UNIT 1 THE ANALYST AS A PROFESSIONAL

Structure

1.0 INTRODUCTION

In the previous units, we have gone through the various stages of Systems Analysis and Design. This unit shall take you to the general but very interesting and important aspects of the multifaceted personality that every Systems Analyst should have. It draws your attention to the knowledge and skills that a systems analyst must acquire, the code of ethics and standards of practice that are expected from him. This unit also emphasises the practical need of the situation i.e. the role of the systems analyst while an organisation goes through different stages in the assimilation of new technology and at the same time planning for averting and coping with disasters. You will also find a reference to the computer and software related crimes and the systems analyst's duty to take care of privacy and data protection while designing any systcrn.

1 . OBJECTIVES

After going through this unit you shall be able to

- enumerate the attributes which a good systcrn analyst must have,
- have an idea of the factors which make it possible to implement a new systcrn in a changing environment,
- appreciate the precautionary measures to be taken to cope with possible of disasters,
- know about the computer crimes and software piracy.

1.2 ATTRIBUTES OF A GOOD ANALYST

Having gone through the earlier courses on hardware software and a variety of programming languages, it would have become apparent that system anaiysis is an activity that requires inputs from a number of directions. The task of a Systems Analyst is not algorithmic in nature. where he can pursue vigorously a series of steps and come out with the appropriate systems.

On the contrary, it would seem that an Analyst is like a juggler who maintains the delicate balance between different objects and the pressures and pulls arising from them to ensure that the show goes on successfully.

In fact, there have bccn systematic research studies to find out as to who can be a good Systems Analyst.

1.2.1 Knowledge and Skills Repertory

In the contcxt of what has been referred to above, G.Wcinberg and I. Shemer have summarised that a good Systcms Analyst should demonstrate:

> logical ability, mature judgement, thoroughness, practicality, ability to observe, ability to work with others, resourcefulncss, dislike of inefficiency, imagination, initiative, oral ability, integrity, intelligence, abstract reasoning, emotional balance, intcrest in technology, interest in analysis, intcrest in staff work, writing ability, numerical ability, curiosity, opcn-mindedness, decisivencss, selling ability, empathy, and intuition;

and be well versed **in:**

> organisational theory, the art of expression, law, information analysis, the **art** of interviewing, software engineering, project management, programming, economics, databases, uscr training. .

Apparently, the education of such a person is going to take time, possibly a lifetime, May be even more than a lifetime.

What has been stated above seems to be a tall order, and there could be valid sceptism whcthcr such training can be imparted at all. The natural conclusion would be that on the strength of some technical background as provided by good quality courses and training materials, a person aspiring to become a good Systems Analyst must continue to **learn** and gather knowledge from associate disciplincs as :vell as keep in touch with the progress in the main stream. Thcre is, therefore, no alternative but to adopt a commitment to life long learning.

1.2.2 Attitudes and Beliefs

Because the Systcms Analyst is in some sense at the core of the organisation, apart from his knowledge in the computer field and cven in the somcwhat rclcvant social sciences, his personality must reflect attitudes and beliefs which further his work and lead to greater success. Some of the important parameters which such a person must build in to his working style, is one of increased efficiency. Since it is not possible to cope with the vast arnount of information required to do the job, and the multifarious interactions with the numerous persons, the analyst is well advised to follow certain principles which help in doing work more efficiently. These have been encapsulated by Winston Flctchcr in his work on "supcr-efficiency", as follows:

(a) Persuasive communication

(b) Time rnanagcrnent

(c) Stopping procrastination

(d) Dominating data

(e) Innovative Ideas

(f) Travelling crcativcly

(g) People management

This is not to say that this is the only model which can be followed but to indicate that these should bc major concerns and positive effort would have to be made towards inculcating such a style.

1.2.3 Ecological Awareness and Green P.C.

In recent times, the consciousness and awareness of the finiteness of the earth, our resources arid the rapidly increasing consumptive pattern of society have become a cause of global concern. There is, therefore, now a backlash towards conservationism towards lesser exploitation of our natural rcsourccs and towards a'more positive attitude to reconstruction and rehabilitation of man-made destruction that may have been caused recently.

The above discussion translated into the context of computer based information systems is to urge the systems analyst to apply this consciousness so that unnecessary cohsumption is reduced. The consequences of higher rated power supply, hazardous radiation coming through video display units, the use of non bio-degradable materials in the hardware system and so on.

There are as of now no existing standards or regulations in India to enforce strict control measures. In contrast to say the laws for air and water pollution control. Even noise pollution is typically covered only under the general iaw of nuisance.

For example, it is common practice to suggest that any computer system should be placed only in air-conditioned surroundings. While this may add to the comfort level of the workers and to that extent contribute to some increase in productivity, the overall requirement of the electricity and the heat generated would definitely cause fair amount of thermal pollution. In contrast the storage of documents in digital form through high density compact storage media, results in saving of vast quantities of paper. Savings on this account could be equated to saving large tracts of forest areas from deforestation on account of otherwise having to fulfil the need for paper production. Of course, the fact lhat the plastic used in some of these media is not bio-degradable is also to be borne in mind.

The concern for the environmental factors has given rise lo the emergence of the term "Green P.C." to refer to a machine whose design has borne in mind such considerations. After the lead taken by many international companies in the field, in India too, various vendors have announced their own 'Green P.C.'. They are characterised by consumption of less power and the feature of consuming only say 30 watts in the stand-by mode. Kdocs not use chloro-fluoro carbons in the manufacturing process and uses recyclable packaging material.

Green P.C.

Defining A **Green** PC

A green PC consumes less than 30W of power in STANDBY mode. Its distinctive feature of vital importance is that its manufacturing process docs not include the CHLORO FLUORO CARBONS which arc responsible for harming the ozone layers. It also makes use of the recyclable packaging material.

