections of digital content. Copyrights, trademarks and patents each, and in some cases jointly, impact prospects for electronic commerce, access to computer software, the possibility of marketing cultural goods, the availability of educational content and much more. In short, intellectual property regulation permeates all aspects of the development opportunities occasioned by the commercialisation of information technology.

Broad Applications of Information Technology

Information technology has been applied to enhance four major categories of activities: governance, growth and supply / distribution of goods and services, adding value to existing services and the creation of new products and services. The range of activities that can benefit from information technology appears to be unlimited. Specifically however, the important issues for developing countries include how information technology can be used to overcome existing barriers in markets such as high transaction costs, inefficiencies in production, distribution and supply, while adding value to existing products and services and also creating new ones. Economists have noted that the failure of credit markets has been a major reason for underdevelopment. The prospects for secure electronic funds transfer may open up opportunities for financing entrepreneurial activity, which is important to stimulate local investment in information products. Investment in physical capital is critical to facilitate the use of new technologies in the production process. Investment in software is also particularly important. In OECD countries, software investments in the year 2000 accounted for over 50% of the investment in information technology. For local productivity to benefit from information technology, then, access to equity will be a vital component. Such access may be enhanced and facilitated by financial agreements through business to business (B2B) collaborations or other forms of financing by financial services available through the Internet.

Another key factor for growth is the quality of local labor. In this regard, the vast amount of educational resources available on the Internet is a critical resource for developing countries, as well as by linkages to institutions in developed countries. This extends beyond prospects for formal education. Specialised learning and ongoing informal education can take place through chat-rooms and other interactive forums enabled by the Internet. While the Internet cannot and should not replace structured educational systems, it is important to point out that the Internet has made it possible to access recent and up to date information about any number of subjects, and to improve the quality of materials currently available in developing and least developed countries. These uses can also have a hortatory effect on the quality of life in developing countries by improving the quality of general participation in civil society and ultimately, democratic governance and delivery of government services.

Information technology can be used to address infrastructural barriers that have hindered traditional supply and distribution chains in developing countries. However, this benefit only goes to products or services that have no "real time/space" component. In reality, most e-commerce transactions still require physical infrastructure such as a dependable postal service, electricity, phone lines, etc., to function effectively. Only fully digital products are significantly insulated from the need for and dependence on the infrastructural capacity. With respect to developing countries then, it is important to identify how applications of information technology might contribute to economic growth, the particular sectors that would benefit particularly from information technology, and the legal rules that are most closely related to these sectors.

Some Emerging Considerations

i) The Information Technology and Intellectual Property Interface

Despite indications of commitment from developed countries to support the integration of information technologies into development programs, most of the activities undertaken in the light of these commitments have failed to examine the important relationship between the regulation of information technology and global rules for intellectual property protection. As some scholars have argued, the information economy may require different rules with respect to the protection of content or even hardware, than the traditional economy. The contested boundaries between trademarks for domain names, business method patents for Internet businesses, and copyright protection for content all threaten precipitously to recreate high margins of difference between developed and developing countries. The irrepressible move to create a global property rights system in data and databases, both of which are the primary constitutive elements of the Internet and associated applications, together with the existing multilateral agreements create an unhealthy environment for development. In this "back to the future" paradigm, developing countries will be bound by international agreements that constrain their efforts to access the building blocks of economic growth which consist of access to content and competitive opportunities to create new markets and new products. It is important to note that this problem is not limited to developing countries; there continue to be conflicts and heated negotiations between stakeholders in developed countries about the nature and extent of rules designed for social and economic use of the information.

ii) Appropriating the Benefits of the Information Age

The Internet offers a dynamic set of technological tools, and is the subject of experimental regulatory frameworks and legal rules. It is unlikely that anything firm or consistently predictable will emerge any time soon to govern this digital space. For developing countries this presents both opportunities and challenges. Appropriating the benefits of the information age is directly related to how investments in information technology are influenced and supported by regulatory frameworks that promote innovation, access and use. In addition to capital investments in information technology, developing countries should undertake to invest in the necessary macroeconomic policies that will facilitate an environment where the domestic population is able to adapt to the existence of the Internet, and to encourage entrepreneurial uses of the different opportunities that information technology can offer to deal with existing distribution, dissemination and communication problems that bedevil developing country markets.

Information asymmetries introduced or supported by legal rules such as intellectual property rights, or regulatory policies affecting competition in the provision of telecommunications services, can skew the competitive advantages that information technologies offer for developing countries. The following points summarize important factors that need to be kept in mind in formulating information policies with a development focus.

1) Despite the emphasis on the need for a strong telecommunications infrastructure for greater physical access to the Internet, the development of third generation Internet technologies through satellite suggests that in a short period of time even this major problem may not be a significant barrier for access to the Internet. An important task, then, is to develop guidelines concerning how much developing country resources should be invested in adapting to the current Internet state of the art given the dynamic rate of innovation in communications technology. These are questions that require careful and sustained empirical analysis to ensure that in developing countries the digital divide does not remain a permanent feature of the information age.

2) Exploiting the potential of the Internet to facilitate development objectives requires access to hardware (computers), software and content. Innovation, competition and deregulation in the telecommunications industry will enhance the opportunities for access to hardware by citizens. Intellectual property agreements have important implications for access to software and digital content. In the context of software, developing countries need to explore alternatives to proprietary regimes, the most important being the Open Source model which has proven to be a dynamic and, in some instances, more effective model of software development. For developing countries the Open Source model is not just beneficial for improving access to software, but also for the opportunities it offers to facilitate the training of domestic software engineers, and the relatively low cost of complementary technologies.

3) Business method patents can have inhibiting effects on competition in new markets and the opportunities made possible by information technologies. Most economic analyses of business method patents suggest that such patents have an inimical effect on competition and organizational innovation. Developing countries should preserve domestic policy space to make decisions that are consistent with development priorities by adopting, as India has done, a *per se* rule against the patentability of business methods.

4) International copyright agreements have a significant and unavoidable impact on access to creative works in the digital age. The two WIPO Internet treaties have been implemented in a few developed countries in a manner that is highly restrictive and that imposes undue social costs on consumers. Developing countries should be aware that these two treaties affect access by wire and wireless means, and domestic limitations or exceptions to the rights granted by the treaties are likely to be influenced by interpretations of the TRIPS Agreement. Developing countries must insist on the possibility of enacting domestic limitations, including the application of compulsory licenses, to digital works.

5) The Appendix to the Berne Convention is currently the most prominent access model to literary works in international copyright law (Reference: www.unesco.org/culture/laws/copyright/images/copyrightconvention.rtf, The complete text of the Berne Convention and appendices can also be found at http://www.law.cornell.edu/treaties/berne/overview.html) However, developing countries have not successfully utilized the provisions of the Appendix with regard to facilitating access to protected works through compulsory licenses. Consequently, an alternative model must be considered. *Developing countries should consider, for example, adopting ad hoc provisions to deal with copyright*

in digital works, rather than adopting wholesale treaty provisions that may deprive them of policy options more conducive to national priorities. What is ultimately important is that, in the context of multilateral or bilateral negotiations, developing countries must appreciate the importance of copyright to the ability to access and realize the benefits of information technology and information goods. Robust access principles in the international agreements, or the freedom to impose such access mechanisms domestically, must be preserved for development purposes.

6) Institutions of higher learning are an important aspect of developing a strong technology base in any society. The possibility of distance education learning should occupy a central place in development strategies for the information age. This will require implementation of copyright treaties in a way that ensures that proprietary rights are balanced with public policy limitations that permit use and access for educational purposes, distinct from other socially beneficial uses.

4.3 MORAL DIMENSIONS

There are five moral dimensions (a) information rights, (b) property rights, (c) accountability, liability, and control, (d) system quality, and (e) the quality of life. Let us examine these in details.

a) Information Rights

With respect to privacy and freedom in an Information Society there have been some attempts to regulate the collection and use of information about individuals, as explained in Table 1.

Table 1: Principles of Fair Information Practices

1. There should be no personal records system whose existence is secret.
2. Individuals have right to access, inspect, review and amendment to systems that contain information about them.
3. Without prior consent there must be no use of personal information for purposes other than those for which it was gathered.
4. Managers of systems are responsible and can be held accountable and liable for the damages done by systems for their reliability and security.
5. Governments have the right to intervene in the Information relationships among private parties.

Many of us take our **privacy** and freedom for granted. It needs to be noted how technology is changing and challenging our basic assumptions about these issues; for example, video rental records are more protected from misuse and prying than are your medical records.

We all assume that the Constitution guarantees by us personal privacy and freedom from surveillance. If someone sets up a video camera inside your drawing room or on your front porch to monitor your every movement, what would you do? Such cases have happened, it's a fact. So how do we protect our privacy and freedom from surveillance in a high-tech world?

