Department of Information Technology

**SRM University**

**COMPILATION NOTES**

**IT1002: IT FUNDAMENTALS**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 15IT213 | P | IT Fundamentals | 2 | 0 | 0 | 2 |

**PURPOSE**

Any discipline of engineering, when learned through formal education programs, necessitates having a specially designed course which covers the fundamentals of various focus areas of that discipline. With this in mind, the course on IT fundamentals is designed to provide the students with fundamental know how’s of different topics in Information Technology in addition to stressing the need for interpersonal skills development.

**INSTRUCTIONAL OBJECTIVES**

1. Describe the components of IT systems and their interrelationships

2. Describe the relationship between IT and other computing disciplines

3. Describe the elements of an IT application and Business process integration

4. Develop and follow the professional skills that are expected out of an IT professional

5. Understand the application domain of IT

**UNIT I-PERVASIVE THEMES IN IT** **(8 hours)**

Components of IT Systems (Hardware, Software, Networks, User) - Data and Information - Information Management – ICT - Networking - Programming –HCI design principles - Web and Multimedia foundations – Information Assurance and Security

**UNIT II-IT AND ITS RELATED DISCIPLINES** **(5 hours)**

Problem Space of Computing - Computing Disciplines – Definition of IT - Relationship between IT and other computing disciplines - Relationship between IT and non computing disciplines

**UNIT III-ORGANIZATIONAL ISSUES** **(7 hours)**

Emergence of complexity in IT – Tools and Techniques to handle complexity – Elements of an IT application – Business Processes - Project Management – Cost Benefit Analysis - Integration of Processes

**UNIT IV-CHARACTERISTICS OF IT PROFESSIONAL** **(5 hours)**

Professionalism–Responsibility - Interpersonal Skills - Life-long Learning- Computing Ethics - Crime, Law, Privacy and Security

**UNIT V-APPLICATION DOMAIN**  **(5 hours)**

Medical Applications- Business Applications- Law Enforcement and Political Processes- E-commerce- Manufacturing- Education- Entertainment – Agriculture– Bio Informatics

**TEXT BOOK**

1. Compilation Notes, Department of Information Technology, SRM University

**REFERENCES**

1. Brian.K.Williams, Stacey.C.Sawyer,Using Information Technology – A

Practical Introduction to Computers and Communication, Tata McGraw Hill

Publishing Company Ltd., New Delhi, 6th Education, 2005.

2. Jedlicka.L, Computers in Our World, Thompson Course Technologies, 2003

3. Shelley.G, Vermaat.M, Cashman.T, Discovering Computers 2005: A

Gateway to Information, Thompson Course Technologies, 2005

Introduction to Information Technology, TL Education Solutions Limited, Pearson Education India, 2011

**UNIT 1**

**PERVASIVE THEMES IN IT**

***(‘The line separating good and evil passes not between states nor between classes nor between parties [individuals] either, but through the middle of every human heart.’)***

*The pervasive nature of information technology means that there are a wide range of available careers and professions at every level of professional development and to suit virtually any interest. Information Technology is pervasive, and people in almost all working environments will be immersed in it in one form or another. The pervasive nature of information technology leads to a presbyopic sense of confidence in our ability to understand and manage its uses.*

**USER CENTEREDNESS**

***What do we mean by “user”? A user is a person who will use the system for performing tasks that are part of his/her job or leisure activities***.

The approaches in User-Centered Design (UCD) vary from Participatory Design (PD) to model-based engineering. No matter the approach, UCD is not the simple, clear-cut way to successful systems development as is sometimes made out. What does user centered design and participatory design mean? And what does user mean? Depending on which discipline you represent, whether you are an academic or practitioner, whether your user population is well defined or not, these concepts are interpreted differently.

In order to be able to discuss the practical consequences of user centered design we needed to define these concepts. Based on the international standard ISO/DIS 13407 (Human Centered Design Process for Interactive Systems), an approach to software and hardware design that identifies four different basic principles is given below:

1. An appropriate allocation of function between user and system

2. Active involvement of users,

3. Iterations of design solutions and

4. Multidisciplinary design teams.

In addition to this it is important for a truly user-centered design approach to ground the design process on observations of the users’ practices in the real world. Similarly we regard Participatory Design as a specific mode of User Centered Design which implies the involvement of the users not only at the beginning and/or at the end of the process, but through all the design process. In a PD approach the users actually participate in and are in charge of the making of the design decisions.

PD suggests a bespoke product with the participants being the real users of the system being developed. UCD can apply to either kind of product - but in one case you might be working with the real users, while in others working with “representative” users.

What do we mean by “user”? A user is a person who will use the system for performing tasks that are part of his/her job or leisure activities. People, who are only circumstantially affected by the system, are considered stakeholders, e.g. managers or support personnel.

**User Centered Versus Participatory:**

It may seem that User Centered Design (UCD) and Participatory Design (PD) are very similar, almost equivalent terms, with PD being a subset of UCD. Actually these are two overlapping sets, with an uncertain amount of overlap.

For example, participation by management and trade union representatives in design reviews (or even in a larger design effort) does not ensure that the designers center their designs on the user and the users' needs. It seemed to be generally agreed that reducing the size of the PD set that is not also user-centered was the most immediate challenge to UCD in practice. PD, particularly in North America, is so much more than systems development. It is closely connected to the democratization process in the workplace, i.e. breaking down power structures and empowering the workers. UCD rarely involves such aspects. It is usually limited to ensuring the influence of specific users in a systems development process. It would probably be more or less impossible for most systems development projects in practice to address democracy matters and issues of power structures. In Scandinavia, PD is no longer as tightly connected to democratization or the

influence of the unions as it was in the seventies. This might be due to the fact that in Sweden the work environment legislation facilitates user involvement. The Swedish Work Environment Law states, among other things, that “the worker should be given the possibility to participate in the design of his /her own working conditions and in development work that concerns his/her work”.

**User Participation**

UCD should be integrated in all design processes but how this is done depends on the

type of project and product.

Different approaches to UCD must be adopted if the user population is 1) known and

accessible, 2) known and not accessible, or 3) unknown and therefore not accessible.

The below sections discuss how UCD could be integrated in different situations.

**With or Without Users**

It is always important to find out who the users are. The discussion included examples where user-centered design was performed without users, as well as examples where the project team met the users at several occasions throughout the process.

Several examples were described where the users were known but not accessible. The reasons for this could be that management prohibited contacts with the users of security reasons, e.g. military applications. Or that management considered their knowledge of the users’ ways of working as better and more precise than the users’ own versions. In one example management also feared that user participation would preserve old routines based on the current system. Other arguments against letting the developers get in contact with the users included heavy workload or simply because of tactical reasons. UCD must be possible even when we cannot work with the users, even though practical user participation always should be preferred. When working without users we can focus on the users, for instance by working with scenarios, based on observations (without directly involving the users), created by the design group and make use of the prevalent psychological expertise about people. This way of working may also be useful when the users are not known and therefore not accessible. If the system is intended for the general public, focus groups, in which representatives of the general public participate, can be used in the development process.

If the total user population is so small that we could fit all of them into the project other methods can be used. The learning process, of the users and the systems developers, that takes place in such a development project is very useful for comprehending the resulting system.

**User Representatives**

You can choose to work with representatives for the user group. A user representative represents a group of users or a specific category of users, e.g. disabled users, for a specific reason. One should always try to maximize the difference between the people you involve, i.e. try to cover as many different categories of users as possible. When developing for a specific organization all different types of work activities that a system is to support should be covered by the skills of the user representatives. Management and unions are not to be viewed as representatives for a user group, although they are important for the justification of a project. Some of the representatives should be involved throughout the whole project so that they get to know the project and get committed to its purpose. However, it is well known that users after having participated in a project no longer are representatives of the typical users, e.g. in evaluations. They learn over time and get a lot more involved in the technology that is being developed. Therefore, you should involve other representatives for shorter periods for analysis and evaluations, just to overcome the risk of having the user representatives influence the project in a way that is not suitable for other users.