There are two types of green PCs, viz. **LIGHT** GREEN and **DARK** GREEN PC's. A Dark Green PC consumes 15-20W in standby mode. It spins down the IDE and shuts off display. The use of it reduces system's clock speed to 8 MHZ. Its user can set the Power down timings of it. Also the options available with Hot Keys of it, facilitate the powering down system.

A Light Green PC consumes 25-30W in standby mode, which is more compared to a Dark Green PC. It also spins down IDE and shuts off display. But unlike the **Dark** Green PC, its IDE spin down timing is fixed.

Origin **of the** Green PC

In the US, PCs account for nearly 50% of all office automation equipment power consumption. A strange fact about the use of these PCs in the US is that these are rarely switched off over there. Hence, even during inactivity the PC continues to draw the same power. In June 1992 the Environment Protection Agency (EPA) of USA announced the Energy **Star** Programme to reduce electrical consumption and the resources required lo produce electricity. If power consumption on all PCs in the US could be cut down, then they calculated that:

TWO MEGA SIZED POWER PLANTS NEED NOT BE CONSTRUCTED

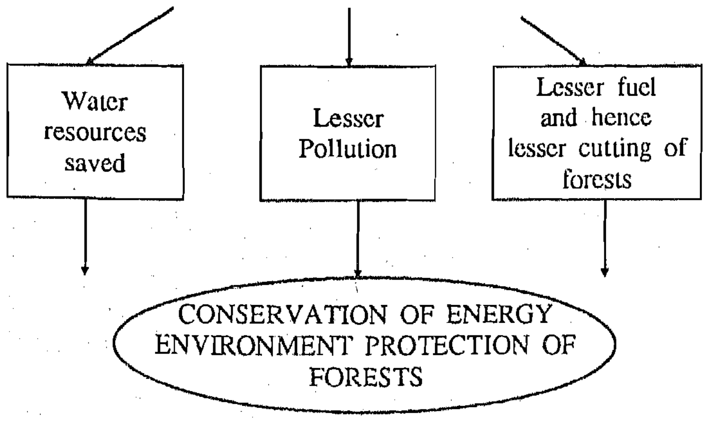
Water resources saved
Lesser Pollution
Lesser fuel and hence lesser cutting of forests
CONSERVATION OF ENERGY ENVIRONMENT PROTECTION OF FORESTS

Figure 1

PCs which were compliant with E.P.A. norms would be certified with the ENERGY STAR logo. In March, 1993, President Clinton ordered that within six months all PCs purchased by the Federal Government would have to be Energy Star compliant.

Designing a Green PC

POWER CONSUMPTION IN DARK GREEN PCs

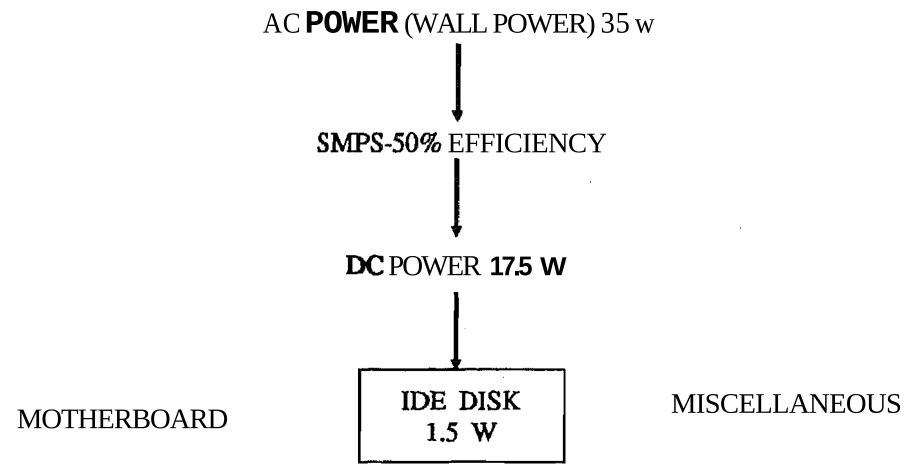

Figure 2

1. Motherboard: Power reduction is brought about by reducing system clock to 8 MHz (from 33 MHz) (Full power is 25.54 W and Green mode is 7.2 W).

2. IDE Drives: Green drives are different from the normal drives. (Seek mode (read or write) is 5.7 W, IDLE is 3.5 W and Green/inactive mode is 1.5 W).

3. CPU: An implementation called FREQUENCY SCALING uses an interrupt called STPCLK to reduce operating frequency from 33 MHz to 8 MHs. This is the minimum frequency required to keep the system functions operational. Here the full power is 4.75 Wand green mode is 0.80 W.

4. Display: Monitors should be designed to be DPMS (Display Power Management Signalling) compatible. Vertical and horizontal SYNC signals in a monitor are blocked for effective power management. Here the normal mode is 60 W A/C and green mode is 30 W A/C.

Power Down Setting

There are three options for setting the time after which the PC centres green mode.

Timer: Sleep timing is set by the user. The set up has different user definable time (e.g. 5110115 minutes) after which PC centres green mode.

Hot key: This is a combination of keys (similar to Ctrl-Alt-Del) which power down the PC.

Fixed: In light green PCs the IDE powers down automatically after a fixed duration of 10 minutes. The display power down can be set by the above two options.

1.2.4 Ethical Issues

All professionals, when they get -well established, and become responsible for their actions to society at large, as well as to the direct users of their services, then become in significant measures accountable for their actions. There are well defined qualifications and procedures for entry into the profession, there are bodies which regulate the conduct of the members of the profession and if necessary take disciplinary action including if necessary, debar a member from practice of the profession. This happens in the field of medicine, engineering, law, chartered accountants and so on. The recent emergence of the computer professions has been so new and a computer professional can be inducted from a number of different directions, that strict regulations for the profession have not so far been possible. There is today, no equivalent of the computer 'quack' as is understood for example in the field of medicine.

