Pokhara University

Bachelor of Computer Engineering

Lecture Notes

In

Social & Professional Issues in IT

Compiled by: Mohan Bhandari

1. History of Computing

Computers manipulate data i.e. process and transform given representations of information in order to obtain a desired result. Within this basic description of computer behavior we can divide into two fundamental ideas:

- Representation: A concrete, symbolic encoding of information, e.g. numbers, words, names.
- Transformation: The steps (recipe, program, algorithm) used to calculate a specific result.

The reason for assisting the above fundamental fact has two consequences if no mechanical aid is employed:

- The computation will take a long time to complete.
- The answers may be incorrect, because of human error, and so the same computation may have to be carried out several times.

Pre-History of Computing

- Archaeological discoveries have established that the `tally system' was independently developed by many early cultures. Regardless of its undeveloped nature, these systems have important features that were to be preserved in afterward systems. The most important of these is the concept of counting in multiples of some basic number.

  Although the tally system has several advantages - it is easy to understand, simple arithmetic operations such as addition, subtraction and multiplication can be performed without great difficulty. It is extremely weighty when used to represent large numbers, such as might arise in recording population sizes, and it is not suitable for more complicated computational tasks, e.g. division.

  Attempts to address the first problem can be separated in the notational systems used by Greek and Roman societies (from ca. 1000 B.C for Greek, 700 B.C, Roman), that the Roman Numerals.

  A task such as multiplication, conceivable in the tally system, present major difficulties in Roman numerals, still Roman numerals remained the predominant means of representing quantities in European culture well into the 14th century.

- They were ultimately replaced by a system which contributed what was one of the most important discoveries of early science: a fully positional notation with a representation for the number zero. The Arabic system employed 10 different symbols representing the numbers 0,1,2,...,9 and formed the basis of the decimal system that is used today.
- The abacus represents the state of a calculation by the position of beads strung into columns on wires.

The important dates along with the events in ancient time were:

Date	**Event**
80000 BC	Two notched rib bones may have been used for counting
2400 BC	The abacus – the first known calculator, was probably invented by the Babylonians
1115 BC	The south-pointing chariot was invented in ancient China.
500 BC	First known use of zero by mathematicians in ancient India around this date.
500 BC	The Panini-Backus form used to describe most modern programming languages
300 BC	Indian mathematician/scholar/musician Pingala first described the binary number system

200 BC	The Chinese invented the Chinese abacus which was widely used until the invention of the modern calculator, and continues to be used in some cultures today.
125 BC	A clockwork, analog computer believed to have been designed
100 BC	Chinese mathematicians first used negative numbers.
200	Indian Jaina mathematicians invented logarithms.
600	Indian mathematician was the first to describe the modern place-value numeral system (Hindu-Arabic numeral system).
724	Chinese inventor built the world's first fully mechanical clock; water clocks,
996	Persian astronomer invented the first geared mechanical astrolabe, featuring eight gear-wheels.
1015	Arab astronomer invented a mechanical analog computer device used for finding the longitudes and positions of the Moon, Sun and planets
1235	Persian astronomer invented a geared calendar
1400	Kerala school of astronomy and mathematics in South India invented the floating point number system.
1492	Leonardo da Vinci produced drawings of a device consisting of interlocking cog wheels which can be interpreted as amechanical calculator capable of addition and subtraction..
1588	Joost Buerghi discovered natural logarithms.
1614	Scotsman John Napier reinvented a form of logarithms and an ingenious system of movable rods (referred to as Napier's Rods or Napier's bones).
1622	William Oughtred developed slide rules based on natural logarithms as developed by John Napier.

History of Computer Hardware

Computing hardware has been an important component of the process of calculation and data storage since it became useful for numerical values to be processed and shared. The earliest computing hardware was probably some form of tally stick. Devices to aid computation have changed from simple recording and counting devices to the abacus, the slide rule, analog computers, and more recent electronic computers. Even today, an experienced abacus user using a device hundreds of years old can sometimes complete basic calculations more quickly than an unskilled person using an electronic calculator.

Generation of Computer:

First Generation (1940-1956) Vacuum Tubes

The first computers used vacuum tubes for circuitry and magnetic drums for memory, and were often enormous, taking up entire rooms. They were very expensive to operate and in addition to using a great deal of electricity, the first computers generated a lot of heat, which was often the cause of malfunctions.

First generation computers relied on machine language, the lowest-level programming language understood by computers, to perform operations, and they could only solve one problem at a time, and it could take days or weeks to set-up a new problem. Input was based on punched cards and paper tape, and output was displayed on printouts.

The UNIVAC and ENIAC computers are examples of first-generation computing devices. The UNIVAC was the first commercial computer delivered to a business client, the U.S. Census Bureau in 1951.

Second Generation (1956-1963) Transistors

Transistors replace vacuum tubes and ushered in the second generation of computers. The transistor was invented in 1947 but did not see widespread use in computers until the late 1950s. The transistor was far superior to the vacuum tube, allowing computers to become smaller, faster, cheaper, more energy-efficient and more reliable than their first-generation predecessors.

Though the transistor still generated a great deal of heat that subjected the computer to damage, it was a vast improvement over the vacuum tube. Second-generation computers still relied on punched cards for input and printouts for output.

Second-generation computers moved from cryptic binary machine language to symbolic, or assembly, languages, which allowed programmers to specify instructions in words. High-level programming languages were also being developed at this time, such as early versions of COBOL and FORTRAN. These were also the first computers that stored their instructions in their memory, which moved from a magnetic drum to magnetic core technology.

The first computers of this generation were developed for the atomic energy industry.

Third Generation (1964-1971) Integrated Circuits

The development of the integrated circuit was the hallmark of the third generation of computers. Transistors were miniaturized and placed on silicon chips, called semiconductors, which drastically increased the speed and efficiency of computers.

Instead of punched cards and printouts, users interacted with third generation computers through keyboards and monitors and interfaced with an operating system, which allowed the device to run many different applications at one time with a central program that monitored the memory. Computers for the first time became accessible to a mass audience because they were smaller and cheaper than their predecessors.

Fourth Generation (1971-Present) Microprocessors

The microprocessor brought the fourth generation of computers, as thousands of integrated circuits were built onto a single silicon chip. What in the first generation filled an entire room could now fit in the palm of the hand. The Intel 4004 chip, developed in 1971, located all the components of the computer—from the central processing unit and memory to input/output controls—on a single chip.

In 1981 IBM introduced its first computer for the home user, and in 1984 Apple introduced the Macintosh. Microprocessors also moved out of the realm of desktop computers and into many areas of life as more and more everyday products began to use microprocessors.

As these small computers became more powerful, they could be linked together to form networks, which eventually led to the development of the Internet. Fourth generation computers also saw the development of GUIs, the mouse and handheld devices.

Fifth Generation (Present and Beyond) Artificial Intelligence

Fifth generation computing devices, based on artificial intelligence, are still in development, though there are some applications, such as voice recognition, that are being used today. The use of parallel processing and superconductors is helping to make artificial intelligence a reality. Quantum computation and molecular and nanotechnology will radically change the face of computers in years to come. The goal of fifth-generation computing is to develop devices that respond to natural language input and are capable of learning and self-organization.

The major important dates for the Computer Hardware history are:

Date	Event
1851	Thomas de Colmar launched the mechanical calculator industry by starting the manufacturing of a much simplified Arithmometer
1858	The first Tabulating Machine was made
1869	The first practical logic machine was built by William Stanley Jevons.
1871	Babbage produced a prototype section of the Analytical Engine's mill and printer.
1875	Martin Wiberg produced a reworked difference-engine-like machine intended to prepare logarithmic tables.
1878	Ramon Verea, invented a calculator with an internal multiplication table
1885	A multiplying calculator more compact than the Arithmometer entered mass production.
1886	Herman Hollerith developed the first version of his tabulating system
1889	Dorr Felt invented the first printing desk calculator.
1896	Herman Hollerith introduced an Integrating Tabulator that could add numbers encoded on punched cards
1901	The Standard Adding Machine Company released the first 10-key adding machine
1906	Henry Babbage, Charles's son, with the help of the firm of R. W. Munro, completed the 'mill' from his father's Analytical Engine
1906	Vacuum tube invented by Lee De Forest.
1906	Herman Hollerith introduces a tabulator with a
1919	William Henry Eccles and F. W. Jordan published the first flip-flop circuit design.
1928	IBM standardizes on punched cards with 80 columns of data and rectangular holes.
1931	IBM introduced the IBM 601 Multiplying Punch, an electromechanical machine that could read two numbers
1937	George Stibitz of the Bell Telephone Laboratories (Bell Labs), New York City, constructed a demonstration 1-bit binary adder using relays.
1939Nov	First machine to calculate using vacuum tubes.
1942Summer	Atanasoff and Berry completed a special-purpose calculator for solving systems of simultaneous linear equations, later called the 'ABC' ('Atanasoff–Berry Computer').
1943 Sep	Williams and Stibitz completed the 'Relay Interpolator', later called the 'Model II Relay Calculator'.
1944 Aug 7	The IBM Automatic Sequence Controlled Calculator was turned over to Harvard University, which called it the Harvard Mark I.
1945	Vannevar Bush developed the theory of the memex, a hypertext device linked to a library of books and films.
	John von Neumann drafted a report describing the future computer eventually built as

Date	Event
	the EDVAC (Electronic Discrete Variable Automatic Computer).
	ENIAC (Electronic Numerical Integrator and Computer): One of the first totally electronic, valve driven, digital, program-controlled computers was unveiled
1946	The trackball was invented as part of a radar plotting system
1947	Invention of the transistor at Bell Laboratories,
	Howard Aiken completed the Harvard Mark II.
1948 Jul 21	SSEM, Small-Scale Experimental Machine or 'Baby' was built at the University of Manchester. It ran its first program on this date
1949	CSIR Mk I Australia's first computer ran its first test program.
1949	MONIAC was created in 1949 to model the economic process of the UK.

History of Software : Programming Language and Operating System

Computer software or simply software is any set of machine-readable instructions that directs a computer's processor to perform specific operations. Computer software is non-tangible, contrasted with computer hardware, which is the physical component of computers. Computer hardware and software require each other and neither can be realistically used without the other.

Programming Language:

An outline (algorithm) for what would have been the first piece of software was written by Ada lovelace in the 19th century, for the planned analytical engine. However,neither the analytical engine nor any software for it was ever created.

First, there was **Ada Lovelace**, writing a rudimentary program (1843) for the Analytical Machine, designed by Charles Babbage in 1827, but the machine never came into operation. Then, there was **George Boole** (1815-1864), a British mathematician, who proved the relation between mathematics and logic with his algebra of logic (Boolean algebra or binary logic) in 1847.

John Von Neumann's first concept became known as "shared-program technique". This technique states that the actual computer hardware should be simple and not need to be hand-wired for each program.

In 1949, a few years after Von Neumann's work, the language Short Code appeared. It was the first computer language for electronic devices and it required the programmer to change its statements into 0's and 1's by hand. Still, it was the first step towards the complex languages of today. In 1951, **Grace Hopper** wrote the first compiler, A-0.

In 1957, the first of the major languages appeared in the form of **FORTRAN**. Its name stands for FORmula TRANslating system. The language was designed at IBM for scientific computing. Though FORTAN was good at handling numbers, it was not so good at handling input and output, which mattered most to business computing.

Business computing started to take off in 1959, and because of this, **COBOL** was developed. It was designed from the ground up as the language for businessmen. Its only data types were numbers and strings of text. It also allowed for these to be grouped into arrays and records, so that data could be tracked and organized better.

In 1958, John McCarthy of MIT created the **LISt Processing** (or LISP) language. It was designed for Artificial Intelligence (AI) research. Because it was designed for such a highly specialized field, its syntax has rarely been seen before or since.

The **Algol** language was created by a committee for scientific use in 1958. Its major contribution is being the root of the tree that has led to such languages as Pascal, C, C++, and Java. It was also the first language with a formal grammar.

Pascal was begun in 1968 by Niklaus Wirth. Its development was mainly out of necessity for a good teaching tool. Pascal was designed in a very orderly approach; it combined many of the best features of the languages in use at the time, COBOL, FORTRAN, and ALGOL.

C was developed in 1972 by Dennis Ritchie while working at Bell Labs in New Jersey. C uses pointers extensively and was built to be fast and powerful at the expense of being hard to read. Ritchie developed C for the new UNIX system being created at the same time. Because of this, C and UNIX go hand in hand. UNIX gives C such advanced features as dynamic variables, multitasking, interrupt handling, forking, and strong, low-level, input-output.

In the late 1970's and early 1980's, a new programming method was being developed. It was known as **Object Oriented Programming**, or OOP. Objects are pieces of data that can be packaged and manipulated by the programmer. Bjarne Stroustroup liked this method and developed extensions to C known as "C with Classes." This set of extensions developed into the full-featured language **C++,** which was released in 1983.C++ was designed to organize the raw power of C using OOP, but maintain the speed of C and be able to run on many different types of computers.

Netscape licensed **Java** for use in their internet browser, Navigator. At this point, Java became the language of the future and several companies announced applications which would be written in Java, none of which came into use.

Visual Basic is often taught as a first programming language today as it is based on the BASIC language developed in 1964 by John Kemeny and Thomas Kurtz.

Microsoft has extended BASIC in its Visual Basic (VB) product. The heart of VB is the form, or blank window on which you drag and drop components such as menus, pictures, and slider bars.

Further,Programming languages have been under development for years and will remain so for many years to come. They got their start with a list of steps to wire a computer to perform a task. These steps eventually found their way into software and began to acquire newer and better features.

High-level Language

1. Learning

High-level languages are easy to learn.

2 Understanding

High0level languages are near to human languages.

3. Execution

Programs in high-level languages are slow in execution.

4. Modification

Programs in high-level languages are easy to modify.

5. Facility at hardware level

High-level languages do not provide much facility at hardware level.

6. Knowledge of hardware Deep

Knowledge of hardware is not required to write programs.

7. Uses

These languages are normally used to write application programs.

Low-level languages

1. Learning

Low-level languages are difficult to learn.

2 Understanding

Low-level languages are far from human languages.

3. Execution

Programs in low-level languages are fast in execution.

4. Modification

Programs in low-level languages are difficult to modify.

5. Facility at hardware level

Low-level languages provide facility to write programs at hardware level.

6. Knowledge of hardware Deep

Deep knowledge of hardware is required to write programs.

7. Uses

These languages are normally used to write hardware programs.

Operating System:

Computer operating systems provide a set of functions needed and used by most application programs on a computer, and the links needed to control and synchronize computer hardware.

On the first computers, with no operating system, every program needed the full hardware specification to run correctly and perform standard tasks, and its own drivers for peripheral devices like printers and punched paper card readers.

Mainframe OS:

The earliest computers were mainframes that lacked any form of operating system. Each user had sole use of the machine for a scheduled period of time and would arrive at the computer with program and data, often on punched paper cards and magnetic or paper tape. The program would be loaded into the machine, and the machine would be set to work until the program completed or crashed.

The first operating system used for real work was GM-NAA I/O, produced in 1956 by General Motors' Research division for its IBM 704. Most other early operating systems for IBM mainframes were also produced by customers.

For the UNIVAC 1107, UNIVAC, the first commercial computer manufacturer, produced the EXEC-I operating system, and Computer Sciences Corporation developed the EXEC II operating system and delivered it to UNIVAC. EXEC II was ported to the UNIVAC 1108.

Minicomputer OS:

Digital Equipment Corporation created several operating systems for its 16-bit PDP-11 machines, including the simple RT-11 system, the time-sharing RSTS operating systems, and the RSX-11 family of real-time operating systems, as well as the VMS system for the 32-bit VAX machines.

The Pick operating system was another operating system available on a wide variety of hardware brands. Commercially released in 1973 its core was a BASIC-like language called Data/BASIC and a SQL-style database manipulation language called ENGLISH.

Microcomputer OS:

The development of microprocessors made inexpensive computing available for the small business and hobbyist, which in turn led to the widespread use of interchangeable hardware components using a common interconnection. The decreasing cost of display equipment and processors made it practical to provide graphical user interfaces for many operating systems, such as the generic X Window System that is provided with many UNIX systems, or other graphical systems such as Microsoft Windows.

Since the late 1990s there have been three operating systems in widespread use on personal computers: Microsoft Windows, Apple Inc.'s OS X, and the open source Linux.

History of Networking

A **computer network** or **data network** is a telecommunication network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other along network links (data connections). The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

The chronology of significant computer-network developments includes:

- In the late 1950s early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE).
- In 1959 Anatolii Ivanovich Kitov proposed to the Central Committee of the Communist Party of the Soviet Union a detailed plan for the re-organisation of the control of the Soviet armed forces and of the Soviet economy on the basis of a network of computing centres
- In 1960 the commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected mainframes.
- In 1962 J.C.R. Licklider developed a working group he called the "Intergalactic Computer Network", a precursor to the ARPANET, at the Advanced Research Projects Agency(ARPA).
- In 1964 researchers at Dartmouth College developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by General Electric and Bell Labs used a computer to route and manage telephone connections.
- Throughout the 1960s, Leonard Kleinrock, Paul Baran, and Donald Davies independently developed network systems that used packets to transfer information between computers over a network.

- In 1965, Thomas Marill and Lawrence G. Roberts created the first wide area network (WAN). This was an immediate precursor to the ARPANET, of which Roberts became program manager.
- Also in 1965, Western Electric introduced the first widely used telephone switch that implemented true computer control.
- In 1969 the University of California at Los Angeles, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah became connected as the beginning of the ARPANET network using 50 kbit/s circuits.
- In 1972 commercial services using X.25 were deployed, and later used as an underlying infrastructure for expanding TCP/IP networks.
- In 1973, Robert Metcalfe wrote a formal memo at Xerox PARC describing Ethernet, a networking system that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii. In July 1976, Robert Metcalfe and David Boggs published their paper "Ethernet: Distributed Packet Switching for Local Computer Networks" and collaborated on several patents received in 1977 and 1978. In 1979 Robert Metcalfe pursued making Ethernet an open standard.
- In 1976 John Murphy of Datapoint Corporation created ARCNET, a token-passing network first used to share storage devices.
- In 1995 the transmission speed capacity for Ethernet increased from 10 Mbit/s to 100 Mbit/s. By 1998, Ethernet supported transmission speeds of a Gigabit. The ability of Ethernet to scale easily (such as quickly adapting to support new fiber optic cable speeds) is a contributing factor to its continued use as of 2015.

Pioneers of Computing

Aristotle (384 BC, Stagira, Greece, 322 BC, Athens, Greece)

He was one of the greatest ancient Greek philosophers of his time. Many of his thoughts have become the back bone of computing and artificial Intelligence. His work in the natural and social sciences greatly influenced virtually every area of modern thinking

Muhammad ibn Musa al-Khwarizmi (800 - 847, Baghdad, Iraq):

Muhammad ibn Musa al-Khwarizmi was born sometime before 800 A.D. in an area not far from Baghdad and lived at least until 847. He wrote his *Al-jabr wa'l muqabala* (from which our modern word "algebra" comes) while working as a scholar at the House of Wisdom in Baghdad. In addition to this treatise, al-Khwarizmi wrote works on astronomy, on the Jewish calendar, and on the Hindunumeration system. The English word "algorithm" derives from the Latin form of al-Khwarizmi's name.

Henry Briggs (Feb 1561 Worley Wood, Yorkshire):

Briggs is especially known for his publication of tables of logarithms to the base 10, first Logarithmorum chilias prima, 1617, and later Arithmetica logarithmetica, 1624. He also composed a work on trigonometry (basicallytables, both of the functions and of the logs of sines and tangents) that was left unfinished at his death; Gellibrand completed and published it. And he left quite a few mathematical manuscripts that remained unpublished.

Charles Babbage:

Charles Babbage(December 1791 –18 October 1871) was an English polymath.A mathematician, philosopher, inventor and mechanical engineer, Babbage is best remembered for originating the concept of a programmable computer.

Considered a "father of the computer",Babbage is credited with inventing the first mechanical computer that eventually led to more complex designs. His varied work in other fields has led him to be described as "pre-eminent" among the many polymaths of his century.

Parts of Babbage's uncompleted mechanisms are on display in the London Science Museum. In 1991, a perfectly functioning difference engine was constructed from Babbage's original plans. Built to tolerances achievable in the 19th century, the success of the finished engine indicated that Babbage's machine would have worked.

Bailse Pascal:

Bailse Pascal (19 June 1623 – 19 August 1662) started some pioneering work on calculating machines. After three years of effort and fifty prototypes, he built 20 finished machines (called Pascal's calculators and later Pascalines) over the following ten years,establishing him as one of the first two inventors of the mechanical calculator.

George Boole (Nov 2, 1815 - Dec 8, 1864, Lincoln, England)

George Boole laid the groundwork for what we know today as Information Theory through the publication of his masterpiece, *An Investigation of the laws of Thought,on which are founded the Mathematical Theories of Logic and Probabilities.* In this work, published when the author was 39, Boole reduced logic to an extremely

simple type of algebra, in which 'reasoning' is carried out through manipulating formulas simpler than those used in second-year traditional algebra. His theory of logic, which recognizes three basic operations - AND, OR and NOT - was to become germane to the development of telephone circuit switching and the design of electronic computers.

Herman Hollerith :

Herman Hollerith (February29, 1860 – November 17, 1929) was an American statistician and inventor who developed a mechanical tabulator based on punched cards to rapidly tabulate statistics from millions of pieces of data. He was the founder of theTabulating Machine Company that later merged to become IBM.

Timothy John Berners-Lee:

Professor Sir Timothy John Berners-Lee (born 8 June 1955),also known as TimBL, is an English computer scientist, best known as the inventor of the World Wide Web. He made a proposal for an information management system in March 1989, and he implemented the first successful communication between a Hypertext Transfer Protocol (HTTP) client and server via the Internet sometime around mid-November of that same year.

John Vincent Atanasoff (October 4, 1903, Hamilton, New York, USA, June 15, 1995, Monrovia, USA)

John Vincent Atanasoff was born on 4 October 1903 in Hamilton, New York. He is the inventor of the electronic digital computer. He is, along with being an Inventor, a Mathematical Physicist and a Businessman.

Steve Jobs:

Steven Paul Jobs (February 24, 1955 – October 5, 2011) was an American businessman. He was best known as the co-founder, chairman, and chief executive officer (CEO) of Apple Inc. Jobs is widely recognized as a pioneer of the microcomputer revolution of the 1970s, along with Apple co-founder Steve Wozniak.

[Note: Refer some more peoples also]

The other peoples who researched in the invention of digital computer and the mathematician who developed their algorithmic information theory are listed as below.