**User Selection**

Different strategies can be adopted when selecting user representatives. Selecting users on a random basis, of course, may provide you with some information on how the average user would behave. Often projects need to be able to arrive at consensus about specific solutions and in this situation it may be preferable to work with randomly selected users. In other cases, however, you need to focus especially on the conflicting goals of the users. Your concern is not to develop systems for average users but to develop systems that support all user categories. Therefore you should cover the differences in user types. Try to maximize the differences by selecting users of, for instance different age, with different skills, various disabilities, and different computer experience.

**Commitment**

Having users that are committed to the development project is of course central. User commitment can be enhanced by means of, for instance, the users’ participation within their normal work tasks, which give them the possibility of seeing directly how a new system could influence their work conditions. Voluntary participation of course increases the degree of commitment, as it is something the participants wish to do. Whether the users are being rewarded for their participation or not, in terms of increased salaries or benefits, travels, better positions, etc. is of course also central for user commitment. When the users act on a non-profitable basis difficulties can occur. During the project it is important that the users really feel that they contribute to the project. For this to happen it is necessary to clearly show the participating users that all their suggestions and comments are addressed.

**Working with Groups or Individuals**

An example of working with representatives for a group of workers was given in which a homogenous group of about four representatives was formed in order to make them strong enough to work directly with researchers, designers and UCD facilitators. If possible, you should work with both individual users and groups but at different occasions and with different activities in the process. Working with groups of people tends to be more conducive to creativity – people are less creative on their own. Having a group of users solving a particular problem is much more efficient than asking single users. Group work could also shift the balance of power from the development team to the user group. Regardless of whether you work with individual users or user groups, users must be treated as equals regarding power and expertise. The goal should be to have at least be as many users as other participants in a project.

**Humbleness and Respect**

It is important to think about how to co-operate with users and that we have to take care of this contact. The keywords for success are humbleness and respect. The ways in which we interact with the users controls the result. Unfortunately attitudes both from the developer side and user side can be obstacles in this process.

It is what people think, say, feel and do that is important and what the context is.

**When do We Meet?**

In reality the users are often invited in the beginning and at the end of the development phase only. Sometimes, they are only involved in the scenario process and evaluations of a full-scale prototype. This is very unfortunate. In the phases where there is no user participation several decisions are made that affect the usability of the resulting system, that would not have been made if the users had been consulted. It is important to have user participation continuously throughout the process to preserve the usability aspects in the final product.

**Working on the Field**

Do we meet on neutral ground or do we let the users enter the design ground? Where do

we meet?

It is important that not only the UCD facilitators but also the designers and developers should go out into the field and have direct contact with the users. Field observations might give the designers some impressions and ideas that they would not have been able to obtain otherwise. After all, users are clients that the designers and developers are supposed to deliver products to.

The designers must get to know their users but it is equally important that the users get a notion of the technological possibilities and limitations. Therefore, you should also invite the users to the designers’ office: "Let the users leave their trace in the design office". This can be done, for instance, by means of modifications to a prototype or a mock-up, or by means of sketches of the system.

**Video Documentation**

Video is a very useful medium for analysis and for visualizing current and future scenarios. Video is also a very efficient medium for showing developers how users actually use the products that they have designed. When a developer has seen a user perform the same error a couple of times there is no need for further convincing that the design must be changed. In order to facilitate fruitful and informative interviews and to learn about the hierarchies of the workplace in advance, spending time at the workplace with a video camera could be very useful.

**CASE STUDY:**

**Why FOCUS on The User?**

All Web sites have users. A user is anyone who visits a site. Depending on the type of site, its goals and audience a user can be many different things. A user can be a reader, a shopper, an information gatherer, a content contributor or a host of other things.

For a Web site to be successful there must be FOCUS put on the user from the beginning to the end. A site is nothing without it's users and every effort should be made to understand the user and meet their goals when developing a site. If the user's goals aren't met the site will be a failure. It's as simple as that.

**Get to Know The User**

Anyone with a Web site wants it to succeed, to achieve the goals laid out for it. One of the first steps toward achieving these goals is determining the audience for the Web site and getting to know those who will use the site. It is nearly impossible to design and build a Web site properly without having a clear understanding of who will be using the site and what for. There are many ways to learn about the users of a site. These include:

* Interviewing potential users or existing customers
* Analysis of the competition
* Surveys
* Focus Groups
* Statistical observation

Depending on the situation and the particularities of the project, getting to know the users can be fairly easy or rather complicated. At the very least the effort needs to be made, even a little understanding goes along way. Sounds practical doesn't it? Of course, but it's surprising how often sites get built with no effort gone into learning about those folks who will be using the site.

**Establish User Goals**

Once the users have been identified it's time to work with them to establish goals. The foundation of any project is it's goals and the user goals are as important as any to a sites success.

Good clear goals can take many forms, and these will vary from project to project, as will the importance of user goals. Make no mistake, having user goals will always make decisions easier and help insure the success of a Web site. A goal can be as simple as "Have clear, readable text" to as complex as "Every page must be accessible from a Linux machine running Konqueror."

User goals can be used to help make design and development decisions and become a mechanism to keep a project on track as well. Many times Web projects can easily escalate in scope and knowing the users and their goals can bring projects back under control. Once goals are established it's important to keep track of them and measure the project against them as often as possible.

**Test, Test and Test again**

Usability and user testing doesn't have to be a time consuming, esoteric nightmare. Many Web sites and projects don't need to go though a full cycle of usability to be successful, although depending on the type of site and it's goals this might be the right thing to do. For many sites a little cheap user testing will reveal major usability problems.

Simply gathering some users together, placing them in front of a site and watching them use it can be very, very enlightening. I'm always amazed at what I can learn about my work from watching actual users. If possible this type of user testing should be done at least with a few people. Ideally you will have access to an actual user of your site, but if not use a friend, co worker or neighbor. Some testing is always better than none at all.

**Follow Guidelines and Standards**

There few rules on the Web, if any, and what little there are change all the time. It can be hard to keep up with the technology as well as the wants and needs of your users. Oftentimes a site will need to be redesigned many times to keep up, and this can become costly in many ways. While there are few set rules on the Web, there are many guidelines, standards and best practices that can be used to not only keep the sites of today on track, but future proof for the changes down the road. Understanding the basics and guidelines of Web usability won't replace getting to know your users and their goals, but it will help. Understanding Web standards and best practices in web development can save lots of time, money and frustration.

**Benefits of user FOCUS**

If the time is taken to FOCUS on the user throughout the life cycle of a project it will assuredly be all the better for it. Even a little user FOCUS goes a long way, and there is really no reason why the time shouldn't be taken to make an effort to understand, make goals for and test with users. Add to that some basic usability understanding, guidelines and Web standards and you've got a guaranteed winner.

**COMPONENTS OF IT SYSTEMS**

**Information system,** an integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. For instance, corporations use information systems to reach their potential customers with targeted messages over the Web, to process financial accounts, and to manage their human resources. Governments deploy information systems to provide services cost-effectively to citizens. Digital goods, such as electronic booksand software, and online services, such as auctions and social networking, are delivered with information systems. Individuals rely on information systems, generally Internet-based, for conducting much of their personal lives: for socializing, study, shopping, banking, and entertainment.