It is only recently that professional societies at a number of levels have started taking an interest in creating a code of ethics for computer professionals.

The International Federation for Information Processing(IFIP) is a multinational federation of professional and technical organizations (or national groupings of such organizations) concerned with information processing and computer science. There are currently 43 such organizations in IFIP representing 53 countries.

The aims of IFIP are to promote information science and technology by:

- fostering international cooperation in the field of information processing
- stimulating research, development and the application of information
- furthering the dissemination and exchange of information about the subject
- encouraging education in information processing.

Although the IFIP mentioned above has been in existence since January 1960, it has formally attempted to carry out a code of ethics project only from 1988. The project made a detailed analysis and comparison of 21 codes from Members Societies of IFIP and 7 other codes and it is only in 1994 that the code of ethics was put up for approval by the General Assembly.

In our own country, the Computer Society of India(CSI) which is an apex body of computer professionals has also created a code of ethics which it expects its members to observe. There is also a declaration which the members are required to sign.

Code of Ethics For IT Professionals (Applicable to members of CSI)

1. Aprofessional member of the Computer Society of India (CSI) shall:
   - organise the resources available to him and optimise these in attaining the objectives of his organisation.
   - use the codes of practice conveyed by the CSI from time to time in carrying out his tasks.
   - not misuse his authority or office for personal gains.
   - comply with the Indian laws relating to the management of his organisation particularly with regard to Privacy and Piracy and operate within the spirit of these laws.
   - conduct his affairs so as to uphold, project and further the image and reputation of the CSI.
   - maintain integrity in research and publications.

Codes of Practice

2. As regards his ORGANISATION an IT professional should:
   - act with integrity in carrying out the lawful policy and instructions of his organisation and uphold its image and reputation.
   - plan, establish and review objectives and tasks for himself and his subordinates which are compatible with the Codes of Practice of other professionals in the enterprise, and direct all available effort towards the success of the enterprise rather than of himself,
   - fully respect the confidentiality of information which comes to him in the course of his duties, and not use confidential information for personal gain or in a manner which may be detrimental to his organisation or his clients.
   - not snoop around in other people's computer files.
   - in his contacts and dealings with other people, demonstrate his personal integrity and humanity and when called to give an opinion in his professional capacity, shall, to the best of his ability, give an opinion that is objective and reliable.
3. As regards the EMPLOYEES, an IT professional should:
   - set an example to his subordinates through his own work and performance, through his leadership and by taking account of the needs and problems of his subordinates.
   - develop people under him to become qualified for higher duties.

- pay proper regard to the safety and well-king of the personnel for whom he is responsible.
- share his experience with fellow professionals.

4. As regards the CLIENTS, an IT professional should:
   - ensure that the terms of all contracts and terms of business be stated clearly.and unambiguously and honoured.
   - in no circumstance supply inherently unsafe goods or services.
   - not use the computer to harm other people or to bear false witness.
   - be objective and impartial when giving independent advice.
5. As regards the COMMUNITY,an IT professional should:
   - make the most effective use of all natural resources employed.
   - be ready to give professional assistance in community affairs..
   - not appropriate other people's intellectual output.
   - always use a computer in ways that ensure considemtion and respect for fellow humans.

Code of Ethics

UNDERTAKING

I, ________________________________ affirm that as a professional member, I shall abide by the Code of Ethics of the Computer Society of India (CSI). I further undertake that I shall uphold the fair name of the Computer Society of India by maintaining high standards of integrity and professionalism.

I am aware that any breach of the Code of Ethics may lead to disciplinary action against me under the Byelaws and rules of the CSI. 'I hereby confirm that I shall be bound by any decision taken by the CSI in such matters.

Place:______________ ______________

Date:_______________ (Signature)

However, such societies and professional groups have only a limited authority in meeting with the, requirements. There are occasions where the issues go beyond the regime of the professional society and into the courts of law. Some of these matters are discussed in a later section which relate to the interactions between the system analyst and the law.

1.3 ORGANISATIONAL ISSUES

In the previous sub-section, attention was drawn to the knowledge and skills that an analyst must acquire and the kind of attitudes and beliefs that he must inculcate.

Beyond the self, the analyst has to be involved in the organisation. If he is working for a software development company itself, then in fact, he has to go across two organisational cultures that of his own and that of a client. These organisational issues are of direct interest of the systems analyst. The most important of these is the different stages through which an organisation goes through in the assimilation of new technology. It is important to understand these phases of induction in new technology so that the activity is done in a successful manner.

1.3.1 Organisational Characteristics

Organisations that may decide to use computer based information systems may vary from small to large mega corporations. The decision making authorities and hierarchical structure prevailing in organisations vary significantly and the systems analysts must be able to appreciate the specific nature of authority in a given organisation. But for most situations, the characteristics which concerned the analysts are related to response of an organisation to the induction of new technology, This has an almost similar pattern across different organisations.

The first stage of course, is the decision to make an investment in the new technology. This is the result of some feasibility studies resulting in a commitment by the organisation to experiment with a new technology. Computers and other related equipment is bought, the organisation identifies to undertake one or a few development projects to begin with. New staff is sometimes brought in and the potential users undergo a training programme.

At this stage normally, two types of attitudes prevail Lhroughout the organisation, one welcoming the change and expecting a lot of benefits, possibly being over optimistic in their expectations and the contrary current urging continuance of the status quo. Both the streams have their leaders and a balance has to be maintained by curtailing the enthusiasm of the supporters and explaining to the critics the benefits of the expected new tcchnology.

If the first or the first few projects which are undertaken turn out to be successful, and the user groups begin to see an advantage by way of speeding up of their work and increased productivity, there is a clamour for new applications beyond those that were considered in the original plan.

User groups take a greater interest in refining their understanding of the technology and urge management for expanding the application areas.