Person	Achievement	Ach. Date
al-Khwārizmī	The term "algorithm" is derived from the algorism, the technique of performing arithmetic with Hindu-Arabic numerals developed	1200~
Charles Babbage	- Originated the concept of a programmable general-purpose computer. - Designed the Analytical Engine and built a prototype for a less powerful mechanical calculator.	1822 1837
John Atanasoff	Built the first electronic digital computer, the Atanasoff–Berry Computer, though it was neither programmable nor Turing-complete.	1939
John Backus	Invented FORTRAN (Formula Translation)	1954
Tim Berners-Lee	- Worldwide web. With Robert Cailliau - sent first HTTP communication between client and server.	1989 1990
George Boole	Formalized Boolean algebra	1847
Vint Cerf	The primary data communication protocols of the Internet and other computer networks.	1978
Edmund M. Clarke	Developed model checking	1981
Edgar F. Codd	Proposed and formalized the relational model of data management, the theoretical basis of relational databases.	1970
James Cooley	With John W. Tukey, created the Fast Fourier Transform.	1965
J. Presper Eckert	With John Mauchly, designed and built the ENIAC	1943 1951
Tommy Flowers	Designed and built the Mark 1 and the ten improved Mark 2	1943
Herman Hollerith	Widely regarded as the father of modern machine data processing.	1889
Joseph Marie Jacquard	Built and demonstrated the Jacquard loom, a programmable mechanized loom controlled by punch cards.	1801
Stephen Cole Kleene	Pioneered work with Alonzo Church on the Lambda Calculus that first laid down the foundations of computation theory.	1936
Sergei	Independently designed the first electronic computer in the	1951

Person	Achievement	Ach. Date
Alekseyevich Lebedev	Soviet Union, MESM, in Kiev, Ukraine.	
Gottfried Leibniz	Made advances in symbolic logic, such as the Calculus.	1670~
Ada Lovelace	Began the study of scientific computation, analyzing Babbage's work in her Sketch of the Analytical Engine, and was the namesake for theAda programming language.	1843
John Mauchly	With J. Presper Eckert, designed and built the ENIAC, the first modern (all electronic, Turing-complete) computer, and the UNIVAC I	1943 1951
John McCarthy	Invented LISP, a functional programming language.	1955
Marvin Minsky	Co-founder of Artificial Intelligence Lab at Massachusetts Institute of Technology, author of several texts on AI and philosophy.	1963
John von Neumann	Formulated the von Neumann architecture upon which most modern computers are based.	1945
Blaise Pascal	Invented the mechanical calculator.	1642
Dennis Ritchie	With Ken Thompson, pioneered the C programming language and the Unix computer operating system at Bell Labs.	1967
Saul Rosen	Designed the software of the first transistor-based computer. Also influenced the ALGOL programming language.	1958–1960
Konrad Zuse	Designed the first high-level programming language, Plankalkül.	1943–1945

2. Social Context of Computing

Society and Technology

- A human society is a group of people involved in persistent social interaction, or a large social grouping sharing the same geographical or social territory, typically subject to the same political authority and dominant cultural expectations. Human societies are characterized by patterns of relationships (social relations) between individuals who share a distinctive culture and institutions; a given society may be described as the sum total of such relationships among its constituent members. In the social sciences, a larger society often evinces stratification or dominance patterns in subgroups.
- **Essential elements of a society**

  1. ***Plurality:*** society is composed of population of all ages and of the both the sexes.
  2. ***Stability:*** a society is permanent in character. The social life is organized mainly on the basisof division of labor.
  3. ***Likeness:*** in earlier societies the sense of likeness was focused on kinship i. e., bloodrelationships. In modem societies the concept has been broadened by the principle ofnationality. A society would not be possible without some mutual understanding and thatunderstanding depends on the likeness which each apprehends in the others.
  4. ***Differences:*** society also includes differences. All our social systems involve relationship inwhich differences complement one another, for example, in a family, apart from biologicaldifferences of gender, there are other differences of opinions, diversities of interests and etc.In social life, there is an indefinite interplay of likeness and differences, of cooperation andconflict, of agreement and dissent
  5. ***Interdependence:*** it is also an essential element to constitute a society. Family is an exampleof interdependency. Today, even the countries depend on each other.
  6. ***Cooperation:*** without cooperation no society can exists. The members of a family cooperate with each other to live happily.
- Technology is the collection of techniques, skills, methods and processes used in the production of goods or services or in the accomplishment of objectives, such as scientific investigation. Technology can be the knowledge of techniques, processes, etc. or it can be embedded in machines, computers, devices and factories, which can be operated by individuals without detailed knowledge of the workings of such things
- Technology and society refers to cyclical co-dependence, co-influence, co-production of technology and society upon the other (technology upon culture, and vice versa). This synergistic relationship occurred from the dawn of humankind, with the invention of simple tools and continues into modern technologies such as the printing press and computers. The academic discipline studying the impacts of science, technology, and society and vice versa is called (and can be found at) Science and technology studies.

  Technology has become a huge part of everydaysociety's life. When a society knows more about the development in a technology, they become able to take advantage of it. When an innovation achieves a certain point after it has been presented and promoted, this technology becomes part of the society. Digital technology has entered each process and activity made by the social system. In fact, it constructed another worldwide communication system in addition to its origin.

Since the creation of computers achieved an entire better approach to transmit and store data. Digital technology became commonly used for downloading music, and watching movies at home either by DVDs or purchasing it online. Digital music records are not quite the same as traditional recording media.

Impact of Technology On Society and Vice Versa

The technological growth taking place in the world today is doing so very rapidly and there are new advancements being made with each passing day and this is possible owing to the large number of extensive program of technological research currently being done by a large number of researchers working within non-profit research organizations, business and universities. The developments being made today are very strong and are very enveloping forces in the business environment today. Technology can easily be referred to as the scientific knowledge to the practical problems we are experiencing in the world today. There is no denying that the impact of technology in the world today is huge and can be categorized into how it affects our society today and how it influences the business activities and operations.

Technology has without doubt an impact on society. As a matter of fact, we experience this effect in our daily lives. It has an effect on the growth of the economy, our culture and our living standards. It is however important to note that the benefits are a double-edged sword with some being detrimental and other being beneficial. One should be very careful and get to know how the effects on society get to effect the business activities and operations.

Influence of technological change on society

1. Mass production of goods through machines
2. Automation
3. Faster means of transportation
4. Mass communication
5. Availability of labor saving devices
6. Faster pace of life
7. Commercialized recreation
8. Emphasis on high degree of specialization

Family system and technological change:

Technical change has affected traditional family system in the following manner:

- Emergence of nuclear family
- Women’s involvement in male dominated area of work
- Change in standard of living
- New way of socialization of the children
- Change in orthodox values

Some demerits brought by the technical changes to the family system:

- Mechanical life-style
- Formal type of relationships
- Change in existing social customs

- Less family ties between family members

Religion and technological change

Followings are the some of the effects of technical change on religion:

- Analysis of religious doctrines and traditions
- The rigidity in caste system has been relaxed
- Men are free from religious rituals
- Religion has become the secondary thing not a primary one

Rural life and technological change

Followings are the some of the effects of technical change on rural life:

- Migration towards urban areas
- Increase in consciousness of rural people
- Change in method of farming
- Life became comfortable than before
- Change in life pattern

Urban life and technological change

Followings are the some of the effects of technical change on urban life:

- Shortage of land and houses
- Increase in slums
- Problem of transportation
- Increase in crimes
- Expensive life
- Money has became the most important thing

Impact of Information Technology

Concern over Technology has always been present, especially with the advent of IT. As the entirediscipline of information technology (here after IT) is less than 50 years old, it is not mature withfundamental concepts, definitions, notations, and tools, as compared to those available inconventional branches of science and engineering. Information Technology does not only effects;technical people but people at various stages but even a common man, a business class man etc. Itcan change buying habits of a customer, way a service provider provides a service. The need is tothink about the effect of IT on social living and the way it can be best utilized.

For example, when a software engineer undertakes a problem to provide a solution, he does not havefundamental axioms to guide him. There is no law in software engineering comparable to the law ofthermodynamics, Ohm’s laws, etc. Therefore it is high time for a proper education and developmentof the manpower and engineers. It is also necessary to predict in which way the technology is goingand what will be its repercussions, for the role of the visionary is vital. It is the moral responsibilityof the sociologist, business people and benign thinkers to think about the way technology is affectingpeople and in which way can it be, best utilized. It needs greater attention for sustainable growth anddevelopment and proper use of information technology.

People working in computer mediated environment will be definitely lack in social contacts andwould become alienated. The type of work may also become less interesting and monotonous type asseen in the second example. The modern communications systems such as e-mail and v-mail supportadditional contact between people separated geographically or organizationally adding a newdimension to the social relationship. The new concepts towards downsizing and telecommutingincrease isolation and alienation because the organization is now reducing the number of people andsecondly permitting people to work from their homes also has significant affect on the social contextof people.

Issues related to IT

The relationship between information technology and society in general is very strong. It needs agreater attention of all classes of people to think how best we can utilize this technology. The firstand foremost need is of developing a better manpower in IT, the other issues include Present dayChange in Work Environment, Job Design in IT-Enabled Processes, Resistance to Change and itsManagement and Human-Centric Design.

The Need of Education for a Better IT Manpower Development

In the area of information technology, there is always a gap between the projected manpower andthat supplied to this industry. The type of manpower that is produced is, basically of programmers,who know the tits and bits of the program, the engineers who are responsible for the core design ofthe systems. But the application spectrum of IT is quite vast, ranging from automated control of astepper motor to stock exchange activity, from nuclear reactor to space sampling robots, thus in thisscenario, programmers nor the engineers can do justice to the entire domain of informationtechnology.

However the need is in a systematic process of education and experience so that it is possible toanalyze and model the problem, tracing out inconsistencies, ambiguities, and incompleterequirements of the problem in the field of IT. Therefore, the professionals from various fieldsshould involve in the process of IT manpower development. The holistic approach would be toreveal the characteristics of a problem not by an individual component, but by a system engineeringapproach where people from different fields must participate to develop manpower that meets thecurrent requirements. The students on the other hand are required to practice concept of this type oflearning. This type of teaching not only generalizes the problem but removes unnecessity details atthe beginning and provides the students the right skills and knowledge to proceed towards thesolution in the field of IT.

Today majority of the IT related jobs are in the application areas. One has to understand how businesses areconducted, how operation of a business links with the environment, and so on in order to come up as acompetent IT literate. Therefore, IT education needs business professionals who can give a clear and entirepicture of the problem and a complete solution to the students. It is required to be a good audience of theabstract subjects, professional subjects, before becoming a good IT solution provider. To achieve this, mereskill in programming may not be sufficient rather the IT literates should acquire knowledge from variousassociated disciplines.

Present day Change in Work Environment

It is a fact that more amounts of jobs are being done through computers and automated systems, day by day,which is often called computer meditated work. As a consequence, meaningfulness of work is getting reduced.

The abstractness of work is a related issue; because computer mediated work does not involve direct physicalcontact with the object of the task. There are many situations in which working through a computer affects theway workers experience their work. Here the user has to work on the symbols on a computer screen ratherthan a more reality workplace. If the work is done nicely, the participant user feels it is not his credit but thecredit of the machine or the system.

Example: Word processing provides obvious benefits: 1) mistakes can be easily corrected 2) documents andtemplates can be saved and re-used 3) spell checking. **However, there are problems:** Users make many morerevisions than they otherwise would do, but apparently without improving quality; Difficult to master (foraverage user); Too many features, many of which are never used; Little compatibility between packages.

Consider the example of a bank auditor in the e-Banking system. He also has to do all the work on the dataand information, rather than travel to branches and talk with different people, and examine the financial paperwork. Although some tasks were quicker and easier, still the auditor tends it more difficult to work withinformation only and without any human interaction. He feels the job has become abstract for better or worseand he does not like this kind of auditing.

There are also users who feel somewhat different in different types of computer mediated work. Some of theaspects of different systems are as follows.

Intellectual System: In this type of systems the computer is used as a tool for creating ideas, performinganalysis, etc. Analysis and manipulation of information is done through a computer, in new and differentways. However, this system may sometimes compel a switch over to a different method after a majorinvestment in one method. This is a major concern in the business practice. This can be tackled by the Re-Engineering concept. The users of this type of system may find it helpful and interesting to work with.

Production System: The worker in a production system enters instructions into a computer terminal attachedto a robot or NC machine. The machine does the work based on instructions, instead of the person holdingtools and doing the work, in reality. The person feels himself more like a programmer. This type of workaccounts for isolation in social relationship and the user may feel alienated.

Office Assistance System: The worker uses a computer terminal to store and retrieve data information insteadof writing on paper. The work is done through a key board and display screen. As the computer is the entirework space for the clerk steno, he cannot move here to there, in guise of searching a file or a piece of paper.

As a result he feels uncomfortable in his work place.

Control and Supervision: The worker receives instructions through the computer or is monitored based onthe rate or accuracy of inputs into a computer Her e, Feedback is based on computer recorded data and not onthe supervision directed observation Therefore, the worker feels it unnecessary and sometimes neglects it andwhich more often causes confusion among the line managers and workers.

Job Design in IT-Enabled Processes

There is a basic need for designing scheduling of different jobs in any IT-enabled process. It is clear from thelast section, as more numbers of innovations and inventions are coming in the field of InformationTechnology, the work environments are getting changed with more computerization, advancedcommunication and intelligent robots, There is a challenge before the operation and production department ofany enterprises, to design the work system taking both man and machines together. There is an urge for thedivision of labor between these two entities, utilizing their respective strengths and weaknesses It is a verydifficult task before the production and operation manager and has to be done considering the time and motionstudy of the man and machine it has been observed that the people are good at jobs involving understanding,imagination, arid the ability to visualize a situation as a whole. Machine is especially good at repetitive tasksinvolving perseverance, consistency, speed, and execution of unambiguous instructions.

There are two schools of thoughts based on the scheduling of jobs of work systems. They are human-centricdesign and machine-centric design. The difference in the two groups of thinking is in the design process oftechnologies and work systems. In human-centric design, the technology or the work process is designed tomake participant’s work effective and satisfying as far as possible. On the other hand, in machine- centricdesign, the technology or work process is designed to improve or simplify the procedure of the machine, andparticipants are expected to adjust to the machine’s weaknesses and limitations. Machine-centric design hasbeen the tradition in many computerized systems, where the basic assumption is that participant users willread the procedures, regardless of how confusing or contradictory the technology may be. There has beenmuch progress recently in this direction, considering the human factors after consultation with sociologist,anthropologist and personnel manager.

The rewards and punishments also differ with respect to the two design processes. In the machine centricdesign, when accidents occur, the user is the one to be blamed, rather than the work system or the technology.

Resistance to Change and its Management

The cause of resistance to change is more or less clear from the last subsection. It can be defined as any actionor inaction that obstructs a change in the existing process. It is a complex phenomenon because it involves acombination of motives It can be a highly rational response motivated by a desire to help thy organization, oron the other hand, it can have a selfish or vindictive motive of some individual element, due to some personalrivalry. Resistance may pose in many forms, either in the form of a public debate about the reason and effectof change, or complete closure shutdown of the work system Public debate can take a shape of directstatements about the shortcomings of the proposed system or a statement like “the system is unnecessary orundesirable”. Closure/shutdown can occur through conscious misuse and incorrect handling of data or otherforms. Even with a lot of effort to make the change process successful, many systems encounter significantresistance from potential participants/ Users.

For managing resistance and overcoming it, what is required is to think about the multiple causes of resistanceby looking at various aspects such as characteristics of the people and the characteristics of the system andtheir interaction. Awareness of the different causes of resistance is helpful in overcoming the implementationproblems. Secondly, there must be group discussions and common consensus from different sections of usersfor the implementations of the new systems.

Human-Centric Design

User-friendliness is one of the main features in the human-centric design of the work system. A system iscalled user-friendly if most users can use it easily with minimal learning and training time and users find ituseful. User friendly work systems are more productive because users waste less time and effort strugglingwith the system features that come on the way of getting the work done through the computer.

At the beginning, computers and computerized systems were more user-hostile rather than user friendly. Atechnology is user hostile when it is non-interactive and could be programmed only in languages appropriatefor professional programmers. But advances in computer languages, interactive computing and graphicalinterfaces make the computer and the IT-enabled systems more user-friendly systems. Features andcharacteristics of computer systems can be designed using intelligent tools and other advanced concepts to make them more friendly. Factors contributing to the user-friendliness of a system are: i) what the usermust learn and remember. ii)the nature of applications. iii) The nature of application programs and IV) thenature of the user interfaces. These factors have been discussed below.

i) What the User must learn: The users have to learn basic principles but do not have to remember the exactspelling or grammar for commands. All types of applications have a similar organization and appearance andare therefore easier to learn. ft interacts with the user in readily understandable terms, never forcing the user tolearn or pay attention to arbitrary or irrelevant details. In this case, user manual is not required regularly,except as a reference. The users can know how the system works by playing with or modifying one or twoexamples.

ii) Nature of the Application: A user-friendly system pro ides easy ways to access and reuse previous workby the users, by building templates as starting points. It includes task flexibility, i.e. permitting the user to dothe task in more than one way. Secondly, it is designed to minimize errors by users and to make it easy to fixany error that may occur.

iii) Nature of the Interface. Different methods arc combined to make the work more efficient, by using theinterface with different applications. The menus are well structured, easy to understand, and consistent withmenus in other applications. The system adjusts to, what the user knows. Novices can use basic features, onlyafter a careful observation. Experts need not have to interact the same way as novices.

Social Implications of Information Technology

The implications of IT in the society can be studied under different headings like: -

- Social Applications
- Employment and Productivity
- Competition
- Quality of Life
- Privacy

Social Applications

Computers can have many direct beneficial effects on society when they are used to solve human and socialproblems through social applications such as medical diagnosis, computer assisted instructions, governmentalprogram planning, environmental quality control and law enforcement. Computers can be used to helpdiagnose an illness, prescribe necessary treatment, and monitor the progress of hospital patients. Computerassistedinstruction (CAI) allows a computer to serve as “tutor” since it uses conversational computing totailor instruction to the needs of a particular student. This is a tremendous benefit to students, especially thosewith learning disabilities.

Computes can be used for crime control through various law enforcement applications that allow police toidentify and respond quickly to evidences of criminal activity. Computers have been used to monitor the levelof pollution in the air and in bodies of water, to detect the sources of pollution, and to issue early warningswhen dangerous levels are reached, Computers are also used for the program planning of many governmentagencies in such areas as urban planning, population density and land use studies, highway planning andurban transit studies. Computers are being used in job placement systems to help match unemployed personswith available jobs. These and other applications illustrate that computer -based information systems can beused to help solve the problems of society.

Impact on Employment and Productivity

The impact of computers on employment and productivity is directly related to the use of computers toachieve automation. There can be no doubt that the use of computers has created new jobs and increasedproductivity, while also causing a significant reduction in some types of job opportunities. Computers used foroffice information processing or for the numerical control of machine tools are accomplishing tasks formerlyperformed by many clerks and machinists. Also, jobs created by computers within a computer-usingorganization require different types of skills and education than do the jobs eliminated by computers.

Therefore, individuals within an organization may become unemployed unless they can be retrained for newpositions or new responsibilities.

However, there can be no doubt that the computer industry has created a host of new opportunities for themanufacture, sale, and maintenance of computer hardware and software, and for other information systemservices. Many new jobs, such as systems analysts, computer programmers, and computer operators, havebeen created in computer -using organizations. New jobs have also been created in service industries thatprovide services to the computer industry and to computer using firms. Additional jobs have been createdbecause computers make possible the production of complex industrial and technical goods and services thatwould otherwise be impossible to produce. Thus, jobs have been created by activities that are heavilydependent on computers, in such areas as space exploration, microelectronic technology, and scientific.

Impact on Competition

The impact of computers on competition concerns the effect computer systems have on the size and marketcontrol of business organizations. Computers allow large firms to become more efficient or gain strategiccompetitive advantages. This can have several anti-competitive effects. Small business firms that could existbecause of the inefficiencies of large firms are now driven out of business or absorbed by the larger firms. The efficiency and technological superiority of the larger firms allows them to continue to grow and combine withother business firms and thus create large corporations or strategic business alliances.

It is undoubtedly true that computers allow large organizations to grow larger and become more efficient.

Organizations grow in terms of people, market share, business alliances, productive facilities, and suchgeographic locations as branch offices and plants. Only computer -based information systems are capable ofcontrolling the complex activities and relationships that occur. However, it should be noted that the cost andsize of computer systems continue to decrease; due to the development of microcomputers andminicomputers, and that the availability of computer and telecommunications services continue to increase,due to the offerings of computer service bureaus, time-sharing companies, telecommunications carriers, andcooperative industry ventures. Therefore even small firms can take advantage of the productivity, efficiency,and strategic advantages generated by computer -based systems.

Impact on the Quality of Life

Since computerized business systems increase productivity, they allow the production of better-quality goodsand services at lower costs, with less effort and time. Thus, the computer is partially responsible for the highstandard pf living and increased leisure time many people enjoy. In addition, the computer has eliminatedmonotonous or obnoxious tasks in the office and the factory that formerly had to be performed by people. Inmany instances, this allows people to concentrate on more challenging and interesting assignments, upgradesthe skill level of the work to be performed, and creates challenging jobs requiring highly developed skills inthe computer industry and within computer-using organizations. Thus, computers can be said to upgrade thequality of life because they can upgrade the quality of working conditions and the content of work activities.

Of course, it must be remembered that some jobs created by the computer - data entry, for example - are quiterepetitive and routine and can create an “electronic sweatshop” work environment, especially if computers areused to monitor worker productivity. Also, to the extent that computers are utilized in some types ofautomation, they must take some responsibility for the criticism of assembly-line operations that require thecontinual repetition of elementary tasks, thus forcing a worker to work like a “machine” instead of like askilled craftsperson. Such effects do have a detrimental effect on the quality of life, but they are more thanoffset by the less burdensome and more creative jobs created by computers.

Impact on Privacy

Modem computer systems make it technically and economically feasible to collect, score, integrate,interchange, and retrieve data and information quickly and easily. This characteristic has an importantbeneficial effect on the efficiency and effectiveness of computer -based information systems. However, thepower of the computer to store and retrieve information can have a negative effect on the right to privacy ofevery individual. Confidential information on individuals contained in centralized computer databases bycredit bureaus, government agencies, and private business firms could be m issued and result in the invasion ofprivacy and other injustices. The unauthorized use of such information would seriously invade the privacy ofindividuals. Errors in such data files could seriously hurt the credit standing or reputation of an individual.

Such developments were possible before the advent of computers. However, the speed and power of largecomputers with centralized direct access databases and remote terminals greatly increases the potential forsuch injustices. The trend toward nationwide information systems with integrated databases by business firmsand government agencies substantially increases the potential for the misuse of computer -stored information.

Individual Aspect of Information Technology

People are related indirectly to the Information Technology, but any business is directly related. We canperform a Work Centered Analysis of any Business Process (BP) to reveal four links connected to this andthey are: -

1. Technology
2. Information
3. Participants and
4. Product / Services

Impact on individual can be studied in the following headings: -

· Ergonomics and Work Environments

· Solution of RMI

· Autonomy and Power

· Skill and Knowledge

· Involvement and Commitment

· Variety and Scope of Work

Ergonomics and Work Environments

Ergonomics is the scientific study of individuals and their physical relationship with the work environment orin other word, it is the study of the mental and physical capacities of persons with respect to the various kindsof work. The word “ergonomics” comes from the Greek word, “ergos” means work and “nomos” means laws.

Impacts of health, related to the physical relationship between people and their work environment are studiedin this field. Thus, the science of ergonomics can be defined as the study of th e laws of nature and their effectson the work environment. With respect to the office environment, this includes how the body interacts withworkspace, computers, tools, and furniture.

Occupational disease/injuries were first studied by Bernardino Ramnazzini during 17th century. He is knownas the father of occupational medicine. He identified that certain diseases were due to irregular motions andunnatural postures, which over time led to discomfort, pain or impaired function. This is known as *RepetitiveMotion Injuries* (RMI). RMI are also known as Repetitive Strain Injuries (RSI), Cumulative Trauma Disorder(CTD) and Carpal Tunnel Syndrome (CTS), which are the most common musculoskeletal injuries currentlyreported in the computer related health magazin e. Let us know about the origin of this disease.

Human body is made for free movement. Holding the body or a part of it in a particular position causes staticmuscle contractions. Muscles cannot maintain static contractions for more than a few seconds withoutexperiencing some fatigue. Muscles engaged in static work require more than 12 times longer to recover fromfatigue than muscles engaged in dynamic work. Prolonged and excessive static work causes the weakness injoints, ligaments, and tendons. This makes the workers more prone to pain and injuries. On the other hand,dynamic work allows muscles to contract and relax during the work cycle, therefore making muscles moreresistant to fatigue and injury. The symptoms of RMIs are as follows:

i) Pain or stiffness in the fingers, hands wrists, forearms, elbows, or shoulders

ii) Pain or stiffness in the back or neck

iii) Tingling or numbness in the hands or fingers

iv) Loss of strength or co-ordination in the hands

Autonomy and Power

Autonomy in a job means the degree of discretion of individuals or group in the process of planning,regulation, and control of their own work. *Power* is the ability to get other people to do things. Informationtechnology may increase or decrease autonomy and power in the work systems. It is said to be moreautonomous in work system, when the individual can control the use of the tools and techniques to get theoutput independently. For example, a *Data Analysis System* might give more autonomy to a manager in theanalysis work, which required previously, the assistance of a data analyst. Usually, professionals such asengineers and lawyers use IT-enabled systems to do work for them. It gives them more autonomy andflexibility over their work.

On the other hand, sometimes information technology is used to reduce autonomy, as and when it is required.

Transaction processing and record keeping systems are examples of such systems, which require limitedautonomy. These are designed to use the same rules for processing the same data in the same format byeveryone involved in this repetitive process, such as order taking or producing pay checks, etc. If Individualswill be allowed for autonomy, there will be a total collapse of the system. IT -enabled system, which monitorworkers closely and decrease autonomy often give rise to threats to the workers. Secondly, systems thatincrease employee monitoring may lead to resistance and may result in jettisoning of personnel.

Just as an IT-enabled system affects the autonomy, it can also affect power by redistributing information,changing responsibilities, and shifting the balance of power in an organization. It has increased the power ofpeople in the entire organization, who operate on facts, information and technical competence and at the sametime has reduc ed availability of information across the entire organization has made it possible to resolveconflicts based on facts rather than on opinions and power.

An IT-enabled system has another impact in reducing the power of middle managers in the organization.Higher-level executives are now getting information directly, by using MIS or EIS and moderncommunication system, such as e-mail and v-mail. In addition to this, they can go directly to the individualswho know about a particular. Therefore, middle level managers feel IT-enabled systems pose a threat to theirjob.