If ebay.com or rediff.com or Buy.com wants to collect information about your surfing habits and sell it to other companies, there is nothing to stop them. Absolutely nothing! However, in May 2006 with regard to Privacy for Phone Calls an Act has been passed by Govt. of India (rajyasabha.nic.in/bills-ls-rs/2006/XLI_2006.pdf)). As per this Act no body can make unsolicited calls for commercial or other illegal benefits.

Think about this: If information is supposedly collected for one purpose, is it ethical for that information to be used for a totally different purpose without your knowing it? Is it fair to require you to provide medical information that is primarily intended to be used to pay your insurance bills and then have that same information used against you when the insurance company deems you too expensive and cancels your policy? Is it fair to have that same information used against you in denying you employment because you're too expensive to hire?

Spamming (unsolicited emails) has been challenged in the courts by Internet Service Providers (ISP) as an unfair practice. The ISPs say the thousands of emails clog their systems and no one wants them anyway. The spammers argue that their right to Freedom of Speech is violated if they can't send emails to anyone they want. Which side are you on?

b) Property Rights: Intellectual Property

Intellectual property issues have been around for hundreds of years. Some of the laws and policies in place to settle disputes about **copyrights, patents**, and **trade secrets** have to be rewritten to apply to the Internet. Intellectual property is a result of someone's effort to create a product of value based on their experiences, knowledge, and education. In short, intellectual property is brain power.

What if you wrote the next great American novel, hoping to cash in big time? Maybe you could retire to the Bahamas and drink lemonade on the beach all day. But then you find out that someone posted your next great American novel to the Internet and everyone is reading it free of charge. Now you're back in your hometown drinking lemonade at the local mall while you decide whether to look for a job at McDonald's or Burger King. The good news is everyone loves your book!

Unfortunately, that sort of thing happens too often in cyber-world. You're pretty excited to get that free copy of the newest game software while the poor guy who spent hours of his time and effort writing it is not so excited to realise he's not getting any compensation.

Everything on the Web is considered to be protected under **copyright** and **intellectual property** laws unless the Web site specifically states that the content is public domain. The Web site doesn't need to carry the copyright symbol © in order for it to be protected. In the US, President Clinton signed a law in January 1998 making it a federal offense to violate copyright laws on the Internet, punishable with a fine up to $250,000.

Copyright laws and intellectual property rights cannot be violated on the Internet any more than they can be violated in other mediums. While this isn't a law class, you should be aware of the fine line between acceptable and legal usage of materials and the illegal theft of materials. When it comes to copyright material, the underlying ideas are not protected, just the publication of the material. On the other hand, a patent grants a monopoly on the underlying concepts and ideas. Before you use anything, especially any material on the World Wide Web, make sure you are using it legally and ethically.

Get past the idea that because everything on the Web is free, easy, and available 24 hours a day, it must be okay to use it however you want. The question you should be asking yourself is "s it ethically right and legal?"

c) Accountability, Liability, and Control

Many of our laws and court decisions establishing precedents in the area of **accountability**, **liability**, and **control** were firmly in place long before computers were invented. Many of them date back to the early 1900s, and some simply don't make sense in this day and age. That's what we were referring to when we talked about new questions for organisations, companies, and the workplace in general. No issue makes this subject more important than the Internet laws our government has tried and still tries to pass. Government of India has enacted a comprehensive law in the form of IT Act 2000 (Ref http://www.legalserviceindia.com/cyber/cyber.htm).

However, in the US, the opinion of the Communications Decency Act (struck down by the courts) and the Child Online Protection Act (currently in the courts) is that Internet Service Providers should somehow be liable for content placed on the Internet through their users. Ask yourself these questions: If you receive an obscene phone call, is the telephone company responsible and liable for the problem? If you receive a threatening letter in the mail, is the Post Office authority responsible for reading every piece of mail on the chance that there might be a problem in one of the letters?

d) System Quality: Data Quality and System Errors

As we rely on Information Systems more, data quality issues are gaining importance. These issues affect you as a consumer and as a user.

When the credit reporting agencies mess up your credit record and you can't get a car loan, whose fault is it? Yours or of the credit agency? What if you're driving down the road, the computer chip controlling your brake system fails, and you have a rather nasty crash? Who is at fault? You, the car company, or the company that made the computer chip?

Most of us use software that the manufacturer knows has bugs. Once in a while these bugs will affect our computer usage. Usually they are nothing more than an aggravation. If you review *Table 2* you'll see some instances of data quality problems that can severely affect businesses and corporations.

As more and more companies do business on the Internet, will Internet Service Providers be held accountable for equipment outages rendering those businesses unable to process transactions?

Table 2: Examples of Reported Data Quality

1. An airline inadvertently corrupted its database of reservations while installing new software and for months planes took off with half load.
2. A manufacturer attempted to recognise its files by customer number only to discover the sales staff had been entering a new customer number for each sale because of special incentives for new accounts. One customer was entered 7000 times. The company scrapped the software project after spending $ 1 million.
3. A manufacturing company nearly scrapped a $12 million data warehouse project because of inconsistently defined product data.
4. J.P.Morgan, a New York bank, discovered that 40% of the data in its credit risk management was incomplete, necessitating double check by users.
5. Several studies have established that 5 to 12 % of bar code sales at retail grocery and merchandise chains are erroneous and that the ratio of overcharges to undercharges runs as high as 5.1 with 4.1 as a norm. The problem tends to be human error keeping shelf prices accurate and corporate policy that fails to allocate sufficient resources to price checking, auditing and development of error file policies.

e) Quality of Life: Equity, Access, Boundaries

Invariably, when discussing online technology, some people mention their concern about losing the face-to-face contact with other human beings. We hear stories about children who haven't developed normal social skills because they spend all their time in front of a computer. No discussion about the quality of life issues would be complete without mentioning on-line love affairs. Of course, many people lose their jobs and their way of life because of technology. These are all valid concerns.

One quality of life issue that affects more and more people personally is the ability to work from home. Most telecommuters used to have a regular day job 9 to 5, five days a week in a typical office setting. If they didn't get their work done today, they would wait until they were back in the office tomorrow or Monday. Now because of technology they can work seven days a week, all hours of the day, at home. And sometimes they do. The impact on personal and family life can be considerable.

There is an upside to the jobs issue, though. Many parents like telecommuting because they can stay home with, or at least be nearer, their children. More and more people are leaving the big cities and moving to small towns for the quality of life, yet they can still keep their well-paying jobs. Many small companies are able to expand their customer base because of technology, which in turns helps the employees immensely. Completely new businesses are born because of technology.

Some people think we've reached the limit when they learn that we can now buy groceries online. After all, when you have everything loaded into the car, trying to find your way around a strange town, have three screaming kids in the back seat, and everyone is stressed out from the travel, the last thing you want to do is hunt down a grocery store. Why not email ahead and have your food and treats waiting for you when you check into your accommodations? What a terrific idea!

Computer crime is one area that has been extremely hard for our society and our governments to keep up with. Many laws have to be rewritten and many new laws must be implemented to accommodate the changes. **Computer crime and abuse** extends to any wrongdoing involving equipment and Internet usage, as *Table 3* shows. Anonymity cannot be a license for socially unacceptable behaviour. You should remember that everything you do on a network or the Internet is recorded and can be tracked. Many people committing computer crimes and abuse have been caught and prosecuted.

Table 3: Internet Crime and Abuses

Problem	Description
Hacking	Hackers exploit weaknesses in Web site security to obtain access to proprietary data such as customer information and password. They often use Trojan Horses posing as legitimate software to obtain information from the host computers.
Jamming	Jammers use software routines to tie up the computers hosting a Web site so that legitimate visitors cannot access the site.
Malicious Software	Cyber vandals use data flowing through the Internet to transmit computer viruses, which can disable computers they infect.
Sniffing	Sniffing is a form of electronic eavesdropping by placing a piece of software to intercept information passing from a user to the computer hosting a Web site. This information can include credit card numbers and other confidential data.
Spoofing	Spoofing is fraudulently misrepresents themselves as other organizations, setting up false Web sites where they can collect confidential information from unsuspecting visitors to the site.

Other issues affecting our society include job losses and career changes caused by technology. You can argue the positive or negative effects, but one thing is clear: you'll be a part of the evolution of technology for the rest of your life. You will have to continually update your skills and knowledge in order to remain competitive in the job market. As companies continue to embrace new technology and new methods of using it, you'll be responsible for ensuring your skills remain current.

Our government recognises the danger of allowing unequal access to technology to continue. It has enlisted the help of private individuals and corporations in an effort to install computers and Internet access in public schools and libraries across the nation. Most schools are now wired for networks and are learning to incorporate technology into the curriculum.

