Data, Information, Knowledge, and Wisdom

by Gene Bellinger, Durval Castro, Anthony Mills

There is probably no segment of activity in the world attracting as much attention at present as that of knowledge management. Yet as I entered this arena of activity I quickly found there didn't seem to be a wealth of sources that seemed to make sense in terms of defining what knowledge actually was, and how was it differentiated from data, information, and wisdom. What follows is the current level of understanding I have been able to piece together regarding data, information, knowledge, and wisdom. I figured to understand one of them I had to understand all of them.

According to Russell Ackoff, a systems theorist and professor of organizational change, the content of the human mind can be classified into five categories:

1. **Data**: symbols
2. **Information**: data that are processed to be useful; provides answers to "who", "what", "where", and "when" questions
3. **Knowledge**: application of data and information; answers "how" questions
4. **Understanding**: appreciation of "why"
5. **Wisdom**: evaluated understanding.

Ackoff indicates that the first four categories relate to the past; they deal with what has been or what is known. Only the fifth category, wisdom, deals with the future because it incorporates vision and design. With wisdom, people can create the future rather than just grasp the present and past. But achieving wisdom isn't easy; people must move successively through the other categories.

A further elaboration of Ackoff's definitions follows:

Data... data is raw. It simply exists and has no significance beyond its existence (in and of itself). It can exist in any form, usable or not. It does not have meaning of itself. In computer parlance, a spreadsheet generally starts out by holding data.

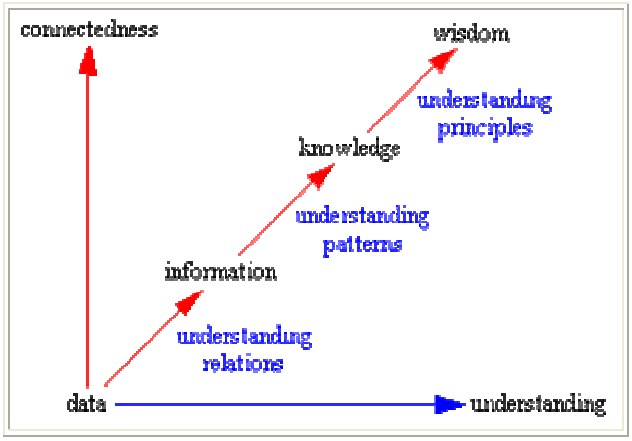
Information... information is data that has been given meaning by way of relational connection. This "meaning" can be useful, but does not have to be. In computer parlance, a relational database makes information from the data stored within it.

Knowledge... knowledge is the appropriate collection of information, such that it's intent is to be useful. Knowledge is a deterministic process. When someone "memorizes" information (as less-aspiring test-bound students often do), then they have amassed knowledge. This knowledge has useful meaning to them, but it does not provide for, in and of itself, an integration such as would infer further knowledge. For example, elementary school children memorize, or amass knowledge of, the "times table". They can tell you that "2 x 2 = 4" because they have amassed that knowledge (it being included in the times table). But when asked what is "1267 x 300", they can not respond correctly because that entry is not in their times table. To correctly answer such a question requires a true cognitive and analytical ability that is only encompassed in the next level... understanding. In computer parlance, most of the applications we use (modeling, simulation, etc.) exercise some type of stored knowledge.

Understanding... understanding is an interpolative and probabilistic process. It is cognitive and analytical. It is the process by which I can take knowledge and synthesize new knowledge from the previously held knowledge. The difference between understanding and knowledge is the difference between "learning" and "memorizing". People who have understanding can undertake useful actions because they can synthesize new knowledge, or in some cases, at least new information, from what is previously known (and understood). That is, understanding can build upon currently held information, knowledge and understanding itself. In computer parlance, AI systems possess understanding in the sense that they are able to synthesize new knowledge from previously stored information and knowledge.

Wisdom... wisdom is an extrapolative and non-deterministic, non-probabilistic process. It calls upon all the previous levels of consciousness, and specifically upon special types of human programming (moral, ethical codes, etc.). It beckons to give us understanding about which there has previously been no understanding, and in doing so, goes far beyond understanding itself. It is the essence of philosophical probing. Unlike the previous four levels, it asks questions to which there is no (easily-achievable) answer, and in some cases, to which there can be no humanly-known answer period. Wisdom is therefore, the process by which we also discern, or judge, between right and wrong, good and bad. I personally believe that computers do not have, and will never have the ability to posses wisdom. Wisdom is a uniquely human state, or as I see it, wisdom requires one to have a soul, for it resides as much in the heart as in the mind. And a soul is something machines will never possess (or perhaps I should reword that to say, a soul is something that, in general, will never possess a machine).