Issue of Skill and Knowledge

Information technology has positive or negative effects on people's skills. Consider the example of the use ofa pocket calculator to do arithmetic. One can get the right answer quickly, but the ability to do arithmeticmanually deteriorates through repetitive use of calculator. Here, the calculator has the positive impact ofcalculating more quickly and the negative impact of deteriorating ones skill of manual calculation.

New IT -enabled system has enhanced the skills in a wide range of jobs like MIS and EIS. It helps the managerto learn how to manage an organization, based on analysis of facts and information rather than just onintuition. Decision Support Systems (DSS) and execution systems such as CAD have helped professionalsanalyze data, define alternatives, and solve problems in new ways. Automating the job components also tendsto reduce peoples' skill by encouraging mental dis -engagement.

IT-enabled system also has a negative effect in some cases, as in automated judgment and discretion system.In such systems, an individual's autonomy and power has been replaced with computer-programmed Expertssystems for consistency and control. As a result, a less skilled person could do the same task, and the expert in that area has been devalued. Reducing the value of skills is called de-skilling. Therefore while automating thework systems; one must be vary careful in designing. The tasks, which require repetition, perseverance, andspeed of operation, should be automated, rather than the tasks, which require flexibility, creativity, andjudgment.

IT-enabled systems operate successfully only if participants have the necessary skills and knowledge. Itrequires new skills to be learnt by the professionals, and the technical staffs. The skill may involve newanalytical methods or new ways to obtain information for professionals and may only be literacy for nonprofessionalworkers. The system sometimes also requires knowledge about how to use computers for specifictasks and how to interpret information in that particular system.

Involvement and Commitment

People have a tendency to do work in the same fashion they were doing earlier. Therefore, they oppose thechange in the work systems. It is known as 'Social Inertia". It is required to overcome this social inertia. Themain factor to counter balance the social inertia is involvement and commitment by participants and theirmanagers. The involvement and commitment may be of different degrees, like non-involvement, low leveland high-level involvement.

The situation of non-involvement will arise if the users are unable to participate or they are not invited toparticipate or the system is imposed on them. In this situation, involvement through advice and sign-off helpsto initiate input about the priorities and features of the system and therefore reduces political problems.

Secondly, if the participants are invited and properly explained and trained about the system, th e system willrun nicely and it can be converted to a high-level involvement.

Low level of involvement and commitment makes IT based system prone to failures, although implementedproperly. It always leads to overlooking the system shortcomings and organizational issues, which otherwiselead to active participation. The highest level of involvement requires continuous involvement by theparticipants in the project team. Sometimes a representative of the team may also manage the system. Thismay lead to chaos after his retirement or departure. Higher level of involvement can solve different issuessuch as mutually inconsistent requests from different users and different needs that cannot all be supporteddue to resource constraints.

Variety and Scope of Work

Information technology can either increase or decrease the variety and scope of work. It reduces variety ifthey force the worker to focus on a small aspect of work. The range of different types of works people do atworkplace is called *task variety.* Almost all workers want a variety in their work environments and feel itmonotonous if the work becomes too routined and repetitive. *Scope of Work* is the size of the work/tasksrelative to the overall purpose of the organization. If the specialization is very narrow, just like a single job inan assembly line, it is a work with minimal scope. Assembling the entire job or a few numbers of jobs is a taskwith greater scope.

Impact of Internet

Internet culture

The Internet is also having a profound impact on work, knowledgeand worldviews. In addition to the creation of electronic commerceand communication with clients by email and related means, theInternet is transforming other aspects of the workplace. Certaincompanies have adopted the use of blogs, which are largely used asonline diaries, for promotional purposes. Since most people searchthe Web looking for information, these easily-updatable websitescan be filled with advice on the company's area of specialization.The company's hope is that, when the visitor finds this freeinformation, they will note the appearance of expert knowledge and may be drawn to the business'site as a result. An example of this practice is Microsoft, which has allowed its developers to publishtheir own personal blogs in order to pique the public's interest in their work.

Graphic representation of the WWW, a service running over the Internet, as represented byHyperlinks

The World Wide Web

Through keyword-driven Internet research using search engines like Google, millions worldwidehave easy, instant access to a vast and diverse amount of online information. Compared toencyclopedias and traditional libraries, the Internet has enabled a sudden and extremedecentralization of information and data.

Cultural awareness

From a cultural awareness perspective, the Internet has both an advantage and a liability. For peoplewho are interested in other cultures and the worldviews of those cultures it provides a significantamount of information and an interactivity that would be unavailable otherwise. However, for peoplewho are not interested in other cultures and worldviews there is some evidence indicating that theInternet enables them to avoid contact to a greater degree than ever before.

Current and potential problems

The Internet, along with its benefits, has a lot of negative publicity associated with it ranging fromgenuine concerns to tabloid scaremongering.

Child abuse

According to children's charities, the number of annual convictions for child pornography offenceshave increased by over 1000% since the Internet was first available to the public in the late 1980s.

With the recent growth in Chat rooms and instant messaging services in the late 1990s, the potentialfor a new form of child abuse has emerged: so-called grooming. This involves a pedophilepretending to be a child in a chat room/instant message conversation, to gain the trust of a childbefore arranging to meet up.

Copyright infringement

Copyright infringement has also been the focus of much media attention, mainly through peer-to-peerfile sharing software, but also through private members-only chat rooms, so-called warez sites(which openly offer illegal copies of software or the means to crack k copy protection), or even thesale of counterfeit CDs, DVDs and software masquerading as legitimate product. Many ordinaryInternet users are less concerned about the actual infringement itself but more about the effect on theInternet as a whole if tighter controls result from the infringement.

Viruses

In the 1980s and early 1990s, when very few people had access to the Internet, viruses were not ahuge problem. They did exist and did cause just as much damage to computers as modern viruses cantoday, but there was no fast-moving epidemic because there was no means for a virus to directlyinfect other computers. Before the Internet, the only way for a computer to be infected was throughuse of a removable disc that was itself infected. As a result, virus infections were mercifully rare.

Using Technology for Proverty Alleviation:

More than one third of the world's population lacks the resources and information to meet basic human needs such as adequate food, clean drinking water, sanitation, good health provision, shelter and education. Science, technology and innovation can play a crucial role in alleviating poverty. They have led to a wide array of developments, from boosting agricultural productivity to providing the means to generate energy cheaply. Developments in science and technology can make a significant contribution to meeting the key commitments of the Millennium Development Goals. They include reducing extreme poverty and child mortality rates, fighting disease and creating a global partnership for development.

Some of the routine for poverty alleviation with the help of technology may include:

- Use of new technologies to meet global challenges

  The implementation of simple technological ideas will enhance the lives in profound economic and social way. New advancesin scientificfields such aselectronics andnanotechnologycould provideenablingtechnologies toalleviate povertyon many fronts
- Innovation in disease control

  Improving health is a major issue in developing countries and is a field where innovation and technology can play a significant role.
- Overcoming illiteracy

  Literacy and poverty alleviation are directly proportional. Technologies can be used in different ways to reduces illiteracy which reduces the poverty.

Health Related Issue for an IT Professional

The Health Issues Due to Posture:

Back Pain or Low Backache:

- The lower portion of back pains. The problem becomes severe that one cannot bend forward. This is typically noticed when you get up from your seat after sitting for long hours. Your body feels stiffened and you take a few minutes to get back into your flexible movement.

Prevention:

- The posture does matter when it is sitting in front of the computer. Just check out the curve you make from the lower back. Lesser the curve you make, better the posture it is. Try to sit erected and don't bend forward to type or to see the monitor closely.

Health Disorders Because of the Distance

Computer Eye Strain

- Eye strain, dark circles and redness –the eyes are most delicate part of our body. If you have less distance between eyes and the monitor, the rays coming from it will affect your eyes badly.
- Computer Vision Syndrome or Dry Eye Syndrome –The eyes are red, itchy and constantly irritating. The simple reason is the screen, its radiation and resolution (means the brightness and contrast).Prevention:
- Ideally, the distance should be 18-24 inches to keep your eyes healthy. Take off the keyboard from the computer desk and arrange it somewhere nearer to you. Have enough lighting in the room, don't operate computer in dark or poor light condition.
- Keep blinking. Look at the objects or scenery that is at long distance every half an hour. Keep eye lubricants with you and hydrate your eyes every 3-5 hourly.

Neck pain due to monitor level

- Cervical pain –this happens due to improper level of the computer screen and your eyes. Constant looking low at the monitor will cause this problem as it'll stiffen the muscles of the neck and make them rigid.

Prevention:

- Adjust the level of the computer monitor and maintain the viewing angle. If this is not possible, adjust your chair –make it higher or shorter with the help of level provided. Regular massage helps

Major Health Problems Due to Lack of Motion

Constipation & Piles

- If you sit for longer hours daily for years, the intestine becomes slow. It is also due to improper timing of the meals that is observed in the IT professionals. The intestines then give up their work or become too slow.

Prevention:

- Take your meals on time. Include fiber in your diet (dark, green and leafy vegetables) and avoid too oily and junk food. After every hour, simply stand up, stretch your body, press your stomach gently and sit down.

Heart Problem

- The increase in cholesterol in IT professionals could be due to improper food timing, junk food, lack of motion and exercises. Improper breathing, chronic constipation, and poor blood circulation can also cause this issue.

Prevention:

- Remain active. Regularly go for the jogging as cardio exercises are the best to prevent this problem. Prefer stairs over elevators and park your vehicle a bit far from the parking place so that you walk down to the office.

Obesity in IT professionals

Obesity or overweight

- This is typical problem that IT professionals face these days. The reason is simple again, lack of motion, activities and exercises. Constant sitting on the chair in front of the computer add extra pounds to your body.

Prevention:

- Avoid junk food. Stop munching every time and if you cannot, keep sprouts, salads (carrots and cucumbers are best for this) or something fiber rich edible. Regular exercise and jogging will be great for this.

Carpal Tunnel Syndrome

- We have tunnel in our wrists. This tunnel consists of muscles, nerves, blood vessels etc. The pain in this tunnel due to continuous use of keyboard and mouse. You move your fingers and hand in particular direction several hundred times a day. Stiffness and pain in the wrist, numbness in the fingers and tingling sensation in the hand are few of the symptoms.

Prevention:

- Rotate your wrist every hour; flex and relax the fingers several times. Put something spongy under your wrist.

Internet Addiction

- Internet addiction brings a lot of health hazards due to over computer and handheld (internet enabled) devices. While enjoying the exemption from social stigmas, the internet users find themselves more comfortable on the imaginary World Wide Web than this vale of tears.
- Common problems include depression, dependency, anxiety, Obsessive Compulsive Disorder (OCD), complex problem, stubbornness, lack of social responsibilities, disrespect toward the elders (especially in children) and mood swings.

Prevention**:**

- Keep your kids' computers in the public hall and periodically check the history of webpages they visit in your absence. Fix up something like Team Viewer or simply block certain addictive websites.

International Issues of Information Society

This section attempts to synthesize issues that have come to be seen as constitutive of a hypotheticalinformation society. These issues have been articulated by government, business and civil societythrough their input into processes in the UN sphere and other selected bodies. These includedeclarations to which UN member states were signatories; input into the World Summit on theInformation Society (WSIS) by the Coordinating Committee of Business Interlocutors (CCBI),which includes the World Economic Forum; and regional and international statements of civilsociety formations involved in the WSIS process.

The Foundations of an Information Society

Information systems have long been seen as entities that not only embed society, but also as agentsthat help to define it. From a global perspective, the major task here has been to develop a sharedunderstanding of the concept of an information society. Such a vision might be best articulated interms of the fundamental basis of an information society and the roles of societal actors -governments, business and civil society - within it.

Two general perspectives on the fundamental basis of information society seemed to have emerged:-

1. Information society as a consumer-oriented environment containing tools, applications and services; or
2. Information society as a global commons enabled by ICTs in which human needs are central.

Many civil society entities have, on the other hand, articulated positions that would place human atthe center of a conception of an information society. In this viewpoint, an information society'spurposes, development, operation, and governance would take place within established human rightsframeworks and would be evaluated on its ability to meet human needs.

Governments have articulated a spectrum of positions on their roles in an information society. Thesearticulations have been made individually and collectively. The Millennium Declaration of theUnited Nations states that governments should "...ensure that the benefits of new technologies,especially 'information and communication technologies..." are enjoyed by all people. Oneimplication of this declaration is that ICTs are to be seen as major tools for meeting the series ofhighly ambitious goals it set forth, including the provision of elementary education to all children by

2015. The G8 nations articulated a similar, but less-specific message. One role of government in aninformation society that is implicit in these efforts is as a catalyst and organizer for business and civilsociety processes concerning an information society. For example, the G8 initiated the DigitalOpportunity Task Force (DOT Force) to address the digital divide and other societal matters.

Positions of member states with respect to these declarations vary. The European Union sees, in part,its role as bringing "the Information Society closer to all citizens of Europe, develop the economicwealth, address growing social needs , and focus on cultural identity and diversity".

A significant number of IT -related NGOs and other NGOs that have added IT issues to their agendashave adopted positions on the role of civil society that might be characterized as running counter topositions articulated by some governments and business or, at the very least, as acting as a balance.

Many see civil society as providing oversight for governmental and business activities within aninformation society that has become global and increasingly privatized. To this end, many entitieswithin civil society have called for greater transparency and citizen involvement in the operation ofan information society.

Digital Divide and Bridging the Digital Divide

Digital divide

- Digital divide is an economic and social inequality with regard to access to, use of, or impact of information and communication technologies. The divide within countries may refer to inequalities between individuals, households, businesses, or geographic areas, usually at different socioeconomic levels or other demographic categories. The divide between differing countries or regions of the world is referred to as the global digital divide,examining this technological gap between developing and developed countries on an international scale.

  The term Digital divide describes a gap in terms of access to and usage of information and communication technology, including the skills to make use of those technologies within a geographic area, society or community. The gap in a digital divide may exist for a number of reasons. Obtaining access to ICTs and using them actively has been linked to a number of demographic and socio-economic characteristics: among them income, education, race, gender, geographic location (urban-rural), age, skills, awareness and political, cultural and psychological attitudes.

Bridging the Digital Divide

- An individual must be able to connect in order to achieve enhancement of social and cultural capital as well as achieve mass economic gains in productivity. Therefore, access is a necessary (but not sufficient) condition for overcoming the digital divide
- ICT-enabled volunteering has a clear added value for development. If more people collaborate online with more development institutions and initiatives, this will imply an increase in person-hours dedicated to development cooperation at essentially no additional cost.
- Social media websites serve as both manifestations of and means by which to struggle the digital divide.

Internet Governance:

No one person, company, organization or government runs the Internet. It is a globally distributed network comprising many voluntarily interconnected autonomous networks. It operates without a central governing body with each constituent network setting and enforcing its own policies. Its governance is conducted by a decentralized and international network of interconnected autonomous groups.

However, to help ensure interoperability, several key technical and policy aspects of the underlying core infrastructure and the principal namespaces are administered by the Internet Corporation for Assigned Names and Numbers (ICANN), which is headquartered in Los Angeles, California. ICANN oversees the assignment of globally unique identifiers on the Internet, including domain names, Internet protocol addresses, application port numbers in the transport protocols, and many other parameters.

A working group established after a UN-initiated World Summit on the Information Society (WSIS) proposed the following definition of Internet governance as part of its June 2005 report:

> Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

E-Governance and E-government System:

E-Governance:

Electronic governance or e-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework. Through e-governance, government services will be made available to citizens in a convenient, efficient and transparent manner. The three main target groups that can be distinguished in governance concepts are government, citizens and businesses/interest groups. In e-governance there are no distinct boundaries.

Generally four basic systems are available.

- **government-to-citizen (customer)**

The goal of Government to Customer (G2C) e-Governance is to offer a variety of ICT services to citizens in an efficient and economical manner, and to strengthen the relationship between government and citizens using technology.

- **government-to-employees**

  E-Governance to Employee partnership (G2E) is one of the main primary interactions in the delivery model of E-Governance. It is the relationship between online tools, sources, and articles that help employees maintain communication with the government and their own companies. E-Governance relationship with Employees allows new learning technology in one simple place as the computer.

- **government-to-government**

  Government-to-Government (abbreviated G2G) is the online non-commercial interaction between Government organizations, departments, and authorities and other Government organizations, departments, and authorities.

- **government-to-business**

  Government-to-Business (G2B) is the online non-commercial interaction between local and central government and the commercial business sector with the purpose of providing businesses information and advice on e-business 'best practices'. G2B refers to the conduction through the Internet between government agencies and trading companies. B2G refers to Professional transactions between the company and the district, city, or federal regulatory agencies. B2G usually include recommendations to complete the measurement and evaluation of books and contracts.

3. Computer Ethics and Ethical Theories

Computer Ethics is a part of practical philosophy which deals with how computing professionals should make decisions regarding professional and social conduct. Margaret Anne Pierce, a professor in the Department of Mathematics and Computers at Georgia Southern University has categorized the ethical decisions related to computer technology and usage into 3 primary influences:

- The individual's own personal code.
- Any informal code of ethical conduct that exists in the work place.
- Exposure to formal codes of ethics

Philosophical Ethics:

Philosophical ethics seeks to establish positions not by empirical methods (observation or experimentation), extra-rational approaches (revelation or magic), or non-rational strategies (dogmatism or tradition). Philosophical ethics is based on the careful rational scrutiny of alternative positions and theories. The philosopher looks for such things as inner consistency, coherence with other strong theoretical positions, usefulness in application, and correspondence with relevant data. The philosopher brings all of the techniques and strategies of logic to bear on his or her study.

Philosophical ethics includes two different domains. The first is what is generally called "prescriptive ethics," which is the examination of alternative moral values, principles, and conduct, and the recommendation of some values, principles, or conduct as more rational or humane. Prescriptive ethics seeks to answer the question, "How should the moral person behave?"

The second domain of philosophical ethics is called "metaethics." It is a more recent phenomenon and has received its primary attention in this century. Metaethics is the examination of the logic and language of moral reflection, moral discourse, and moral action. The person doing metaethics does not make recommendations on how people should behave but rather seeks to gain insight on the nature of moral terms, on the logical structure and interrelatedness of moral assertions, and the like. Any recommendation offered by the metaethician would be on how we ought to view and use moral discourse. Metaethics seeks to answer the question, "What is the nature of moral discourse?" The reading by Ayer is an example of metaethics.

How does philosophical ethics differ from other approaches to ethics?

Social scientists generally approach ethics in a more descriptive fashion. Such people are more interested in describing the moral behavior of individuals or societies and in explaining why they behave in that way. In general, social scientists shy away from recommending a value system or a mode of behavior, but when such people do make these recommendations (as at times such people as Carl Rogers and B. F. Skinner do); they are really entering the domain of philosophical ethics.

Educational theorists may explore how some aspect of morality can be or should be taught. Sometimes this involves the recommendation of particular values or ethical positions, and sometimes it does not. While philosophers like Plato have explored the issue of teaching ethics, this is normally an issue separate from the philosophical examination of ethics. The moral educator would often make use of philosophical ethics, whether carefully or carelessly, before going to the next step of moral education.

Religionists often develop moral theories and make moral judgments, but they would normally make some use of revelation in this. Philosophers would confine themselves to the use of reason alone. In addition, as they do philosophy, philosophers seek to employ an open-mindedness which gives full consideration to a full range of positions and is not concerned to foster a particular religion or religious position. One of the most important goals of philosophy is intellectual honesty and integrity.

Legislators, law enforcement officials, lawyers, and others establish or deal with a society's laws. While there is an interesting and complex relationship between the law and morality, they are also distinct. There are actions judged normally to be immoral that would not usually be considered illegal (such as parents lying to their children) or vice versa (such as starting on a house without first obtaining a permit or using an unlicensed car for an emergency trip to the hospital when it is the only car available). Indeed, some legal theorists speak strongly against "legislating morality." Nevertheless, like the moral educator, the legislator and lawyer may make use of philosophical ethics in establishing or interpreting the law.

Is it possible to judge some moral positions or theories as better than others?

A view which is fairly common in academic circles but rejected by most philosophers as rationally unsound is moral or ethical relativism--the view that moral values, principles, and conduct vary significantly and that there are no firm criteria for judging one form of them to be better than or superior to another. This position may take the form either of societal or cultural relativism (that morality varies from culture to culture and that there is no basis for judging superiority between them) or individual subjectivism (that morality varies from individual to individual and that there is no basis for judging between them). There are three main arguments given for ethical relativism. I will here present them and offer brief responses.

First, it is sometimes argued that since the moral values and systems of cultures do in fact vary or since those of individuals do in fact vary, this shows that it is quite appropriate that they do vary; there are no over-arching values or principles that they share, so there is no way to judge one over against the other. It is often replied to this that because something is a certain way does not provide an argument for saying that it should be that way. Moreover, it seems reasonable to claim that a position which espouses racism, sexism, or the brutal treatment of other individuals or societies is inferior to a position that espouses the opposite, but true relativism would not accept this claim.

Second, it is often argued that relativism is correct because there are no absolute values or standards by which one can judge various systems. But often we make a relative judgment that something is better than something else without having an absolute standard to use in the judging. Thus, we may claim that broiled turkey is a more healthful food to eat than fried bacon is even though we don't have an absolute standard of what constitutes a healthful food. Our present knowledge of food and health indicates that factors which are involved in judging healthful foods include presence of vitamins, minerals, protein, etc. and the absence of cholesterol and fat, but this knowledge is constantly being modified. In the same way one might say that our present knowledge of ethics allows us to judge value systems or conduct on the basis of whether they respect the right of others, promote happiness, and promote truth and beauty, but this is also being modified. Thus, we don't need an absolute set of values to evaluate something; what is needed is a set of criteria which is developing through critical examination and reflection.

Third, it is sometimes thought that if a person is tolerant, this requires one to be relativistic. But tolerance requires rather that one not force views on another person. A person may be tolerant (and open-minded) but still believe that some positions are better than others. Such a person would be tolerant if he or she respected the right of another person to make his or her own choices on moral issues. (It might also be noted that a true relativist would not think there is a basis for finding tolerance morally preferable to intolerance.)

Professional Ethics:

Professional ethics encompass the personal, organizational and corporate standards of behaviour expected of professionals. Professionals and those working in acknowledged professions, exercise specialist knowledge and skill. How the use of this knowledge should be governed when providing a service to the public can be considered a moral issue and is termed as professional ethics.

Professionals are capable of making judgment, applying their skills and reaching informed decisions in situations that the general public cannot, because they have not received the relevant training.

Most professionals have internally enforced codes of practice that members of the profession must follow to prevent exploitation of the client and to preserve the integrity of the profession. This is not only for the benefit of the client but also for the benefit of those belonging to the profession. Disciplinary codes allow the profession to define a standard of conduct and ensure that individual practitioners meet this standard, by disciplining them from the professional body if they do not practice accordingly. This allows those professionals who act with conscience to practice in the knowledge that they will not be undermined commercially by those who have fewer ethical qualms. It also maintains the public’s trust in the profession, encouraging the public to continue seeking their services.

Some professional organizations may define their ethical approach in terms of a number of discrete components. Typically these include:

- Honesty
- Integrity
- Transparency
- Accountability
- Confidentiality
- Objectivity
- Respectfulness
- Obedience to the law
- Loyalty

For example, a fully trained doctor (with the correct equipment) would be capable of making the correct diagnosis and carrying out appropriate procedures. Failure of a doctor to help in such a situation would generally be regarded as negligent and unethical. An untrained person would not be considered to be negligent for failing to act in such circumstances and might indeed be considered to be negligent for acting and potentially causing more damage and possible loss of life.

Descriptive and Normative Claims:

Descriptive ethics is about what motivates pro-social behavior, how people reason about ethics, what people believe to have overriding importance, and how societies regulate behavior (such as by punishing people for doing certain actions). We know that empathy helps motivate pro-social behavior (such as giving to charity) and we know that our beliefs about what has overriding importance is somewhat based on the culture we live in.

What behaviors are punished in a society tells us something about what the people find to be of overriding importance. Punishment could even be social pressure, such as being criticized for doing something unethical.

Descriptive ethics is a form of empirical research into the attitudes of individuals or groups of people. In other words, this is the division of philosophical or general ethics that involves the observation of the moral decision-making process with the goal of describing the phenomenon. Those working on descriptive ethics aim to uncover people's beliefs about such things as values, which actions are right and wrong, and which characteristics of moral agents are virtuous. Research into descriptive ethics may also investigate people's ethical ideals or what actions societies reward or punish in law or politics. What ought to be noted is that culture is generational and not static. Therefore, a new generation will come with its own set of morals and that qualifies to be their ethics. Descriptive ethics will hence try to oversee whether ethics still holds its place.