As major new technologies for recording and processing information have been invented over the millennia, new capabilities have appeared. The invention of the printing press by Johannes Gutenbergin the mid-15th century and the invention of a mechanical calculator by Blaise Pascal in the 17th century are but two examples. These inventions led to a profound revolution in the ability to record, process, and disseminate information and knowledge. The first large-scale mechanical information system was Herman Hollerith’s census tabulator. Invented in time to process the 1890 U.S. census, Hollerith’s machine represented a major step in automation, as well as an inspiration to develop computerized information systems.

One of the first computers used for such information processing was the UNIVAC I, installed at the U.S. Bureau of the Census in 1951 for administrative use and at General Electric in 1954 for commercial use. Beginning in the late 1970s, personal computers brought some of the advantages of information systems to small businesses and to individuals. Early in the same decade the Internet began its expansion as the global network of networks. In 1991 the World Wide Web, invented by Tim Berners-Leeas a means to access the interlinked information stored in the computers connected by the Internet, was installed to become the principal service delivered on the network. The global penetration of the Internet and the Web has enabled access to information and other resources and facilitated the forming of relationships among people and organizations on an unprecedented scale. The progress of electronic commerce over the Internet has resulted in a dramatic growth in digital interpersonal communications (via e-mail and social networks), distribution of products (software, music, e-books, and movies), and business transactions (buying, selling, and advertising on the Web). With the emergence of smartphones, tablets, and other computer-based mobile devices, all of which are connected by wireless communication networks, information systems have been extended to support mobility as the natural human condition.

As information systems have enabled more diverse human activities, they have exerted a profound influence over society. These systems have quickened the pace of daily activities, affected the structure and mix of organizations, changed the type of products bought, and influenced the nature of work. Information and knowledge have become vital economic resources. Yet, along with opportunities, the dependence on information systems has brought new threats. Intensive industry innovation and academic research continually develop new opportunities while aiming to contain the threats.

*Components of information systems*

The main components of information systems are computer hardware and software, telecommunications, databases and data warehouses, human resources, and procedures. The hardware, software, and telecommunications constitute information technology (IT), which is now ingrained in the operations and management of organizations.

### Computer hardware

Today even the smallest firms, as well as many households throughout the world, own or lease computers. These are usually microcomputers, also called personal computers. Individuals may own multiple computers in the form of smartphones and other portable devices. Large organizations typically employ distributed computer systems, from powerful parallel-processing servers located in data centres to widely dispersed personal computers and mobile devices, integrated into the organizational information systems. Together with the peripheral equipment, such as magnetic or solid-state storage disks, input-output devices, and telecommunications gear, these constitute the hardware of information systems. The cost of hardware has steadily and rapidly decreased, while processing speed and storage capacity have increased vastly. However, hardware’s use of electric power and its environmental impact are concerns being addressed by designers.

### Computer software

Computer software falls into two broad classes: system software and application software. The principal system software is the operating system. It manages the hardware, data and program files, and other system resources and provides means for the user to control the computer, generally via a graphical user interface (GUI). Application software is programs designed to handle specific tasks for users. Examples include general-purpose application suites with their spreadsheet and word-processing programs, as well as “vertical” applications that serve a specific industry segment—for instance, an application that schedules, routes, and tracks package deliveries for an overnight carrier. Larger firms use licensed applications, customizing them to meet their specific needs, and develop other applications in-house or on an outsourced basis. Companies may also use applications delivered as software-as-a-service (SaaS) over the Web. Proprietary software, available from and supported by its vendors, is being challenged by open-source software available on the Web for free use and modification under a license that protects its future availability.

### Telecommunications

Telecommunications are used to connect, or network, computer systems and transmit information. Connections are established via wired or wireless media. Wired technologies include coaxial cable and fibre optics. Wireless technologies, predominantly based on the transmission of microwaves and radio waves, support mobile computing. Pervasive information systems have arisen with the computing devices embedded in many different physical objects. For example, sensors such as radio frequency identification devices (RFIDs) can be attached to products moving through the supply chain to enable the tracking of their location and the monitoring of their condition. Wireless sensor networks that are integrated into the Internet can produce massive amounts of data that can be used in seeking higher productivity or in monitoring the environment.

Various computer network configurations are possible, depending on the needs of an organization. Local area networks (LANs) join computers at a particular site, such as an office building or an academic campus. Metropolitan area networks (MANs) cover a limited densely populated area. Wide area networks (WANs) connect widely distributed data centres, frequently run by different organizations. The Internet is a network of networks, connecting billions of computers located on every continent. Through networking, users gain access to information resources, such as large databases, and to other individuals, such as coworkers, clients, or people who share their professional or private interests. Internet-type services can be provided within an organization and for its exclusive use by various intranets that are accessible through a browser; for example, an intranet may be deployed as an access portal to a shared corporate document base. To connect with business partners over the Internet in a private and secure manner, extranets are established as so-called virtual private networks (VPNs) by encrypting the messages.

### Databases and data warehouses

Many information systems are primarily delivery vehicles for data stored in databases. A database is a collection of interrelated data (records) organized so that individual records or groups of records can be retrieved to satisfy various criteria. Typical examples of databases include employee records and product catalogs. Databases support the operations and management functions of an enterprise. Data warehouses contain the archival data, collected over time, that can be mined for information in order to develop and market new products, serve the existing customers better, or reach out to potential new customers. Anyone who has ever purchased something with a credit card—in person, by mail order, or over the Web—is included within such data collections.

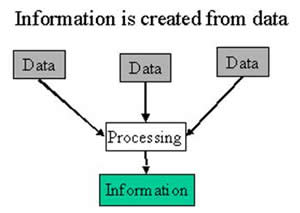
### Human resources and procedures

Qualified people are a vital component of any information system. Technical personnel include development and operations managers, business analysts, systems analysts and designers, database administrators, computer programmers, computer security specialists, and computer operators. In addition, all workers in an organization must be trained to utilize the capabilities of information systems. Billions of people around the world are learning about information systems as they use the Web.

Procedures for using, operating, and maintaining an information system are part of its documentation. For example, procedures need to be established to run a payroll program, including when to run it, who is authorized to run it, and who has access to the output.

**DIFFERENCE BETWEEN DATA AND INFORMATION**

##### **Key difference:** Data and information are interrelated. Data usually refers to raw data, or unprocessed data. It is the basic form of data, data that hasn’t been analyzed or processed in any manner. Once the data is analyzed, it is considered as information. Information is "knowledge communicated or received concerning a particular fact or circumstance." Information is a sequence of symbols that can be interpreted as a message. It provides knowledge or insight about a certain matter.



Data and information are interrelated. In fact, they are often mistakenly used interchangeably. Data is considered to be raw data. It represents ‘values of qualitative or quantitative variables, belonging to a set of items.’ It may be in the form of numbers, letters, or a set of characters. It is often collected via measurements. In data computing or data processing, data is represented by in a structure, such as tabular data, data tree, a data graph, etc.

Data usually refers to raw data, or unprocessed data. It is the basic form of data, data that hasn’t been analyzed or processed in any manner. Once the data is analyzed, it is considered as information.

Information is "knowledge communicated or received concerning a particular fact or circumstance." Information is a sequence of symbols that can be interpreted as a message. It provides knowledge or insight about a certain matter. Information can be recorded as signs, or transmitted as signals.

Basically, information is the message that is being conveyed, whereas data are plain facts. Once the data is processed, organized, structured or presented in a given context, it can become useful. Then data will become information, knowledge.

Data in itself is fairly useless, until it is interpreted or processed to get meaning, to get information. In computing, it can be said that data is the computer's language. It is the output that the computer gives us. Whereas, information is how we interpret or translate the language or data. It is the human representation of data.