Depending upon the success of the first phase, the computer professional gives increasing pressure from both directions. On the one hand, an increasing demand for new applications as end users become morc excited and computer become widespread and cheap. On the other hand, since the organisation is now become more dependent upon the new technology, there is an increasing problem of maintaining the old applications and seeing that the quality of support is maintained at the previous levels. The result of the third phase is that of the development of precise controls to guide the use of the technology. These controls become necessary to prevent duplication, to promote standardisation and to see that in the enthusiasm and excitement, energies of workers are not distracted or dissipated. Also on the basis of the experience that the organisation would have gained such controls would help in seeing that the later applications of the technology are more cost efficient than the first.

The next phase is an acceptance of the technology by other groups in the organisation and hence a greater pressure to speed up. This may then want networking strategies, E-Mail communication and if an organisation progress sufficiently fast successfully, may be used of Electronic Data Inter-change (EDI) as a means of application to application communication between departments and organisations.

1.3.2 Working in Teams

The Analyst as mentioned earlier has to work in a group which comprises for computer professional usually programmers and also a management and administrative representatives of the organisation. As the size of the project increases, even the computer group itself form a sub-team and they must comprise certain styles of functioning in order to be effective. We of course, begin with the assumption that the members from this team are competent and efficientin their respective areas of functioning. The kind of the structure that is successful for the software development activity has been adverted to by Edward Yourdon, who is regarded as a Software Guru. His conclusions are that a successful software team typically needs the following different kinds of people. Firstly, you need a chairman or leader. Then you need a visionary - the architect who has got the entire system in his head. You need a sceptic. You need a provocator, someone to provoke radically new ideas. You need an ordinary worker. A lot of projects, to be successful, need a scavenger - a resources manager who can get things for the project in the right time.

And then you need a diplomat, somebody who can sense the mood of the team members. With software people there are often emotional arguments. Some people believe that women are more suitable in that role. They are aware of those nuances, Men are often very macho and aggressive. And lastly, you need the completer, whose primary passion is to see the end of the project—who is desperate to bring in all the pieces together. A lot of other members of the team see the project as a lifetime exercise-as if it will go on for ever.

The visionary has to be a technical person. The chairman who gives leadership and direction doesn't necessarily have to be one, but the visionary has to be.

The above observations of Yourdon deserve to be imbibed by any practitioner, because in the absence of a well knit and cohesive team, group work instead of proceedings towards completion is morc likely to dissipate resulting in an infructuous endeavour.

1.3.3 Disaster Recovery Planning

It is common for an analyst to be so much enthusiastic and excited about conversion from an existing manual system to a computerised information system or re-engineering an existing information system to put in place a more appropriate information system, that the scenario when the new systems are in place and are heavily depended upon tend to be lost sight of.

As users begin to rely more and more on a new efficient information system, they discover to their chagrin that non- availability of the system almost spells disaster for the organisation.. Of course one anticipates possible threats to a system and provides for elementary remedial measures such as adequate stabilised power supply, backing up of software and data and so on. However, inspite of the preventive action that may be contemplated, there are always events beyond one's control. There are a number of examples even in the developed countries which illustrate the fragility of advanced planning against disaster.

Hurricane Hugo. the California earthquakes, the AT&T brownout, the Chicago floods, the Hinsdale telephone switch fire and the Penn Mutual and First interstate fires are all examples of natural disasters beyond human control, which have destroyed many company's information systems and in a number of cases resulted in the termination of the business itself. Developing countries such as India, which are rapidly moving towards dependence on computer based systems for their work, are even more prone to such disasters. The Latoor earthquake, or for that matter, the earthquake in Uttar Kashi took place in non-commercial areas. The impact of the kind of Bomb Blast that took place in the Bombay Stock Exchange can easily be seen to have effected the fortunes of many in a few years from now. The importance of Information System Disaster Recovery(IS-DR) planning, therefore, cannot be under-mined. The purpose of this discussion is to draw attention to this issue and to give some pointers as to the manner in which such a plan could be formulated.

The financial implication of the proposed disaster recovery plan must be borne in mind. Of course, some non-quantifiable aspects such as the reputation and goodwill of the organisation may also have to be assigned notional financial values. We do not have any specific analysis for the Indian context, but it has been suggested by experts in the field that a manufacturer and distributor in the developed world whose gross sales are in the range of $200 million annually. will lose more than $100,000 after 4 days of being deprived of Information Systems Services and $1 million after 10 days. It has also been estimated that almost half of the firms which fail to recover within a period of about 10 days will never recover at all and possibly go bankrupt.

Having thus seen the importance of time in the recovery plan, it is important that the organisation is able to prioritize its recovery needs. Although some detailed contextual analysis would have to be done to determine the priorities, a rough and ready guide is to classify recovery needs in the following four classes :

1. Critical – Critical needs are those which are absolutely essential to the running of the business and because of their high complexity cannot be replaced with manual methods.

2. Vital – These needs are those where the organisation could somehow continue for the better part of a working week, that is 4-5 days but the services must be restored in that time. These can not be replaced by manual operations at all but the organisation could bear with them for some time. .

3. Sensitive – These belong to such tasks and operations that are more efficiently performed with the help of computers, but with some difficulty could be performed manually as well. For example typing of some kind of letters and making of indents and orders.

4. Non-Critical – Non-critical needs are those whose effects are seen over larger time scale of several weeks. If the services are restored over that period, externally the organisation is not much the worse for the breakdown. There would of course, be some loss in money terms and possibly in terms of the quality of services although it is not likely to lead to total business failure.

Having identified the nature of the different information system, the needs of the organisation and their criticality, the disaster recovery options would have to be exercised.

There are more or less five options that are available to provide services for a site which has been afflicted with the kind of disaster referred to in the.earlier part of the section.

(A) Hot Sites

The term hot site is used for a site which is almost a replica of the afflicted site and is commercially available 'on demand'. The advantage of such an arrangement is that it is very fast and a continuity of operations can be maintained fairly easily. The pre-dominant disadvantage is that it is likely to be quite expensive.