Personally I contend that the sequence is a bit less involved than described by Ackoff. The following diagram represents the transitions from data, to information, to knowledge, and finally to wisdom, and it is understanding that support the transition from each stage to the next. Understanding is not a separate level of its own.



Data represents a fact or statement of event without relation to other things.

Ex: It is raining.

Information embodies the understanding of a relationship of some sort, possibly cause and effect.

Ex: The temperature dropped 15 degrees and then it started raining.

Knowledge represents a pattern that connects and generally provides a high level of predictability as to what is described or what will happen next.

Ex: If the humidity is very high and the temperature drops substantially the atmospheres is often unlikely to be able to hold the moisture so it rains.

Wisdom embodies more of an understanding of fundamental principles embodied within the knowledge that are essentially the basis for the knowledge being what it is. Wisdom is essentially systemic.

Ex: It rains because it rains. And this encompasses an understanding of all the interactions that happen between raining, evaporation, air currents, temperature gradients, changes, and raining.

Yet, there is still a question regarding when is a pattern knowledge and when is it noise. Consider the following:

- Abugt dbesbt regtc uatn s uitrzt.
- ubtxte pstye ysote anet sser extess
- ibxtedstes bet3 ibtes otesb tapbesct ehracts

It is quite likely this sequence represents 100% novelty, which means it's equivalent to noise. There is no foundation for you to connect with the pattern, yet to me the statements are quite meaningful as I understand the translation with reveals they are in fact Newton's 3 laws of motion. Is something knowledge if you can't understand it?

Now consider the following:

- I have a box.
- The box is 3' wide, 3' deep, and 6' high.
- The box is very heavy.
- The box has a door on the front of it.
- When I open the box it has food in it.
- It is colder inside the box than it is outside.
- You usually find the box in the kitchen.
- There is a smaller compartment inside the box with ice in it.
- When you open the door the light comes on.
- When you move this box you usually find lots of dirt underneath it.
- Junk has a real habit of collecting on top of this box.

What is it?

A refrigerator. You knew that, right? At some point in the sequence you connected with the pattern and understood it was a description of a refrigerator. From that point on each statement only added confirmation to your understanding.

If you lived in a society that had never seen a refrigerator you might still be scratching your head as to what the sequence of statements referred to.

Also, realize that I could have provided you with the above statements in any order and still at some point the pattern would have connected. When the pattern connected the sequence of statements represented knowledge to you. To me all the statements convey nothing as they are simply 100% confirmation of what I already knew as I knew what I was describing even before I started.

WHAT YOU NEED TO KNOW ABOUT DECISIONS

1. All managers engage in problem solving and decision making.
2. This process is obviously apparent at all organizational levels.
3. Individual management decisions affect the entire organization.
4. A manager makes decisions constantly while performing the functions of planning, organizing, staffing, leading, and controlling.
5. Decision making is not a separate, isolated function of management, but rather a common core of the other functions. That is, it applies to all functions.
6. Decision making is universal and applicable throughout an organization.
7. Whether managers realize it or not, they must go through a process to make successful decisions on a regular basis.

SEVEN-STEP DECISION-MAKING PROCESS

A. Defining the Problem or Opportunity

1. Defining the problem is the critical step.
2. The accurate definition of a problem affects all the steps that follow; if a problem is inaccurately defined, every other step in the decision-making process will be based on that incorrect point.
3. A manager needs to focus on the problem and its causes, not the symptoms.
4. A tool a manager can use is the funnel approach.
5. The consequences of not properly defining the problem are wasted time and energy.

B. Identifying Limiting Factors

1. Limiting factors are those constraints that rule out certain alternative solutions.
2. Limitations include the following resources: personnel, money, facilities, equipment, and time.

C. Developing Potential Alternatives

1. Alternatives are solutions to the problem.
2. The alternatives should eliminate, correct, or neutralize the problem.
3. While building the list of alternatives, it is wise to avoid being critical or judgmental about any alternative that occurs to you or those assisting you.
4. Initially, the alternatives should be separate and distinct solutions to the problem.
5. After the initial list is developed, variations will develop and combinations will emerge.
6. Sources for alternatives include past experience; other persons whose opinions and judgments are respected; the practice of successful managers; group opinions through the use of task forces and committees; and the use of outside resources, including managers in other organizations.