Some differences between data and information:

* Data is used as input for the computer system. Information is the output of data.
* Data is unprocessed facts figures. Information is processed data.
* Data doesn’t depend on Information. Information depends on data.
* Data is not specific. Information is specific.
* Data is a single unit. A group of data which carries news are meaning is called Information.
* Data doesn’t carry a meaning. Information must carry a logical meaning.
* Data is the raw material. Information is the product.

|  |  |  |
| --- | --- | --- |
| **Meaning** | Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized. | When data is processed, organized, structured or presented in a given context so as to make it useful, it is called Information. |
| **Example** | Each student's test score is one piece of data | The class' average score or the school's average score is the information that can be concluded from the given data. |
| **Definition** | Latin 'datum' meaning "that which is given". Data was the plural form of datum singular (M150 adopts the general use of data as singular. Not everyone agrees.) | Information is interpreted data. |

www.slideshare.net/EinsteinX2/**data**-**vs**-**information**‎- Use this link to get additional information.

**INFORMATION MANAGEMENT**

**(*Information management is characterized by the phrase of 'Getting the right information to the right person at the right place at the right time'.)***

Information management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. This sometimes involves those who have a stake in, or a right to that information. Management means the organization of and control over the structure, processing and delivery of information.

Throughout the 1970s this was largely limited to files, file maintenance, and the life cycle management of paper-based files, other media and records. With the proliferation of information technology starting in the 1970s, the job of information management took on a new light, and also began to include the field of Data maintenance. No longer was information management a simple job that could be performed by almost anyone. An understanding of the technology involved, and the theory behind it became necessary. As information storage shifted to electronic means, this became more and more difficult. By the late 1990s when information was regularly disseminated across computer networks and by other electronic means, network managers, in a sense, became information managers. Those individuals found themselves tasked with increasingly complex tasks, hardware and software. With the latest tools available, information management has become a powerful resource and a large expense for many organizations.

Information management is characterized by the phrase of 'Getting the right information to the right person at the right place at the right time'. It does not, however, address the question of what constitutes the 'right information'. This omission can be addressed through the philosophy of Informational management (IaM). IaM is characterized by the phrase, 'Knowing what information to gather, knowing what to do with information when you get it, knowing what information to pass on, and knowing how to value the result' (adapted from G. Russell Swanborough). This identifies the 'right information' and the resulting whole solution is worth more than the sum of its parts.

Following the behavioral science theory of management, mainly developed at Carnegie Mellon University and prominently represented by Barnard, Richard M. Cyert, March and Simon, most of what goes on in service organizations is actually decision making and information processes. The crucial factor in the information and decision process analysis is thus individuals’ limited ability to process information and to take decisions under these limitations.

According to March and Simon, organizations have to be considered as cooperative systems with a high level of information processing and a vast need for decision making at various levels. They also claimed that there are factors that would prevent individuals from acting strictly rational, in opposite to what has been proposed and advocated by classic theorists. Instead, they proposed that any decision would be sub-optimum due to the bounded rationality of the decision-maker.

Instead of using the model of the economic man, as advocated in classic theory, they proposed the administrative man as an alternative based on their argumentation about the cognitive limits of rationality.

While the theories developed at Carnegie Mellon clearly filled some theoretical gaps in the discipline, March and Simon, did not propose a certain organizational form that they considered especially feasible for coping with cognitive limitations and bounded rationality of decision-makers. Through their own argumentation against normative decision-making models, i.e., models that prescribe people how they ought to choose, they also abandoned the idea of an ideal organizational form.

In addition to the factors mentioned by March and Simon, there are two other considerable aspects, stemming from environmental and organizational dynamics. Firstly, it is not possible to access, collect and evaluate all environmental information being relevant for taking a certain decision at a reasonable price, i.e., time and effort. In other words, following a national economic framework, the transaction cost associated with the information process is too high. Secondly, established organizational rules and procedures can prevent the taking of the most appropriate decision, i.e., that a sub-optimum solution is chosen in accordance to organizational rank structure or institutional rules, guidelines and procedures, an issue that also has been brought forward as a major critique against the principles of bureaucratic organizations.

According to the Carnegie Mellon School and its followers, information management, i.e., the organization's ability to process information, is at the core of organizational and managerial competencies. Consequently, strategies for organization design must be aiming at improved information processing capability. Jay Galbraith has identified five main organization design strategies within two categories — increased information processing capacity and reduced need for information processing.

* Reduction of information processing needs
* Environmental management
* Creation of slack resources
* Creation of self-contained tasks
* Increasing the organizational information processing capacity
* Creation of lateral relations
* Vertical information systems
* Environmental management.

Instead of adapting to changing environmental circumstances, the organization can aim at modifying its environment. Vertical and horizontal collaboration, i.e. cooperation or integration with other organizations in the industry value system are typical means for reducing uncertainty. An example for reducing uncertainty in the relation with the prior or demanding stage of the industry system is the concept of Supplier-Retailer collaboration or Efficient Customer Response.

**Creation of slack resources**.

In order to reduce exceptions, performance levels can be reduced, thus decreasing the information load on the hierarchy. These additional slack resources, required to reduce information processing in the hierarchy, are representing an additional cost to the organization and the choice of this method is clearly depending on the alternative costs of other strategies.

**Creation of self-contained tasks.**

Achieving a conceptual closure of tasks is another way of reducing information processing. In this case, the task-performing unit has all the resources required to perform the task. This approach is concerned with task (de-)composition and interaction between different organizational units, i.e. organizational and information interfaces.

**Creation of lateral relations.**

In this case, lateral decision processes are established that cut across functional organizational units. The aim is to apply a system of decision subsidiarity, i.e. to move decision power to the process, instead of moving information from the process into the hierarchy for decision-making.

**Investment in vertical information systems**.

Instead of processing information through the existing hierarchical channels, the organization can establish vertical information systems. In this case, the information flow for a specific task (or set of tasks) is routed in accordance to the applied business logic, rather than the hierarchical organization.

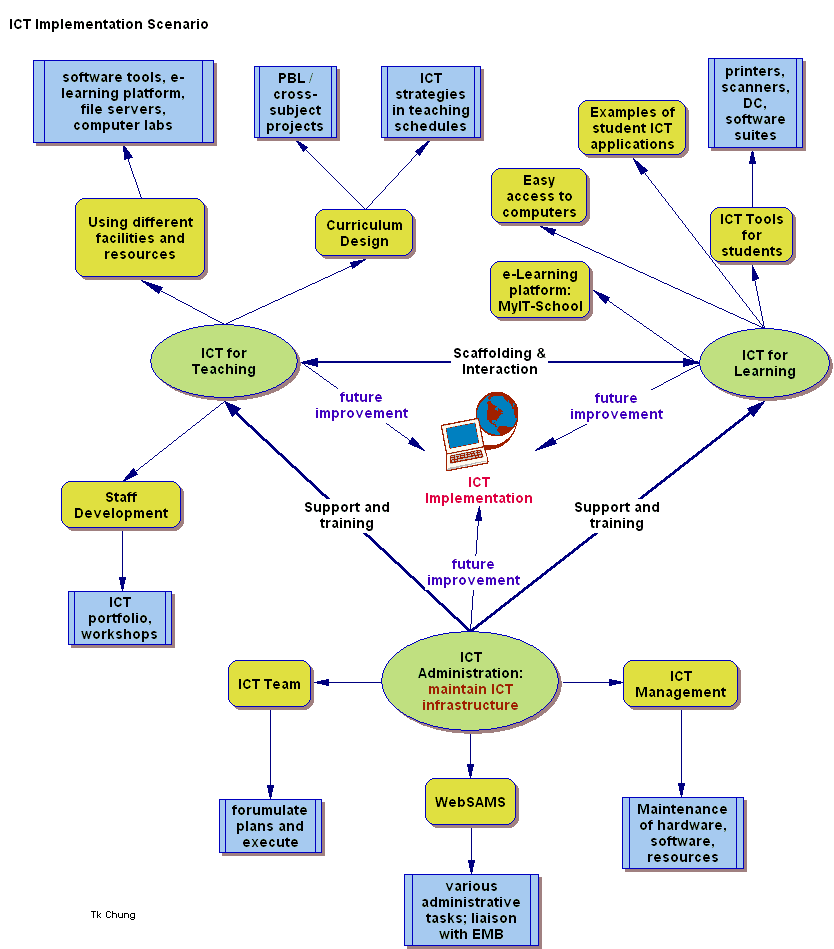
Following the lateral relations concept, it also becomes possible to employ an organizational form that is different from the simple hierarchical information. The Matrix organization is aiming at bringing together the functional and product departmental bases and achieving a balance in information processing and decision making between the vertical (hierarchical) and the horizontal (product or project) structure. The creation of a matrix organization can also be considered as management's response to a persistent or permanent demand for adaptation to environmental dynamics, instead of the response to episodic demands.