Lawrence Kohlberg is one example of a psychologist working on descriptive ethics. In one study, for example, Kohlberg questioned a group of boys about what would be a right or wrong action for a man facing a moral dilemma: should he steal a drug to save his wife, or refrain from theft even though that would lead to his wife's death? Kohlberg's concern was not which choice the boys made, but the moral reasoning that lay behind their decisions. After carrying out a number of related studies, Kohlberg devised a theory about the development of human moral reasoning that was intended to reflect the moral reasoning actually carried out by the participants in his research. Kohlberg's research can be classed as descriptive ethics to the extent that he describes human beings' actual moral development. If, in contrast, he had aimed to describe how humans ought to develop morally, his theory would have involved prescriptive ethics.

Normative ethics is the study of ethical action. It is the branch of philosophical ethics that investigates the set of questions that arise when considering how one ought to act, morally speaking. Normative ethics is also distinct from descriptive ethics, as the latter is an empirical investigation of people’s moral beliefs. To put it another way, descriptive ethics would be concerned with determining what proportion of people believe that killing is always wrong, while normative ethics is concerned with whether it is correct to hold such a belief. Hence, normative ethics is sometimes called prescriptive, rather than descriptive.

Ethical Relativism

Ethical relativism is the theory that holds that morality is relative to the norms of one's culture. That is, whether an action is right or wrong depends on the moral norms of the society in which it is practiced. The same action may be morally right in one society but be morally wrong in another. For the ethical relativist, there are no universal moral standards -- standards that can be universally applied to all peoples at all times. The only moral standards against which a society's practices can be judged are its own. If ethical relativism is correct, there can be no common framework for resolving moral disputes or for reaching agreement on ethical matters among members of different societies.

Most ethicists reject the theory of ethical relativism. Some claim that while the moral practices of societies may differ, the fundamental moral principles underlying these practices do not. For example, in some societies, killing one's parents after they reached a certain age was common practice, stemming from the belief that people were better off in the afterlife if they entered it while still physically active and vigorous. While such a practice would be condemned in our society, we would agree with these societies on the underlying moral principle -- the duty to care for parents. Societies, then, may differ in their application of fundamental moral principles but agree on the principles.

Also, it is argued, it may be the case that some moral beliefs are culturally relative whereas others are not. Certain practices, such as customs regarding dress and decency, may depend on local custom whereas other practices, such as slavery, torture, or political repression, may be governed by universal moral standards and judged wrong despite the many other differences that exist among cultures. Simply because some practices are relative does not mean that all practices are relative.

Other philosophers criticize ethical relativism because of its implications for individual moral beliefs. These philosophers assert that if the rightness or wrongness of an action depends on a society's norms, then it follows that one must obey the norms of one's society and to diverge from those norms is to act immorally. This means that if I am a member of a society that believes that racial or sexist practices are morally permissible, then I must accept those practices as morally right. But such a view promotes social conformity and leaves no room for moral reform or improvement in a society. Furthermore, members of the same society may hold different views on practices. In the United States, for example, a variety of moral opinions exists on matters ranging from animal experimentation to abortion. What constitutes right action when social consensus is lacking?

Perhaps the strongest argument against ethical relativism comes from those who assert that universal moral standards can exist even if some moral practices and beliefs vary among cultures. In other words, we can acknowledge cultural differences in moral practices and beliefs and still hold that some of these practices and beliefs are morally wrong. The practice of slavery in pre-Civil war U.S. society or the practice of apartheid in South Africa is wrong despite the beliefs of those societies. The treatment of the Jews in Nazi society is morally reprehensible regardless of the moral beliefs of Nazi society.

For these philosophers, ethics is an inquiry into right and wrong through a critical examination of the reasons underlying practices and beliefs. As a theory for justifying moral practices and beliefs, ethical relativism fails to recognize that some societies have better reasons for holding their views than others.

But even if the theory of ethical relativism is rejected, it must be acknowledged that the concept raises important issues. Ethical relativism reminds us that different societies have different moral beliefs and that our beliefs are deeply influenced by culture. It also encourages us to explore the reasons underlying beliefs that differ from our own, while challenging us to examine our reasons for the beliefs and values we hold.

Utilitarianism and Deontological theories

There are two major ethics theories that attempt to specify and justify moral rules and principles;

- Utilitarianism ethics
- Deontological ethics.

Utilitarianism (also called consequentialism) is a moral theory developed and refined in the modern world by Jeremy Bentham (1748-1832) and John Stuart Mill (1806-1873). There are several varieties of utilitarianism. But basically, a utilitarian approach to morality implies that no moral act (e.g., an act of stealing) or rule (e.g., “Keep your promises”) is intrinsically right or wrong. Rather, the rightness or wrongness of an act or rule is solely a matter of the overall non-moral good (e.g., pleasure, happiness, health, knowledge, or satisfaction of individual desire) produced in the consequences of doing that act or following that rule. In sum, according to utilitarianism, morality is a matter of the non-moral good produced that results from moral actions and rules, and moral duty is instrumental, not inherent. Morality is a means to some other end; it is in no way an end in itself.

Space does not allow for a detailed critique of utilitarianism here. Suffice it to say that the majority of moral philosophers and theologians have found it defective. One main problem is that utilitarianism, if adopted, justifies as morally appropriate things that are clearly immoral. For example, utilitarianism can be used to justify punishing an innocent man or enslaving a small group of people if such acts produce a maximization of consequences. But these acts are clearly immoral regardless of how fruitful they might be for the greatest number.

For this and other reasons, many thinkers have advocated a second type of moral theory, deontological ethics. **Deontological ethics** is in keeping with Scripture, natural moral law, and intuitions from common sense. The word "deontological" comes from the Greek word deon which means "binding duty."

Deontological ethics has at least three important features. First, duty should be done for duty's sake. The rightness or wrongness of an act or rule is, at least in part, a matter of the intrinsic moral features of that kind of act or rule. For example, acts of lying, promise breaking, or murder are intrinsically wrong and we have a duty not to do these things.

This does not mean that consequences of acts are not relevant for assessing those acts. For example, a doctor may have a duty to benefit a patient, and he or she may need to know what medical consequences would result from various treatments in order to determine what would and would not benefit the patient. But consequences are not what make the act right, as is the case with utilitarianism. Rather, at best, consequences help us determine which action is more in keeping with what is already our duty. Consequences help us find what our duty is; they are not what make something our duty.

Rights

Rights are legal, social, or ethical principles of freedom or entitlement; that is, rights are the fundamental normative rules about what is allowed of people or owed to people, according to some legal system, social convention, or ethical theory. Rights are of essential importance in such disciplines as law and ethics, especially theories of justice and deontology.

Rights are often considered fundamental to civilization, being regarded as established pillars of society and culture, and the history of social conflicts can be found in the history of each right and its development. According to the Stanford Encyclopedia of Philosophy, "rights structure the form of governments, the content of laws, and the shape of morality as it is currently perceived.

Natural rights versus legal rights

- **Natural rights** are rights which are "natural" in the sense of "not artificial, not man-made", as in rights deriving from deontic logic, fromhuman nature, or from the edicts of a god. They are universal; that is, they apply to all people, and do not derive from the laws of any specific society. They exist necessarily, inhere in every individual, and can't be taken away. For example, it has been argued that humans have a natural right to life. These are sometimes called moral rights or inalienable rights.
- **Legal rights**, in contrast, are based on a society's customs, laws, statutes or actions by legislatures. An example of a legal right is the right to vote of citizens. Citizenship, itself, is often considered as the basis for having legal rights, and has been defined as the "right to have rights". Legal rights are

sometimes called civil rights or statutory rights and are culturally and politically relative since they depend on a specific societal context to have meaning.

Claim rights versus liberty rights

- A **claim right** is a right which entails that another person has a duty to the right-holder. Somebody else must do or refrain from doing something to or for the claim holder, such as perform a service or supply a product for him or her; that is, he or she has a claim to that service or product (another term is thing in action).In logic, this idea can be expressed as: "Person A has a claim that person B do something if and only if B has a duty to A to do that something." Every claim-right entails that some other duty-bearer must do some duty for the claim to be satisfied. This duty can be to act or to refrain from acting. For example, many jurisdictions recognize broad claim rights to things like "life, liberty, and property"; these rights impose an obligation upon others not to assault or restrain a person, or use their property, without the claim-holder's permission. Likewise, in jurisdictions where social welfare services are provided, citizens have legal claim rights to be provided with those services.
- A **liberty right** or privilege, in contrast, is simply a freedom or permission for the right-holder to do something, and there are no obligations on other parties to do or not do anything. This can be expressed in logic as: "Person A has a privilege to do something if and only if A has no duty not to do that something." For example, if a person has a legal liberty right to free speech, that merely means that it is not legally forbidden for them to speak freely: it does not mean that anyone has to help enable their speech, or to listen to their speech; or even, per se, refrain from stopping them from speaking, though other rights, such as the claim right to be free from assault, may severely limit what others can do to stop them.

Liberty rights and claim rights are the inverse of one another: a person has a liberty right permitting him to do something only if there is no other person who has a claim right forbidding him from doing so. Likewise, if a person has a claim right against someone else, then that other person's liberty is limited. For example, a person has a liberty right to walk down a sidewalk and can decide freely whether or not to do so, since there is no obligation either to do so or to refrain from doing so. But pedestrians may have an obligation not to walk on certain lands, such as other people's private property, to which those other people have a claim right. So a person's liberty right of walking extends precisely to the point where another's claim right limits his or her freedom.

Positive rights versus negative rights

In one sense, a right is a permission to do something or an entitlement to a specific service or treatment from others, and these rights have been called positive rights. However, in another sense, rights may allow or require inaction, and these are called negative rights; they permit or require doing nothing. For example, in some democracies e.g. the US, citizens have the positive right to vote and they have the negative right to not vote; people can choose not to vote in a given election without punishment. In other democracies e.g. Australia, however, citizens have a positive right to vote but they don't have a negative right to not vote, since voting is compulsory. Accordingly:

- **Positive rights** are permissions to do things, or entitlements to be done unto. One example of a positive right is the purported "right to welfare.

- **Negative rights** are permissions not to do things, or entitlements to be left alone. Often the distinction is invoked by libertarians who think of a negative right as an entitlement to non-interference such as a right against being assaulted.

Virtue Ethics

Before moving on to the ethical issues surrounding computer and information technology, one othertradition in ethical theory should be mentioned. In recent ears, interest has arisen in resurrecting thetradition of virtue ethics, a tradition going all the way back to Plato and Aristotle. These ancientGreek philosophers pursued the question: What is a good person? What are the virtues associatedwith being a good person? For the Greeks virtue meant excellence, and ethics was concerned withexcellences of human character. A person possessing such qualities exhibited the excellences ofhuman good. To have these qualities is to function well as a human being.

The list of possible virtues is long and there is no general agreement on which is most important,but the possibilities include courage , benevolence, generosity, honesty, tolerance, and self-control.

Virtue theorists try to identify e list of virtues and to give an account of each - what is courage? Whatis honesty? They also give an account of why the virtues are important.

Virtue theory seems to fill a gap left by other theories we considered, because it addresses thequestion of moral character, while the other theories focused primarily on action and decisionmaking. What sort of character should we be trying to develop in ourselves and in our children? Welook to moral heroes, for example, as exemplars of moral virtue. Why do we admire such people?

What is it about their character and their motivation that are worthy of tour admiration?

Virtue theory might be brought into the discussion of computer technology and ethics at any numberof points. The most obvious is, perhaps, the discussion of professional ethics, where we want to thinkabout the characteristics of a good computer professional. Good computer professionals will,perhaps, exhibit honesty in dealing with clients and the public. They should exhibit courage whenaced with situations in which they are being pressured to do something illegal or act counter topublic safety. A virtue approach would focus on these characteristics and more, emphasizing thevirtues of a good computer professional.

Individual and Social Policy Ethics

One final distinction will be helpful. In examining problems or issues, it is important to distinguishlevels of analysis, in particular that between macro and micro level issues or approaches. One canapproach a problem from the point of view of social practices and public policy, or from the point ofview of individual choice. Macro level problems are problems that arise for groups of people, acommunity, a state, a country. At this level of analysis, what is sought is a solution in the form of alaw or policy that specifies how people in that group or society ought to behave, what the rules ofthat group ought to be. When we ask the following questions, we are asking macro level questions:

Should the United States grant software creators a legal right to own software? Should softwareengineers be held liable for errors in the software they design? Should companies be allowed toelectronically monitor their employees?

On the other hand, micro level questions focus on individuals (in the presence or absence of law orpolicy). Should I make a copy of this piece of soft ware? Should I lie to my friend? Should I work ona project making military weapons?

Social Context of a Design

We only have identified the primary factors in a computer system to be performance, reliability, andcost. The factors such as usability and fit-to-task figuring in any software system are not consideredby us. A limited effort is included in the analysis of social context in traditional software design. Oneof the central challenges faced by software designers is how to balance the highly structured natureof computer artifacts with the need to integrate them into different settings. A software designerinevitably faces situations in which design choices are constrained by:

· The conflicting goals and values held by the different parties who have a stake in the changesthat new technologies will bring to the work

· Further, Workers and managers have many

o Common interests

o Different stakes

The question will be how computers in the workplace change productivity, working conditions, andjob satisfaction.

Design for People at Work

Well-designed systems can boost

· Productivity

· Enhance

· Job satisfaction and give both workers and managers a clearer sense of what is going on inthe organization.

But a system that interferes with crucial work practices:

· Can result in reduced effectiveness and efficiency,

· Reduced satisfaction and autonomy,

· Increased stress and health problems for the people who use the system.

Design Approaches

The basic design approaches are

· Technology-centered approach

· Work-Oriented Approaches

Work-Oriented approaches are further classified into two design approaches:

· Human-centered design

4. Professional Ethics

Profession

A **profession** is an art founded upon specialized educational training, the purpose of which is to supply disinterested objective warning and service to others, for a direct and definite return, wholly apart from expectation of other business gain.

A profession arises when any trade or occupation transforms itself through "the development of formal qualifications based upon education, apprenticeship, and examinations, the emergence of regulatory bodies with powers to admit and discipline members, and some degree of monopoly rights.

Professions enjoy a high social status, regard and esteem conferred upon them by society. This high esteem arises primarily from the higher social function of their work, which is regarded as vital to society as a whole and thus of having a special and valuable nature. All professions involve technical, specialized and highly skilled work often referred to as "professional expertise." Training for this work involves obtaining degrees and professional qualifications without which entry to the profession is barred (occupational closure). Updating skills through continuing education is required through training.All professions have power. This power is used to control its own members, and also its area of expertise and interests.

Job and Occupation

A person's **job** is their role in society. A job is an activity, often regular and often performed in exchange for payment. Many people have multiple jobs, such as those of parent, homemaker, and employee. A person can begin a job by becoming an employee, volunteering, starting a business, or becoming a parent. The duration of a job may range from an hour (in the case of odd jobs) to a lifetime (in the case of some judges). The activity that requires a person's mental or physical effort is work (as in "a day's work"). If a person is trained for a certain type of job, they may have a profession. The series of jobs a person holds in their life is their career.

Jobs can be categorized by the hours per week into full time or part time. They can be categorized as temporary, odd jobs, seasonal, self-employment, consulting, or contract employment.

Jobs can be categorized as paid or unpaid. Examples of unpaid jobs include volunteer, homemaker, mentor, student, and sometimes intern.

Jobs can be categorized by the level of experience required: entry level, intern, and co-op.

Some jobs require specific training or an academic degree.

Those without paid full-time employment may be categorized as unemployed or underemployed if they are seeking a full-time paid job.

Moonlighting is the practice of holding an additional job or jobs, often at night, in addition to one's main job, usually to earn extra income. A person who moonlights may have little time left for sleep or leisure activities.

Job vs Occupation/Employment vs Profession

Occupation and employment are similar, but job is the one that specifically refers to a professional vocation.

A job specifically refers to something you are doing for money or work. i.e. A job at the supermarket, or a thief 'doing a job' at the bank. It has a nuance as well of something being in your responsibility.

Occupation can refer to a job, but it can also mean any activity in which a person is engaged.

Occupation is like something you are occupied with, and you're not necessarily doing it as a 'business' thing.

Employment is the same as occupation, and can refer to something you are employed in doing, but not necessary a job done for work or money

More precisely:

Occupation — any work for hire or employment through which someone makes a living

Job — any work for hire, regardless of the skills level involved and the responsibility involved

Profession — virtue of his fundamental education and his training in a certain filed of expertise, to apply the scientific method and outlook he has gained in the analysis of the problem its respective field, solving it diligently and accordingly.

Characteristics of a Profession

The characteristics of profession can be specialized into following characters:

1. **Great responsibility:** Professionals deal in matters of vital importance to their clients and are therefore entrusted with grave responsibilities and obligations. Given these inherent obligations, professional work typically involves circumstances where carelessness, inadequate skill, or breach of ethics would be significantly damaging to the client and/or his fortunes.
2. **Accountability:** Professionals hold themselves ultimately accountable for the quality of their work with the client. The profession may or may not have mechanisms in place to reinforce and ensure adherence to this principle among its members.
3. **Based on specialized, theoretical knowledge:** Professionals render specialized services based on theory, knowledge, and skills that are most often peculiar to their profession and generally beyond the understanding and/or capability of those outside of the profession. Sometimes, this specialization will extend to access to the tools and technologies used in the profession (e.g. medical equipment).
4. **Institutional preparation:** Professions typically require a significant period of hands-on, practical experience in the protected company of senior members before aspirants are recognized as professionals. After this provisional period, ongoing education toward professional development is compulsory. A profession may or may not require formal credentials and/or other standards for admission.
5. **Autonomy:** Professionals have control over and, correspondingly, ultimate responsibility for their own work. Professionals tend to define the terms, processes, and conditions of work to be performed for clients (either directly or as preconditions for their ongoing agency employment).
6. **Clients rather than customers:** Members of a profession exercise discrimination in choosing clients rather than simply accepting any interested party as a customer (as merchants do).
7. **Direct working relationships:** Professionals habitually work directly with their clients rather than through intermediaries or proxies.
8. **Ethical constraints:** Due to the other characteristics on this list, there is a clear requirement for ethical constraints in the professions. Professionals are bound to a code of conduct or ethics specific to the distinct

profession (and sometimes the individual). Professionals also aspire toward a general body of core values, which are centered upon an uncompromising and un conflicted regard for the client's benefit and best interests.

9. **Merit-based:** In a profession, members achieve employment and success based on merit and corresponding voluntary relationships rather than on corrupted ideals such as social principle, mandated support, or extortion (e.g. union members are not professionals). Therefore, a professional is one who must attract clients and profits due to the merits of his work. In the absence of this characteristic, issues of responsibility, accountability, and ethical constraints become irrelevant, negating any otherwise-professional characteristics.
10. **Capitalist morality:** The responsibilities inherent to the practice of a profession are impossible to rationally maintain without a moral foundation that flows from a recognition of the singular right of the individual to his own life, along with all of its inherent and potential sovereign value; a concept that only capitalism recognizes, upholds and protects.

Computing and Engineering as a profession

Computational Science and Engineering is a rapidly developing field that brings together applied mathematics (especially numerical analysis), computer science, and scientific or engineering applications. This focuses on developing problem-solving methodologies and robust tools for numerical simulation. To understand phenomena and processes from science and engineering, we no longer need to depend only on theory and experiment, but can also use computations. Numerical simulations supplement experiments and can even allow the examination of systems and problems that would be too time-consuming, expensive, or dangerous (if possible at all) to study by experiment alone.

The high level of detail and realism in these simulations requires advanced skills in mathematical modeling, numerical analysis, efficient algorithms, computer architecture, software design and implementation, validation, and visualization of results.

Having the detailed knowledge about the engineering and computing skills, one can easily dilute in the digital world and make the same as their profession in different sectors like numerical simulation and analysis(sectors where numbers are the key points like banks etc), designing (sectors where graphics act as a key point like CAD, CAM, civil works like house, bridge design, mechanical works like machine and electronics design), software (sector where coding is the basic requirement) etc.

Professional responsibility

Professional responsibility is the area of legal practice that encompasses the duties of attorneys to act in a professional manner, obey the law, avoid conflicts of interest, and put the interests of clients ahead of their own interests. Some more responsibilities may include

- Confidentiality
- Avoiding conflict of interest
- Due diligence and Competence (law)
- Avoid commingling
- Avoid self-dealing
- Effective assistance
- Avoid fee splitting

Professional responsibility violations in normal may include

- Conflicts of interest.
- Incompetent representation.
- Mishandling of client money.
- Fee-splitting arrangements.
- Disclosure of confidential information

Conflict of Interest (**COI**)

A **conflict of interest** (**COI**) is a situation in which a person or organization is involved in multiple interests, financial interest, or otherwise, one of which could possibly corrupt the motivation of the individual or organization.

The presence of a conflict of interest is independent of the occurrence of impropriety. Therefore, a conflict of interest can be discovered and voluntarily defused before anycorruption occurs. A widely used definition is: "A conflict of interest is a set of circumstances that creates a risk that professional judgement or actions regarding a primary interest will be unduly influenced by a secondary interest. Primary interest refers to the principal goals of the profession or activity, such as the protection of clients, the health of patients, the integrity of research, and the duties of public office. Secondary interest includes not only financial gain but also such motives as the desire for professional advancement and the wish to do favours for family and friends, but conflict of interest rules usually focus on financial relationships because they are relatively more objective, fungible, and quantifiable. The secondary interests are not treated as wrong in themselves, but become objectionable when they are believed to have greater weight than the primary interests. The conflict in a conflict of interest exists whether or not a particular individual is actually influenced by the secondary interest. It exists if the circumstances are reasonably believed (on the basis of past experience and objective evidence) to create a risk that decisions may be unduly influenced by secondary interests.

The following are the most common formsof conflicts of interests:

- Self-dealing, in which an official who controls an organization causes it to enter into a transaction with the official, or with another organization that benefits the official only. The official is on both sides of the "deal."
- Outside employment, in which the interests of one job conflict with another.

COI is sometimes termed **competition of interest** rather than "conflict", emphasizing a suggestion of natural competition between valid interests rather than violent conflict with its suggestion of victimhood and unfair aggression.

Whistle blowing:

Whistle blowing is the process of exposing any kind of information or activity that is deemed illegal, dishonest, or not correct within an organization that is either private or public. The information of suspected wrongdoing can be classified in many ways: violation of company policy/rules, law, regulation, or threat to public interest/national security, as well as fraud, and corruption. Those who become whistleblowers can choose to bring information or allegations to surface either internally or externally. Internally, a whistleblower can bring his/her accusations to the attention of other people within the accused organization. Externally, a whistleblower can bring allegations to light by contacting a third party outside of an accused organization. He/She can reach out to the media, government, law enforcement, or those who are concerned.

Types of Whistle blowing

A distinction is often made between internal and external whistle blowing.

Internal Whistle blowingoccurs when an employee goes over the head of an immediate supervisor to report a problem to ahigher level of management. Or, all levels of management are bypassed, and the employee goesdirectly to the president of the company or the board of directors, However it is done, the whistle blowing is kept within the company or organization.

External Whistle blowingoccurs whenthe employee goes outside the company and reports wrongdoing to newspapers or law-enforcementauthorities. Either type of whistle blowing is likely to be perceived as disloyalty. However, keeping itwithin the company is often seen as less serious than going outside of the company.

There is also a distinction between acknowledged and anonymous whistle blowing. AnonymousWhistle blowing occurs when the employee who is blowing the whistle refuses to divulge his namewhen making accusations. These accusations might take the form of anonymous memos to uppermanagement or of anonymous phone calls to the police. The employee can also talk to the newsmedia but refuse to let her name be used as the source of the allegations of wrongdoing.

Acknowledged whistle blowing, on the other hand, occurs when the employee puts his name behindthe accusations and is willing to withstand the scrutiny brought on by his accusations.

Whistle blowing can be very bad from a corporation point of view because it can lead to distrust,disharmony, and an inability of employees to work together. Similarly, in business, whistle blowing is perceived as an act of extreme disloyalty to the company and to co-workers.

When Should Whistle blowing Be Attempted?

Whistle blowing should only be attempted if the following four conditions are met:

Need

There must be a clear and important harm that can be avoided by blowing the whistle. In decidingwhether to go public, the employee needs to have a sense of proportion. You do not need to blow thewhistle about everything, just the important things Of course, if there is a pattern of many smallthings that are going on, this can add tip to a major and important matter requiring that the whistle beblown.

Proximity

The whistleblower must be in a very clear position to report on the problem. Hearsay is not adequate.Firsthand knowledge is essential to making an effective case about wrongdoing. This point alsoimplies that the whistleblower must have enough expertise in the area to make a realistic assessmentof the situation. This condition stems from the clauses in several codes of ethics that mandate that making assessments about whether wrongdoing is taking place.

Capability

The whistleblower must have a reasonable chance of success in stopping the harmful activity. Youare not obligated to risk your career and the financial security of your family if you can’t see the casethrough to completion or you don’t feel that you have access to the proper channels to ensure that thesituation is resolved.