Health Risks: RSI, CTS, and Technostress

As managers, you should be acutely aware of the health issues caused by computer usage. Why? Because these health issues cost businesses huge amounts of money each year in medical treatment claims and lost productivity. **Carpal tunnel syndrome (CTS)** is the most serious health issue plaguing businesses. It doesn't take much to avoid the problems associated with computer usage. Ergonomics, the study of the relationship between humans and machines, has helped determine that it's cheaper to purchase equipment that reduces the health risks associated with computers such as different keyboards, monitors that reduce eye strain, and desks that allow proper body positions.

Too much of a good thing can be bad. You've heard of road rage, the anger people experience when driving. We are now experiencing road rage on the Information Superhighway, where it is called **techno-stress**. Managers should encourage employees to take frequent breaks from their computer and to recognize and understand the dangers of isolation. We may be a wired nation, but we still need the human touch.

How has all this technology affected you? Think about it. Ultimately, there is a positive and a negative side to everything. How you handle it determines how it affects you.

Management Actions: A Corporate Code of Ethics.

Many firms have not established a Code of Ethics or a policy for employee conduct when computing in today's workplace. Some corporations are confused about what to include and how to approach this new dilemma. It is felt that the five moral dimensions would be a good start. Businesses and their managers should recognise:

- The information rights to privacy and freedom
- The property rights to individual ideas and efforts
- The accountability, liability and control issues involved in using technology
- The system quality requirements of businesses and individuals
- The quality of life impact of technology

Companies can no longer ignore the necessity of establishing rules for technology usage. The issue will only continue to grow. If you work for a company that doesn't have a policy, you should encourage it to establish one immediately. If you're a manager in a company, you should get busy and establish a policy for your employees — it's the only fair thing to do.

4.4 TECHNOLOGY TRENDS AND ETHICAL ISSUES

New computer technologies for gathering, storing, manipulating, and communicating data are revolutionising the use and spread of information. Along the way, they are also creating ethical controversies. The speed and efficiency of electronic information systems, which include local and global networks, databases, and programs for processing information, force people to confront entirely new rights and responsibilities in their use of information and to reconsider standards of conduct shaped before the advent of computers.

The *Table 4* indicates the achievement due to technological progress of the Information System and their impact on the ethical issue.

Table 4: Information System Achievements and Issues

Achievement due to technological progress of Information System	**Impact / issue**
Computing power doubles every 18 months	Dependence on computer systems increases
Rapidly declining data storage costs	Easy to track a lot about individuals
Data mining advances	Analysis of vast quantities of data
Networking advances and the Internet	Remotely access, copy, share, and transfer personal data
New data and software standards agreed upon	data can be shared and processed easily
Mobile computing and tracking (radio frequency identification (RFID) product tracking tags	Effect: can be found anywhere & uniquely identified

The Importance of Ethics in Information Systems

Information is a source of power and, increasingly, the key to prosperity among those with access to it. Consequently, developments in information systems also involve social and political relationships — and so make ethical considerations in how information is used all the more important. Electronic systems now extend into all levels of government, into the workplace, and into private lives to such an extent that even people without access to these systems are affected in significant ways by them. New ethical and legal decisions are necessary to balance the needs and rights of everyone.

Ethics Fill the Gap as Legal Decisions Lag Behind Technology

As in other new technological arenas, legal decisions lag behind technical developments. Ethics fill the gap as people negotiate how use of electronic information should proceed. The following paragraphs define the broad ethical issues now being negotiated. Since laws deciding some aspects of these issues have been made, these paragraphs should be read in conjunction with Legal Issues in Electronic Information Systems.

Ethical Issues Specific to Electronic Information Systems

Ethics include moral choices made by individuals in relation to the rest of the community, standards of acceptable behaviour, and rules governing members of a profession. The broad issues relating to electronic information systems include control of and access to information, privacy and misuse of data, and international considerations. All of these extend to electronic networks, electronic databases, and, more specifically, to geographic information systems. Specific problems within each of the three areas, however, require slightly different kinds of ethical decisions.

Computer Crimes

Computer crime can be defined as an act of using a computer to commit an illegal act. The broad definition of computer crime can include the following:

- Targeting a computer while committing an offense (e.g., gaining entry to a computer system in order to cause damage to the computer or the data it contains).
- Using a computer to commit an offense (e.g., stealing credit card numbers from a company database).
- Using computers to support criminal activity (e.g., drug dealer using computers to store records of illegal transactions).

Computer Crimes and the Impact on Organisations

Dealing with viruses, PC theft and other computer-related crimes costs U.S. businesses a staggering $67.2 billion a year, according to the FBI report published in January 2006. The FBI calculated the price tag by extrapolating results from a survey of 2,066 organisations. The survey released found that 1,324 respondents, or 64 percent, suffered a financial loss from computer security incidents over a 12-month period.

The average cost per company was more than $24,000, with the total cost reaching $32 million for those surveyed. Often survey results can be skewed, because poll respondents are more likely to answer when they have experienced a problem. So, when extrapolating the survey results to estimate the national cost, the FBI reduced the estimated number of affected organisations from 64 persent to a more conservative 20 percent.

Under attack

Almost a fifth of U.S. businesses said they suffered 20 or more incidents such as virus infections in an FBI survey of computer security incidents at companies in the past year.

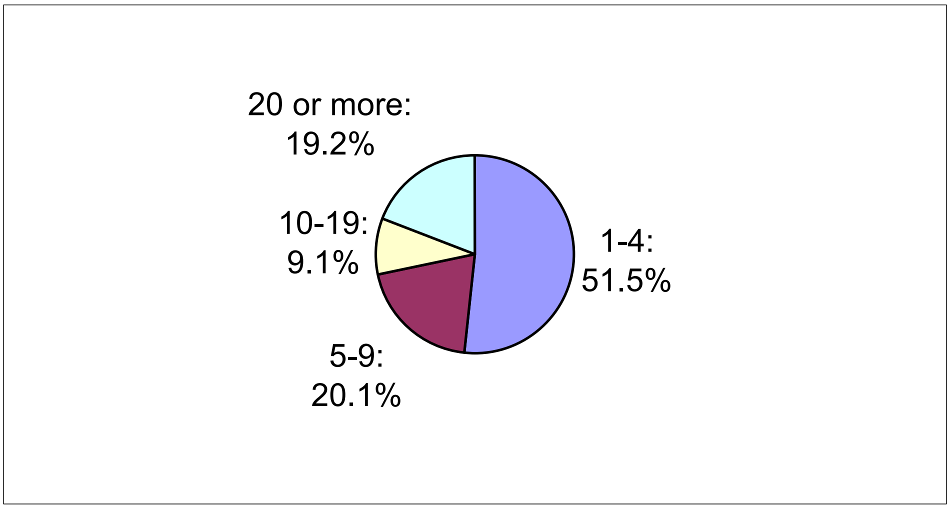

Figure 1: Loss by companies due to computer

This would be 2.8 million U.S. organisations experiencing at least one computer security incident, according to the 2005 FBI Computer Crime Survey. With each of these 2.8 million organisations incurring a $24,000 average loss, this would total $67.2 billion per year.

By comparison, telecommunication fraud losses are about only $1 billion a year, according to the U.S. Secret Service. Also, the overall cost to Americans of identity fraud reached $52.6 billion in 2004, according to Javelin Strategy and Research.

Other surveys have attempted to put a dollar amount on cyber security damages in the past, but the FBI believes its estimate is the most accurate because of the large number of respondents.

AS per FBI the data set is three or four times larger than in past surveys. It is obviously a staggering number, but that is the reality of what is seen.
Responding to worms, viruses and Trojan horses was most costly, followed by computer theft, financial fraud and network intrusion, according to the survey. Respondents spent nearly $12 million to deal with virus-type incidents, $3.2 million on theft, $2.8 million on financial fraud and $2.7 million on network intrusions. These figures do not include much of the staff, technology, time and software employed to prevent security incidents,. Also, losses to individuals who are victims of computer crime or victims in other countries are not included.

Defenses in place

As per FBI report survey respondents use a variety of security products for protection. Antivirus software is almost universally used, with 98.2 persent of respondents stating they use it. Firewalls follow in second place, with 90.7 persent, and anti-spyware and anti-spam are each used by about three-quarters of respondents.

The results mean that close to one in 10 organisations does not have a hardware or software firewall. Or perhaps they don't know they have one — the Windows Firewall in Windows XP, for example. Some are very small businesses that should have that technology, but they don't.

Biometrics and smart cards--both relatively new security technologies--were used only by 4 percent and 7 percent of survey respondents respectively. Intrusion prevention or detection systems were used by 23 percent and VPNs, or virtual private networks, by 46 percent.

Organisations were attacked despite use of security products, with nine out of 10 respondents saying they experienced a security incident. In fact, the most common attacks aligned with the most commonly used defenses. Computer viruses, worms or Trojan horses plagued 84 percent of respondents, 80 percent reported spyware trouble, and 32.9 percent said attackers were probing their systems using network port scans.