**INFORMATION AND COMMUNICATION TECHNOLOGY**

ICT and computers are **NOT** the same thing. An **ICT system** is a set-up consisting of hardware, **software**, **data** and the people who use them. It very often also includes communications technology, such as the **Internet**. **Computers** are the **hardware** that is often part of an ICT system.  ICT Systems are used in a whole host of places such as offices, shops, factories, aircraft and ships in addition to being used in activities such as communications, medicine and farming. They are everyday and ordinary yet extraordinary in how they can add extra power to what we do and want to do.

**ICT systems** have become important because by using them we are:

* More productive - we can complete a greater number of tasks in the same time at reduced cost by using computers than we could prior to their invention.
* Able to deal with vast amounts of information and process it quickly.
* Able to transmit and receive information rapidly.



Types of ICT system

There are three main types of ICT system:

**Information systems**  
This type of ICT system is focused on managing **data and information.** Examples of these are a sports club membership system or a supermarket stock system.

**Control Systems**  
These ICT systems have **controlling** machines as their main aim. They use input, process and output, but the output may be moving a robot arm to weld a car chassis rather than information.

**Communications Systems**  
The output of these ICT systems is the successful **transport of data** from one place to another.

**Input, output & system diagrams**

What comes out of an **ICT system** is largely dependant on what you put into the system. The acronym **GIGO** is a good way of thinking about this.

GIGO can be interpreted in 2 ways:

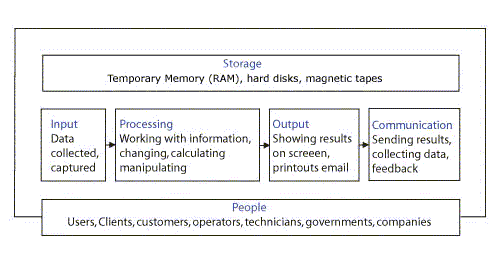
**1. Good Input, Good Output**  
ICT systems work by taking inputs (instructions and **data**), processing them and producing outputs that are stored or communicated in some way. The higher the quality and better thought-out the inputs, the more useful will be the outputs.

**2. Garbage In, Garbage Out**  
ICT systems cannot function properly if the inputs are inaccurate or faulty; they will either not be able to process the data at all, or will output data which is erroneous or useless. That's why the term GIGO is sometimes used to stand for "Garbage In, Garbage Out".

GIGO is a useful term to remember in the exam - it can help explain many issues such as why **validation** is needed and why accurate data is valuable.

**An ICT system diagram**

A system is an assembly of parts that together make a whole. ICT systems are made up of some or all of the parts shown in the diagram. Various devices are used for input, processing, output and communication.



**Media Integration**

Methods used for input to and output from ICT systems vary a lot. In your revision you need to be familiar with examples of input and output formats.

Input and output formats are the different kinds of media that are used to:

EITHER gather up and collect data and instructions

OR to display, present or issue the outputs of processing.

Up until recently most media formats required dedicated devices to run on - for example, digital cameras to take digital photographs, scanners to digitise images for use on a computer, or VCR players for video playback - so you needed the correct matching device in order to work with each media format.

There is now a growing tendency for multi-purpose ICT devices. The driving force is the communication power of the Internet, and the increasing availability of small high-powered electronic technology. This means that you can now get an all-in-one box that can do the same thing as several different ones did before. Here are some examples:

combined printers, scanners and photocopiers

televisions with built in Internet connections and web browsers

mobile phones with Internet access and digital cameras.

laptop, palmtop and table computers that have mobile Internet access and built in handwriting recognition.

There are now single devices available which incorporate the following features: phone, camera, disk storage, TV and Internet access.

**NETWORKING**

Computer networking is the engineering discipline concerned with communication between computer systems or devices. Networking, routers, routing protocols, and networking over the public Internet have their specifications defined in documents called RFCs.[1] Computer networking is sometimes considered a sub-discipline of telecommunications, computer science, information technology and/or computer engineering. Computer networks rely heavily upon the theoretical and practical application of these scientific and engineering disciplines.

A computer network is any set of computers or devices connected to each other with the ability to exchange data.[2] Examples of networks are:

**Local area network (LAN)**, which is usually a small network constrained to a small geographic area.

**Wide area network (WAN)** that is usually a larger network that covers a large geographic area.

**Wireless LANs and WANs (WLAN & WWAN)** is the wireless equivalent of the LAN and WAN

All networks are interconnected to allow communication with a variety of different kinds of media, which including twisted-pair copper wire cable, coaxial cable, optical fiber, and various wireless technologies.[3] The devices can be separated by a few meters (e.g. via Bluetooth) or nearly unlimited distances (e.g. via the interconnections of the Internet[4]).

**Views of networks**

Users and network administrators often have different views of their networks. Often, users that share printers and some servers form a workgroup, which usually means they are in the same geographic location and are on the same LAN. A community of interest has less of a connotation of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Network administrators see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e.g., routers, bridges and application layer gateways that interconnect the physical media. Logical networks, called, in the TCP/IP architecture, subnets , map onto one or more physical media. For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using virtual LAN (VLAN) technology.

Both users and administrators will be aware, to varying extents, of the trust and scope characteristics of a network. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e.g. employees) (RFC 2547). Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e.g. business partners, customers)RFC 3547.

Informally, the Internet is the set of users, enterprises,and content providers that are interconnected by Internet Service Providers (ISP). From an engineering standpoint, the Internet is the set of subnets, and aggregates of subnets, which share the registered IP address space and exchange information about the reachability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

Over the Internet, there can be business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) communications. Especially when money or sensitive information is exchanged, the communications are apt to be secured by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users, using secure Virtual Private Network (VPN) technology.

**HUMAN COMPUTER INTERACTION**

Human–computer interaction (HCI), alternatively man–machine interaction (MMI) or computer–human interaction (CHI) is the study of interaction between people (users) and computers. It is often regarded as the intersection of computer science, behavioral sciences, design and several other fields of study. Interaction between users and computers occurs at the user interface (or simply *interface*), which includes both software and hardware, for example, general purpose computer peripherals and large-scale mechanical systems, such as aircraft and power plants.

"Human-computer interaction is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them."

**Goals**

A basic goal of HCI is to improve the interactions between users and computers by making computers more usable and receptive to the user's needs. Specifically, HCI is concerned with:

* methodologies and processes for designing interfaces (i.e., given a task and a class of users, design the best possible interface within given constraints, optimizing for a desired property such as learnability or efficiency of use)
* methods for implementing interfaces (e.g. software toolkits and libraries; efficient algorithms)
* techniques for evaluating and comparing interfaces
* developing new interfaces and interaction techniques
* developing descriptive and predictive models and theories of interaction

A long term goal of HCI is to design systems that minimize the barrier between the human's cognitive model of what they want to accomplish and the computer's understanding of the user's task.