(B) .Private Hot Sites

In the absence of the availability of a hot site, or the decision not to use such a site for confidentiality or other strategic reasons, some organisations establish their very own hot site for such emergencies. The biggest advantage is that there is no dependency on any other organisation and, therefore, no sharing of resources. Naturally, the biggest advantage also flows from this and that is that it would cost exactly twice cost of the original site. Since this site would not be used very often, it effectively doubles the cost of the capital invested in the business.

(C) Warm or Cold Sites

Such a site does not have the entire physical equipment in place and'is essentially a shell that is ready to be installed with the required equipment. In some cases, this may even be a mobile unit. There would of course, be a separate contract with a supplier to supply within the specified time frame (on an emergency scale) the required hardware and software. This would be a cheaper location, but the time required for the services to be up and ready is greater. Of course, it is assumed that the most critical software and data have been archived in a safe manner at a site sufficiently far away from the afflicted site.

(D) Service Bureaus

Service Bureaus usually could not be a good solution for rapid recovery in an emergency. Most service bureaus would manage their operations on a scale which leads to an almost complete utilisation of their hardware, software and human resources. It is extremely difficult to visualize the situation where a service bureau would be ablc to provide the level, quality and timely needs of services that would be critical to an organisation. Of course, if a service bureau arrangement would be workable, it would be the cheapest solution.

(E) Reciprocal Agreements

Such agreements are made between two organisations, who may have used a fairly similar strategy in their information systems planning and implementation. It would be a first requirement for such arrangement to bc workable that each one's systems would run on the other one's infrastructure. If this is so and both the parties are able to provide that much spare capacity in the eventuality of a crisis in the other organisation, then this usually would be the most desirable of all solutions. However, this advantage must be weighed against the possibility of both the organisations being simultaneously affected. Such a situation can arise during flash floods, cycloncs, earthquakes, etc.

1.4 THE SYSTEMS ANALYST AND LAW

It is not immediately apparent that a person who has equipped himself with knowledge of computers and hopes.to be involved in the development of computer based information systems would have anything to do with law as part of his work. However, as the penetration of information systems into organisations increases and their utility becomes apparent and dependance on computer based systems for provision of a variety of services becomes routine, the impact of the law is also felt.

This section draws the attention to those aspects which would concern the systems analysts and awareness and understanding of which would hold him in good standing.

1.4.1 Software Piracy

What is Software Piracy?

The PC industry is barely 20 years old. In that time; both the quality and quantity of available software programs have increased dramatically.

Although approximately 70 percent of the worldwide market is today supplied by developers in the United States, important development work is carried out in scores of nations around the world.

But in both the United States and elsewhere, unauthorized copying of personal computer software is a serious problem. On the average, for every authorized copy of PC software in use, at least one unauthorized copy is made.

Unauthorized copying is known as software piracy, and in 1993 it cost the software industry in excess of US $12.8 billion.

Software theft is widely practiced and widely tolerated. In some countries, legal protection for software is nonexistent, laws are unclear or not enforced with sufficient public commitment to cause those making unauthorized copies to take legal prohibitions on copying seriously.

Significant piracy losses are suffered in virtually every region of the world. In some areas the rate of unauthorized copies is believed to be in excess of 99 percent

Software piracy harms all software companies and ultimately the end-user.

Piracy results in higher prices for honest users and reduced level of support for customers.

Why is Piracy so Prevalent?

Software presents a unique problem because it is so easy to duplicate and because the copy is often undistinguishable from the original. Unlike other works, such as audio and video tapes, there is no degeneration in quality from copy to copy.

A program that reflects many years of effort by a team of software developers and large investments in money, takes only seconds to copy. Although software is expensive to develop, it costs little or nothing to duplicate and virtually any PC can be used to make unauthorized copies.

Software piracy takes many forms. The reasons for unauthorized software copying range from sheer carelessness, lack of awareness of the law and general disregard for the importance of treating software as valuable intellectual property.

Even, in the "best" countries, piracy remains a significant and extremely costly problem for the individual, local economies and the software industry as a whole.

Forms of Software Piracy

The forms of software piracy seen around the world include:

1. Hard Disk Loading

Hard disk loading occurs when computer dealers load unauthorized copies of software onto the hard disk of personal computer as an incentive for the end-user to buy hardware from the particular dealer.

These dealers do not provide original disks, documentation or the end-user license agreement that comes with a legitimate copy of the product.

Hard disk loading is a wide-spread problem, but this form of piracy is easy to detect.

Some end-users unwittingly receive illegitimate software already installed, but the absence of disks, documentation, registration forms and software licensing should alert them to the problem. Hard disk loading leaves enough evidence to make prosecution straightforward.

Industry focus on hard disk loading over the last two years has begun to reduce the practice in countries around the world.

Dealer cases involving hard disk loading are often the first enforcement efforts undertaken in many countries due to the relative ease of proving infringement.

2. Softlifting

Unauthorized copying of personal computer software within organizations, also called 'softlifting', occurs when extra copies are made within an organization for employees to use in the office, or to take home.

Disk swapping among friends and associates outside of the corporate environment is also included in this category. Software is often copied from the corporate work-place and distributed to friends outside the work-place, but other sharing of software is also quite common.

Unauthorized copying of software within organizations is the most pervasive form of software piracy faced by many software publishers. It is estimated to be responsible for more than half of the total revenues lost by the personal computer software industry worldwide.

This practice is widespread not only in corporations, but also within institutions such as schools, public agencies, government offices and nonprofit organizations.

3. Software Counterfeiting

Software counterfeiting is the illegal duplication and sale of copyrighted software in a form usually designed to make it appear to be legitimate.

Unlike corporate violators, software counterfeiters operate purely for profit. Counterfeiting occurs in all regions of the world, but the problem is particularly acute in Pacific Rim areas.