Last Resort

Whistle blowing should be attempted only if there is no one else more capable or more proximate toblow the whistle and if you feel that all other lines of action within the context of the organizationhave been explored and shut off.

Preventing Whistle blowing

There are four ways in which to solve the whistle blowing problem within a corporation.

First, there must he a **strong corporate ethics culture** . This should include a clear commitment toethical behavior, starting at the highest levels of management, and mandatory ethics training for allemployees. All managers must set the tone for the ethical behavior of their employees.

Second, there should be **clear lines of communication** within the corporation. This openness givesan employee who feels that there is something that must be fixed a clear path to air his concerns.

Third, all employees must have **meaningful access to high-level managers** in order to bring theirconcerns forward. This access must come with a guarantee that there will be no retaliation. Rather,employees willing to come forward should be rewarded for their commitment to fostering the ethicalbehavior of the company.

Finally, there should be willingness on the part of management to **admit mistakes**, publicly ifnecessary. Thisattitude will set the stage for ethical behavior by all employees.

Code of ethics

Code of ethics are adopted by organizations to assist members in understanding the difference between 'right' and 'wrong' and in applying that understanding to their decisions. An ethical code generally implies documents at three levels: codes of business ethics, codes of conduct for employees, and codes of professional practice.

Many companies use the phrases 'ethical code' and 'code of conduct' interchangeably but it may be useful to make a distinction. A code of ethics will start by setting out the values that underpin the code and will describe a company's obligation to its stakeholders. The code is publicly available and addressed to anyone with an interest in the company's activities and the way it does business. It will include details of how the company plans to implement its values and vision, as well as guidance to staff on ethical standards and how to achieve them. However, a code of conduct is generally addressed to and intended for employees alone. It usually sets out restrictions on behavior, and will be far more compliance or rules focused than value or principle focused. Also this code is good for the Non Governmental Organization.

Code of ethics of Nepal Engineering Council

The professional Code of Conduct to be followed by the registered Engineers of the Council, subject to the provision of the Nepal Engineering Council (NEC) Act, 2055 (1998) and the Nepal Engineering Council Regulation,2057(2000), has been published as follows :

1. **Discipline and Honesty:** The Engineering service/profession must be conducted in a disciplined manner with honesty, not contravening professional dignity and well-being .
2. **Politeness and Confidentiality:** Engineering services for customers should be dealt with in a polite manner and professional information should remain confidential except with written or verbal consent of

the customers concerned. This, however, is not deemed to be a restriction to provide such information to the concerned authority as per the existing laws.

3. **Non-discrimination:** No discrimination should be made against customers on the grounds of religion, race, sex, caste or any other things while applying professional knowledge and skills.

4.**Professional Work:** Individuals should only do professional work in their field or provide recommendations or suggestions only within the area of their subject of study or obtained knowledge or skills. With regard to the works not falling within the subject of one's profession, such works should be recommended to be done by an expert of that subject matter.

5. **Deeds which may cause harm to the engineering profession:**With the exception of salary, allowance and benefits to be received for services provided, one shall not obtain improper financial gain of any kind or conduct improper activities of any kind, which would impair the engineering profession.

6. **Personal responsibility:** All individuals will be personally responsible for all works performed in connection with his/her engineering profession.

7. **State name, designation and registration no**: While signing the documents or descriptions such as the design, map, specifications and estimates etc, relating to the engineering profession, the details should include, the name, designation and NEC registration No. and should be stated in a clear and comprehensible manner.

8. **No publicity or advertisement must be made which may cause unnecessary effect:** In connection with the professional activities to be carried out**,** no publicity or advertisement shall be made so as to cause unnecessary effect upon the customers.

Note: *Engineers, working with government, quasi government, private sectors, NGOs, INGOs, bilateral and multilateral agencies and consultants etc., if not registered with NEC, can be punished as it would be against the Law of Land. NEC is not responsible for registering engineers who complete their studies from any institute or through any engineering programs unless and until such programs are inspected/ monitored & approved by NEC.*

Code of ethics of IEEE

The code of ethics of IEEE approved by the IEEE Board of Directors February 2006 is:

We, the members of the IEEE , in recognition of the importance of ourtechnologies in affecting the quality of life throughout the world and in accepting apersonal obligation to our profession, its members and the communities we serve, dohereby commit ourselves to the highest ethical and professional conduct and agree:

IEEE CODE OF ETHICS

1. To accept responsibility in making decisions consistent with the safety, health andwelfare of the public, and to disclose promptly factors that might endanger thepublic or the environment;
2. To avoid real or perceived conflicts of interest whenever possible, and to disclosethem to affected parties when they do exist;
3. To be honest and realistic in stating claims or estimates based on available data;
4. To reject bribery in all its forms;
5. To improve the understanding of technology, its appropriate application, andpotential consequences;

6. To maintain and improve our technical competence and to undertake technologicaltasks for others only if qualified by training or experience, or after full disclosureof pertinent limitations;

7. To seek, accept, and offer honest criticism of technical work, to acknowledge andcorrect errors, and to credit properly the contributions of others;

8. To treat fairly all persons regardless of such factors as race, religion, gender,disability, age, or national origin;

9. To avoid injuring others, their property, reputation, or employment by false ormalicious action;

10. To assist colleagues and co-workers in their professional development and tosupport them in following this code of ethics.

Code of ethics of ACM

ACM Code of Ethics and Professional Conduct

Adopted by ACM Council 10/16/92.

Preamble

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

1. GENERAL MORAL IMPERATIVES.

As an ACM member I will ....

1.1 Contribute to society and human well-being.

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

1.2 Avoid harm to others.

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, and employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5 regarding thorough evaluations.

1.3 Be honest and trustworthy.

Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society,all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

1.5 Honor property rights including copyrights and patent.

Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

1.6 Give proper credit for intellectual property.

Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

1.7 Respect the privacy of others.

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages,without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

1.8 Honor confidentiality.

The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.

As an ACM computing professional I will ....

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.

Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

2.2 Acquire and maintain professional competence.

Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

2.3 Know and respect existing laws pertaining to professional work.

ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review.

Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm, including the reporting of professional violations.

2.6 Honor contracts, agreements, and assigned responsibilities.

Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences.

However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

2.7 Improve public understanding of computing and its consequences.

Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so.

Theft or destruction of tangible and electronic property is prohibited by imperative 1.2- "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4). No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.

As an ACM member and an organizational leader, I will ....

BACKGROUND NOTE:This section draws extensively from the draft IFIP Code of Ethics,especially its sections on organizational ethics and international concerns. The ethical obligations of organizations tend to be neglected in most codes of professional conduct, perhaps because these codes are written from the perspective of the individual member. This dilemma is addressed by stating these imperatives from the perspective of the organizational leader. In this context"leader" is viewed as any organizational member who has leadership or educational responsibilities. These imperatives generally may apply to organizations as well as their leaders. In this context"organizations" are corporations, government agencies,and other "employers," as well as volunteer professional organizations.

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.

Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore,organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.

Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.

Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.

Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems.In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

4. COMPLIANCE WITH THE CODE.

As an ACM member I will ....

4.1 Uphold and promote the principles of this Code.

The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

4.2 Treat violations of this code as inconsistent with membership in the ACM.

Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

This Code and the supplemental Guidelines were developed by the Task Force for the Revision of the ACM Code of Ethics and Professional Conduct: Ronald E. Anderson, Chair, Gerald Engel, Donald Gotterbarn, Grace C. Hertlein, Alex Hoffman, Bruce Jawer, Deborah G. Johnson, Doris K. Lidtke, Joyce Currie Little, Dianne Martin, Donn B. Parker, Judith A. Perrolle, and Richard S. Rosenberg. The Task Force was organized by ACM/SIGCAS and funding was provided by the ACM SIG Discretionary Fund. This Code and the supplemental Guidelines were adopted by the ACM Council on October 16, 1992.

Hacker ethics and Netiquette

Hacker ethic is a term for the moral values and philosophy that are common in the hacker community. The MIT group defined a *hack* as a project undertaken or a product built to fulfill some constructive goal, but also with some wild pleasure taken in mere involvement. The hacker ethic was described as a "new way of life, with a philosophy, an ethic and a dream". However, the elements of the hacker ethic were not openly debated and discussed; rather they were implicitly accepted and silently agreed upon.

The free software movement was born in the early 1980s from followers of the hacker ethic. Its founder, Richard Stallman, is referred to by Steven Levy as "the last true hacker". Modern hackers who hold true to the hacker ethics —especially the Hands-On Imperative—are usually supporters of free and open source software. This is because free and open source software allows hackers to get access to the source code used to create the software, to allow it to be improved or reused in other projects.

Richard Stallman describes:

The hacker ethic refers to the feelings of right and wrong, to the ethical ideas this community of people had—that knowledge should be shared with other people who can benefit from it, and that important resources should be utilized rather than wasted.

Netiquette

"Netiquette" is network etiquette, the do's and don'ts of online communication. Netiquette covers both common courtesy online and the informal "rules of the road" of cyberspace.

The following can be the Core Rules of Netiquette:

- Rule 1: Remember the Human
    - Rule 2: Adhere to the same standards of behavior online that you follow in real life
    - Rule 3: Know where you are in cyberspace
    - Rule 4: Respect other people's time and bandwidth
    - Rule 5: Make yourself look good online
    - Rule 6: Share expert knowledge

  - Rule 7: Help keep flame wars under control
  - Rule 8: Respect other people's privacy
- Rule 9: Don't abuse your power
- Rule 10: Be forgiving of other people's mistakes

5. Risk and Responsibilities

Risk

A risk is a potential problem that might or might not happen. It is necessary to identify risk so that potential problems can be avoided.

Two characteristics of risk

- Uncertainty
- Loss

Associated Definitions and Concepts

There are a number of key terms that should be understood to manage risk. Some of these terms will be defined here because they are used throughout the remainder of the chapter.

Risk: The possibility of suffering harm or loss.

Risk management: The overall decision-making process of identifying threats and vulnerabilities and their potential impacts, determining the costs to mitigate such events, and deciding what actions are cost-effective for controlling these risks.

Risk assessment (or risk analysis): The process of analyzing an environment to identify the threats, vulnerabilities, and mitigating actions to determine (either quantitalively or qualitatively) the impact of an event that would affect a project, program, or business.

Asset: Resource or information an organization needs to conduct its business.

Threat: Any circumstance or event with the potential to cause harm to

Vulnerability: Characteristic of an asset that can be exploited by a threat to cause harm.

Impact: The loss resulting when a threat exploits vulnerability.

Control (also called countermeasure or safeguard): A measure taken to detect, prevent, or mitigate the risk associated with a threat.

Qualitative risk assessment: The process of subjectively determining the impact of an event that affects a project, program, or business. Qualitative risk assessment usually involves the use of expert judgment, experience, or group consensus to compel the assessment, often used to attach a potential monetary loss to a threat.

Quantitative risk assessment: The process of objectively determining the impact of an event that affects a project, program, or business. Quantitative risk assessment usually involves the use of metrics and models to complete the assessment.

Qualitative vs. Quantitative Risk Assessment

It is recognized throughout industry that it is impossible to conduct risk management that is purely quantitative. Usually risk management includes both qualitative and quantitative elements, requiring both analysis and judgment or experience. It is important to note that in contrast to quantitative assessment, it is possible to accomplish purely qualitative risk management.

It is easy to see that it is impossible to define and quantitatively measure all factors that exist in a given risk assessment. It is also easy to see that a risk assessment that measures no factors quantitatively but measures them all qualitatively is possible.

Computer Security and Liability

Information insecurity is costing us billions. We pay for it in theft: information theft, financial theft. We pay for it in productivity loss, both when networks stop working and in the dozens of minor security inconveniences we all have to endure. We pay for it when we have to buy security products and services to reduce those other two losses. We pay for security, year after year.

The problem is that all the money we spend isn't fixing the problem. We're paying, but we still end up with insecurities.

The problem is insecure software. It's bad design, poorly implemented features, inadequate testing and security vulnerabilities from software bugs. The money we spend on security is to deal with the effects of insecure software.

And that's the problem. We're not paying to improve the security of the underlying software. We're paying to deal with the problem rather than to fix it.

The only way to fix this problem is for vendors to fix their software, and they won't do it until it's in their financial best interests to do so.

Today, the costs of insecure software aren't borne by the vendors that produce the software. In economics, this is known as an externality, the cost of a decision that's borne by people other than those making the decision.

There are no real consequences to the vendors for having bad security or low-quality software. Even worse, the marketplace often rewards low quality. More precisely, it rewards additional features and timely release dates, even if they come at the expense of quality.

If we expect software vendors to reduce features, lengthen development cycles and invest in secure software development processes, it needs to be in their financial best interests to do so. If we expect corporations to spend significant resources on their own network security -- especially the security of their customers -- it also needs to be in their financial best interests.

Liability law is a way to make it in those organizations' best interests. Raising the risk of liability raises the costs of doing it wrong and therefore increases the amount of money a CEO is willing to spend to do it right. Security is risk management; liability fiddles with the risk equation.

Basically, we have to tweak the risk equation so the CEO cares about actually fixing the problem, and putting pressure on his balance sheet is the best way to do that.

Clearly, this isn't all or nothing. There are many parties involved in a typical software attack. There's the company that sold the software with the vulnerability in the first place. There's the person who wrote the attack tool. There's the attacker himself, who used the tool to break into a network. There's the owner of the network, who was entrusted with defending that network. One hundred percent of the liability shouldn't fall on the shoulders of the software vendor, just as 100% shouldn't fall on the attacker or the network owner. But today, 100% of the cost falls directly on the network owner, and that just has to stop.

We will always pay for security. If software vendors have liability costs, they'll pass those on to us. It might not be cheaper than what we're paying today. But as long as we're going to pay, we might as well pay to fix the problem. Forcing the software vendor to pay to fix the problem and then pass those costs on to us means that the problem might actually get fixed.

Liability changes everything. Currently, there is no reason for a software company not to offer feature after feature after feature. Liability forces software companies to think twice before changing something. Liability forces companies to protect the data they're entrusted with. Liability means that those in the best position to fix the problem are actually responsible for the problem.

Malfunction of Computer

Computers have become an important part of everyday life so when the machine we depend on begins to malfunction it’s easy to panic. The truth is that many computer problems also have an easy fix. Learn to recognize the problem and you’re well on your way to finding a solution.

1. One of the first signs of trouble is when a computer begins to slow down. A slow down can be caused by many things including too many programs at start up, a full hard drive, too little ram or the presence of a virus or spyware. The good news is that most of these problems are easy to fix and you may just need to clean up your computer.
2. When a computer freezes you may have no option but to reboot and lose any information or projects you had open. Freezes can be signs of not enough ram, registry conflicts, corrupt or missing files or spyware. Often cleaning up the system will help solve the problem.
3. A noisy computer is a sign of a hardware malfunction. Hard drives are noted for making noises just before they fail but it may also be a noisy fan. A fan is an easy fix and you can often salvage the information from your hard drive either before it fails completely or with the use of recovery software.
4. Dropped Internet connections can be frustrating. It may be due to a bad cable or phone line which is an easy fix. More serious problems can include viruses, a bad network card or modem or a problem with the drivers.
5. If your computer clock is out of sync, it may be that your CMOS battery needs replacing. Reset the time and if it continues to lag, replace the battery.
6. It can be quite a surprise when our browser homepage is hijacked, especially when it seems impossible to change it back. This is often caused by a virus or some type of marketing software. Get rid or the virus or the software and you can get back control of your browser.
7. If your computer turns on by itself you may wonder if it’s possessed but if the BIOS is set to “wake on modem” or “wake on LAN”, you might experience this problem.
8. Unexpected reboots can be a sign of hardware problems such as a faulty power supply, a bad processor or a dirty intake fan. Try using canned air to clean out the fans and see if it solves the problem.
9. If your computer is connecting to the Internet on its own adware or spyware is the likely issue. They will run in the background on your computer and open an Internet connection when they need to update. Viruses, trojans and dialers installed by malicious websites may also be the culprit.
10. When a computer refuses to boot completely it may be a driver problem or some type of conflict. If you can boot into Safe Mode use the System Configuration Utility to load just the basic devices and services. This may allow you to boot the computer and track down the problem.

In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Some common countermeasures are listed in the following sections:

Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.
- Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security comprises mainly "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of mostUNIX-based operating systems such as Linux, built into the operating system kernel) to provide real time filtering and blocking. Another implementation is a so-called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet.

However, relatively few organisations maintain computer systems with effective detection systems, and fewer still have organised response mechanisms in place. As result, as Reuters points out: "Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets".The primary obstacle to effective eradication of cyber crime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using packet capture appliances that puts criminals behind bars.

Reducing vulnerabilities

While formal verification of the correctness of computer systems is possible, it is not yet common. Operating systems formally verified include seL4, and SYSGO'sPikeOS – but these make up a very small percentage of the market.

Cryptography properly implemented is now virtually impossible to directly break. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.

Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or other piece of hardware. This increases security as an unauthorized person needs both of these to gain access.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Even in a highly disciplined environment, such as in military organizations, social engineering attacks can still be difficult to foresee and prevent.

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful backing up and insurance.

Security by design

Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature.

Some of the techniques in this approach include:

- The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way even if an attacker gains access to that part, they have only limited access to the whole system.
- Automated theorem proving to prove the correctness of crucial software subsystems.
- Code reviews and unit testing, approaches to make modules more secure where formal correctness proofs are not possible.
- Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.

Security architecture

The Open Security Architecture organization defines IT security architecture as "the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and assurance services".

Techopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible." The key attributes of security architecture are:

- the relationship of different components and how they depend on each other.
- the determination of controls based on risk assessment, good practice, finances, and legal matters.
- the standardization of controls.

Hardware protection mechanisms

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process, hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated backdoor access) required in order to be compromised. Each of these is covered in more detail below.

- USB dongles are typically used in software licensing schemes to unlock software capabilities, but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as Advanced Encryption Standard (AES) provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs). In addition, a USB dongle can be configured to lock or unlock a computer.

- Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access
- Computer case intrusion detection refers to a push-button switch which is triggered when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.
- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves. Tools exist specifically for encrypting external drives as well.
- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by Network World as the most common hardware threat facing computer networks
- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low energy(LE), Near field communication (NFC) on non-iOS devices and biometric validation such as thumb print readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.

Secure operating systems

One use of the term "computer security" refers to technology that is used to implement secure operating systems. Much of this technology is based on science developed in the 1980s and used to produce what may be some of the most impenetrable operating systems ever. Though still valid, the technology is in limited use today, primarily because it imposes some changes to system management and also because it is not widely understood. Such ultra-strong secure operating systems are based on operating system kerneltechnology that can guarantee that certain security policies are absolutely enforced in an operating environment. An example of such a Computer security policy is the Bell-LaPadula model. The strategy is based on a coupling of special microprocessor hardware features, often involving the memory management unit, to a special correctly implemented operating system kernel. This forms the foundation for a secure operating system which, if certain critical parts are designed and implemented correctly, can ensure the absolute impossibility of penetration by hostile elements. This capability is enabled because the configuration not only imposes a security policy, but in theory completely protects itself from corruption. Ordinary operating systems, on the other hand, lack the features that assure this maximal level of security. The design methodology to produce such secure systems is precise, deterministic and logical.

Secure coding

If the operating environment is not based on a secure operating system capable of maintaining a domain for its own execution, and capable of protecting application code from malicious subversion, and capable of protecting the system from subverted code, then high degrees of security are understandably not possible. While such secure operating systems are possible and have been implemented, most commercial systems fall in a 'low security' category because they rely on features not supported by secure operating systems (like portability, and others). In low security operating environments, applications must be relied on to participate in their own protection. There are 'best effort' secure coding practices that can be followed to make an application more resistant to malicious subversion.

In commercial environments, the majority of software subversion vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. These defects can be used to cause the target system to execute putative data. However, the "data" contain executable instructions, allowing the attacker to gain control of the processor.

MisInterpretation

Misrepresentation

Misrepresentation is a TORT, or a civil wrong. This means that a misrepresentation can create civil liability if it results in a pecuniary loss. Forexample, assume that a real estate speculator owns swampland but advertises it as valuable commercially zoned land. This is amisrepresentation. If someone buys the land relying on the speculator's statement that it is commercially valuable, the buyer may sue thespeculator for monetary losses resulting from the purchase.

To create liability for the maker of the statement, a misrepresentation must be relied on by the listener or reader. Finally, the listener's reliance on the statement must have beenreasonable and justified, and the misrepresentation must have resulted in a pecuniary loss to the listener.

A misrepresentation need not be intentionally false to create liability. A statement made with conscious ignorance or a reckless disregard forthe truth can create liability. Nondisclosure of material or important facts by a fiduciary or an expert, such as a doctor, lawyer, or accountant,can result in liability. If the speaker is engaged in the business of selling products, any statement, no matter how innocent, may createliability if the statement concerns the character or quality of a product and the statement is not true.

A misrepresentation in a contract can give a party the right to rescind the contract. A **Rescission** of a contract returns the parties to thepositions they held before the contract was made. A party can rescind a contract for misrepresentation only if the statement was material, orcritical, to the agreement.

A misrepresentation on the part of the insured in an insurance policy can give the insurer the right to cancel the policy or refuse a claim. Aninsurer may do this only if the misrepresentation was material to the risk insured against and would have influenced the insurer in determiningwhether to issue a policy. For example, if a person seeking auto insurance states that she has no major chronic illnesses, the insurer'ssubsequent discovery that the applicant had an incurable disease at the time she completed the insurance form probably will not give theinsurer the right to cancel the auto policy.

Common Problems in Software Development and Design

Problem #1: Requirements Gathering

Problem #2: Planning & Estimation

Problem #3: Development

Problem #4: Testing

Problem #5: Collaboration

Problem #6: Deployment

Hardware Design Issue

Real time/reactive operation

Real time system operation means that the correctness of a computation depends, in part, on the time at which it is delivered. In many cases the system design must take into account worst case performance. Predicting the worst case may be difficult on complicated architectures, leading to overly pessimistic estimates erring on the side of caution. The Signal Processing and Mission Critical example systems have a significant requirement for real time operation in order to meet external I/O and control stability requirements.

Reactive computation means that the software executes in response to external events. These events may be periodic, in which case scheduling of events to guarantee performance may be possible. On the other hand, many events may be aperiodic, in which case the maximum event arrival rate must be estimated in order to accommodate worst case situations. Most embedded systems have a significant reactive component.

Design challenge:

- Worst case design analyses without undue pessimism in the face of hardware with statistical performance characteristics

Small size, low weight

Many embedded computers are physically located within some larger artifact. Therefore, their form factor may be dictated by aesthetics, form factors existing in pre-electronic versions, or having to fit into interstices among mechanical components. In transportation and portable systems, weight may be critical for fuel economy or human endurance. Among the examples, the Mission Critical system has much more stringent size and weight requirements than the others because of its use in a flight vehicle, although all examples have restrictions of this type.

Design challenges:

- Non-rectangular, non-planar geometries.
- Packaging and integration of digital, analog, and power circuits to reduce size.

Safe and reliable

Some systems have obvious risks associated with failure. In mission-critical applications such as aircraft flight control, severe personal injury or equipment damage could result from a failure of the embedded computer. Traditionally, such systems have employed multiply-redundant computers or distributed consensus protocols in order to ensure continued operation after an equipment failure. However, many embedded systems that could cause personal or property damage cannot tolerate the added cost of redundancy in hardware or processing capacity needed for traditional fault tolerance techniques. This vulnerability is often resolved at the system level as discussed later.

Design challenge:

- Low-cost reliability with minimal redundancy.

Harsh environment

Many embedded systems do not operate in a controlled environment. Excessive heat is often a problem, especially in applications involving combustion (*e.g.*, many transportation applications). Additional problems can be caused for embedded computing by a need for protection from vibration, shock, lightning, power supply fluctuations, water, corrosion, fire, and general physical abuse. For example, in the Mission Critical example application the computer must function for a guaranteed, but brief, period of time even under non-survivable fire conditions.

Design challenges:

- Accurate thermal modelling.
- De-rating components differently for each design, depending on operating environment.

Cost sensitivity

Even though embedded computers have stringent requirements, cost is almost always an issue (even increasingly for military systems). Although designers of systems large and small may talk about the importance of cost with equal urgency, their sensitivity to cost changes can vary dramatically. A reason for this may be that the effect of computer costs on profitability is more a function of the proportion of cost changes compared to the total system cost, rather than compared to the digital electronics cost alone. For example, in the Signal Processing system cost sensitivity can be estimated at approximately $1000 (*i.e.*, a designer can make decisions at the $1000 level without undue management scrutiny). However, with in the Small system decisions increasing costs by even a few cents attract management attention due to the huge multiplier of production quantity combined with the higher percentage of total system cost it represents.

Design challenge:

- Variable "design margin" to permit tradeoff between product robustness and aggressive cost optimization.