Computer Crimes – Who Commits Them?

Not all threats came from outside the organisation. More than 44 percent of the FBI survey respondents reported intrusions from within the company. Companies may be unaware of the internal potential for computer security incidents.

Unauthorised access Trend

As per the data available the unauthorised data access is decreasing (see *Figure 2*) because of the growing awareness of the users who are using various protection techniques.

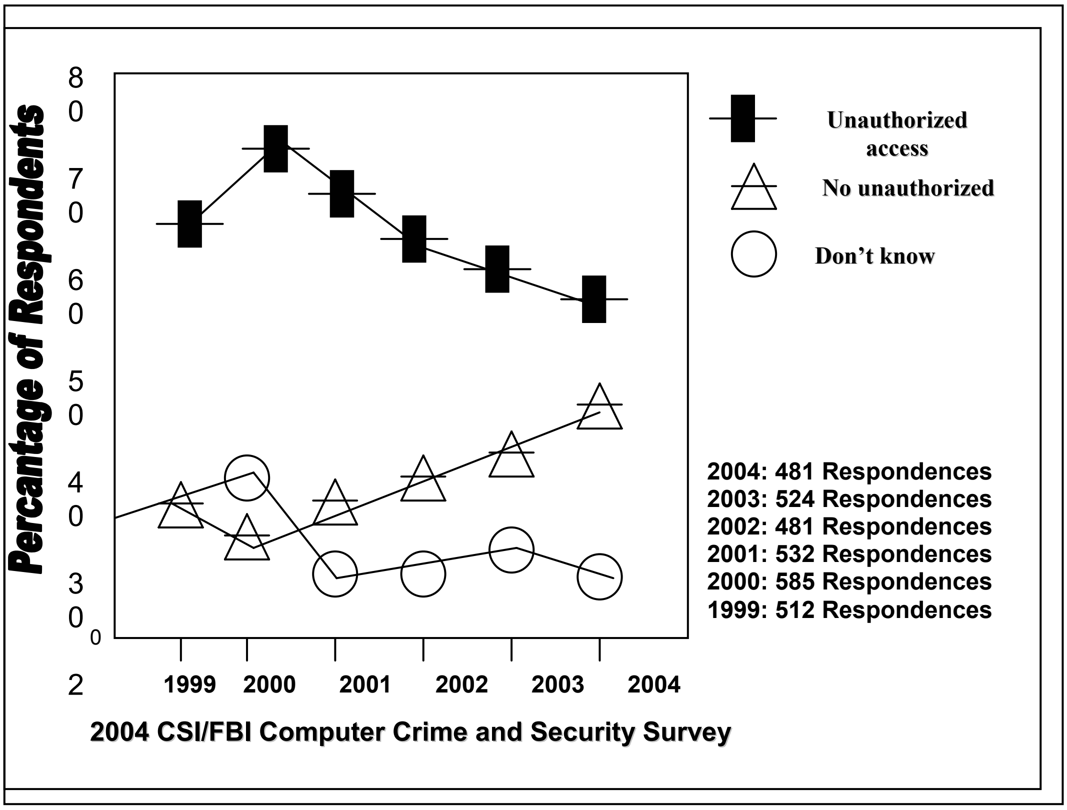

Figure 2: Unauthorized computer access trend

Computer Crime – Various Types

Let us look at the various types of computer crimes as explained in *Table 5*.

Table 5: Types of Computer Crimes

Data Diddling	The changing of data going into or out of a computer; for example, a student breaks into his/her university's grade recording system and changes the grades he/she earned in last semester's classes, thus raising his/her grade point average.
Salami Slicing	A form of data diddling that occurs when a person shaves small amounts from financial accounts and deposits them in a personal account, for example a bank employee deposits a few Rupees from each of thousands of accounts into an account set up in a fictitious name. The amounts are too small to raise flags, but over time the thief collects a substantial sum.
Phreaking	Crime committed against telephone company computers with the goal of making free long distance calls, impersonating directory assistance or other operator services, diverting calls to numbers of the perpetrator's choice, or otherwise disrupting telephone service for subscribers.
Cloning	Cellular phone fraud in which scanners are used to steal the electronic serial numbers of cellular phones, which are used for billing purposes and are broadcast as calls are made. With stolen serial numbers, clones can be made to make free calls that are billed to the owner of the original cell phone.
Carding	Refers to the practice of stealing credit card numbers online, to be resold or used to charge merchandise against victim's account.

Piggybacking or shoulder surfing	The act of simply standing in line behind a card user at an automated teller machine (ATM), looking over the person's shoulder, and memorizing the card's personal identification number (PIN). With the right equipment, the stolen numbers can then be placed on counterfeit access cards and used to withdraw cash from the victim's account.
Social Engineering	Gaining information needed to access computers by means of tricking company employees by posing as a magazine journalist, telephone company employee, or forgetful coworker to order to persuade honest employee to reveal password and other information. The information is then used to break into a computer system or to steal company equipment and other contraband.
Dumpster diving	This approach requires no technical expertise, since it consists simply of going through dumpsters and garbage cans for company documents, credit card receipts, and other papers containing information that might be useful.
Spoofing	A scam used to steal password for legitimate accounts on computers in which the spoofer uses a program that duplicates an organisation's login screen. When legitimate users login to the system, the counterfeit screen responds with an error message but secretly captures the user's ID and password. The swindle lets intruders pass as legitimate users, thus allowing them to steal computer time and resources.

Computer Crimes — Hacking and Cracking

Hackers is a term to describe unauthorised access to computers based entirely on a curiosity to learn as much as possible about computers. It was originally used to describe MIT students in the 1960s who gained access to mainframes. It was later used universally for gaining unauthorised access for any reason.

Crackers is a term to describe those who break into computer systems with the intention of doing damage or committing crimes. This was created because of protests by true hackers.

Computer Crime – Software Piracy

Software Piracy is the practice of buying one copy and making multiple copies for personal and commercial use or for resale is illegal in most countries while others offer weak or nonexistent protections. This has become an international problem as shown in *Table 6*.

Table 6: Software Piracy Levels in Various Regions

Region	Piracy Levels (%)	Dollar Loss ($M)
North America	23	7,232
Western Europe	36	9,600
Asia Pacific	53	7,553
Latin America	63	1,273
Mid East / Africa	56	1,026
Eastern Europe	71	2,111
(Source: BSA, 2004)		

Destructive Codes that Replicate

Viruses are the programs which disrupt the normal function of a computer system though **harmless pranks** or by **destroying files** on the infected **computer**. They come in several types:

- **Boot Sector** attaches to the section of a hard disk or floppy disk that boots a computer.
- **File Infector** attach themselves to certain file types such as .doc, .exe, etc.
- **Combination** viruses can change types between boot sector and file infector to fool antivirus programs
- **Attachment** released from an e-mail when an attachment is launched. Can also send themselves to address book

Worms are the destructive codes which also replicate and spread through networked computers but do damage by **clogging up memory** to slow the computer versus destroying files

Destructive Codes that do not Replicate

Trojan Horses are the programs which do not replicate but can do damage as they run hidden programs on the infected computer that appears to be running normally (i.e., a game program that creates an account on the unsuspecting user's computer for unauthorised access).

Logic or Time Bombs are a variation of a Trojan horse that also do not replicate and are hidden but they are designed to lie in wait for a triggering operation. (i.e., a disgruntled employee who sets a program to go off after leaving the company).

- **Time Bombs** are set off by dates (e.g., a birthday)
- **Logic Bombs** are set off by certain operations (e.g., a certain password).

Cyber war and Cyber terrorism

Cyber war is an organised attempt by a country's military to disrupt or destroy the information and communications systems of another country. Common targets include:

- Command and control systems
- Intelligence collection and distribution systems
- Information processing and distribution systems
- Tactical communication systems
- Troop and weapon positioning systems
- Friend-or-Foe identification systems
- Smart weapons systems.

Cyber terrorism is carried out through the use of computer and networking technologies against persons or property to intimidate or coerce governments, civilians, or any segment of society in order to attain political, religious, or ideological goals

Responses to the Threat

At greatest risk are those that depend highly on computers and networking infrastructure (i.e., governments, utilities, transportation providers, etc.) Responses include:

- Improved intelligence gathering techniques.
- Improved cross-government cooperation.
- Providing incentives for industry security investment.

4.5 ETHICAL PRINCIPLES AND DILEMMA

In today's information age, the social and ethical implications of information and communication technology (ICT) are enormous – and ICT is developing so rapidly that new possibilities emerge before the social consequences can be assimilated. New social / ethical policies for the information age, therefore, are urgently needed to fill rapidly multiplying "policy vacuums". But filling such vacuums is a complex social process that will require active participation of individuals, organisations, and governments – and ultimately the world community.