Counterfeiters range from individuals running mail-order operations om of their homes to dealers who duplicate and sell software.

There are several form of counterfeiting. One involves the entire copying of the product package, whereby end-users are deliberately misled into thinking that the product they are buying is the legitimate product from the original source.

Another form includes the sale of illegal duplicated software marketed under a completely different name, with no attempts made to represent the copy as having been distributed by the original software developer.

4. Bulletin Board Piracy

Downloading copy-righted software to users connected by modem to an electronic bulletin board is another form of piracy.

Piracy of copyrighted software via electronic bulletin boards should not be confused with sharing public domain software or providing 'shareware'.

Shareware is software that may or may not be copyrighted but is specifically offered by the author for nearly unrestricted use, including copying and sharing with others, with usually a small fee given to the developer if the user finds it useful,

5. Software Rental

The industry has encountered three forms of pirate software rental; product rented from a retail outlet for use on the renter's home or office computer; product rented through mail order 'clubs'; and product installed on computers which are in turn rented for temporary use.

Those establishments which rent software only, whether a retail storefront or mail order operation, operate in much the same way as video rental stores.

The customer chooses software, pays a small sum, and takes the product away for a limited period often, to make another copy for permanent use on their personal computer.

Some companies have asked for and been granted permission to provide software with rented computer hardware, as there are clearly circumstances under which such arrangements are legitimately required.

The explicit right to restrict rental is unfortunately often unclear or absent from national copy-right laws,

Forms of Agreement

There is obviously a large variety of possible relations between software developers and users. The right which a person acquires upon purchase of a software product is not absolutely ownership rights in the sense of some other products, but a right to its usage while complying with certain conditions. It is in the sense that the word licencee is used when we refer to a purchase of software product. This is not the appropriate place to have an exhaustive discussion on bow such contract should be framed but for giving a feel of the kind of issues that can be involved in a typical software release agreement is given below. In order to keep this general, the acronym NOSP has been used for the Name of the Software Product and NOSS has been used for Name of the Software Supplier. It is common practice in such matters of contract to have 2 copies signed and one copy retained by the licencee and the other by the licensor.

SOFTWARE RELEASE AGREEMENT

Licensee's Copy

The undersigned, being an authorised person representing the Institute or Company named and to be referred to as the Licensee, accepts the software and associated documentation known as Name of Software Product (NOSP) and agrees to the terms and conditions as laid out in the Terms and Conditions of Software Release Agreement. The Name of Software Supplier (NOSS) to be referred as the Licenser, grants the Licensee a non-exclusive, non-transferable licence to use NOSP on the specified computer at the named address. New releases are not automatically covered by this licence.

Two types of licences are available for the NOSP system. One is the licence for a limited use of one year from the date of purchase of NOSP. The other is the licence for permanent use.

Licensee

Institution/Company :

Authorised person

Licence type

Machine type

Address

Signature

Date

For Official Use

Licensor : NOSS

Authorised signature :

Date

Note : Please complete this form and return it to NOSS. This will be returned to you with the signature of the authorised person from NOSS.

TERMS AND CONDITIONS OF SOFTWARE RELEASE AGREEMENT

NOSP

1. Prerequisites

The licensee is responsible for obtaining any further licence that may be necessary to provide the computing environment required such as MS-DOS, UNIX and MS-WINDOWS.

2. Non-transferable rights

NOSP will be used only on machines which are located at the address of the Licenseeas filled-in in the Software Release agreement. The Licensee shall not distribute NOSP or any part of NOSP to others.

3. Software Protection

The Licensee shall take all precautions to prevent copies of NOSP being made. These precautions shall be equivalent to those employed by the Licensee to protect theu own documents and software from being copies.

4. Non-exclusive rights

The Licensee recognises that NOSP is released on a non-exclusive basis and that the Licensor shall have the exclusive right to grant licences to others or make such use of NOSP as it shall desire.

5. Credits

All credits in NOSP, both in listings and/or documentation, whether names of individuals or organisations, will be retained in place by the Licensee. The Licensee will acknowledge in any published documentation or in any other use of NOSP the authorship of NOSP and the fact that NOSP was developed by the Licensor.

6. Product Warranty

NOSP is released on an "as is" basis, and there is no warranty expressed or implied as to the functioning or performance or effect on the hardware or other software. The Licensee recognises that the Licensor is not obliged to provide maintenance, consultation or revision of NOSP.

7. Liability

Neither NOSS nor the individuals responsible for the development and/or maintenance of NOSP accept any liability for indirect, consequential or special damages of any kind.

8. Future Releases and Versions

New releases will be announced if and when there are major changes. New versions will be announced when there are improvements of relatively lower significance. Version numbering will be x.0, x.1, x.2, etc. This licence does not automatically entitle the Licensee to updates of NOSP when they become available. The Licensor, however, will inform all those who have a NOSP licence about updates within the same release and the charges for these updates.

1.4.2 Civil Liability

The concept of intellectual property in general have undergone a tremendous change since the last few decades in India as well as the world. 'New issues have emerged in this field in the recent years. Traditional intellectual property laws were enacted either to safeguard the rights of the authors, or to put a stop on its illegitimateuse and in cases of patents to assure proper use of the discovery. But the rule of the game has changed. Intellectual property right owners now have a duty to assure that others are not harmed due to their work. Due care and precaution has been added as the liability of an author. Previously such sanctions were available with the State only and that to in a limited sense as it was used in cases where it opposed to the public policy.

Examples of such change in regulation can be seen in country guide books that carry the caption "the author is not liable if the reader suffers loss due to the information provided in this book". Such captions are followed on cookery books and other work. There is complete paucity of case law in this field in India but the message is very clear that if the author can lead the reader in a situation where his life or property is endangered, he has a duty to compensate for such loss.