Professional practitioners in HCI are usually designers concerned with the practical application of design methodologies to real-world problems. Their work often revolves around designing graphical user interfaces and web interfaces.

Researchers in HCI are interested in developing new design methodologies, experimenting with new hardware devices, prototyping new software systems, exploring new paradigms for interaction, and developing models and theories of interaction.

**Design Methodologies**

A number of diverse methodologies outlining techniques for human–computer interaction design have emerged since the rise of the field in the 1980s. Most design methodologies stem from a model for how users, designers, and technical systems interact. Early methodologies, for example, treated users' cognitive processes as predictable and quantifiable and encouraged design practitioners to look to cognitive science results in areas such as memory and attention when designing user interfaces. Modern models tend to focus on a constant feedback and conversation between users, designers, and engineers and push for technical systems to be wrapped around the types of experiences users want to have, rather than wrapping user experience around a completed system.

User-centered design: user-centered design (UCD) is a modern, widely practiced design philosophy rooted in the idea that users must take center-stage in the design of any computer system. Users, designers and technical practitioners work together to articulate the wants, needs and limitations of the user and create a system that addresses these elements. Often, user-centered design projects are informed by ethnographic studies of the environments in which users will be interacting with the system.

Principles of User Interface Design: these are seven principles that may be considered at any time during the design of a user interface in any order, namely Tolerance, Simplicity, Visibility, Affordance, Consistency, Structure and Feedback.

**HCI DESIGN PRINCIPLES:**

**Shneiderman’s Eight Golden Rules of Interface Design**

Shneiderman’s eight golden rules provide a convenient and succinct summary of

the key principles of interface design.

1. *Strive for consistency* in action sequences, layout, terminology, command use and so on.

2. *Enable frequent users to use shortcuts*, such as abbreviations, special key sequences and macros, to perform regular, familiar actions more quickly*.*

3. *Offer informative feedback* for every user action, at a level appropriate to the

magnitude of the action*.*

4. *Design dialogs to yield closure* so that the user knows when they have completed a task.

5. *Offer error prevention and simple error handling* so that, ideally, users are prevented from making mistakes and, if they do, they are offered clear and informative instructions to enable them to recover.

6. *Permit easy reversal of actions* in order to relieve anxiety and encourage

exploration, since the user knows that he can always return to the previous state*.*

7. *Support internal locus of control* so that the user is in control of the system, which responds to his actions*.*

8. *Reduce short-term memory load* by keeping displays simple, consolidating

multiple page displays and providing time for learning action sequences.

These rules provide a useful shorthand for the more detailed sets of principles

described earlier. Like those principles, they are not applicable to every eventuality

and need to be interpreted for each new situation. However, they are broadly useful

and their application will only help most design projects.

**Norman’s Seven Principles for Transforming Difficult Tasks**

**into Simple Ones**

1. *Use both knowledge in the world and knowledge in the head*. People work better when the knowledge they need to do a task is available externally – either explicitly or through the constraints imposed by the environment. But experts also need to be able to internalize regular tasks to increase their efficiency. So systems should provide the necessary knowledge within the environment and their operation should be transparent to support the user in building an appropriate mental model of what is going on.

2. *Simplify the structure of tasks*. Tasks need to be simple in order to avoid complex problem solving and excessive memory load. There are a number of ways to simplify the structure of tasks. One is to provide mental aids to help the user keep track of stages in a more complex task. Another is to use technology to provide the user with more information about the task and better feedback. A third approach is to automate the task or part of it, as long as this does not detract from the user’s experience. The final approach to simplification is to change the nature of the task so that it becomes something more simple. In all of this, it is important not to take control away from the user.

3. *Make things visible*: bridge the gulfs of execution and evaluation. The interface should make clear what the system can do and how this is achieved, and should enable the user to see clearly the effect of their actions on the system.

4. *Get the mappings right*. User intentions should map clearly onto system controls. User actions should map clearly onto system events. So it should be clear what does what and by how much. Controls, sliders and dials should reflect the task – so a small movement has a small effect and a large movement a large effect.

5. *Exploit the power of constraints*, both natural and artificial. Constraints are things in the world that make it impossible to do anything but the correct action in the correct way. A simple example is a jigsaw puzzle, where the pieces only fit together in one way. Here the physical constraints of the design guide the user to complete the task.

6. *Design for error*. To err is human, so anticipate the errors the user could make and design recovery into the system.

7. *When all else fails, standardize*. If there are no natural mappings then arbitrary mappings should be standardized so that users only have to learn them once. It is this standardization principle that enables drivers to get into a new car and drive it with very little difficulty – key controls are standardized. Occasionally one might switch on the indicator lights instead of the windscreen wipers, but the critical controls (accelerator, brake, clutch, steering) are always the same.

**PROGRAMMING LANGUAGES**

Computer programming (often shortened to programming or coding) is the process of writing, testing, debugging/troubleshooting, and maintaining the source code of computer programs. This source code is written in a programming language. The code may be a modification of an existing source or something completely new, the purpose being to create a program that exhibits a certain desired behavior (customization). The process of writing source codes requires expertise in many different subjects, including knowledge of the application domain, specialized algorithms, and formal logic.

Within software engineering, programming (the *implementation*) is regarded as one phase in a software development process.

In some specialist applications or extreme situations a program may be written or modified (known as patching) by directly storing the numeric values of the machine code instructions to be executed into memory.

There is an ongoing debate on the extent to which the writing of programs is an art, a craft or an engineering discipline.[1] Good programming is generally considered to be the measured application of all three, with the goal of producing an efficient and maintainable software solution (the criteria for "efficient" and "maintainable" vary considerably). The discipline differs from many other technical professions in that programmers generally do not need to be licensed or pass any standardized (or governmentally regulated) certification tests in order to call themselves "programmers" or even "software engineers".

Another ongoing debate is the extent to which the programming language used in writing programs affects the form that the final program takes. This debate is analogous to that surrounding the Sapir-Whorf hypothesis in linguistics

Programming languages

Different programming languages support different styles of programming (called *programming paradigms*). The choice of language used is subject to many considerations, such as company policy, suitability to task, availability of third-party packages, or individual preference. Ideally, the programming language best suited for the task at hand will be selected. Trade-offs from this ideal involve finding enough programmers who know the language to build a team, the availability of compilers for that language, and the efficiency with which programs written in a given language execute.

Allen Downey, in his book "How To Think Like A Computer Scientist" wrote: The details look different in different languages, but a few basic instructions appear in just about every language: input: Get data from the keyboard, a file, or some other device. output: Display data on the screen or send data to a file or other device. math: Perform basic mathematical operations like addition and multiplication. conditional execution: Check for certain conditions and execute the appropriate sequence of statements. repetition: Perform some action repeatedly, usually with some variation.

**Modern programming**

**Quality requirements**:

Whatever the approach to the software development may be, the program must finally satisfy some fundamental properties; bearing them in mind while programming reduces the costs in terms of time and/or money due to debugging, further development and user support. Although quality programming can be achieved in a number of ways, following five properties are among the most relevant:

**Efficiency**: it is referred to the system resource consumption (computer processor, memory, slow devices, networks and to some extent even user interaction) which must be the lowest possible.

**Reliability**: the results of the program must be correct, which not only implies a correct code implementation but also reduction of error propagation (e.g. resulting from data conversion) and prevention of typical errors (overflow, underflow or zero division).

**Robustness:** a program must anticipate situations of data type conflict and all other incompatibilities which result in run time errors and stop the program. The focus of this aspect is the interaction with the user and the handling of error messages.