Globalisation has been given a practical shape by ICT developments and cyberspace has brought the word community closer for interaction and ICT has made possible – for the first time in history – a genuinely global conversation about ethics and human values. Such a conversation has implications for social policy that we can only begin to imagine. Traditional borders and barriers between countries have now become less meaningful because most countries are interconnected by the Internet. For this reason, individuals, companies and organisations in every culture can engage in global business transactions, distance education, cyber-employment, discussions of social and political issues, sharing and debating of values and perspectives. The points to be considered are; whether this "global conversation" will bring about better understanding between peoples and cultures? New-shared values and goals and new national and international laws and policies? Will individual cultures become "diluted," homogenized, blurred?

Issues: The worldwide nature of the Internet has already led to many issues which need of policies to resolve them. For example, if sexually explicit materials are provided on a web site in a culture in which they are permitted, and then they are accessed by someone in a different culture where such materials are outlawed as "obscene," then, whose laws and values apply? Should the "offending" person in the first culture be extradited to the second culture and prosecuted as a purveyor of pornography? Should the values of the first culture be permitted to undermine those of the second culture via the Internet?

Let us consider business transactions in cyberspace: Whose laws apply to business on the Internet? When people in one country purchase goods and services from merchants in another country, who should regulate or tax the transactions? And how will "cyber business" in a global market affect local business, local tax collections and local unemployment? What new laws, regulations, rules, practices should be adopted, and who should formulate them? What policies would be fair to all concerned?

And how will global cyber business affect the gap between rich nations and poor nations? Will that gap get even worse? Will ICT lead to a "new colonialism" in which the information-rich lord it over the information poor? Will economic and political rivalries emerge to threaten peace and security? What kinds of conflicts and misunderstandings might arise, and how should they be handled? – and by whom?

Or consider cyber medicine: medical advice and psychological counseling on the Internet, "keyhole" surgery conducted at a distance, medical tests and examinations over the net, "cyber prescriptions" for medicine written by doctors in one part of the world for patients in other parts of the world – these are just a few of the medical services and activities that already exist in cyberspace. How safe is cyber medicine? Who should regulate, license, control it?

Or consider education in cyberspace: hundreds of universities and colleges worldwide now offer educational credit for courses and modules. But when students earn university credits from all around the globe, who should set the standards? Who should award degrees and certify "graduates"? Will there be a "Cyber University of the World"? Will thousands of "ordinary" teachers be replaced by a handful of

"Internet-superstar teachers"? – or perhaps by teams of multimedia experts? – or even by educational software? Would such developments be wonderful new learning opportunities, or instead be educational disasters? What policies, rules, practices should be adopted and who should develop them?

At the social/political level of education, what will be the impact upon previously uneducated peoples of the world when they suddenly gain access to libraries, museums, newspapers, and other sources of knowledge? How will access to the world's great newspapers affect "closed" societies with no free press? Are democracy and human rights necessary consequences of an educated population with access to a free press? Will the Internet foster global democracy? – or will it become a tool for control and manipulation of the masses by a handful of powerful governments? – or powerful corporations?

Human Relationships: Of course, not all social/ethical issues which arise from ICT depend upon its global scope. Consider, for example, the impact of ICT on human relationships. How will family relationships or friendships be affected by mobile phones, palmtop and laptop computers, telecommuting to work and school, virtual-reality conferencing, cyber-sex? Will the efficiency and convenience of ICT lead to shorter work hours and more "quality time" with the family? – or will ICT create instead a more hectic and breathless lifestyle which separates family and friends from each other? Will people be isolated in front of a computer hour after hour, or will they find new friendships and relationships in "virtual communities" in cyberspace – relationships based upon interactions that never could occur in regular space-time settings? How fulfilling and "genuine" can such relationships be, and will they crowd out better, more satisfying face-to-face relationships? What does all this mean for a person's self-realization and satisfaction with life? What policies, laws, rules, practices should be put in place?

Social Justice: As more and more of society's activities and opportunities enter cyberspace – business opportunities, educational opportunities, medical services, employment, leisure-time activities, and on and on – it will become harder and harder for ICT "have-nots" to share in the benefits and opportunities of society. Persons without an "electronic identity" may have no socially recognised identity at all! Therefore social justice (not to mention economic prosperity) requires that society develop policies and practices to more fully include people who, in the past, have had limited access to ICT resources: women, the poor, the old, rural residents, persons with disabilities, even technophobes.

A good example is "assistive technology" for persons with disabilities. A variety of hardware and software has been developed in recent years to enable persons with disabilities to use ICT easily and effectively. As a result, people who would otherwise be utterly dependent upon others for almost everything suddenly find their lives transformed into happy, productive, "near-normal" ones. Visual impairments and blindness, hearing impairments and deafness, inability to control one's limbs, even near-total paralysis need no longer be major impediments to happiness and productivity. Given such dramatic benefits of assistive technology, as well as rapidly decreasing costs, does a just society have an ethical obligation to provide assistive technology to its citizens with disabilities?

Work: Work and the workplace are being dramatically transformed by ICT. More flexibility and choices are possible (e.g., tele-working at home, on the road, at any hour or location). In addition, new kinds of jobs and job opportunities are being created (e.g., webmasters, data miners, cyber-counselors, and so on). But such benefits and opportunities are accompanied by risks and problems, like unemployment of computer-replaced humans, "deskilling" of workers who only push buttons, stress keeping up with high speed machines, repetitive motion injuries, magnetism and radiation from computer hardware, surveillance of workers by monitoring software, and ICT "sweat shops" that pay "slave wages." A wide range of new laws, regulations, rules and practices are needed if society is to manage these workplace developments efficiently and justly.

Government and Democracy: ICT has the potential to significantly change the relationship between individual citizens and governments – local, regional and national. Electronic voting and referenda, as well as e-mailed messages to legislators and ministers, could give citizens more opportunities to make timely input into government decisions and law making. Optimists point out that ICT, appropriately used, can enable better citizen participation in democratic processes, make government more open and accountable and provide easy citizen access to government information, reports, services, plans and proposed legislation. Pessimists, on the other hand, worry that government officials who are regularly bombarded with e-mail from angry voters might be easily swayed by short-term swings in public mood, that hackers could disrupt or corrupt electronic election processes, that dictatorial governments might find ways to use ICT to control and intimidate the population more effectively than ever before. What policies should be put in place to take account of these hopes and worries?

Intellectual Property and Ownership: In the information age, the "information rich" will run the world, and the "information poor" will be poor indeed! Possession and control of information will be the keys to wealth, power and success. Those who own and control the information infrastructure will be amongst the wealthiest and most powerful of all. And those who own digitized intellectual property – software, databases, music, video, literary works, and educational resources – will possess major economic assets. But digitized information is easily copied and altered, easily transferred across borders, and therefore the piracy of intellectual property will be a major social problem. Even today, for example, in some countries over ninety percent of the software is pirated – not to mention the music and video resources! What new laws, regulations, rules, international agreements and practices would be fair and just, and who should formulate or enforce them?

It is also possible to mix and combine several types of digitized resources to create "multimedia" works of various kinds. A single program, for example, might make use of bits and snippets of photographs, video clips, sound bites, graphic art, newsprint and excerpts from various literary works. How large must a component of such a work be before the user must pay copyright royalties? Must the creator of a multimedia work identify thousands of copyright holders and pay thousands of copyright fees in order to be allowed to create and disseminate his/her work? What should the rules be and who should enforce them? How can they be enforced at all on the new frontiers of cyberspace?

4.6 RESPONSIBILITY, ACCOUNTABILITY AND LIABILITY

In the Information Systems discipline, increasing attention is being paid to the issues of professional ethics. Ethical choices are decisions made by individuals who are responsible for the consequences of their actions. Key elements include:

- **Responsibility:** An individual accepting the potential costs, duties, and obligations for decisions they make. May require social norms and laws to enable.
- **Accountability:** Mechanisms in social institutions to determine who is responsible and assessing responsibilities for decisions and actions.
- **Liability:** Political means to permit individuals to recover damages via due process. Due process insures laws are applied properly and laws are known and understood, with an ability to appeal to higher authorities.

Responsibility by software users expected by the software developers' is primarily the protection, or violation of that protection, of software programs. Issues relating to the copying of software programs and protection by copyright laws are discussed in detail in unit 4.8. Software users or consumers on the other hand may claim that they have the right to use a product for which they have paid, and indeed have the right to expect **Responsibility by the software vendors** that that product will be free of defects (bugs). This imposes a duty of quality (and professionalism) on the developers of the software to ensure that the software is indeed bug-free. Consumers expect that a product be competitively priced, providing value for money.