This new line of thought has become more popular due to the fact that such danger of loss is far more in the electronic media and has seeped from there to the normal book writing. There is no doubt that the electronic media is much more sensitive and more prone to causing loss. Take for example the case of computer virus, where a few line of information can completely paralyse a computer network. The authors of such virus are liable for the loss their intellectual property have caused to others. Similarly, a computer program designed to cheat non- active accounts to transfer large sums of money is not only a criminal theft or cheating but also carries with it the civil liability of compensation.

The question of law is becoming more and more important as software becomes internalized in many computer based products. Modern VCRs, Washing Machine, Micro-wave Oven etc., all have software of a few kilobytes which is an integral part of equipment. In malfunctioning,a part of the software would have a direct bearing on the functioning of the gadget and if not under principles of conventional civil law, atleast under the new found umbrella of consumer protection, the manufacturer would have to take responsibility for the error in the software. Eventually, it is the system designers and developers who would be answerable.

The usage of Intelligent systems in context beyond experimental and labomtory situations also creates significant liability issues. An expert system based product which helps in analysis of a medical case or a financial expert system product in making financial investment or for that matter a Project Manager implementing a project would also create a liability on the developer of such a system. As a hypothetical example, should the Bhopal Gas disaster have taken place because of a malfunctioning in the software for process control, liability and responsibility would eventually have lo be fixed upon the person responsible for that piece of software.

1.4.3 Computer Crimes

In the previous sub-sections, attention has been drawn to the property aspects of computer softwareand hardware, which is not always obvious at first sight. Just like theft of any other property, there could be theft of data, software and other intellectual property and components of a computer system. In countries, like the USA where Computers have been in large scale commercial use for quite some time, the American Bar Association have been collecting data on compuler crimes for the last 20 years. An interesting conclusion which comes out of such studies is that, a traditional bank robbery results in a typical loss of about $5,000. Although, electronic thefts are still few and far between, the loss due *to* an electronic heist is $500,000. The corresponding figure for India, is Rs.1.2 lakh for a traditional bank robbery and there is not enough information yet on electronic larceny.

Computcr crime can be described as one or any combination of the following events in a computer environment:

- Unauthorised attempt to access,. alter, add, delete or hide data;
- Unauthorised attempt to access, alter, add, delete or hide a program or system;
- Stealing of data or programs in any manner ;
- Unauthorised (physical and/or logical) entry into computer work environment;
- Change or alter the defined systems.

Computer crimes are classified in three broad categories: (i) Data-related crimes (ii) Software-related crimes, and (iii) Physical crimes.

Software-related Crimes

Software-related crimes are sub-classified into several categories. Like the legendary wooden horse used in Troy, the Trojan Horse is a spy sitting comfortably amongst the programs and keeping an eye over the usage of the system. It is either a logic routine embedded into a key program or a separate program, can be a Terminate and Stay Resident (TSR) program, which monitors and/or records the usage of the system.

Trap door is a logic used by system developers frequently during the system development stage, for the testing of programs and systems. The developer/programmer writes an escape route to bypass all security checks, to save extra keystrokes and time, and thus enter the system or specific programs directly. Very often, system developers deliberately leave these trap doors for future usage in case the user forgets the password, or to hedge against future payments from the user.

Typical losses due to computer crimes include money, goodwill, image, quality, service, competitive edge, and credibility. Some of the debilitating effects on an organisation due to computer crimes include-leakage of sensitive data, operations coming to a standstill, corruption of data, blackmail, communications breakdown, tampering of programs, industrial espionage, etc.

While importance of the kind of the crimes that have been mentioned earlier are esoteric and require a high degree of technical expertise to accomplish them, there is one kind of criminal activity which is highly pervasive and to which a lot of attention is being drawn. A good system analyst must be very conscious of unwittingly becoming a party to software piracy, a term which is used to convey the unauthorized copying of data or software. In the early days of usage of pirated software, the companies whose software was copied in an unauthorized manner did not react strongly enough because the expense of attempting to curtail, to go to court or even to educate against software piracy would not have been cost-effective.

But in the recent past, things have changed. The biggest software cornpanics such as Microsoft, Lotus and Autodesk have joined together to form Business Software Alliance (ESA), which is taking very active and firm action to curb the software piracy in India. According to BSA, India has a piracy rate of 76%, which is much lower than Thailand at 99% or Malaysia with 98%, China with 95% or Taiwan with 94%.

However, there is no scope for smugness because these figures must be compared to US which has the rate of 35% and countries like Canada, Australia, Western European countries where it would be between 35 to 508.

The System Analyst has an important role in the curbing of software piracy by advising that software is something which ought to be paid for. The feasibility of any project ought to be determined by a full comprehensive look at the hardware cost, the software cost, the software maintenance cost and the cost related to creating a secure system.

1.4.4 Privacy/Data Protection

The issue of Data Protection, or Privacy, or Confidentiality and Control of Data, is one which is not usually raised as a concern for the Systems Analyst. This is probably because it tends to apply to all records whether paper or computer based. The issue has however been perceived as more significant in recent times because of the ability of computer systems to store, manipulate, retrieve and correlate (match) quantities of data that were unthinkable in paper based systems.

As there is increasing emphasis in the world on this issue it was felt that students should have some exposure, albeit a fairly superficial one, to the issues, and Government and community concerns and expectations.

In India as of now, any action towards a Data Protection Act does not seem to be in progress. However, since dependence of Software arid its usage in business may involve data flow through several nations, it is desirable that one is aware of the existence of such data protection act while one's data is flowing through such a country.

The Issue

Systems Analysts developing information system must be sensitive to issues of privacy and confidentiality. Whereas the former tends to be a concern of citizens, Governments (often under pressure from their citizens) are becoming increasingly aware of the need to prevent. improper collection and use of data relating to citizens or businesses. Data protection laws enacted by Governments seek to safeguard the personal privacy and corporate information. Other motives are sometimes attributed to such moves including accusations of "economic protectionism" where Governments have sought to limit cross-border data flows.