**Portability**: it should work as it is in any software and hardware environment, or at least without relevant reprogramming.

**Readability**: the purpose of the main program and of each subroutine must be clearly defined with appropriate comments and self explanatory choice of symbolic names (constants, variables, function names, classes, methods, ...).

**Algorithmic Complexity**

The academic field and engineering practice of computer programming are largely concerned with discovering and implementing the most efficient algorithms for a given class of problem. For this purpose, algorithms are classified into *orders* using so-called Big O notation, *O(n)*, which expresses resource use, such as execution time or memory consumption, in terms of the size of an input. Expert programmers are familiar with a variety of well-established algorithms and their respective complexities and use this knowledge to choose algorithms that are best suited to the circumstances.

**Methodologies**

The first step in every software development project should be requirements analysis, followed by modeling, implementation, and failure elimination (debugging). There exist a lot of differing approaches for each of those tasks. One approach popular for requirements analysis is Use Case analysis.

Popular modeling techniques include Object-Oriented Analysis and Design (OOAD) and Model-Driven Architecture (MDA). The Unified Modeling Language (UML) is a notation used for both OOAD and MDA.

A similar technique used for database design is Entity-Relationship Modeling (ER Modeling).

Implementation techniques include imperative languages (object-oriented or procedural), functional languages, and logic languages.

Debugging is most often done with IDEs like Visual Studio, NetBeans, and Eclipse. Separate debuggers like gdb are also used.

**MULTIMEDIA**

**Multimedia** refers to content that uses a combination of different content forms. This contrasts with media that use only rudimentary computer displays such as text-only or traditional forms of printed or hand-produced material. Multimedia includes a combination of text, audio, still images, animation, video, or interactivity content forms.

Multimedia is usually recorded and played, displayed, or accessed by information content processing devices, such as computerized and electronic devices, but can also be part of a live performance. Multimedia devices are electronic media devices used to store and experience multimedia content. Multimedia is distinguished from mixed media in fine art; by including audio, for example, it has a broader scope. The term "rich media" is synonymous for interactive multimedia. Hypermedia can be considered one particular multimedia application.

**Categorization of multimedia**

Multimedia may be broadly divided into **linear** and **non-linear** categories. Linear active content progresses often without any navigational control for the viewer such as a cinema presentation. Non-linear uses interactivity to control progress as with a video game or self-paced computer based training. Hypermedia is an example of non-linear content.

Multimedia presentations can be **live** or **recorded**. A recorded presentation may allow interactivity via a navigation system. A live multimedia presentation may allow interactivity via an interaction with the presenter or performer.

**Major characteristics of multimedia**

**Multimedia presentations** may be viewed by person on stage, projected, transmitted, or played locally with a media player. A broadcast may be a live or recorded multimedia presentation. Broadcasts and recordings can be either analog or digital electronic media technology. Digital online multimedia may be downloaded or streamed. Streaming multimedia may be live or on-demand.

**Multimedia games and simulations** may be used in a physical environment with special effects, with multiple users in an online network, or locally with an offline computer, game system, orsimulator.

The various formats of technological or digital multimedia may be intended to enhance the users' experience, for example to make it easier and faster to convey information. Or in entertainment or art, to transcend everyday experience.



magnify-clip

A lasershow is a live multimedia performance.

Enhanced levels of interactivity are made possible by combining multiple forms of media content. Online multimedia is increasingly becoming object-oriented and data-driven, enabling applications with collaborative end-user innovation and personalization on multiple forms of content over time. Examples of these range from multiple forms of content on Web sites like photo galleries with both images (pictures) and title (text) user-updated, to simulations whose co-efficients, events, illustrations, animations or videos are modifiable, allowing the multimedia "experience" to be altered without reprogramming. In addition to seeing and hearing, Haptic technology enables virtual objects to be felt. Emerging technology involving illusions of taste and smell may also enhance the multimedia experience.

**Usage / Application**

### Creative industries

#### Commercial uses

#### Entertainment and fine arts

#### Education

#### Journalism

#### Engineering

#### Industry

#### Mathematical and scientific research

#### Medicine

#### Document imaging

#### Disabilities

## WEB TECHNOLOGY

## Introduction

There are many Web technologies, from simple to complex, and explaining each in detail is beyond the scope of this article. However, to help you get started with developing your own Web sites, beyond simple WYSIWYG designing of Web pages in FrontPage, this article provides brief definitions of the major Web technologies along with links to sites where you can find more information, tutorials, and reference documentation.

**Important**   The links included in this article are only a representative set of resources that are available on the Internet. Where appropriate, this article cites Microsoft resources, but you can also find many links to non-Microsoft resources. You can locate additional resources by performing your own Web searches.

## Markup Languages

Markup is used to in text and word processing documents to describe how a document should look when displayed or printed. The Internet uses markup to define how Web pages should look when displayed in a browser or to define the data contained within a Web document.

There are many different types of markup languages. For example, Rich Text Formatting (RTF) is a markup language that word processors use. This section describes the most common markup languages that are used on the Internet.

### HTML

HTML stands for Hypertext Markup Language. HTML is the primary markup language that is used for Web pages. HTML tells the browser what to display on a page. For example, it specifies text, images, and other objects and can also specify the appearance of text, such as bold or italic text.

The World Wide Web Consortium (W3C) defines the specification for HTML. The current versions of HTML are HTML 4.01 and XHTML 1.1.

**Note**   DHTML stands for Dynamic HTML. DHTML combines cascading style sheets (CSS) and scripting to create animated Web pages and page elements that respond to user interaction.

For more information on HTML, see the following resources.

### CSS

CSS stands for cascading style sheets. Cascading style sheets provide the ability to change the appearance of text (such as fonts, colors, spacing) on Web pages. Using CSS, you can also position elements on the page, make certain elements hidden, or change the appearance of the browser, such as changing the color of scroll bars in Microsoft Internet Explorer.

Cascading style sheets can be used similar to FrontPage Themes. For example, you can apply a cascading style sheet across all the pages in a Web site to give the site a uniform look and feel. Then all you need to do is to change the CSS style formatting in a single file to change the look and feel of an entire Web site.

For more information on CSS, see the following resources.

### XML

XML stands for Extensible Markup Language. Similar to HTML, XML is a markup language designed for the Internet. However, unlike HTML, which was designed to define formatting of Web pages, XML was designed to describe data. You can use XML to develop custom markup languages.

As with HTML, the W3C defines the specifications for XML. See Extensible Markup Language on the W3C Web site.

For more information on XML, see the following resources.

### XSLT

XSLT is an abbreviation for XSL Transformations. XSLT uses the Extensible Stylesheet Language (XSL), which you use to define the appearance of an XML document or change an XML document into another kind of document—XML, HTML, or another markup language format.

As with other Web markup languages, the W3C defines the specifications for XSL and XSLT.

For more information on XSLT, see the following resources.

**INFORMATION SECURITY AND ASSURANCE**

Perhaps security has always been an issue to humans. Ancient humans must have found locations where they could secure their families from attacks by wild animals or from unfriendly neighbors. They built houses to keep themselves safe and secure from bad weather. Computing technology has given the topic of security an all new meaning. Computing technology creates new opportunities and new tools for attack, and crime has unfortunately followed. The 2006 eCrime Survey of United States companies, universities and governmental groups reported that the average reporting business lost over $740,000 to computer security in 2005

The term “computer security” isn’t quite proper, because a computer is only a container. It is actually, the information that is contained within the computer that needs to be secured. By securing a computer we are, in fact, assuring the security of the information. Therefore, another common name for a course like this is Information Assurance.