D. Analyzing the Alternatives

1. The purpose of this step is to decide the relative merits of each alternative.
2. Depending on the type of problem and the potential solutions developed, the manager might need to make a more thorough analysis by applying specific decision-making aids.

E. Selecting the Best Alternative

1. Sometimes the optimal solution is a combination of several of the alternatives.
2. Find a solution that appears to offer the fewest serious disadvantages and the most advantages.

F. Implementing the Decision

1. Managers are paid to make decisions, but they are also paid to get results from these decisions. Results must follow decisions.
2. Everyone involved with the decision must know what he or she must do, how to do it, why to do it, and when to do it.
3. Programs, procedures, rules, or policies must be thoughtfully put into effect. Carelessness at this stage causes problems.

G. Establishing a Control and Evaluation System

1. Ongoing actions need to be monitored. They cannot be forgotten.
2. The system should provide feedback on how well the decision is being implemented, what the results are, and what adjustments are necessary to get results that were wanted when the solution was chosen.

Information Systems: Definitions and Components

What Is an Information System?

Information system has been defined in terms of two perspectives: one relating to its function; the other relating to its structure. From a **functional perspective**; an information system is a technologically implemented medium for the purpose of recording, storing, and disseminating linguistic expressions as well as for the supporting of inference making. From a **structural perspective**; an information system consists of a collection of people, processes, data, models, technology and partly formalized language, forming a cohesive structure which serves some organizational purpose or function.

The functional definition has its merits in focusing on what actual users - from a conceptual point of view- do with the information system while using it. They communicate with experts to solve a particular problem. The structural definition makes clear that IS are socio-technical systems, i.e., systems consisting of humans, behavior rules, and conceptual and technical artifacts.

An information system can be defined ***technically*** as a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organization. In addition to supporting decision making, coordination, and control, information systems may also help managers and workers analyze problems, visualize complex subjects, and create new products.

Three activities in an information system produce the information that organizations need to make decisions, control operations, analyze problems, and create new products or services. These activities are input, processing,

and output. Input captures or collects raw data from within the organization or from its external environment. Processing converts this raw input into a more meaningful form. Output transfers the processed information to the people who will use it or to the activities for which it will be used. Information systems also require feedback, which is output that is returned to appropriate members of the organization to help them evaluate or correct the input stage.

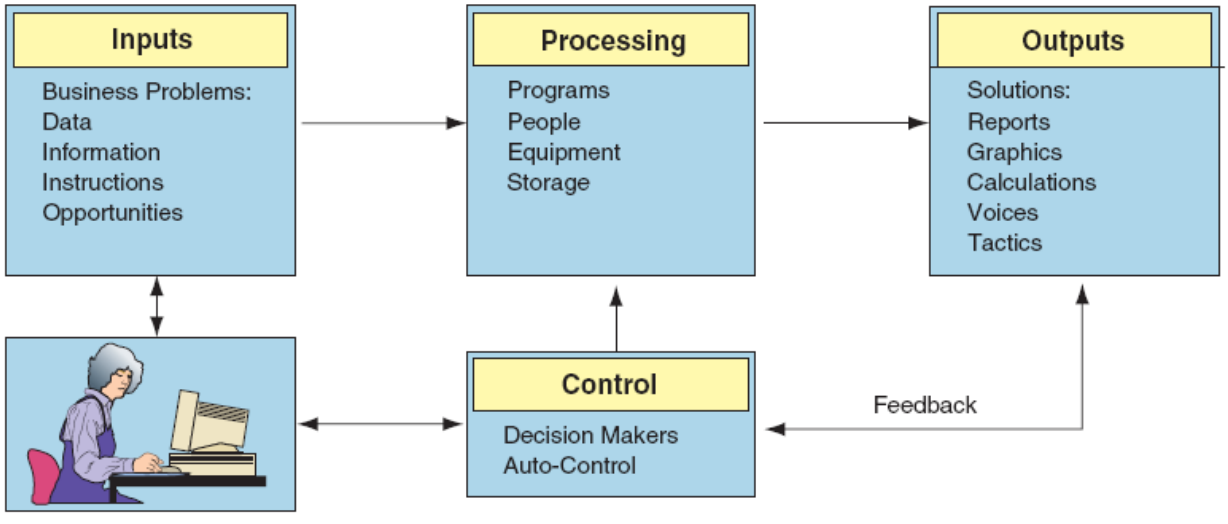


Figure 6: Functions of an information system

What Is A Computer-Based Information System?