India has traditionally been a country where information is controlled and regulated. There are a number of provisions in the law, which permit the state to curtail the free flow of information including the seizing of books, newspapers, magazines etc. The right to privacy, in a form other than the right to a good reputation (which is available in law of defamation) is otherwise not very well enforced. To some extent, issues such as right of access to information may come under the broad interpretation under the Constitution of the right to life, but there is still greater emphasis on control and confidentiality of information than openness of information as a right to its citizens. The greater use of computer and information technology would probably change this, but it is not clear at the moment whether the government would steer more rights for itself or a greater freedom of access lo informalion for the citizens. Even the recent Ordinance regarding Cable Operators puts a number of restrictive and onerous conditions on what they may offer to their viewers.

The Duty of Care

Allowing access to data by unauthorised persons either deliberately, accidentally or negligently may result in an organisation or person facing commercial or legal penalties.

To avoid claims ("liability in negligence") organisations need to:

- implement security procedures that are reasonable in all circumstances;
- specify what security procedures should be implemented, including standards for creating and storing records;
- insert a clause into the relevant agreements for failure to meet reasonable standards; this will however be viewed with suspicion by the courts, and, if inserted by the dominant partner, may be regarded as evidence of "unconscionablc conduct", and therefere not enforceable.

The UK which took a lead in creating a Data Protection Act in 1984, enjoined a duty of care for information held in electronic form upon the custodian,of such information.

Legislative Trends

Many countries are concerned with privacy or data protection. In Europe 17 countries have enacted forms of data protection legislation.

It was recently reported that the Law Reform Commission in Hong Kong has spend three years drafting new legislation covering the area of data protection. This has been accelerated by developments in this area by the European community which seek to limit data transfers to countries that do not have data protection and privacy laws as stringent as those in force in the EEC. Hong Kong has recognised that any restrictions on information flow could adversely affect trade. The practical effects of the bill are to create an Office of the Privacy Commissioner to which all registered companies would have to submit returns covering "the main features of the data that they hold".

The commissioner would have the power of inspection, in the event of a complain relating to the unfair use of information or invasion of privacy, or on his own recognisances if there is a suspicion of "wrong doing". The Hong Kong definition of data incorporates paper, as well as computer files.

It should be noted that what is viewed as the extremism of the Hong Kong and European draft data protection directives have attracted criticism from various quarters.

In Hong Kong there were concerns that the proposed legislation was "so wide they might be open to abuse in some cases, too restrictive in others and could be too costly for many companies to implement".

In Europe the criticism has centred on the proposals being "too extreme", getting the balance wrong between privacy and public policy objectives such as "freedom of information", putting too much emphasis on the "holding of data" rather than the "abuses arising from the use to which the data is put" and being too bureaucratic, onerous and costly. Other issues raised related to what "the status of intra-company data exchanges" might be, the concern that the directives could "have serious implications for data exchange with parties in third countries" and that "increasingly important economic activities within the EEC such as broad-casting, direct mailing, market research, credit assessment might be seriously affected.

In the UK there is now legislation to control access to personal data through the UK Data Protection Act 1984. Whilst there is yet no definition of what constitutes "appropriate security measures" under Principle 8 of the Act, these will be forthcoming. Much has been written by security consultants on what constitutes acceptable access controls in operating systems. Their views will no doubt be highly relevant to the definition of appropriate security measures. Users have different access control requirements and are subject to varying financial limits. However, by building in the facility to enable implementation of security processing, the degree of control can be varied to accommodate both individual users and future requirements.

India does not seem to have made any move yet towards a data protection act, but in keeping with the international trends, it will possibly be having one in the future. Also in view of the tradition of English law, it is likely to be closest to the corresponding UK Data Protection Act 1984.

1.5 SUMMARY

In this unit, a number of concerns have been addressed, which are not readily apparent but are likely to become more important in the future. The unit begins with an exhortation that a systems analyst's training is never finished. Since an analyst does not work in isolation, some features of teams and organisation characteristics have been discussed. Systems have to be reliable but if the systems fail, anticipation of needs in case of disastrous failures have been drawn attention to. Issues related to law such as arising in software piracy, computer crimes and privacy, data protection have also been drawn attention to, so that the analyst is aware of these considerations while working on the development of appropriate systems.

UNIT 2 HUMAN COMPUTER INTERACTION

Structure

2.0 INTRODUCTION

In designing computer systems, it must be borne in mind that they are meant for use eventually by humans, and therefore, the way in which the system interacts wilh humans is of great importance in the design of such systems. In the initial stages, when the users were few, this was not important but as information technology is becoming ubiquitous, the need for more "humane" intcrface is gaining attention in the industry. Till sometime back the interface was thought as going beyond data entry to direct data capture using OMR, OCR, etc. and in terms of pen-based input, speech and gesture recognition, possibly a variety of languages such as English, Hindi, Japanese, Chinese, etc. and other input/output technologies. Howcver, in recent times, a realisation has come that the top layer of the software programs has also a major component. Since this is the layer experienced by the user, it is very important. The success of Apple Macintosh and Windows have dcmonstrated this and most software designers are giving utmost attention to it,

This unit is of course a brief overview of some of the issues involved and by no means exhaustive.

2.1 OBJECTIVES

After completing this unit, you will be able to :

- appreciate that computers are meant for use by humans;
- realise that there cannot be a single user-friendly interface;
- appreciate the relevant factors in designing the human- machine interface:
- appreciate the human problems in an organisation moving towards information technology; and
- give adequate importance to ergonomics in the design of computer-based systems.

2.2 THE WHAT, WHY, WHEN AND WHERE OF HUMAN COMPUTER INTERACTION

Human Computer Interfaces (HCI) are tools for helping human beings and machines to work together more effectively. Every tool used by human being has a human intcrface. When one rides about in a Bicycle, the pedal and the handle arc the interfaces through which riding the bicycle is possible. In the case of a car, this may change to the steering wheel, the brake,