End-product utility

The utility of the end product is the goal when designing an embedded system, not the capability of the embedded computer itself. Embedded products are typically sold on the basis of capabilities, features, and system cost rather than which CPU is used in them or cost/performance of that CPU.

One way of looking at an embedded system is that the mechanisms and their associated I/O are largely defined by the application. Then, software is used to coordinate the mechanisms and define their functionality, often at the level of control system equations or finite state machines. Finally, computer hardware is made available as infrastructure to execute the software and interface it to the external world. While this may not be an exciting way for a hardware engineer to look at things, it does emphasize that the total functionality delivered by the system is what is paramount.

Design challenge:

- Software- and I/O-driven hardware synthesis (as opposed to hardware-driven software compilation/ synthesis).

System safety & reliability

An earlier section discussed the safety and reliability of the computing hardware itself. But, it is the safety and reliability of the total embedded system that really matters. The Distributed system example is mission critical, but does not employ computer redundancy. Instead, mechanical safety backups are activated when the computer system loses control in order to safely shut down system operation.

A bigger and more difficult issue at the system level is software safety and reliability. While software doesn't normally "break" in the sense of hardware, it may be so complex that a set of unexpected circumstances can cause software failures leading to unsafe situations. This is a difficult problem that will take many years to address, and may not be properly appreciated by non-computer engineers and managers involved in system design decisions.

Design challenges:

- Reliable software.
- Cheap, available systems using unreliable components.
- Electronic *vs.* non-electronic design tradeoffs.

Controlling physical systems

The usual reason for embedding a computer is to interact with the environment, often by monitoring and controlling external machinery. In order to do this, analog inputs and outputs must be transformed to and from digital signal levels. Additionally, significant current loads may need to be switched in order to operate motors, light fixtures, and other actuators. All these requirements can lead to a large computer circuit board dominated by non-digital components.

In some systems "smart" sensors and actuators (that contain their own analog interfaces, power switches, and small CPUS) may be used to off-load interface hardware from the central embedded computer. This brings the additional advantage of reducing the amount of system wiring and number of connector contacts by employing an embedded network rather than a bundle of analog wires. However, this change brings with it an additional computer design problem of partitioning the computations among distributed computers in the face of an inexpensive network with modest bandwidth capabilities.

Design challenge:

- Distributed system tradeoffs among analog, power, mechanical, network, and digital hardware plus software.

Power management

A less pervasive system-level issue, but one that is still common, is a need for power management to either minimize heat production or conserve battery power. While the push to laptop computing has produced "low-power" variants of popular CPUs, significantly lower power is needed in order to run from inexpensive batteries for 30 days in some applications, and up to 5 years in others.

Design challenge:

- Ultra-low power design for long-term battery operation.

Responsibility of the Computer Professional

Personal and professional responsibility must be the foundation for discussions of all topics in this subject area. Since student response to specific issues will be at least partly determined by the ways they understand their own individual responsibility, it is crucial for each student to understand that the ethical principles of honesty, fairness, autonomy, justice, and beneficence define personal responsibility. Personal responsibilities are those held in common with other people, regardless of technical expertise or position. They should not be thought of as the obligations of socially isolated individuals for they are often the result of group memberships, including family, political entities, cultures, and professional affiliations.

Professional responsibilities are those additional responsibilities that computing professionals should undertake because of their special knowledge and skill, their association with others who share that knowledge and skill, and the trust that society places in them because of that knowledge and skill. The knowledge of these responsibilities, and the practice of them, is fundamental to ethical thought and behavior among computer professionals. The five areas to be covered under the responsibility of the computer professional are:

1) History of the development and impact of computer technology,
2) why be ethical?
3) Major ethical models,
4) definition of computing as a profession, and
5) codes of ethics and professional responsibility for computer professionals.

History of the development and impact of computer technology

To set the stage for an understanding of the professionalism, ethics and social impact of computing, it is necessary for students to see how computing has evolved in the historical and social context. Tracing the history of the mechanization of computation, the development of programmable devices, and the evolution of information representation, transmission and storage will help students to understand how computers are a cultural artifact with profound social impact. When students realize how young the computing profession is relative to other professions and how rapidly it is changing, they have a better appreciation about why there are so many unresolved ethical and social issues with which they will have to deal.

Why be ethical?

Many students come to computer science with a hacker mentality; that is, they view the computer as a personal intellectual challenge, a test of their ability to solve logical problems and to control the computer. Such a narrow approach to computing emphasizes the relation between a solitary programmer and the computer. It implicitly denies any ethical responsibility or social obligation in the practice of computing skills. It is important to help students to become aware of the tremendous responsibility to other people that comes with the practice of their expertise. It is necessary to make a strong case for ethical behavior in the context of professional practice. Analogies with medicine, law, and engineering help students to understand the importance of ethical behavior.

Major ethical models.

In order to understand the basis for personal and professional responsibility, students need to learn about several major ethical models that can be used to evaluate alternatives and aid in decision-making. Ethical models developed by philosophers such as Bentham's Utilitarianism, Kant's Moral Imperative, and Rawles' negotiation of social contracts have been effectively used to provide a formal basis for discussion of ethical dilemmas.

Definition of computing as a profession.

A major criterion for "professional" status is the expectation of some autonomy in the exercise of responsibilities. Some computer professionals have a great deal of autonomy in the decisions they make. Other computer professionals are employees of large firms and software shops where they are quite restricted in their duties and autonomy. They often work on only a small part of a larger system and have little knowledge of or control over decisions made about the larger project. The extent to which computer professionals are 'professional' is more analogous to accountants or engineers who claim special expertise, have professional associations, and adhere to a code of ethics and professional conduct. As they prepare for a computing career, it is very important for computing students to realize early in their education that they will be entering a profession, not just a job market.

Codes of ethics and professional responsibility for computer professionals.

To the extent that computing is a profession, its adherents have a responsibility to shape that profession in ways that are benefit society. An important part of the evolution of computing into a profession has been the development of codes of ethics and professional practice which delineate the responsibilities of the computer professional. The knowledge of these responsibilities, and the practice of them, is fundamental to ethical thought and behavior among computer professionals. For this reason, a careful study and application of professional codes of ethics is crucial to ethical practice in computer science.

Responsibility versus Accountability

The roles taken on by public relations practitioners imply a responsibilityto perform certain functions associated with those roles. Business historianVincent E. Barry has defined the term *responsibility,* when used in businessaffairs, as referring to “a sphere of duty or obligation assigned to a personby the nature of that person’s position, function, or work.”Responsibilitycould thus be viewed as a bundle of obligations associated with a job orfunction. Narrowly defined, *role* refers to a job description, which, in turn,encompasses, but is not limited to, *function.* For instance, a practitioner’srole may be that of media relations. Function would refer to the specificsof the job, including press release writing and dissemination, as well as themaintenance of good media relations. In this sense, responsibility refers tomore than just the primary function of a role; it refers to the multiple facetsof that function—both processes and outcomes (and the consequences ofthe acts performed as part of that bundle of obligations). A responsible actormay be seen as one whose job involves a predetermined set of obligationsthat must be met in order for the job to be accomplished. For example, theprimary functional obligation of someone involved in media relations isthe same as cited in the foregoing sentence: to maintain a good workingrelationship with the media in order to respond to queries and to successfullywork with them to "get out the message." In many cases, simply dischargingthis primary obligation (the function associated with the role) may besufficient unto itself; however, responsibility can also include *moral obligations*that are in addition and usually related to the functional obligations ofthe role. Thus, responsibility assumes that the actor becomes also a moralagent possessed of a certain level of moral maturity and ability to reason.

It is important to note that as early as Aristotle, moral responsibility wasviewed as originating with the moral agent (decision maker), and grew outof an ability to reason (an awareness of action and consequences) and a willingness

to act free from external compulsion. For Aristotle, a decision isa particular kind of desire resulting from deliberation, one that expresses theagent's conception of what is good. As Australian ethicist Will Barretpoints out,

Moral responsibility assumes a capacity for making rational decisions, whichin turn justifies holding moral agents accountable for their actions. Given thatmoral agency entails responsibility, in that autonomous rational agents are inprinciple capable of responding to moral reasons, accountability is a necessaryfeature of morality.

For example, the moral obligations of the role of a media relationsspecialist might include such admonitions as "don't lie to the media" and"use language responsibly, free from intentional obfuscation." These moral obligations are naturally joined to the parallel functional obligations associatedwith the role. Responsibility, then, is composed of a duty to dischargenot only the *functional* obligations of role, but also the *moral* obligations.

In addition, teleological (consequential) considerations tend to demand alevel of accountability commensurate with the level of responsibility. Inother words, if it is the job of a media relations specialist to carry out theprimary functions outlined above, shouldn't that person be held accountablefor mismanaged information, bad publicity, lack of credibility, or other troublesassociated with the functional obligations? If responsibility is defined asa bundle of obligations, functional and moral, associated with a role, thenaccountability might be defined as "blaming or crediting someone for anaction"—normally an action associated with a recognized responsibility. Aproblem arises, however, in that while responsibility and accountability areoften conflated, and admittedly importantly linked, they are not identical bydefinition or moral implication.

According to ethics activist Geoff Hunt, accountabilityis the readiness or preparedness to give an explanation or justification to relevantothers (stakeholders) for one's judgments, intentions, acts and omissionswhen appropriately called upon to do so.

It is [also] a readiness to have one's actions judged by others and, where appropriate,accept responsibility for errors, misjudgments and negligence andrecognition for competence, conscientiousness, excellence and wisdom. It is apreparedness to change in the light of improved understanding gained fromothers.

The simplest formula is that a person can be held accountable if

(1) Theperson is functionally and/or morally responsible for an action,

(2) Someharm occurred due to that action, and

(3) The responsible person had nolegitimate excuse for the action.

6. Privacy

Privacy and its Value

Privacy has been defined in many ways over the last century. Warren and Brandeis called it "the right to be let alone". Pound and Freund have defined privacy in terms of an extension of personality or person hood. Westin and others including myself have cashed out privacy in terms of in for? Still others have insisted that privacy consists of a form of autonomy over personal matters. Parent offers a purely descriptive account of privacy.

"Privacy is the condition of not having undocumented personal knowledge about one possessed by others. Finally, with all of these competing conceptions of privacy some have argued that there is no overarching concept of privacy but rather several distinct core notion that have been lumped together.

Privacy Risks in Using Computers

There are a variety of risks we take, using software programs. These risks are usually classified according to the form of attack employed by the harmful program:

- Integrity attacks damage the information stored in the computer's files.
- Privacy attacks copy information stored on the computer's disk without your permission.
- Denial of service attacks prevents you from using the computer.

Let's examine each of these forms of attack.

Integrity Attacks

A malicious computer program can scramble your disk and remove all your files. This is called an *integrity* attack, because it damages the integrity of your system. You can recover from such an attack if you have backup copies of your files. Some information may be lost forever if there is no back up.

Integrity attacks can also be directed towards the computer's hardware and peripherals, although this is very rare. For example, an integrity attack could exploit a known deficiency in a display driver to burn out a computer's display.

Integrity attacks are usually very damaging, and are detected right away. Finding the culprit is not always easy, because the attacker could erase itself along with all the other files and leave no trace.

Privacy Attacks

Privacy attacks have the effect of making information that should be private available to others who are not allowed by you to have access to it. For example, a privacy attack could watch your keyboard and record the keystrokes you type when you give your password to log on to an online service. Then, after the password is obtained, the attacking software transmits it to the criminal who instigated the attack.

These attacks are, like integrity attacks, very damaging. Additionally they are not recoverable (you can not regain the confidentiality of information once leaked), and they are also not easily detectable. For example, you may only learn that your password for logging on to your online service provider is no longer your private knowledge when you notice that someone has used your account and has racked up huge bills for usage.

The attacker may use her ability to break into your files or observe what you do while using the computer to obtain information about *you*: your habits, tastes, sexual preferences, investment goals, political affiliation or any other information you trust to computers and files. Information transmitted over email is especially vulnerable to being compromised by a privacy attack.

Privacy attacks can appear to be relatively innocuous, but they really are rather insidious sometimes. For example, I heard recently about a privacy attack by an employer on her employees, measuring the speed with which employees typed on their keyboards and their typing habits in general. How would anyone use such information, and why do I consider this a privacy attack? Well, in this case, it is claimed that the information was used to promote fast typing employees. It is also claimed that the information was used to demote employees who were deemed to be at risk of developing RSI (a work related disease that prevents one from effectively using a keyboard to enter information into a computer).

An example of a non-computer related privacy attack: Long distance calling cards are a prime target for such attacks, usually in airports. The thieves position themselves to be able to see when you type in your access code and make a call. Later, they steal the card and use it to run up huge long distance bills. Some especially sophisticated and daring criminals just *borrow* the card and later return it after using it, claiming to do you a favor by returning the card you supposedly dropped.

Denial Of Service Attacks

Denial of service attacks intend to prevent you from fully using your computer's capabilities. They are usually a nuisance, but most of the time they do not do permanent damage. For example, the attacker may display an obnoxious message on the screen of your computer every five seconds, or append a derogatory statement about you to every file on your disk. Or she may consume every free byte on your disk, leaving no space for you to save the files you have just been editing.

Some denial of service attacks is obvious and immediately detectable. Others are much more difficult to detect. For example, the attacker consumes CPU time on your computer when there is a lot of work for it to do, but nearly no CPU time when the computer is idle. This has the effect of slowing down the computer when you most want to use it, but being nearly undetectable when you stop working to go looking for the cause of the slowness.

In some situations, denial of service attacks is very dangerous and damaging. For example, in a combat control station, if the computer displaying the battle-field situation is even temporarily incapacitated, the enemy troops may be able to use this to good advantage.

Relative Importance Of Preventing Each Attack

Most computer users agree that preventing integrity attacks is of the utmost importance. We all want the information we store on the computer's disk to be there when we need it.

However, some situations require the prevention of privacy attacks over protection against integrity attacks. This occurs when the information can be recovered easily, but must be kept private at all cost.

In some cases, users require protection against denial of service attacks but privacy attacks or integrity attacks need not be prevented. This usually occurs when the information can be easily computed but its value declines rapidly over time -- online stock brokers are a prime example of this situation.

So there really is no one way to assign relative importance to the prevention of these attacks. Each situation warrants careful examination, taking into account what risks you are exposed to and what you are trying to do with the computer.

Government Information

The information produced by the government is vast in terms scope (it is hard to find a subject the government does not publish on) and breadth (the government has been publishing research, statistics, reports since its inception). For a random example, the Census Bureau collects annual data on mode and time of transportation to work by age, sex, occupation, annual income range, etc for multiple geographic areas. While this example may not be of direct interest to you, it illustrates the kind of interests and detailed data that governments collect.

Government information is also considered to be a primary source, which are important documents for conducting original research (A primary source is a document, speech, or other sort of evidence written, created or otherwise produced during the time under study. Primary sources offer an inside view of a particular event).

One of the most significant resources for finding government information is the librarians and staff in the Government Documents Library. We are here SPECIFICALLY to help you find the information you are looking for. Reference services (via in-person reference and consultation, email, instant messaging, and phone) are available to affiliates of the university and the general public. You can also browse the many user guides at our Government Information Guides and Course Guides to get a sense of the scope of information. Because of certain idiosyncrasies specific to government publications and their organization even experts in their fields consult the government documents librarians to find print and electronic sources.

Consumer Information

According to FACTA, "consumer information" is considered to be "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report."

This would include "information that results in whole or in part from manipulation of information taken from a consumer report, and information that has been combined with other types of information."

The rule is now limited to "information that identifies particular individuals," and includes "a variety of personal identifiers beyond simply a person’s name, including, but not limited to, a social security number, driver’s license number, phone number, physical address, and e-mail address."

The definition has intentionally been left flexible because "depending on the circumstances, data elements that are not inherently identifying can, in combination, identify particular individuals."

Consumer information also means any employee background reports or similar reports that have been prepared by an outside agency or company. The FACTA disposal rules apply to all of these records.

Note that in addition to the actual reports, FACTA also covers any of your own company's records that are **"derived" from** a consumer credit report or employee background report. This means that if your company copies or uses any information from a consumer credit report or employee background report then that document or data is also subject to FACTA disposal rules.

The FTC acknowledges that businesses may not always know whether the information they receive was derived from a consumer report. There is considerable grey area around this issue of the "information derived from" rule, and it has a strong potential to cause unforeseen problems for businesses that handle a large amount of consumer information received from a number of different sources.

Email Privacy:

This should come as no surprise anymore, but one’s email isn't private. In fact, it's one of the least secure methods of communication one can use. In contrast, phone calls typically aren't recorded and stored. Emails are stored at multiple locations: on the sender's computer, in Internet Service Provider's (ISP) server, and on the receiver's computer. Deleting an email from your inbox doesn't mean there aren't multiple other copies still out there. Emails are also vastly easier for employers and law enforcement to access than phone records. Finally, due to their digital nature, they can be stored for very long periods of time

Email privacy is the broad topic dealing with issues of unauthorized access and inspection of electronic mail. This unauthorized access can happen while an email is in transit, as well as when it is stored on email servers or on a user computer.

How to Keep Your Email Private?

-First, to maintain your expectation to privacy in the first place, always use password-protected computers and email clients. After that, there's really only one way to ensure that your emails are kept confidential -- encrypt them.

-The two most popular forms of email encryption are OpenPGP and S/MIME. Encryption scrambles your email into something unintelligible that only someone who has the correct digital "key" can read. Due to speed and convenience issues, however, few people use encryption and most email remains unencrypted and unsecure.

-The best advice is to treat every email as though it were open to the public to read. Don't say things you don't want others to read, and remember that even after you've deleted your emails, they will be available for years from other sources.

Web Privacy

Web privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences. It involves the right of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Web privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large scale computer sharing.

Our personal privacy on the Web might be less secure than you think. Web browsing habits are tracked via cookies, search engines routinely change their privacy policies, and there are always challenges to Web privacy by both private and public organizations. Here are a few common sense tips that can help you guard your Web privacy and stay safe online.

1. Avoid Unnecessary Forms
2. Clean Search History
3. Log Out Of Search Engines
4. Watch Your Downloads
5. Use Common Sense
6. Guard Your Private Information
7. Use Caution When Using Social Media
8. Watch Out For Scams

9. Protect Computer System
10. Monitor Online Reputation

Protecting Privacy

Privacy is an increasingly rare commodity these days. That’s because your personal information, including your email address, phone number and social security number, is worth a lot of money to legitimate businesses and bad guys alike. The bad guys just want to steal from you. Companies want to know as much about you as possible so they can sell you more products and services or serve you ads that are highly relevant to your demographics and preferences.

So take these simple steps to protect your valuable personal information.

1. Don’t fill out your social media profile.

The more information you share online, the easier it’s going to be for someone to get their hands on it. Don’t cooperate.

Take a look at your social media profiles and keep them barren—the people who need to know your birth date, email address and phone number already have them. And what exactly is the point of sharing everything about yourself in your Facebook profile? If you care about your privacy, you won’t do it.

2. Be choosy about sharing your social security number—even the last 4 digits.

Think twice about sharing your social security number with anyone, unless it’s your bank, a credit bureau, a company that wants to do a background check on you or some other entity that has to report to the IRS. If someone gets their hands on it and has information such your birth date and address they can steal your identity and take out credit cards and pile up other debt in your name.

Even the last four digits of your social security number should only be used when necessary. The last four are often used by banks an other institutions to reset your password for access your account.

Plus, if someone has the last four digits and your birth place, it’s a lot easier to guess the entire number. That’s because the first three are determined by where you, or your parents, applied for your SSN. And the second set of two are the group number, which is assigned to all numbers given out at a certain time in your geographic area. So a determined identity thief with some computing power could hack it given time.

3. Lock down your hardware.

Set up your PC to require a password when it wakes from sleep or boots up. Sure, you may trust the people who live in your house, but what if your laptop is stolen or you lose it?

Same thing with your mobile devices. Not only should you use a passcode to access them every time you use them, install an app that will locate your phone or tablet if it’s lost or stolen, as well as lock it or wipe it clean of any data so a stranger can’t get access to the treasure trove of data saved on it.

4. Turn on private browsing.

If you don’t want anyone with physical access to your computer to see where you’re hanging out online you should enable “private browsing,” a setting available in each major web browser. It deletes cookies, temporary Internet files and browsing history after you close the window.

Every company that advertises online is interested in knowing what sites you visit, what you buy, who you’re friends with on social networks, what you like and more. By gathering information about your online activities they can serve you targeted ads that are more likely to entice you to buy something.

For instance, the Facebook, Twitter, and Google+ buttons you see on just about every site allow those networks to track you even if you don't have an account or are logged into them. Other times information collection companies rely on embedded code in banner ads that track your visits, preferences, and demographic information.

If you truly care about your privacy you'll surf the Internet anonymously by hiding your IP address. You can do this using a web proxy, a Virtual Private Network (VPN) or Tor, a free open network that works by routing your traffic through a series of servers, operated by volunteers around the world, before sending it to your destination.

5. Use a password vault that generates and remembers strong and unique passwords.

Most people know better than to use the same password for more than one website or application. In reality, it can be impossible to remember a different one for the dozens of online services you use. The problem with using the same password in more than one place is if someone gets their hands on your password—say, through a phishing attack—they can access all your accounts and cause all sorts of trouble.

To eliminate this dilemma, use a password manager that will not only remember all your passwords, but will generate super strong and unique ones and automatically fill them into login fields with the click of a button.

6. Use two-factor authentication.

You can lock down your Facebook, Google, Dropbox, Apple ID, Microsoft, Twitter and other accounts with two-factor authentication. That means that when you log in, you'll also need to enter a special code that the site texts to your phone. Some services require it each time you log in, other just when you're using a new device or web browser. The Electronic Frontier Foundation has a great overview of what's available.

Two-factor authentication works beautifully for keeping others from accessing your accounts, although some people feel it's too time consuming. But if you're serious about privacy, you'll put up with the friction.

7. Set up a Google alert for your name.

This is a simple way to keep an eye on anything someone might be saying about you on the web. It's just a matter of telling Google what to look for (in this case, your name), as well as what kinds of web pages to search, how often to search and what email address the search engine giant should use to send you notifications. Set up a Google alert here.

8. Pay for things with cash.

According to Business Insider, credit card companies are selling your purchase data to advertisers. Don't want companies knowing how much booze you're buying or other potentially embarrassing habits? Buy things the old fashioned way—with coins and bills.

9. Keep your social network activity private.

Check your Facebook settings and make sure only friends can see what you're doing. Go to the settings cog in the upper right hand corner of your screen, then click on Privacy Settings >> Who can see my stuff.

On Twitter, click on the settings cog, then Settings. From there you can adjust all sorts of privacy settings, such as a box that gives Twitter permission to add your location to tweets as well as the ability to make your tweets private, meaning only people you approve can see them. You can also stop the microblogging platform from tailoring your Twitter experience based on other sites you visit.

If you use Google+, go to Home >> Settings. There you can adjust things like who can interact with you, comment on your posts or start a conversation with you.

10. Don’t give our your zip code when making credit card purchases.

Often stores will ask for your zip code when you’re checking out with a credit card. Don’t give it to them unless you want to donate your details to their marketing database, warns Forbes. By matching your name, taken from your credit card, with your zip code, companies can more easily mine more information, including your address, phone number and email address.

Offensive speech

Offensive speech, outside the law, is speech that attacks a person or group on the basis of attributes such as gender, ethnic origin, religion, race, disability, or sexual orientation.

In law, hate speech is any speech, gesture or conduct, writing, or display which is forbidden because it may incite violence or prejudicial action against or by a protected individual or group, or because it disparages or intimidates a protected individual or group. The law may identify a protected group by certain characteristics. In some countries, a victim of hate speech may seek redress under civil law, criminal law, or both. A website that uses hate speech is called a *hate site*. Most of these sites containInternet forums and news briefs that emphasize a particular viewpoint. There has been debate over how freedom of speech applies to the Internet as well as hate speech in general.

Critics have argued that the term "hate speech" is a contemporary example of Newspeak, used to silence critics of social policies that have been poorly implemented in a rush to appear politically correct

Censorship

Some countries such as Iran and the People's Republic of China restrict what people in their countries can see on the internet. The BBC is proposing to offer its entire range of terrestrial television broadcasting as free downloads, but only to people within the UK. At the moment most internet content is available regardless of where one is in the world, so long as one has the means of connecting to it.

Censorship of information on the Internet has become a much publicized debate that currently has no resolution in sight. There is a great controversy as to whether or not censorship is a necessity in order to maintain a particular moral standard. In the case that there should be a standard, what information should people have access to? Even if there is no single answer that everyone agrees to, it is an issue that has been confronted and is being dealt with. The amount of material generated by this debate alone is huge, but the addition of the world-wide network known as the Internet only makes it grow. During the past several years the Internet has expanded the abilities of the common person to gain information on a global scale. As the Internet industry grows and expands almost daily, new issues of censorship and freedom of expression are arising. Issues such as the exposure of pornography to children as well as the censoring of material to students have caused enormous amounts of controversy.