Before we start to examine computer security/information assurance, it is important to recognize that there is a lot to learn from our past. We can learn much about security by exploring history. The very earliest men probably realized that their tribe was safer when split into separate groups, just like we know that backup data should be stored in a site that is separate from the associated computer files. Just like the Great Wall of China was built to keep out hostile outsiders, we use firewalls to keep out hostile network traffic.

So many of our computer security mechanisms aren’t new at all; although clearly technology has introduced many new concepts. From the beginning security starts with that which we are trying to secure, namely the asset. The assets we secure on a computer might be important company secrets that could be valuable to a competing company or personal information such as the course grades of a university student or even money, since banks now process most money electronically.

The term threat refers to any potentially harmful circumstance or event. Security systems are created for the purpose of protecting assets against threats. If our computer is threatened by viruses, then our security system may include such things as antivirus software, network firewalls and file protection mechanisms to guard against this threat. Sometimes computer scientists confuse the term “threat” with “vulnerability”.

However, the difference is that a threat comes from outside the asset, while a vulnerability is a weakness within the security system intended to protect the asset. No system is ever completely secure, because every system has vulnerabilities. However, damage does not occur unless there is an attack which is defined as a deliberate attempt to exploit a vulnerability. Any mechanism that is designed to guard against a vulnerability is called a mitigation.

Some computer scientists make the distinction between security and safety in terms of intent. Intentional attacks, such as theft and vandalism, are generally the purpose of security; while unintentional attacks, like floods and fire, relate more to safety. Often it is difficult to separate the concepts of security and safety, since many security systems mitigate against both kinds of vulnerabilities.

Computer security begins with even a simple single computer. Every operating system contains flaws that provide vulnerabilities to an attacker. Microsoft Windows operating systems are well known for security problems, but vulnerabilities have been published for others as well. Flaws in software extend to application software also. There are vulnerabilities in applications from email clients to web browsers. While software flaws are a major source or vulnerabilities, perhaps the greatest cause of security problems is simply user ignorance. Users often behave in ways that are insecure - from using their family name as a password to revealing their login information to a stranger, humans are often the greatest security vulnerability.

Vulnerabilities multiply when a single computer is connected to a local area network (LAN). LANs introduce the potential for poor (shoddy) network configuration. For example, many people install wireless hubs in their homes without establishing security protocols and passwords. In such a situation anyone sitting within the transmission range of the wireless hub has unauthorized access.

Even though there are vulnerabilities in every computer and every LAN, the greatest number of vulnerabilities appear only when the computer is connected to the Internet. The Internet is vulnerable to attackers from all over the world - some attackers who are extremely sophisticated and some attackers, called script kiddies, who are not. In addition, there are known weaknesses with network protocols and flaws in the countless servers on the Internet; all of these are vulnerabilities for the computer user connected to the Internet.

It is impossible to list all computer security attacks. It is even difficult to classify attacks. Throughout this course we will examine types of attacks such as Denial of Service (DoS), password cracking, social engineering (including phishing), as well as look at the causes of viruses. But the attacks constantly change. In September, 2004, here were 100 known phishing1 websites; by December the number had increased to 700.

With all of these security-related problems and weaknesses, how do we mitigate the vulnerabilities? There are five major categories of defense to be studied: (1) prevention - prevent an attack from ever occurring, (2) deterrence - deter the attacker in such a way that the risk to the attacker is not worth the potential benefit. (3) deflection - sometimes it is possible to avoid attack by convincing the attacker to attack elsewhere. (4) Detection - sometimes attacks are unpreventable, but detecting that an attack has taken place is often important to best survive the attack. (5) Recovery - once an attack has been detected the computer and/or user should attempt to recover by repairing damages.

Prevention is only a goal; it is not possible to prevent attacks on any practical computer. So we approximate prevention by constructing security systems based upon deflection, deterrence, detection and recovery. Think about all of the security mechanisms you know and which kind (or kinds) of defense they provide. File encryption is a deterrence and possibly a deflection to files that aren’t encrypted. File backups are for recovery. The second word in the name of IDS (Intrusion Detection Systems) identifies their defense category.

**Information security**, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)[1]

Two major aspects of information security are:

* **IT security**: Sometimes referred to as computer security, Information Technology Security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory (even a calculator). IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.
* **Information assurance**: The act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

### Key concepts[edit]

The CIA triad (confidentiality, integrity and availability) is one of the core principles of information security.[11] (The members of the classic InfoSec triad -confidentiality, integrity and availability - are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.) There is continuous debate about extending this classic trio.[2][*citation needed*] Other principles such as Accountability[12] have sometimes been proposed for addition – it has been pointed out[*citation needed*] that issues such as Non-Repudiation do not fit well within the three core concepts, and as regulation of computer systems has increased (particularly amongst the Western nations) Legality is becoming a key consideration for practical security installations.

#### Confidentiality[edit]

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary for maintaining the privacy of the people whose personal information is held in the system.

#### Integrity[edit]

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.[16] This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACIDmodel of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

#### Availability[edit]

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

#### Authenticity[edit]

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

#### Non-repudiation[edit]

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

### Security classification for information[edit]

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The Business Model for Information Security enables security professionals to examine security from systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

* In the business sector, labels such as: **Public, Sensitive, Private, Confidential**.
* In the government sector, labels such as: **Unclassified**, **Sensitive But Unclassified**, **Restricted**, **Confidential**, **Secret**, **Top Secret** and their non-English equivalents.
* In cross-sectoral formations, the Traffic Light Protocol, which consists of: **White, Green, Amber**, and **Red**.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification of a particular information asset that has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.

### Access control[edit]

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication.

Access control is generally considered in three steps: Identification, Authentication, and Authorization.

#### Identification[edit]

**Identification** is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe" they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe. Typically the claim is in the form of a username. By entering that username you are claiming "I am the person the username belongs to".

#### Authentication[edit]

**Authentication** is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe—a claim of identity. The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be. Similarly by entering the correct password, the user is providing evidence that they are the person they username belongs to.

There are three different types of information that can be used for authentication:

* Something you know: things such as a PIN, a password, or your mother's maiden name.
* Something you have: a driver's license or a magnetic swipe card.
* Something you are: biometrics, including palm prints, fingerprints, voice prints and retina (eye) scans.

Strong authentication requires providing more than one type of authentication information (two-factor authentication). The username is the most common form of identification on computer systems today and the password is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate.[*citation needed*] Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

#### Authorization[edit]

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called **authorization**. Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies. Different computing systems are equipped with different kinds of access control mechanisms—some may even offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The **non-discretionary** approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The **discretionary approach** gives the creator or owner of the information resource the ability to control access to those resources. In the **Mandatory access control approach**, access is granted or denied basing upon the security classification assigned to the information resource.

Examples of common access control mechanisms in use today include role-based access control available in many advanced database management systems—simple file permissions provided in the UNIX and Windows operating systems, Group Policy Objects provided in Windows network systems, Kerberos, RADIUS, TACACS, and the simple access lists used in many firewalls androuters.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held **accountable** for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail.[*citation needed*]

Also, **need-to-know principle** needs to be in affect when talking about access control. Need-to-know principle gives access rights to a person to perform their job functions. This principle is used in the government, when dealing with difference clearances. Even though two employees in different departments have a top-secret clearance, they must have a need-to-know in order for information to be exchanged. Within the need-to-know principle, network administrators grant the employee least amount privileges to prevent employees access and doing more than what they are supposed to. Need-to-know helps to enforce the confidential-integrity-availability (C‑I‑A) triad. Need-to-know directly impacts the confidential area of the triad.

### Cryptography[edit]

*Main article: Cryptography*

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU‑T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. Public key infrastructure (PKI) solutions address many of the problems that surround key management.