Professional **accountability** is an issue that is closely tied to many codes of ethical conduct. As per ethical code of conduct it is expected that members shall accept professional responsibility for their work and for the work of their subordinates and associates under their direction, and shall not terminate any assignment except for good reason and on reasonable notice. Members are expected to be accountable for the quality, timeliness and use of resources in the work for which he/she is responsible. In general, accountability lies at the root of vendor-client relationships, and is therefore relevant to both the professionals (from developers as well as from users side). Accountability is important because it shows that high-quality work is valued, encourages professionals to be diligent and responsible in their practice, and establishes just foundations for **Liabilities** and/or compensation when software does not perform according to expectations, or when professional advice turns out to be unreliable. Accountability is also important because computer software is used throughout our society, and is an essential component of many life-critical systems, such as transportation equipment (aircraft, trains, lifts), medical devices, toys, accounting and financial control systems (ATMs), weapons systems, communications devices (radar, telephones, televisions, satellites, networks), and domestic appliances (microwave ovens, TVs, refrigerators, air-conditioning systems).

Through encouraging a strong sense of professional accountability, we can attempt to ensure that those who are responsible for the safe functioning of these systems will do their utmost to ensure that systems are safe, and will minimize risks. Accountability runs a considerable risk of being eroded, however, when computers are made scapegoats for human failings or when developers of computer software deny any responsibility for the consequences of use of the software, even when this use is in accordance with the purpose for which the software was designed. Let us look at a scenario relating to accountability dilemma of this type. A computerized investment system was designed for and purchased by a pension fund management company. The user of the system became familiar with it, and requested IT staff (not the original designer) to make some modifications to the system. Shortly afterwards, substantial losses were incurred and payments to pensioners had to be cut. Who is accountable? The original system designer? The user who requested modifications? It is perhaps all too easy to blame the computer, apologize, and do nothing.

Accountability is generally assumed to include a number of components, viz.: responsibility (direct or indirect) and liability. Liability relates to who should pay compensation (financial redress, community service,…) as a result of being held responsible for an action. In some situations, liability may apply, i.e., requiring the payment of compensation to a victim even though the harm has not arisen through one's deliberate or direct actions. For example take an aircraft systems, if an aircraft crashes due to a system failure, then the airline is subject to liability even though the airline has not deliberately or directly caused the crash. Such cases of liability help to ensure that extraordinary care is taken over the development and maintenance of systems that have the potential to cause loss of life.

Although the definition of accountability is fairly straightforward, four barriers to accountability can be identified: the problem of too many hands; the computer as scapegoat; the problem of bugs; and ownership without liability. Computer software is especially vulnerable to the problem of too many hands, because most (if not all) software is necessarily designed and developed by a number of individuals, often at different points in time. Furthermore, software often has a symbiotic relationship with computer hardware. This makes it very difficult to identify precisely which person should take responsibility for any unexpected action. However, such complexity can be no defense and there is a clear need to attempt to identify who should take responsibility for the problem. If we do not attempt to apportion blame, not only will the responsible person(s) escape blame, but they may cause further problems to happen in the future. The net result is that accountability is eroded, with no one prepared to step forwards and take responsibility.

Information systems are often blamed for human errors because they intermediate communications between people. If a human action is mediated by a computer, there is a strong tendency to blame the computer rather than the human (designer, programmer or user) that caused the computer to produce incorrect information. With the increased use of computers, computers will be made scapegoats for human failings with increasing frequency. In this situation, it is vital to establish lines of responsibility because it is all too easy for humans to shirk their responsibilities.

Bugs include all types of software errors, including those made at the design, modeling and coding stages of system design. Bugs certainly make software unreliable and can cause system failure, with the potential for loss of life or severe damages. There has been an unfortunate tendency for bugs to be seen as an inevitable aspect of computer systems, even as natural hazards that computer users have come to accept. This view is not restricted to the software developers, with prominent commentators on IT ethics voicing similar views, asserting “It is the nature of software programs to have errors…”. However, the very purpose of professional accountability is that we should identify who has caused a harm- whether intentionally or through negligence. If we accept that bugs are inevitable, then accountability becomes impossible - we can merely regret that harm was caused, but defend ourselves by saying that bugs are unavoidable (even expected) and therefore no one should be held responsible for the harm. There may even be resistance to liability — if no one can be identified as accountable, then why should anyone pay compensation - which is precisely why the concept of liability is so important. If, however, we do not view bugs as natural hazards, but as manifestations of unprofessional and sloppy work, we should be able to identify lines of responsibility, particularly for persistent bugs. Furthermore, if we are to act as true professionals, we cannot be satisfied with the notion that bugs are inevitable -it is like saying that the loss of human life through human error is inevitable, and that when we turn on a TV set, there is a reasonable chance that it will short circuit and electrocute us. Society has the right to expect that domestic appliances, and many other essential systems, will function safely.

As we have mentioned previously, the legal aspects of software product reliability are complex. Nevertheless, in order to understand the relationship between bugs and liability, it is instructive to introduce the legal rights and duties of developers and customers. *Strict* liability is generally applied by courts when a person or property is injured or damaged. Thus, purely economic damages are usually not put to Strict Liability. A second category of liability is known as negligence. Developers can avoid accusations of negligence by ensuring that they take reasonable care in the design, coding and testing of their products. One problem here relates to the thoroughness of testing. If a company has followed industry standards with regard to testing, then it would appear that if bugs still exist, it cannot be accused of including such bugs either deliberately or through carelessness. Whilst this does not obviate the requirement for software to be bug-free, it certainly does imply that industry standards may need to be set at very high levels. A third liability category is known as breach of warranty. A warranty is essentially a promise that the developer makes to the customer with regard to the functionality of the software, and forms “part of the contractual agreement between the seller and the buyer.

Having identified these categories of liability, it is important to note that pre-packaged software (Microsoft Word, Netscape Navigator, etc.) are generally recognised to be *products*, but custom-developed applications are considered to be *services*. This distinction is critical since while the standards of liability are applicable to products, they are not to services. Individually customized software must therefore be legally covered by the specific contract that is agreed upon between the developer and the customer, where penalties for non-functionality, lateness of delivery, etc. may be specified.

Computer software developers affirm that they sell a user the licence to install and use (typically) a single copy of a software package; they are not selling the ownership of the software. However, at the same time, software developers employ disclaimers to minimise as far as possible any liability (e.g., for financial or data losses) arising out of the customer's use of the software. Indeed, we note an unfortunate tendency for software producers to deny to the maximum extent possible any responsibility for actions caused by their software. *Same time, consumers are held to be liable for any use of the software that lies outside the narrowly-worded terms of the software license agreement.* This situation has the effect of eroding the rights of the user, since virtually all the risks of using the software (but few of the rights) are transferred to the user. Legally, these disclaimers have been recognised in courts so long as they are explicit and prominently displayed. There is evidence to indicate that the tendency to disclaim liability is growing more serious, noting that many software companies intend to implement measures that would have the effect of further diminishing consumers' rights.

Another consequence of minimizing liability is the software developers' parallel denial of responsibility for any bugs that they may include (intentionally or inadvertently) in the software. Essentially, when you buy software, you install and use it as is, i.e., at your own risk. We argue, however, that such transfer of risk is unreasonable because it imposes upon the developer no duty to ensure that software is bug-free, nor even - so long as these bugs do not cause loss of life or injury - to provide bug-fixes when they are identified. This seems to be both unethical and unprofessional — consumers have the right to use a product that fulfils the agreement with the vendor — explicitly or implicitly. At the same time, developers have a moral duty to ensure that the software they sell is usable and "fulfils the explicit and implicit contract between the buyer and seller. We maintain that if software developers wish to retain their ownership rights, then they should be both responsible and liable for their products, since they are in the best position (owning source code) to have direct control over the quality of their software.

We suggest that accountability and liability to compensate need to be separate. An individual programmer or software designer may be responsible for harm, but liability more properly lies with the employer, since it retains responsibility/ownership for the work of its employees. There is a strong need to clarify and promote standards of care in system design that are acceptable to users and developers alike — perhaps via a code of practice. Furthermore, the practice of extensive disclaims needs to be reviewed. Customers have the right to be informed if there are known bugs, irrespective of whether the developer intends to fix them, and irrespective of whether the developer thinks they are significant or not. Not informing the customer amounts to misrepresentation. Indeed, misrepresentation can be a form of contract violation and so may potentially attract legal penalties of a different kind. With respect to bugs, appropriate standards of testing need to be promulgated and adhered to, while excellent documentation of "who does what" should enable lines of accountability to be established. Independent software auditors may be called upon to verify software quality, if possible applying ISO standards.

Accountability is clearly vital not only for the information systems profession, but also for us as professionals, if we are to be held in the highest regard by those for whom we develop systems.