Anonymity

Anonymity is derived from the Greek word *anonymia*, meaning "without a name" or "namelessness". In informal use, "anonymous" is used to describe situations where the acting person's name is unknown. It can be said as not using your own name, simply. Some writers have argued that namelessness, though technically correct, does not capture what is more centrally at stake in contexts of anonymity. The important idea here is that a person be non-identifiable, unreachable, or un track able. Anonymity is seen as a technique, or a way of realizing, certain other values, such as privacy, or liberty.

An important example for anonymity being not only protected, but enforced by law is probably the vote in free elections. In many other situations (like conversation between strangers, buying some product or service in a shop), anonymity is traditionally accepted as natural. There are also various situations in which a person might choose to withhold their identity. Acts of charity have been performed anonymously when benefactors do not wish to be acknowledged. A person who feels threatened might attempt to mitigate that threat through anonymity. A witness to a crime might seek to avoid retribution, for example, by anonymously calling a crime tip line. Criminals might proceed anonymously to conceal their participation in a crime. Anonymity may also be created unintentionally, through the loss of identifying information due to the passage of time or a destructive event.

In certain situations, however, it may be illegal to remain anonymous.

7. Computer and Cyber Crimes

Introduction to Computer and Cyber Crime

Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individuals private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.
Examples of computer crimes

Below is a listing of the different types of computer crimes today.

- Child pornography - Making or distributing child pornography.
- Cyber terrorism - Hacking, threats, and blackmailing towards a business or person.
- Cyberbully or Cyberstalking - Harassing others online.
- Creating Malware - Writing, creating, or distributing malware (e.g. viruses andspyware.)
- Denial of Service attack - Overloading a system with so many requests it cannot serve normal requests.
- Espionage - Spying on a person or business.
- Fraud - Manipulating data, e.g. changing banking records to transfer money to an account.
- Harvesting - Collect account or other account related information on other people.
- Identity theft - Pretending to be someone you are not.
- Intellectual property theft - Stealing another persons or companies intellectual property.
- Phishing - Deceiving individuals to gain private or personal information about that person.
- Salami slicing - Stealing tiny amounts of money from each transaction.
- Spamming- Distributed unsolicited e-mail to dozens or hundreds of different addresses.
- Spoofing - Deceiving a system into thinking you are someone you really are not.
- Unauthorized access - Gaining access to systems you have no permission to access.
- Wiretapping - Connecting a device to a phone line to listen to conversations.

Cybercrime is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.
Cybercrimes can be best defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise

Software Piracy

The unauthorized copying of software is called Software Piracy. Most retail programs are licensed for use at just one computer site or for use by only one user at any time. By buying the software, you become a *licensed* *user* rather than an owner. You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues.

Software piracy is all but impossible to stop, although software companies are launching more and more lawsuits. Originally, software companies tried to stop software piracy by copy-protecting their software. This strategy failed, however, because it was inconvenient for users and was not 100 percent foolproof. Most software now requires some sort of registration, which may discourage would-be pirates, but doesn't really stop software piracy.

Some common types of software piracy include counterfeit software, OEM unbundling, softlifting, hard disk loading, corporate software piracy, and Internet software piracy.

Computer fraud

Computer fraud is defined as any act using computers, the Internet, Internet devices, and Internet services to defraud people, companies, or government agencies of money, revenue, or Internet access. There are many methods used to perform these illegal activities. Phishing, social engineering,viruses, and DDoS attacks are fairly well known tactics used to disrupt service or gain access to another's funds, but this list is not inclusive.

The United States government first enacted the Comprehensive Crime Control act on October 12, 1984, which has been amended and updated many times in an attempt to prevent computer fraud. The most recent update was in 2008. This act is meant to penalize violators with stiff penalties however; there are many opponents of this act who feel it is too broad and leaves too much leeway in the law's jurisdiction. This view complains that by not being specific enough, that many people are punished that ordinarily would not be considered violators.

Digital Forgery

Forgery is defined as the crime of falsely and fraudulently making or altering a document. So therefore, digital forgery involves falsely altering digital contents such as pictures and documents. Digital forgery has occurred for many years and still remains a relevant topic today. We see it every day in newspapers, magazines, the television, and even the internet. Whether altering the way someone looks, using digital photography in a courtroom, or even bringing a celebrity back from the dead, digital photography and digital television stimulate countless questions and queries about the ethics and morals of digital forgery, with respect to today's technology, and the involvement of digital forgery in our daily lives.

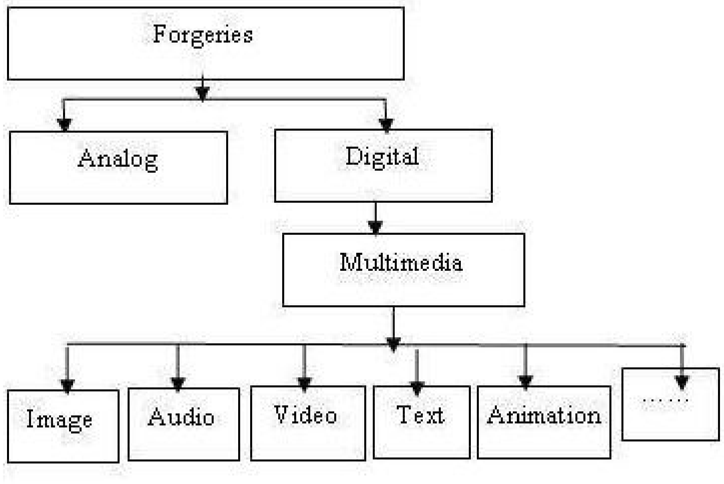

Fig 1: Hierarchical view of forgeries

Phising

Phising is the act of sending an email to a user falsely claiming to be a permissible scheme in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information the user enters on the page.

Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage.

Phishing, also referred to as *brand spoofing* or *carding*, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

Unauthorized access

Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing password or username for an account that was not theirs until they gained access it is considered unauthorized access.

Unauthorized access could also occur if a user attempts to access an area of a system they should not be accessing. When attempting to access that area, they would be denied access and possibly see an unauthorized access message. Some system administrators set up alerts to let them know when there is an unauthorized access attempt, so that they may investigate the reason. These alerts can help stop hackers from gaining access to a secure or confidential system. Many secure systems may also lock an account that has had too many failed login attempts.

Hacking:

In the computer security context, a hacking is process of seeking and exploiting weaknesses in a computer system or computer network. Hacking may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment, or to evaluate those weaknesses to assist in removing them. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community. While other uses of the word *hacker* exist that are related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the longstanding hacker definition controversy about the term's true meaning. In this controversy, the term *hacker* is reclaimed by computer programmers who argue that someone who breaks into computers, whether computer criminal (black hats) or computer security expert (white hats), is more appropriately called a **cracker** instead. Some white hat hackersclaim that they also deserve the title *hacker*, and that only black hats should be called "crackers".

Cracking:

Cracking is the modification of codes to remove or disable features which are considered undesirable by the person cracking the software, especially copy protection features (including protection against the manipulation of software, serial number, hardware key, date checks and disc check) or software annoyances like nag screens and adware.

A **crack** refers to the mean of achieving software cracking, for example a stolen serial number or a tool that performs that act of cracking. Some of these tools are called keygen, patch or loader. A keygen is a handmade product license generator that often offers the ability to generate legitimate licenses in your own name. A patch is a small computer program that modifies the machine code of another program. This has the advantage for a cracker to not include a large executable in a release when only a few bytes are changed.A loader modifies the startup flow of a program and does not remove the protection but circumvents it.

Denial of Service

A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target.

Although a DoS attack does not usually result in the theft of information or other security loss, it can cost the target person or company a great deal of time and money. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial of service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced Web sites accessed by millions of people to temporarily cease operation.

Common forms of denial of service attacks are:

Buffer Overflow Attacks:

The most common kind of DoS attack is simply to send more traffic to a network address than the programmers who planned its data buffers anticipated someone might send. The attacker may be aware that the target system has a weakness that can be exploited or the attacker may simply try the attack in case it might work.

SYN Attack:

When a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up the session. The session-establishing packets include a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply.

Teardrop Attack:

This type of denial of service attack exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system.

Smurf Attack:

In this attack, the perpetrator sends an IP ping (or "echo my message back to me") request to a receiving site The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service.

Computer Invasion of Privacy:

Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy. Invasion of privacy can be a number of things such as spyware, hacking, your ISP interfering with your connection.

Harmful Content Crime:

Harmful content is considered as offensive or disgusting by some people but certainly not criminalized by national laws. So, with in the category of internet content, we are dealing with legal content which may offend some internet users or content that may be thought to harm others. E.g. childaccessing the sexually explicit content. The form of harmful content may include sexually explicit content, political opinions, religious beliefs, views on racial matters and sexuality. The legal definition of harmful content may differ from country to country. For example, even though publishing or distribution of obscene publications may be illegal within the UK under the Obscene Publication Act within the context of internet, browsing or surfing thoroughly sexually explicit and/or obscene content is not an illegal activity for consenting adults. Furthermore, there are no laws making it illegal for a child to view such content in a magazine or on the internet. Therefore, harm remains as a criterion which depends upon cultural differences.

Online pornography

Online pornography or Internet pornography is any pornography that is accessible over the Internet, primarily via websites, peer-to-peer file sharing, or Usenet newsgroups. The availability of widespread public access to the World Wide Web in 1991 led to the growth of Internet pornography. The Internet is an international network and there are currently no international laws regulating pornography; each country deals with Internet pornography differently.

Online Pornography formats

Image files

Pornographic images may be either scanned into the computer from photographs or magazines, produced with a digital camera, or a frame from a video before being uploading onto a pornographic website. The JPEG format is one of the most common format for these images. Another format is GIF which may provide an animated image where the people in the picture move. It often lasts for only a second or two then reruns (repeats) indefinitely. If the position of the objects in the last frame is about the same as the first frame, there is the illusion of continuous action.

Video files and streaming video

Pornographic video clips may be distributed in a number of formats, including MPEG, WMV, and QuickTime. More recently VCD and DVD image files allow distribution of whole VCDs and DVDs. Many commercial porn sites exist that allow one to view pornographic streaming video

Webcams

Another format of adult content that emerged with the advent of the Internet is live webcams. Webcam content can generally be divided into two categories: group shows offered to members of an adult paysite, and 1-on-1 private sessions usually sold on a pay-per-view basis. Currently the most popular video format for streaming live webcams is Flash Video FLV.

Other formats

Other formats include text and audio files. While pornographic and erotic stories, distributed as text files, web pages, and via message boards and newsgroups, have been semi-popular, audio porn, via formats like MP3 and FLV, have seen only very limited distribution. Audio porn can include recordings of people having sex or reading erotic stories.

Online Harrasment

Online Harassment covers a wide range of behaviours of an offensive nature done with the help of computer and internet. It is commonly understood as behaviour which disturbs or upsets, and it is characteristically repetitive. In the legal sense, it is behaviour which appears to be threatening or disturbing. Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. Harassment targeting women and children in the internet also includes revenge pornography.

Harassment as defined in the U.S. computer statutes is typically distinct from cyberbullying, in that the former usually relates to a person's "use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act," while the latter need not involve anything of a sexual nature.

Different types of online harassment:

- **Hate Speech**: Any person using his online persona to promote hate speech against a certain race, sex, religion or political through is considered a cyber-bully. There is a thin line between expressing how you feel or think about an idea and promoting hate speech towards a certain group of people. Any speech that promotes hate culture should be reported to the website immediately.
- **Sexual or Pornographic Content:** Websites who are not supposed to be carrying sexual content but are doing so should also be flagged. Facebook for instance does not allow pornographic content on its pages. So do most of the social media websites.
- **Self Harm:** Promotion of hard drug abuse, cutting or eating disorders should not be dealt with lightly. Most websites where people can share this sort of things work with suicide prevention agencies to help people in distress.
- **Intellectual Property Protection:** If you happen to be someone who shares their work online, you should be well equipped with a license that protects your work from being stolen and linked to another person. This could happen directly with a person stealing you work or indirectly through a person posing as yourself in order to take credit for your work. Intellectual property licenses are everywhere online. Make sure you buy yours.
- **Identity Theft:** Someone stealing your online persona is someone who wants more than just that. Putting your personal life at stake as they might gain access to your bank accounts and credit cards through posing as you. This makes them extremely close to your social circle as well.
- **Cyber-bullying**: Ganging up on a victim and constantly harassing them through the internet or through their mobile phone is an action of cyber-harassment. Being mean in a constant manner to a person online is unacceptable to most social media websites. Sometimes, the victim cannot handle the stress and may resort to suicide. At which point, your bullying will go to court.

Cyber stalking

Cyber stalking, simply put, is online stalking. It has been defined as the use of technology, particularly the Internet, to harass someone. Common characteristics include false accusations, monitoring, threats, identity theft, and data destruction or manipulation. Cyber stalking also includes exploitation of minors, be it sexual or otherwise.

The harassment can take on many forms, but the common denominator is that it's unwanted, often obsessive, and usually illegal. Cyber stalkers use email, instant messages, phone calls, and other communication devices to stalk, whether it takes the form of sexual harassment, inappropriate contact, or just plain annoying attention to your life and your family's activities.

Kids use the term "stalking" to describe following someone's activities via their social network. My own children accuse me of being their "stalker" for keeping tabs on their digital lives. It's important that we not devalue the serious nature of the crime of cyber stalking by using the term incorrectly. A recent television commercial for a major cellular provider depicts a young woman spying on her crush through his bedroom window while she monitors his online activities on her cell phone. While it's meant to be a humorous ad, it's extremely unsettling when stalking occurs in the real world.

Interestingly, this same ad points to an important fact about cyber stalking; it is often perpetrated not by strangers, but by someone you know. It could be an ex, a former friend, or just someone who wants to bother you and your family in an inappropriate way.

How Cyber stalking Harms

Cyber stalking can be terribly frightening. It can destroy friendships, credit, careers, self-image, and confidence. Ultimately it can lead the victim into far greater physical danger when combined with real-world stalking. Yes, we're talking serious stuff here. Victims of domestic violence are often cyber stalking victims. They, like everybody else, need to be aware that technology can make cyber stalking easy. Spyware software can be used to monitor everything happening on your computer or cell phone, giving tremendous power and information to cyber stalkers.

Anti-Stalking Tips

Here are a few important pointers to help you thwart cyber stalking, whether it's directed at you, your PC, or your family:

- Maintain vigilance over physical access to your computer and other Web-enabled devices like cell phones. Cyber stalkers use software and hardware devices (sometimes attached to the back of your PC without you even knowing) to monitor their victims.
- Be sure you always log out of your computer programs when you step away from the computer and use a screensaver with a password. The same goes for passwords on cell phones. Your kids and your spouse should develop the same good habits.
- Make sure to practice good password management and security. Never share your passwords with others. And be sure to change your passwords frequently! This is very important.
- Do an online search for your name or your family members' now and then to see what's available about you and your kids online. Don't be shy about searching social networks (including your friends' and colleagues'), and be sure to remove anything private or inappropriate.
- Delete or make private any online calendars or itineraries--even on your social network--where you list events you plan to attend. They could let a stalker know where you're planning to be and when.
- Use the privacy settings in all your online accounts to limit your online sharing with those outside your trusted circle. You can use these settings to opt out of having your profile appear when someone searches for your name. You can block people from seeing your posts and photos, too.
- If you suspect that someone is using spyware software to track your everyday activities, and you feel as if you're in danger, only use public computers or telephones to seek help. Otherwise, your efforts to get help will be known to your cyber stalker and this may leave you in even greater danger.

- As always, use good, updated security software to prevent someone from getting spyware onto your computer via a phishing attack or an infected Web page. Check the app store for your mobile devices to see what security software is available. Or visit the Norton Mobile page to see what programs are available for your device's platform. Security software could allow you to detect spyware on your device and decrease your chances of being stalked.

Online scam

Online scam or Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them; for example, by stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Internet fraud can occur in chat rooms, email, message boards, or on websites.

Spam

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.

There are two main types of spam, and they have different effects on Internet users. Cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups. (Through long experience, Usenet users have found that any message posted to so many newsgroups is often not relevant to most or all of them.) Usenet spam is aimed at "lurkers", people who read newsgroups but rarely or never post and give their address away. Usenet spam robs users of the utility of the newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts. Furthermore, Usenet spam subverts the ability of system administrators and owners to manage the topics they accept on their systems.

Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spams typically cost users money out-of-pocket to receive. Many people - anyone with measured phone service - read or receive their mail while the meter is running, so to speak. Spam costs them additional money. On top of that, it costs money for ISPs and online services to transmit spam, and these costs are transmitted directly to subscribers.

One particularly nasty variant of email spam is sending spam to mailing lists (public or private email discussion forums.) Because many mailing lists limit activity to their subscribers, spammers will use automated tools to subscribe to as many mailing lists as possible, so that they can grab the lists of addresses, or use the mailing list as a direct target for their attacks.

Malicious Programs:

Malicious Programs or Malicious software (malware) is any software that gives partial to full control of your computer to do whatever the malware creator wants. Malware can be a virus, worm, trojan, adware, spyware, root kit, etc. The damage done can vary from something slight as changing the author's name on a document to full control of your machine without your ability to easily find out. Most malware requires the user to initiate it's operation. Some vectors of attack include attachments in e-mails, browsing a malicious website that installs software after the user clicks ok on a pop-up, and from vulnerabilities in the operating system or programs. *Malware is not limited to one operating system.*

Malware types can be categorized as follows: viruses, worms, Trojans, and backdoors seek to infect and spread themselves to create more havoc. Adware and spyware seek to embed themselves to watch what the user does and act upon that data. Root kits seek to give full access of your machine to the attacker to do what they want.

Network Worms

This category includes programs that propagate via LANs or the Internet with the following objectives:

- Penetrating remote machines.
- Launching copies on victim machines.
- Spreading further to new machines.

Worms use different networking systems to propagate: email, instant messaging, file-sharing (P2P), IRC channels, LANs, WANs and so forth.

Most existing worms spread as files in one form or another: e-mail attachments, in ICQ or IRC messages, links to files stored on infected websites or FTP servers, files accessible via P2P networks and so on.

There are a small number of so-called fileless or packet worms; these spread as network packets and directly penetrate the RAM of the victim machine, where the code is then executed.

Worms use a variety of methods for penetrating victim machines and subsequently executing code, including:

- Social engineering; emails that encourage recipients to open the attachment.
- Poorly configured networks; networks that leave local machines open to access from outside the network.
- Vulnerabilities in operating systems and applications.

Today's malware is often a composite creation: worms now often include Trojan functions or are able to infect exe files on the victim machine. They are no longer pure worms, but blended threats.

Viruses

A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner. A virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

Viruses spread copies of themselves in order to:

- Launch and/or execute code once a user fulfills a designated action.
- Penetrate other resources within the victim's machine.

Unlike worms, viruses do not use network resources to penetrate other machines. Copies of viruses can penetrate other machines only if an infected object is accessed and the code is launched by a user on an uninfected machine. This can happen in the following ways:

- The virus infects files on a network resource that other users can access.
- The virus infects removable storage media which are then attached to a clean machine.
- The user attaches an infected file to an email and sends it to a 'healthy' recipient.

Viruses are sometimes carried by worms as additional payloads or they can themselves include backdoor or Trojan functionality which destroy data on an infected machine.

Trojan Programs

This class of malware includes a wide variety of programs that perform actions without the user's knowledge or consent: collecting data and sending it to a cyber criminal, destroying or altering data with malicious intent, causing the computer to malfunction, or using a machine's capabilities for malicious or criminal purposes, such as sending spam.

A subset of Trojans damage remote machines or networks without compromising infected machines; these are Trojans that utilize victim machines to participate in a Denial of Service "DoS" attack on a designated web site.

Cyber Terrorism

According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."

Unlike a nuisance virus or computer attack that result in a denial of service, a cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.

Cyber terrorism can be also defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives.[1] Objectives may be political or ideological since this can be seen as a form of terrorism.

There is much concern from government and media sources about potential damages that could be caused by cyber terrorism, and this has prompted official responses from government agencies.

Cyber terrorism is sometimes referred to as electronic terrorism or information war.

The following three levels of cyber terror capability is defined by **Monterey group**

- **Simple-Unstructured**: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.
- **Advanced-Structured**: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
- **Complex-Coordinated**: The capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability

Digital forensics

Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events often in relation to computer crime.

The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.

Digital forensics is commonly used in both criminal law and private investigation. Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts. As with other areas of forensics this is often as part of a wider investigation spanning a number of disciplines. In some cases the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings (for example to locate, identify or halt other crimes). As a result, intelligence gathering is sometimes held to a less strict forensic standard.

In civil litigation or corporate matters digital forensics forms part of the electronic discovery (or eDiscovery) process. Forensic procedures are similar to those used in criminal investigations, often with different legal requirements and limitations. Outside of the courts digital forensics can form a part of internal corporate investigations.

A common example might be following unauthorized network intrusion. A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise, both to establish the extent of any intrusion and in an attempt to identify the attacker

The main focus of digital forensics investigations is to recover objective evidence of a criminal activity. However, the diverse range of data held in digital devices can help with other areas of inquiry.

There are four stages of forensics Process:-

1. Identification of Digital Evidence
2. Preservation of Digital Evidence
3. Analysis of Digital Evidence
4. Presentation of Digital Evidence

8. Intellectual Property and Legal Issue

Intellectual Properties

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

Copyright

Copyright is a legal right created by the law of a country that grants the creator of original work exclusive rights for its use and distribution. This is usually only for a limited time. The exclusive rights are not absolute but limited by limitation and exceptions to copyright law, including fair use.

Copyright is a form of intellectual property, applicable to certain forms of creative work. Under US copyright law, legal protection attaches only to *fixed* representations in a tangible medium. It is often shared among multiple authors, each of whom holds a set of rights to use or license the work, and who are commonly referred to as rights holders. These rights frequently include reproduction, control over derivative works, distribution, public performance, and "moral rights" such as attribution.

Copyrights are considered *territorial* rights, which mean that they do not extend beyond the territory of a specific jurisdiction. While many aspects of national copyright laws have been standardized through international copyright agreements, copyright laws vary by country.

Typically, the *duration* of a copyright spans the author's life plus 50 to 100 years (that is, copyright typically expires 50 to 100 years after the author dies, depending on the jurisdiction). Some countries require certain copyright formalities to establishing copyright, but most recognize copyright in any completed work, without formal registration. Generally, copyright is enforced as a civil matter, though some jurisdictions do apply criminal sanctions.

When did Copyright Protection begin, and what is required?

Copyright protection begins when any of the above -described work is actually created and fixed in atangible form.

For example, my brother is a musician and he lives in the United States. When he writes new lyrics,he prints them out on paper, signs his name at the bottom with the Copyright © symbol to show thathe is the author, places it in an envelope and mails it to himself without opening it. His copyrightbegins at the moment he puts his idea in a tangible form by printing the lyrics out on paper. Hecreates proof when he mails it to himself - the postmark establishes the date of creation. He thenregisters his copyright with the U.S. Copyright Office, which is a requirement in order to sue formonetary damages should a violation of his copyright, arise. However, if somebody copies andredistributes his lyrics without permission before his copyright is registered, he still has the right toassert a copyright claim as the true author. The above applies to digital art and graphics. Open a gif, jpg or png file that you created and look atthe properties. It states the date that you saved it to your hard drive as the date of creation. Ifsomebody copies a graphic from your web site, I assure you that the date of creation on your copy ofthe file is earlier than the copy taken off your web site. If that still doesn't feel like enough proof foryou, save everything to a floppy disk and mail it to yourself via certified mail. Keep the envelopesealed, wrap it in protective plastic and put it in a safe place.

Somebody once asked if it was "illegal" to place the copyright © symbol next to your name if youhave not registered your copyright. Unless you have stolen the work from somebody else and you arenot the true author of the work, it is not illegal to place the copyright © symbol next to your name – itis your right to do so.

The proper way to place a copyright notice is as follows: Copyright © (first date of creation) (nameof owner). Like this: Copyright © 2003 John Smith.

When does Copyright Protection end, or expire?

If a copyright statement reads, "© Copyright 1998, 1999 John Smith." does that mean that JohnSmith's copyright expired in 1999. The dates that you see in a copyright statement do not refer to thedates that the owner's material will expire and become public domain - they actually refer to thedates that the material was created.