A computer-based information system (CBIS) is an information system that uses computer technology to perform some or all of its intended tasks. Such a system can include as little as a personal computer and software. Or it may include several thousand computers of various sizes with hundreds of printers, plotters, and other devices, as well as communication networks (wire-line and wireless) and databases. In most cases an information system also includes people. The basic components of information systems are listed below. Note that not every system includes all these components.

Components of Information Systems

1. Resources of people: (end users and IS specialists, system analyst, programmers, data administrators etc.).
2. Hardware: (Physical computer equipments and associate device, machines and media).
3. Software: (programs and procedures).
4. Data: (data and knowledge bases), and
5. Networks: (communications media and network support).

People Resources

- End users: (also called users or clients) are people who use an information system or the information it produces. They can be accountants, salespersons, engineers, clerks, customers, or managers. Most of us are information system end users.
- IS Specialists: people who actually develop and operate information systems. They include systems analysts, programmers, testers, computer operators, and other managerial, technical, and clerical IS personnel. Briefly, systems analysts design information systems based on the information requirements of end uses, programmers prepare computer programs based on the specifications of systems analysts, and computer operators operate large computer systems.

Hardware Resources

- Machines: as computers and other equipment along with all data media, objects on which data is recorded and saved.
- Computer systems: consist of variety of interconnected peripheral devices. Examples are microcomputer systems, midrange computer systems, and large computer systems.

Software Resources

Software Resources includes all sets of information processing instructions. This generic concept of software includes not only the programs, which direct and control computers but also the sets of information processing (procedures). Software Resources includes:

- System software, such as an operating system
- Application software, which are programs that direct processing for a particular use of computers by end users.
- Procedures, which are operating instructions for the people, who will use an information system. Examples are instructions for filling out a paper form or using a particular software package.

Data Resources

Data resources include data (which is raw material of information systems) and database. Data can take many forms, including traditional alphanumeric data, composed of numbers and alphabetical and other characters that describe business transactions and other events and entities. Text data, consisting of sentences and paragraphs used in written

communications; image data, such as graphic shapes and figures; and audio data, the human voice and other sounds, are also important forms of data. Data resources must meet the following criteria:

- Comprehensiveness: means that all the data about the subject are actually present in the database.
- Non-redundancy: means that each individual piece of data exists only once in the database.
- Appropriate structure: means that the data are stored in such a way as to minimize the cost of expected processing and storage.

The data resources of IS are typically organized into:

- Processed and organized data-Databases.
- Knowledge in a variety of forms such as facts, rules, and case examples about successful business practices.

Network Resources

Telecommunications networks like the Internet, intranets, and extranets have become essential to the successful operations of all types of organizations and their computer-based information systems. Telecommunications networks consist of computers, communications processors, and other devices interconnected by communications media and controlled by communications software. The concept of Network Resources emphasizes that communications networks are a fundamental resource component of all information systems. Network resources include:

- Communications media: such as twisted pair wire, coaxial cable, fiber-optic cable, microwave systems, and communication satellite systems.
- Network support: This generic category includes all of the people, hardware, software, and data resources that directly support the operation and use of a communications network. Examples include communications control software such as network operating systems and Internet packages.