4.7 INFORMATION RIGHT AND ACTS

With respect to **Privacy and Freedom** in an Information Society there have been some attempts to regulate the collection and use of information about individuals. This aspect has already been covered in this unit. The information right and act are discussed in the section, so that as a manager, you will be able implement there in better way, however, the details given in this section is according to the initial Right of Information (2005) for updated details. You must list the official website of government of India.

RIGHT TO INFORMATION ACT: The Government of India in the year 2005 has enacted the Right to Information Act" (available at http://www.persmin.nic.in/RTI/WelcomeRTI.htm) to provide for setting out the practical regime of right to information for citizens to secure access to information under the control of Public Authorities in order to promote transparency and accountability in the working of any public authority. The Act is presented below:

ABOUT RIGHT TO INFORMATION

When does it come into force? It came into force on 12th October, 2005 (120th day of its enactment on 15th June, 2005). Some provisions have come into force with immediate effect viz. obligations of public authorities [S.4(1)], designation of Public Information Officers and Assistant Public Information Officers[S.5(1) and 5(2)], constitution of Central Information Commission (S.12 and 13), constitution of State Information Commission (S.15 and 16), non-applicability of the Act to Intelligence and Security Organizations (S.24) and power to make rules to carry out the provisions of the Act (S.27 and 28).

Who is covered? The Act extends to the whole of India except the State of Jammu and Kashmir. [S 12)].

What does 'information' mean? Information means any material in any form including records, documents, memos, e-mails, opinions, advice, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force but does not include file noting [S.2(f)].

What does Right to Information mean? It includes the right to

1) Inspect works, documents, and records.
2) Take notes, extracts or certified copies of documents or records.
3) Take certified samples of material.
4) Obtain information in the form of printouts, diskettes, floppies, tapes, video cassettes or in any other electronic mode or through printouts.[S.2(j)]

OFFICERS AND THEIR OBLIGATIONS

What are the obligations of public authority?: It shall publish within one hundred and twenty days of the enactment:

i) the particulars of its organisation, functions and duties;

ii) the powers and duties of its officers and employees;

iii) the procedure followed in its decision making process, including channels of supervision and accountability;

iv) the norms set by it for the discharge of its functions;

v) the rules, regulations, instructions, manuals and records used by its employees for discharging its functions;

vi) a statement of the categories of the documents held by it or under its control;

vii) the particulars of any arrangement that exists for consultation with, or representation by the members of the public, in relation to the formulation of policy or implementation thereof;

viii) a statement of the boards, councils, committees and other bodies consisting of two or more persons constituted by it. Additionally, information as to whether the meetings of these are open to the public, or the minutes' of such meetings are accessible to the public;

ix) a directory of its officers and employees;

x) the monthly remuneration received by each of its officers and employees, including the system of compensation as provided in its regulations;

xi) the budget allocated to each of its agency, indicating the particulars of all plans, proposed expenditures and reports on disbursements made;

xii) the manner of execution of subsidy programmes, including the amounts allocated and the details and beneficiaries of such programmes;

xiii) particulars of recipients of concessions, permits or authorizations granted by it;

xiv) details of the information available to, or held by it, reduced in an electronic form;

xv) the particulars of facilities available to citizens for obtaining information, including the working hours of a library or reading room, if maintained for public use;

xvi) the names, designations and other particulars of the Public Information Officers.[S.4(1)(b)].

What does a public authority mean? It means any authority or body or institution of self-government established or constituted: [S.2(h)]

- by or under the Constitution;
- by any other law made by Parliament;
- by any other law made by State Legislature;
- by notification issued or order made by the appropriate Government and includes any-
  - (a) body owned, controlled or substantially financed
  - (b) non-Government organization substantially financed directly or indirectly by the appropriate Government

.

Who are Public Information Officers (PIOs)? PIOs are officers designated by the public authorities in all administrative units or offices under it to provide information to the citizens requesting for information under the Act. Any officer, whose assistance has been sought by the PIO for the proper discharge of his or her duties, shall render all assistance and for the purpose of contraventions of the provisions of this Act, such other officer shall be treated as a PIO.

What are the duties of a PIO?

- PIO shall deal with requests from persons seeking information and where the request cannot be made in writing, render reasonable assistance to the person to reduce the same in writing.

- If the information requested for is held by or its subject matter is closely connected with the function of another public authority, the PIO shall transfer, within 5 days, the request to that other public authority and inform the applicant immediately.
- PIO may seek the assistance of any other officer for the proper discharge of his/her duties.
- PIO, on receipt of a request, shall as expeditiously as possible, and in any case within 30 days of the receipt of the request, either provide the information on payment of such fee as may be prescribed or reject the request for any of the reasons specified in S.8 or S.9.
- Where the information requested for concerns the life or liberty of a person, the same shall be provided within forty-eight hours of the receipt of the request.
- If the PIO fails to give a decision on the request within the period specified, he/she shall be deemed to have refused the request.
- Where a request has been rejected, the PIO shall communicate to the person making the requeste — (i) the reasons for such rejection, (ii) the period within which an appeal against such rejection may be preferred, and (iii) the particulars of the Appellate Authority.
- PIO shall provide information in the form in which it is sought unless it would disproportionately divert the resources of the Public Authority or would be detrimental to the safety or preservation of the record in question.
- If allowing partial access, the PIO shall give a notice to the applicant, informing:

  (a) that only part of the record requested, after severance of the record containing information which is exempt from disclosure, is being provided;

  (b) the reasons for the decision, including any findings on any material question of fact, referring to the material on which those findings were based;

  (c) the name and designation of the person giving the decision;

  (d) the details of the fees calculated by him or her and the amount of fee which the applicant is required to deposit; and

  (e) his or her rights with respect to review of the decision regarding non-disclosure of part of the information, the amount of fee charged or the form of access provided.
- If information sought has been supplied by a third party or is treated as confidential by that third party, the PIO shall give a written notice to the third party within 5 days from the receipt of the request and take its representation into consideration.
- Third party must be given a chance to make a representation before the PIO within 10 days from the date of receipt of such notice.

WHAT INFORMATION IS AVAILABLE?

What is not open to disclosure? The following is exempt from disclosure [S.8)]

1) Information, disclosure of which would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State, relation with foreign State or lead to incitement of an offence.

2) Information which has been expressly forbidden to be published by any court of law or tribunal or the disclosure of which may constitute contempt of court;

3) Information, the disclosure of which would cause a breach of privilege of Parliament or the State Legislature;

4) Information including commercial confidence, trade secrets or intellectual property, the disclosure of which would harm the competitive position of a third party, unless the competent authority is satisfied that larger public interest warrants the disclosure of such information;

5) Information available to a person in his/her fiduciary relationship, unless the competent authority is satisfied that the larger public interest warrants the disclosure of such information;

6) Information received in confidence from foreign Government;

7) Information, the disclosure of which would endanger the life or physical safety of any person or identify the source of information or assistance given in confidence for law enforcement or security purposes;

8) Information which would impede the process of investigation or apprehension or prosecution of offenders;

9) Cabinet papers including records of deliberations of the Council of Ministers, Secretaries and other officers;

10) Information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual;

11) Notwithstanding any of the exemptions listed above, a public authority may allow access to information, if public interest in disclosure outweighs the harm to the protected interests.

Is partial disclosure allowed? Only that part of the record which does not contain any information which is exempt from disclosure and which can reasonably be severed from any part that contains exempt information, may be provided. [S.10].

Procedure for requesting information

1) Apply in writing or through electronic means in English or Hindi or in the official language of the area, to the PIO, specifying the particulars of the information sought for.

2) Reasons for seeking information are not required to be given;

3) Pay fees as may be prescribed (if not belonging to the "below poverty line" category).

What is the time limit to get the information?

1) 30 days from the date of application.

2) 48 hours for information concerning the life and liberty of a person

3) 5 days shall be added to the above response time, in case the application for information is given to the Assistant Public Information Officer.

4) If the interests of a third party are involved then time limit will be 40 days (maximum period + time given to the party to make representation).

5) Failure to provide information within the specified period is a deemed refusal.

4.8 INTELLECTUAL PROPERTY AND RIGHTS

The copying of software programs, although nominally protected by copyright laws, is certainly widespread. While some may acknowledge that such copying is tantamount to theft, the activity persists if only because it is so easy, the chance of getting caught is considered negligible, and the software developers are perceived as being rich enough already. Such copying is not restricted to personal users – businesses are involved as well, though often inadvertently. It is not uncommon to notice that employees contribute significantly to the presence of illegal software in the workplace, posing serious financial and legal consequences for their employers. Among those [companies] surveyed, software decision-makers indicate that colleagues bringing software from home (40%), downloading unauthorized copies from the Internet (24%), and sharing programs with other employees (24%) are three of the most common forms of violation occurring in their companies.