When you see several dates in a copyright statement, it simply means that certain things were createdin one year and modified later. It could also mean that new things were created and added in a lateryear. It most definitely does not refer to the date that a copyright will expire. Expiration of acopyright actually takes place much later, and this period of validity begins from the date that yousee in the copyright statement. The Berne Convention establishes a general and minimum period thatlasts the life of the author and fifty years after his (or her) death. Cinematographic works andphotographic works have a minimum period of protection of 50 and 25 years upon the date ofcreation, respectively. This applies to any country that has signed the Berne Convention, and theseare just the minimum periods of protection. A member country is entitled to establish greater periodsof protection, but never less than what has been established by the Berne Convention.

So, what does all this mean? This means that if a copyright statement reads, "© Copyright 1998,1999 John Smith" and John Smith is from a country that has signed the Berne Convention, he createdhis works in 1998 and 1999, and his copyright is not going to expire until at least fifty years after hedies (this period may be greater - remember that member countries may establish longer periods ofprotection). Until that time, his works are not in public domain.

Patent

A **patent** is a set of exclusive rights granted by a sovereign state to an inventor or assignee for a limited period of time in exchange for detailed public disclosure of an invention. An invention is a solution to a specific technological problem and is a product or a process. Patents are a form of intellectual property.

In modern usage, the term *patent* usually refers to the right granted to anyone who invents any new, useful, and non-obvious process, machine, article of manufacture, or composition of matter

The procedure for granting patents, requirements placed on the patentee, and the extent of the exclusive rights vary widely between countries according to national laws and international agreements. Typically, however, a granted patent application must include one or more claims that define the invention. A patent may include many claims, each of which defines a specific property right. These claims must meet relevant patentability requirements, such as novelty, usefulness, and non-obviousness. The exclusive right granted to a patentee in most countries is the right to prevent others, or at least to try to prevent others, from commercially making, using, selling, importing, or distributing a patented invention without permission.

Design

Design is the creation of a plan or convention for the construction of an object or a system (as in architectural blueprints, engineering drawings, business processes, circuit diagrams and sewing patterns). Design has different connotations in different fields In some cases the direct construction of an object (as in pottery, engineering, management, cowboy coding and graphic design) is also considered to be design.

There are countless philosophies for guiding design as the design values and its accompanying aspects within modern design vary, both between different schools of thought and among practicing designers. Design philosophies are usually for determining design goals. A design goal may range from solving the least significant individual problem of the smallest element, to the most holistic influential utopian goals. Design goals are usually for guiding design. However, conflicts over immediate and minor goals may lead to questioning the purpose of design, perhaps to set better long term or ultimate goals.

Design Methods is a broad area that focuses on:

- Exploring possibilities and constraints by focusing critical thinking skills to research and define problem spaces for existing products or services—or the creation of new categories;
- Redefining the specifications of design solutions which can lead to better guidelines for traditional design activities (graphic, industrial, architectural, etc.);
- Managing the process of exploring, defining, creating artifacts continually over time
- Prototyping possible scenarios, or solutions that incrementally or significantly improve the inherited situation

Trademark

A **trademark**, **trade mark**, or **trade-mark** is a recognizable sign, design, or expression which identifies products or services of a particular source from those of others, although trademarks used to identify services are usually called service marks.

A trademark is typically a name, word, phrase, logo, symbol, design, image, or a combination of these elements. There is also a range of non-conventional trademarks comprising marks which do not fall into these standard categories, such as those based on color, smell, or sound (like jingles).

The trademark owner can be an individual, business organization, or any legal entity. A trademark may be located on a package, a label, a voucher, or on the product itself. For the sake of corporate identity trademarks are also being displayed on company buildings.

The owner of a trademark may pursue legal action against trademark infringement. Most countries require formal registration of a trademark as a precondition for pursuing this type of action. The United States, Canada and other countries also recognize common law trademark rights, which means action can be taken to protect an unregistered trademark if it is in use. Still common law trademarks offer the holder in general less legal protection than registered trademarks.

A trademark may be designated by the following symbols:

- **™** (the "trademark symbol", which is the letters "TM", for an unregistered trademark, a mark used to promote or brand goods)

- ℠ (which is the letters "SM" in superscript, for an unregistered service mark, a mark used to promote or brand services)
- ® (the letter "R" surrounded by a circle, for a registered trademark)

Trade Secret

A **trade secret** is a formula, practice, process, design, instrument, pattern, commercial method, or compilation of informationwhich is not generally known or reasonably ascertainable by others, and by which a business can obtain an economic advantage over competitors or customers. In some jurisdictions, such secrets are referred to as "confidential information", but are generally not referred to as "classified information" in the United States, since that refers to government secrets protected by a different set of laws and practices.

The precise language by which a trade secret is defined varies by jurisdiction (as do the particular types of information that are subject to trade secret protection). However, there are three factors that, although subject to differing interpretations, are common to all such definitions: a trade secret is information that:

- Is not generally known to the public;
- Confers some sort of economic benefit on its holder (where this benefit must derive *specifically* from its not being publicly known, not just from the value of the information itself);
- Is the subject of reasonable efforts to maintain its secrecy.

Trade secrets are an important, but an invisible component of a company's intellectual property (IP). Their contribution to a company's value, as seen as its market capitalization, can be major.[4] Being invisible, that contribution is hard to measure. Patents are a visible contribution, but delayed, and unsuitable for internal innovations. Having an internal scoreboard provides insight into the cost of risks of employees leaving to serve or start competitors.

Copyright law of Nepal

Copyright is an intellectual property. It is related to literary, artistic, and scientific and research works. Itprotects the authors from unauthorized copying of their works. It extends protection to form ormanner of expressing ideas. But the idea itself cannot be copyrighted. The authors are the primebeneficiaries of copyright protection. Technology has greatly broadened the scope of copyright inmodem times.

Copyright Act, 2002

The legal provisions about copyright in Nepal are contained in the copyright Act 2002, which has 43sections. The Copyright Rules guide its implementation. The salient features of the copyright Act are

1. Copyright Protection (Sec 3)

The Act extends copyright protection to any work, including literary, artistic, scientific and otherworks, which are original and intellectually presented.

Work has been defined as follows

a) Book, pamphlet, article, research paper

b) Drama, lyrical drama, silent acting

c) Musical works with or without words

d) Audio-visual works, including movies

e) Architectural design

f) Paintings, sculpture, wooden arts, lithography

g) Photographic works

h) Photographic works

i) Drawings, maps, plans, three-dimensional geographical works, topographical andscientific articles and works

j) Computer programs

2. Non-protection of Copyright (Sec 4)

Copyright cannot be protected for

a) Ideas, religion, news, concept, principle

b) Rulings of the courts, administrative decisions

c) Folklores, folk stories, old sayings

d) General statistics

a) Coauthor for joint works

b) Persons or institutions commissioning joint works

c) Persons or institutions paying remuneration for producing the work

d) Publisher for anonymous work until the author is identified.

· Registration of work is not essential to enjoy copyright. The copyright author also has ethical rights.

4. Economic Benefits (Sec. 7-13)

The copyright owner has the following economic benefits

a) Reproduction of works

b) Translation of works

c) Revision of-works

d) Changes in the form of works

e) Sale and renting of works

f) Transfer of copyright

g) Public shows and broadcasting, etc.

5. Term of copyright (Sec. 14-15)

The term of copyright granted is the life of the author plus fifty years after death.

· For joint authorship, the term of copyright is fifty years from the death of author who dieslast.

· For anonymous work, the term is fifty years from the date of publication.

6. Transfer of Copyright (Sec. 24)

Copyright is transferable in whole or in part.

7. Use of Copyright without Permission (Sec. 16-23)

Copyright materials can be reproduced without permission for:

a) Personal use

b) Reference purposes

c) Teaching purposes

d) Library and archives purposes

e) Public knowledge

8. Unauthorized Publication (Sec. 25-26)

The law prohibits unauthorized publication of work. The following acts are regarded unauthorized Publication

a) Sale of copies of other’s work for business purpose to make economic gain without permission.

b) Gain advantage from the prestige of other’s work through advertisement or publicity.

c) Create work by changing the structure or language of other’s work for economic gain.

d) Gain advantage from imitation or advertisements. Import of unauthorized publication is banned.

9. Penalty

- Fine ranging from Rs. 10,000 to Rs. 100,000 or six months imprisonment, or both have beenprescribed for unauthorized publication.
- The penalty is double for second and subsequent offences.The unauthorized copies are also confiscated. Compensation can also be claimed by the owner ofcopyright.
- Unauthorized imports are subject to a fine of Rs. 5000 to Rs. 100,000 plus confiscation ofcopiesimported.

10. Registration

The Registrar of Copyright has been provided to deal with copyright matters.

Conclusions

The copyright Act in Nepal lacks effective implementation.

• The consciousness is lacking about copyright in Nepal. Till 1998, a total of 189 books, 204 audio cassettes, 5 films and 9 paintings were registered for copyright.

4.2 Copyright Rules 1989

Rules are needed to implement the law. The copyright rules in Nepal were formulated for copyrightAct of 1965.

Now rules have not been passed as yet

The copyright rules deal with the following aspects :

1. Registration and Certificate of Copyright

The format of application and fee has been prescribed for registration of copyright. Copies of thework are also required. The format and fee for certificate are also prescribed.

2. Inspection and Copying

Procedures have been laid down for inspection and copy of copyright register.

3. Corrections in copyright Register

The Salient provisions in the law about patent are

Corrections in copyright register can be made in respect of Name and address of the author

• Name of publisher of the work

• Name of printer

3. Economic Beneficiary of copyright (Sec. 6)

The Act vests the ownership of copyright in the author of the work. Exceptions are

• Transfer of copyright

4. Nepali Translation

Procedures have been laid down tor granting permission for Nepali translation. Format has also beenprescribed.

5. Duties, Responsibilities and Powers of the Copyright Advisory

Committee

They are as follows

• Give decisions on problems related to any work

- Solve questions related to copyright
- Give decisions on “Yours and mine” type disputes
- Give decisions on plagiarism of work
- Fix number of copies needed for registration of copyright.
- Solve problems related to implementation of Act and rules.

Provisions relate d to committee meetings have been prescribed.

Patent, Design and Trademark

Patent, design and trademark are intellectual property. They are the creation of human mind.

The Patent, Design and Trademark Act 1965 (amended in 1987), together with Rules, regulatepatent, design and trademark in Nepal.

Patent

Patent has been defined as follows

Patent is any new method or way of constructing, conducting or processing any matter or body ofmatters or any useful invention based on a new principle or formula.

1. Registration

a) A person should register the right of patent in his name. The term of registration is sevenyears. It can be renewed for two terms of seven years each (total life of patent cannot exceed21 years)

b) Copying of patent is not allowed without the permission of the patentee.

c) Patent right can be transferred like a movable property. The transfer should be registered.

d) The application for registration of patent should contain

I. Name, address and occupation of inventor

II. Manner and nature of right acquired, if applicant is not the inventor

III. Manner of producing, using or conducting the patent

IV. Principle or formula on which the patent is based.

V. Map or drawing of the patent with description

e) The registered patents should be published, except those needing confidentiality in thenational interests.

2. Non Registration of Patent

The patent cannot be registered in the following conditions

a) Already registered in another person’s name

b) Not invented by the applicant or the right to patent not received

c) Causes adverse effects on health, good conduct or morality or is prejudicial to national interests

d) Contravenes existing laws of Nepal

3. Archives

The drawing or sample of patent should be provided to National Archives.

4. Punishment

Infringement of patent laws is subject to fine of upto l(s. 2,000 and confiscation of articles connectedwith the offence. Compen sation can also be awarded to the aggrieved party.

5. Foreign Patents

Patents registered in foreign countries must be registered in Nepal to claim right of ownership.

Patents for Nepalese products must first be registered in Nepal to get foreign registration.

Design

Design has been defined as follows:

Design means any feature, pattern or shape of a matter prepared and produced in any manner.

The salient legal provisions about de sign are

a) Registration

Registration is needed to obtain right to design. A person can prepare the design himself or throughothers. The term of design registration is five years. It can be renewed for two terms of five years each (totallife of design cannot exceed 15 years)

• Use or copying of design is not allowed without the permission of the owner. Permissioncan be given by agreement of both parties—owner and the person desiring to use.

• Map or thawing of design with description plus four copies should be submitted forregistration purposes.

• The registered designs can be published for public knowledge. Complaints should be lodgedwithin 35 days of such publication.

b) Non Registration of Design

The design cannot be registered in the following conditions

Already registered in another person's name

• Likely to cause damage to the reputation of an individual or an institution

• Causes adverse effects on good conduct or morality of general public.

c) **Infringement** of design law is subject to fine upto Rs. 800 andconfiscation of articles connected with the offence. Compensation canalso be awarded to the aggrieved party.

d) Foreign Design

• Foreign design must be registered in Nepal to claim right to ownership.

• Nepalese designs must first be registered in Nepal to get foreign registration.

Trademark

Trademark has been defined as follows:

Trademark is any sign, picture or word or their combination used by a person, firm or company todistinguish its goods and services from those of others.

A registered brand is a trademark.

The salient legal provisions about trademark are

a) Registration:

Registration is needed to obtain right of trademark. The term of registration is seven years. It can berenewed for unlimited terms of seven years each. It can be cancelled if not used within one year ofregistration.

• Use or copying of trademark is not allowed without the permission of the owner.

Permission can be given by agreement between the owner and the person desiring to use.

• Publication of trademark can be done for public knowledge.

b) Non Registration of Trademark

The trademark cannot be registered in the following conditions

• Already registered in the another's name; or

• Likely to cause damage to the reputation of an individual or an institution; or

- Likely to harm goodwill of trademark of others; or
- Adversely affects the good conduct or morality of general public; or
- Is prejudicial to national interest.

c) Classification of Goods and Services for Trademark

- The government can classify goods and services for the purposes of trademark registration.
- Separate applications are needed for trademark registration in each category of goods andservices.
- Same trademark can be registered for various classes of goods and services.

d) Infringement of trademark law is subject to fine of up to Rs. 1000 andconfiscation of articles connected with the offence. Compensation canalso be awarded to the aggrieved party.

e) Foreign Trademarks

Foreign trademarks must be registered in Nepal to claim right of ownership

- Trademarks for Nepalese products must first be registered in Nepal to get foreignregistration.
- The government has not yet laid down rules to facilitate implementation of the design andtrademark act.

IT Policy of Nepal

Technology Policy of Nepal

Policies are guidelines for decision making to achieve goals. Technology is a critical factor fordevelopment.

Technology policy of the government greatly affects the technological development ofthe country.

Nepal's science and technology policy was included in the Ninth Plan (1997-2002). The salientfeatures of this policy are :

1. A conducive environment will be created for imparting standard science and technologyeducation at school and higher education levels. The promotion of technical education will begradually increased.
2. Improvements in endogenous and traditional technology will be made and specialconsideration will be given to commercialize it.
3. Advanced technologies will be imported. The selection process for imports will give priorityto export promoting and under employment reducing technologies.
4. Production and productivity will be increased by the compulsory adoption of advancedtechnology in economic and social sectors.
5. Science and Technology Committee and Research and Development (R & D) unit will beformed in all government and semi-government agencies.
6. Private sector will be encouraged to invest a certain percentage of their profits to research.Science and technology sectors will be initiated in districts, municipalities and villagedevelopment Committees.
7. A national science and technology management system will be developed to ensureefficiency and effectiveness of investment.
8. A separate science and technology service will be developed within the civil service.

Incentives will he provided to scientists and technologists involved in R & D. Lateral entrywill be allowed.

9. Research findings of science and technology will be disseminated.
10. A twenty year science and technology perspective plan will be prepared.
11. Necessary institutional framework and system will be developed for science and technology.
12. Brain drain of science and technology personnel will be controlled.

13. Technology parks will be established.

Information Technology (IT) Policy of Nepal

Nepal has formulated Information Technology Policy 2000.

Its salient features are

1. Declare information technology as a priority sector.
2. Follow a single door system for the development of iT.
3. Prioritize research in IT.
4. Create conducive environment to attract private sector investment in IT,
5. Provide internet facilities to all village development commit tees.
6. Render assistance to educational institutions and encourage training to develop qualifiedmanpower in IT.
7. Computerize government records and build websites for flow of information.
8. Increase the use of computer in private sector.
9. Develop physical and virtual information technology park for development of TT.
10. Use IT to promote e-commerce, e-education, e-health and transfer of technology to ruralareas.
11. Establish National Information Technology Center.
12. Establish a national level fund to contribute to R & D in IT.
13. Establish venture capital fund for 1T.
14. Include computer education from the school level.
15. Establish Nepal in global market through the use of IT.
16. Provide legal sanctions to the use of IT.
17. Gradually use IT in all types of government activities.

The vision of Nepal’s Information Technology Policy is to place Nepal on the global map ofinformation technology by 2005.

The objectives of IT policy are

a) Make IT accessible to general public; increase employment through IT.

b) Build knowledge -based society

c) Establish knowledge-based industries.

Right to Information in Nepal

Historical Development

Right to Information is one of the lately recognized rights in Nepal. It has been only two decades of its recognition as fundamental right of Nepalese citizens. For the first time, 1990 Constitution guaranteed right to information as a fundamental right to its citizen. It recognized right of citizens to demand and obtain information held by public agencies on any matter of public importance. Despite the constitutional guarantee, it took a long time to persuade the government to enact law on right to information.

In 1993, then government tabled first draft of Right to Information Act in the parliament. However, the draft was rejected by the parliamentary committee following the opposition of the stakeholders including media. Civil society argued that the draft was aiming to create a formal secrecy regime instead of giving effect to the constitutional guarantee.

In this environment, media organizations and journalist took initiative in 1997 and formed a ten-member independent drafting team on freedom of information. The Bill was tabled in the parliament in 2001. Due to the political upheavals, the bill could not get priority and was never discussed. Frequent political changes stood as a major hindrance for the enactment of freedom of information law in Nepal.

Interim Constitution 2007 was second consecutive constitution which guaranteed right to information as a fundamental right of the citizen. It extended the right by providing access not only to information of public importance but also to individual information. Now every citizen is empowered to seek information of his/her individual interest as well as information of public interest.

Nepal government formed a taskforce on September, 2007 to draft a bill on right to information. Based on that draft, the government enacted a specific law to regulate right to information on July 18, 2007. This law is an outcome of enormous effort by the stakeholders and civil society.

Right to Information Act, 2007 has provided for an independent National Information Commission for the protection, promotion and execution of Right to Information in Nepal. It was established on June 14, 2008. Further, Regulation on Right to Information was ratified and came to effect on Feb 9, 2009.

Existing Legal Framework

Right to information is primarily governed by the Interim Constitution 2007, Right to Information Act 2007, Right to Information Regulation 2009, Classification Guideline issued by the Classification Committee formed pursuant to Article 27 of the Right to Information Act. Apart from these instruments, a number of other statutes regulate right to information.

Interim Constitution, 2007 in its article 27 has ensured Right to Information as the fundamental rights. It provides citizen the right to demand or obtain information on any matters of concern to him / her or to the public. However, it does not compel to provide information which is to be protected by the law.

Section 3 and 30 of Right to Information, 2007 has empowered Nepalese citizens to exercise this right to obtain of information of public importance and individual concern, respectively. This Act has also made a separate provision for the classification and protection of the information in its section 27 and 28. Protection of the whistleblower and the requirement of proactive disclosure by the public agencies are considered as the remarkable provisions of this Act.

Right to Information Regulation 2009 A.D was adopted in accordance with the section 38 of the Right to Information Act, 2007 for the implementation of the right embedded in the Right to Information Act, 2007. This regulation is also important for the proper functioning and management of the issues relating to the National Information Commission. It deals with different procedures relating to the exercise of Right to Information such as process of filing the application, contents of the application, process of appeal to the National Information Commission, provision on limitation etc.

International Obligation

Article 19 of two important international Human Rights laws; Universal Declaration on Human Rights (UDHR), 1948 and International Covenant on Civil and Political Rights, (ICCPR), 1966 has ensured right to freedom of expression.

Nepal is the UN member and has ratified and accepted many international documents including the UDHR. Nepal has also ratified ICCPR without any reservation. Articles of ICCPR, including Article 19 are binding to Nepal. ICCPR is the part of Nepalese legal system according to the Nepal Treaty Act, 1990. Section 9 of this Act has stated that the international laws ratified by Nepal shall come into force as the law of Nepal. Therefore, government of Nepal has the international obligation to guarantee Right to Information to its citizens.

Highlights of the Right to Information Act, 2007

Right to Information Act, 2007 is the result of the continuous effort and pressure of the civil society group of Nepal. This law has carried internationally recognized basic principles of right to information. Some of the positive aspects of the Act are as follows:

Key features of the Act are:

- Proactive Disclosure: Principle of right to information stipulates that public agencies are required to disclose certain key information by themselves even in the absence of any request. Such requirement is termed as proactive disclosure. Section 5 of the RTI Act requires public agencies to update and publish different information by themselves on periodic basis.
- Protection of whistleblower: Section 29 of the Act is another remarkable aspect of this Act which protects whistleblowers. According to that provision it is the duty of employee of public agencies to provide information on any ongoing or probable corruption or irregularities or any deed taken as offence under the prevailing laws. It protects the whistleblower whereby it mentions that no harm or punishment is done to bear any legal responsibility to the whistleblower for providing information. Furthermore, even if any punishment or harm is done to the whistleblower, the whistleblower may complaint, along with demand for compensation.
- Scope of the Act extends to Political Parties and Non-governmental Organization: Another noteworthy aspect of this Act is that it covers political parties and non-governmental organizations in its section 2(a) within its scope and they are also responsible to provide the information like other public agencies.
- National Information Commission: This Act has made a provision for the establishment of an independent National Information Commission for the protection, promotion and practice of right to information in its section 11. National Information Commission has been already established in accordance to this Act on June 14, 2008.
- Timeframe and procedures for providing information: Section 7 of the Act has made detailed procedures to acquire the information from the concerned agencies. In addition, those agencies are required to provide information immediately and if they are not in the position to provide immediately then within 15 days of the application.
- Compensation incase of harm or loss occurred as a result of not providing information: Section 33 says that if any person incur losses and damages due to not providing information, denying to provide information, providing partial or wrong information or due to destruction of information then such person are entitled to get compensation.

Implementation mechanisms

Promulgation of law alone is not adequate to protect the rights of citizens. No laws meet its objectives, until and unless it is backed by proper mechanisms to implement the laws. In the context of Right to Information, different mechanisms have been set up and some of the measures are necessary to be set-up. Some of those measures have been identified as:

- *National Information Commission (NIC):* NIC It is an independent organ established for the implementation of Right to Information in Nepal. The primary responsibility of the commission is to protect, promote and ensure the implementation of Right to Information in Nepal. Government of Nepal constituted the commission on June 14, 2008 comprising of one chief commissioner and two commissioners. The Commission is empowered with power to hear and adjudicate case under the Right to Information Act. Likewise, it has the power to issue orders to the public agencies, to recommend and suggest the government and other public bodies in different issues relating to right to information. It can also impose fine and compensation, make necessary orders and can prescribe timeframe to the public bodies to provide information.
- *Public Information Officer*: Right to Information Act, 2007 requires each and every public agency to appoint Public Information Officer for the purpose of disseminating information held in its agencies. They are appointed with the view of disseminating information to the concerned individuals. Public agencies may create Information Section also for the purpose of disseminating information as per necessity.

Present situation of implementation

Right to Information law came with huge expectations from various section of civil society. Civil society expressed high appreciation and expectation on the promulgation of those laws. Despite the separate Act on Right to information, current situation of implementation is not promising. Till now only dismal sections of Nepalese society have been able to exercise this right. Various studies and researches carried out by NGOs and experts working in this area shows that situation of implementation of this Act is not adequate. In addition, many national and international organizations are dissatisfied with the situation of implementation of this Act and there are debates on the efficacy of the law. National Information Commission has also accepted the fact that Right to Information Act, 2007 has not been properly implemented. Many institutions have rationalized the necessity of creating a favorable environment for its implementation.

Similarly, since the drafting of Right to Information Act, 2007 there has been growing demands from civil society as well as government agencies for the proper implementation of this Act.

Experts believe that one of the common and ongoing problems in Nepal is that laws and regulations are made but, are not implemented properly. The situation of Right to Information laws in Nepal is also facing the similar experience.

Conventional practices relating to secrecy about government activities among civil servants; lack of trained and competent human resource in public agencies; failure of Act to establish monitoring mechanisms to oversee the implementation of the Act; lack of intellectual discourse; lack of awareness of the laws to the citizens; failure of civil society to take adequate initiatives and measures etc are identified as the major reasons for the lack of proper implementation of the Act.

Right to Information can play a crucial role to change the conventional bureaucratic practices; transform Nepalese society towards transparency and accountability and; to establish a democratic society. In order to achieve it, Right to Information law needs to be implemented properly. Various stakeholders such as journalist, bureaucratic channels, government and individual information seeker needs to be educated and make aware to establish open and transparent society by utilizing Right to Information tool.

Secure Password Policy issued by GoN:

(check website)