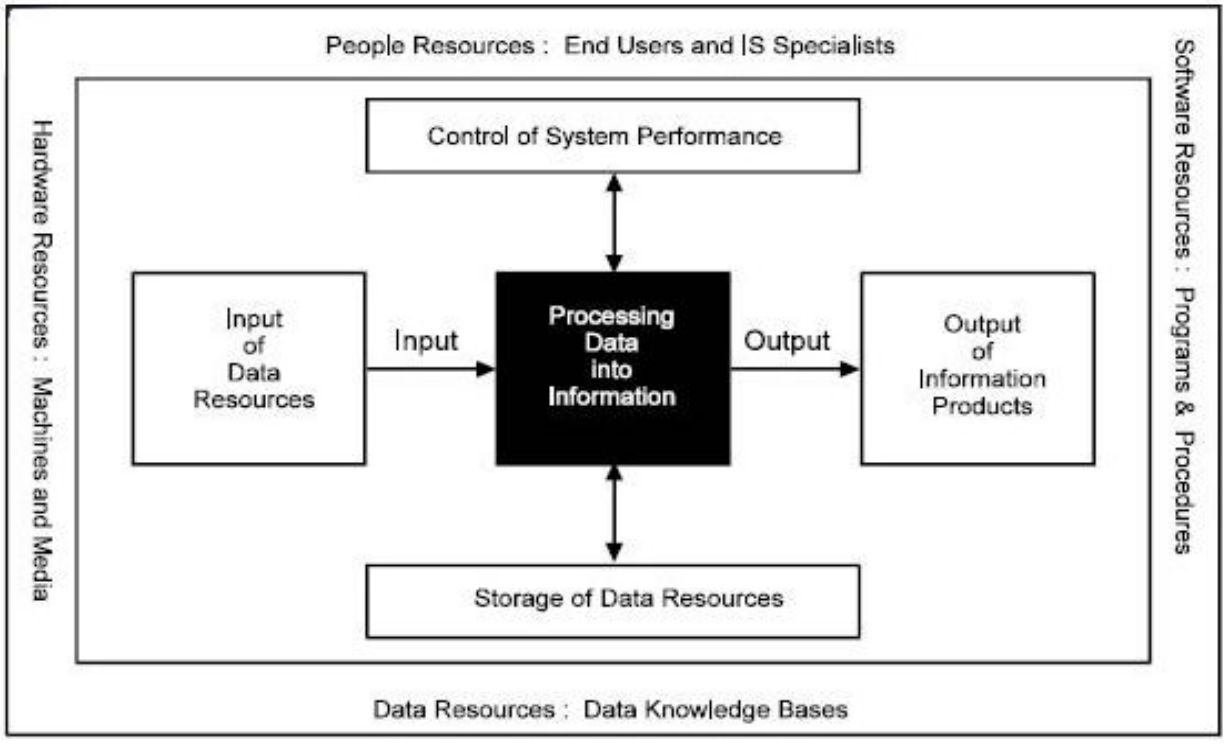


Figure 7: Components of Information System

Difference between Computers and Information Systems

Computers provide effective and efficient ways of processing data, and they are a necessary part of an information system. An IS, however, involves much more than just computers. The successful application of an IS requires an understanding of the business and its environment that is supported by the

IS. For example, to build an IS that supports transactions executed on the New York Stock Exchange, it is necessary to understand the procedures related to buying and selling stocks, bonds, options, and so on, including irregular demands made on the system, as well as all related government regulations.

In learning about information systems, it is therefore not sufficient just to learn about computers. Computers are only one part of a complex system that must be designed, operated, and maintained. A public transportation system in a city provides an analogy. Buses are a necessary ingredient of the system, but more is needed. Designing the bus routes, bus stops, different schedules, and so on requires considerable understanding of customer demand, traffic patterns, city regulations, safety requirements, and the like. Computers, like buses, are only one component in a complex system.

Information Technology and Information Systems

Information technology broadly defined as the collection of computer systems used by an organization. Information technology, in its narrow definition, refers to the technological side of an information system. It includes the hardware, software, databases, networks, and other electronic devices. It can be viewed as a subsystem of an information system. Sometimes, though, the term information technology is also used interchangeably with information system.

The term IT in its broadest sense used to describe an organization's collection of information systems, their users, and the management that oversees them.

A major role of IT is being a *facilitator* of organizational activities and processes. That role will become more important as time passes. Therefore, it is necessary that every manager and professional staff member learn about IT not only in his or her specialized field, but also in the entire organization and in inter-organizational settings as well.

Obviously, you will be more effective in your chosen career if you understand how successful information systems are built, used, and managed. You also will be more effective if you know how to recognize and avoid unsuccessful systems and failures. Also, in many ways, having a comfort level with information technology will enable you, off the job and in your private life, to take advantage of new IT products and systems as they are developed. (Wouldn't you rather be the one explaining to friends how some new product works, than the one asking about it?) Finally, you should learn about IT because being knowledgeable about information technology can also increase employment opportunities. Even though computerization eliminates some jobs, it also creates many more.

The demand for traditional information technology staff—such as programmers, systems analysts, and designers—is substantial. In addition, many excellent opportunities are appearing in emerging areas such as the Internet and e-commerce, m-commerce, network security, object-oriented programming, telecommunications, multimedia design, and document management.