The philosophical basis for software protection lies in the *prima facie* right to private property, particularly property that can be said to be the 'fruit of one's endeavors'. These views are not accepted by all nations with the same gravity. In Chinese society, for instance, the "socialization process emphasizes obligations and duties that promote conformity, collective solidarity, and obedience while downplaying assertiveness and creativity". The similarity between a "preoccupation with social order" in Chinese society and a "preoccupation with individual freedom" in Western societies is a point to be noted. These fundamental cultural and social differences certainly raise difficulties in legislative attempts to provide for universal protection of creativity.

A danger inherent in copyright protection is that when a technology is wholly owned by a single entity (individual, organisation), consumers may be harmed because the opportunity for competition is much diminished. Monopolies can lead to reduced evolution and diffusion of products, as well as overpricing and underproduction. Given these opposing forces, there clearly needs to be a reasonable balance between protection of a product on the one hand, and the right of consumers to avail themselves of the product at reasonable cost on the other. Indeed, in Korea and Japan there is a public assumption that new ideas and technologies should be shared in the public domain so that members of a society can benefit.

In many developing countries, meanwhile, governments are, quite naturally, more concerned that new technology should spread through all of a society as rapidly as possible, enabling the country to leapfrog older generations of technology and catch up with the rest of the world. The notion that technology should in some way be strongly protected, with profits going overseas, is not one that they feel is good for the development of the local economy. In such contexts, much of the argument about INTELLECTUAL PROPERTY AND RIGHTS (IPR) lies in the principles between rights and duties. Software producers claim that they have the right to protect the fruit of their endeavors — the software programs. Furthermore, they have the right to be compensated for the resources that they have expended in the development of that product. This right is translated into a right to charge consumers what they deem a fair price for the software products — a price that covers the various developmental costs, as well as generating profits that can be used for future product research and development. To protect their right to the protect fruit of their endeavors, they claim that consumers have a duty both to pay the price and to respect the intellectual property contained within the product — by not stealing it.

The notion of ownership of something, whether it has a physical form or not, does still make sense as intellectual property. There are a number of laws and agreements throughout the world to protect intellectual property rights. The right to copy or duplicate materials can be granted only by the owners of the information. This is called the copyright. Many documents on the Internet contain a statement that asserts that the document is copyrighted and gives permission for distributing the document in an electronic form, provided it isn't sold or made part of some commercial venture. Even items that don't contain these statements are protected by the copyright laws of the United States, the Universal Copyright Convention, or the Berne Union. Most of the copyright conventions or statutes include a provision so that individuals may make copies of portions of a document for short-term use. If information is obtainable on the Internet, and there is no charge to access the information, it can often be shared in an electronic form. That certainly doesn't mean you can copy images or documents and make them available on the Internet, or make copies and share them in a printed form with others. Quite naturally, many of the folks who create or work at providing material available on the Internet expect to get credit and be paid for their work.

Copyrights

Challenge by Electronic Information Systems : The fluidity of information on the networks has caused some confusion about how copyrights and intellectual property rights apply to electronic files. In the relatively small world of the original network users, an emphasis on free exchange of information and a common understanding of intellectual property allayed most potential conflicts over use of information. Now, as the networks grow larger and attract a broader range of people, some clarification of how electronic files may be used is becoming necessary. The ease with which electronic files can be distributed and the nature of some electronic information create problems within existing copyright law: either the law does not address the peculiarities of electronic information or the law is too easily subverted by the ease with which files can be copied and transferred. Similar problems have arisen with photocopy machines, VCRs, and tape recorders. To make matters more complex, other countries may have different copyright laws, so information made available globally through a network may not have the same protection in other places.

The basic existing copyright principles should keep most network users on ethical grounds.

- Copyrights protect original works of authorship, including literary, musical, dramatic, graphic, audiovisual, and architectural works, and sound recordings.
- The law forbids unauthorised reproduction, distribution, performance, or display of works with copyrights. The general intent of the law is to protect the commercial value of a work.
- Having a copy of a work with a copyright does not mean that the holder also has the right to distribute, reproduce, perform, or display it.
- Copyrights apply to both published and unpublished work. Under the international Berne Convention on copyrights, which the U.S. signed in 1989, a copyright comes into effect from the moment a work is created and is fixed in some form of tangible expression.
- A copyright notice is not required for copyright protection. The only way a copyright can be invalidated is by explicit announcement by the author that copyright protections are waived.
- Copyrights do not apply to titles, short phrases, names, slogans, mere listing of ingredients, or works consisting entirely of unoriginal information (such as standard calendars).
- Copyrights do not extend to ideas, procedures, methods, systems, concepts, principles, discoveries, or devices; these must be patented for protection.
- Remember, Complete international copyright protection does not exist. Works are subject to the laws of individual nations, although most nations have signed international agreements on copyrights.

Law for Work *Created* on a Network: The principles of copyright laws apply easily to work not created in an electronic file. But what about original work that is created within a network? The law applies in sometimes surprising ways, and users should think about copyrights before distributing or reproducing work created by another person. For instance: E-mail.

E-mail is protected by copyright. Information received in e-mail may be discussed, but the specific contents of e-mail have copyright protection.

Usenet postings may also be protected. These may be read and discussed by however, many people have access to the Usenet, but they cannot be reproduced and distributed in any way that may diminish the author's ability to profit from the original work — however farfetched such profit may seem. There is an interesting question concerning network postings, does the fact that anything you say in an on-line system can be downloaded and printed out by anyone who happens to read it create a different class of reproduction than quoting without permission from a commercial publication? If a journalist quotes something from an on-line system and does not obtain permission, did s/he steal it, or overhear it in a conversation? In such cases it can be concluded that whatever seems like fair use probably is, but that actual control of such use is impossible and that good manners are critically important.

Computer programs, which might appear to be ideas, procedures, systems, or devices, may be registered as literary works under the law, and therefore, receive copyright protection.

Check Your Progress 1

1) State whether True or False

(a) Everything on the Web is considered to be protected under copyright and intellectual property laws unless the Web site specifically states that the content is public domain.

True □ False □

(b) As per the data available, unauthorized data access is increasing day by day.

True □ False □

(c) The changing of data going into or out of a computer, for example, a student breaking into his university's grade system to manipulate his grade is known as Phreaking.

True □ False □

(d) Cloning refers to the practice of stealing credit card numbers online, to be resold or used to charge merchandise against victim's account.

True □ False □

(e) Viruses are the Destructive Codes that Replicate and Worms are the Destructive Codes that do not Replicate.

True □ False □

2) (a) What are the five moral dimensions an established organisation and its managers should recognise?

4.9 SUMMARY

In this unit social, ethical and moral aspects were discussed. This unit also covered what possible threats can be there from unknown sources in the form of malicious software or other cheating techniques relating to information systems so that necessary precautions can be taken to avoid these threats. Discussions also covered what are the acts relating to information rights and the Intellectual property rights.

Whether a person is a software developer or a software user, what are their responsibilities, accountabilities and obligations. This issue has also been covered here to make you ready for the industry as a responsible professional.

Since developments and changes relating to Information Systems are quite rapid, it is advisable to keep studying the professional subjects covered here through reading material as well as through the net.

4.10 SOLUTIONS / ANSWERS

Check Your Progress 1

1) (a) True, (b) False, (c) false, (d) False, (e) False,

2) (a) The five moral dimensions an established organization and its managers should recognise are:

- The information rights to privacy and freedom
- The property rights to individual ideas and efforts
- The accountability, liability and control issues involved in using technology
- The system quality requirements of businesses and individuals
- The quality of life impact of technology.

4.11 FURTHER READINGS

1) K.C. Laudon. and J.P. Laudon. *Management Information Systems:* Managing the Digital Firm (8th Edition). Prentice Hall, New Delhi

2) P. Hildreth and C. Kimble. Knowledge Networks: Innovation through Communities of Practice. Idea Group, New Delhi

3) J.R. Hicks. *Management Information Systems:* a User Perspective (3rd Ed). West, 1993, New Delhi

4) G.W. Reynolds. *Information Systems for Managers* (3rd Ed). West, 1992.

5) Robert Schultheis & Mary Sumner, *Management Information Systems:The Manager's View*, Tata McGraw Hill, New Delhi

6) Sadagopan S., *Management Information Systems*, Prentice Hall of India, New Delhi

7) Basandra S.K., *Management Information Systems*, Wheeler Publishing, New Delhi

8) Alter S., *Information Systems: A Management Perspective*, 3/e, Addison Wesley, New Delhi

9) Royce W., *Software Project Management: A unified Framework*, Addison Wesley, New Delhi

10) http://www-users.cs.york.ac.uk/~kimble/teaching/mis/mis_links.html

11) http://members.tripod.com/michaelgellis/tutorial.html

12) http://www.acsac.org/2002/tutorials.html