According to a study by the U.S. Bureau of Labor Statistics, each of the top seven fastest-growing occupations projected through 2010 fall within an IT- or computer related field. These top seven occupations are:

1. Computer software applications engineers

2. Computer support specialists

3. Computer software systems engineers

4. Network and computer systems administrators

5. Network systems and data communications analysts

6. Desktop publishers

7. Database administrators

To exploit the high-paying opportunities in IT, a college degree in any of the following fields, or combination of them, is advisable: computer science, computer information systems (CIS), management information systems (MIS), electronic commerce, and e-business. Within the last few years, many universities have started e-commerce or e-business degrees. Many schools offer graduate degrees with specialization in information technology.

Classification and Evolution of Information Systems

Introduction

Information systems are made out of components that can be assembled in many different configurations, resulting in a variety of information systems and applications, much as construction materials can be assembled to build different homes types. The size and cost of a home depend on the purpose of the building, the availability of money, and constraints such as ecological and environmental legal requirements. Just as there are many different types of houses, so there are many different types of information systems. It is useful to classify information systems into groups that share similar characteristics. Such a classification may help in identifying systems, analyzing them, planning new systems, planning integration of systems, and making decisions such as the possible outsourcing of systems. This classification can be done in several alternative ways. Information systems are classified by organizational levels, mode of data processing, system objectives, and by the type of support provided.

1. Classification by Organizational Levels

Organizations are made up of components such as divisions, departments, and work units, organized in hierarchical levels. For example, most organizations have functional departments, such as production and accounting, which report to plant management, which report to a division head. The divisions report to the corporate headquarters. Although some organizations have restructured themselves in innovative ways, such as those based on cross-functional teams, today the vast majority of organizations still

have a traditional hierarchical structure. Thus, we can find information systems built for headquarters, for divisions, for the functional departments, for operating units, and even for individual employees. Such systems can stand alone, but usually they are interconnected.

Typical information systems that follow the organizational structure are ***functional*** (departmental), ***enterprise***, and ***inter-organizational***. These systems are organized in a hierarchy in which each higher-level system consists of several (even many) systems from the level below it. At a higher level, the enterprise system supports the entire company, and inter-organizational systems connect different companies.

- **Functional Information Systems**

Functional organizations are hierarchical structures and center on a strong concept of supervisors and subordinates. The controlling authority, often called top management, coordinates with each management level and functional department to keep the organization running smoothly. A functional organization analyzes the strengths and weaknesses of each member, groups them into categories and assigns them to tasks that best utilize their skills. Jobs that perform a similar function are grouped in functional areas. Each functional area contains employees with varied skills that are further grouped based on specialization and put in separate units or departments. Information systems which served these functional departments are called functional information systems.

Evolution of Functional Organizations

Functional organizations work best when a single product or service is involved. The chain of command is linear, so everyone knows his position in the organization. By clustering specialists with similar skills, leadership, tutoring and guidance concentrate on one area. Employees have an obvious path for growth and promotion, either up or lateral.

As a company gets larger, some of the positives of functional organizations become negatives. Since decisions travel through the chain of command, the process becomes bureaucratic, and information and decisions move slowly. Functional grouping can result in a narrowed overall perspective. Because of communication and decision-making issues, the functional organization is slow to adapt to environmental changes

- **Enterprise Information Systems**

While a departmental information system is usually related to a functional area, other information systems serve several departments or the entire enterprise. These information systems together with the departmental applications comprise the **enterprise information system** (EIS). One of the most popular enterprise applications is **enterprise resources planning** (ERP), which enables companies to plan and manage the resources of an entire enterprise. ERP systems present a relatively new model of enterprise computing now days.

- **Inter-organizational Information Systems**

Some information systems connect two or more organizations. They are referred to as inter-organizational information systems (IOS's). IOS's support many inter-organizational operations, of which supply chain management is the best known. An organization's **supply chain** describes the flow of materials, information, money, and services from raw material suppliers through factories and warehouses to the end customers. Note that the supply chain includes both physical flows and information flows. Information flows and digitizable products (e.g., music and software) go through the Internet, whereas physical products are shipped. For example, when you order a computer from *www.dell.com*, your information goes to Dell via the Internet. When your transaction is complete (i.e., your credit card is approved and your order is processed), Dell ships your computer to you. Figure below represents information flows and digitizable products (soft products) with dotted lines and physical products (hard products) as solid lines.

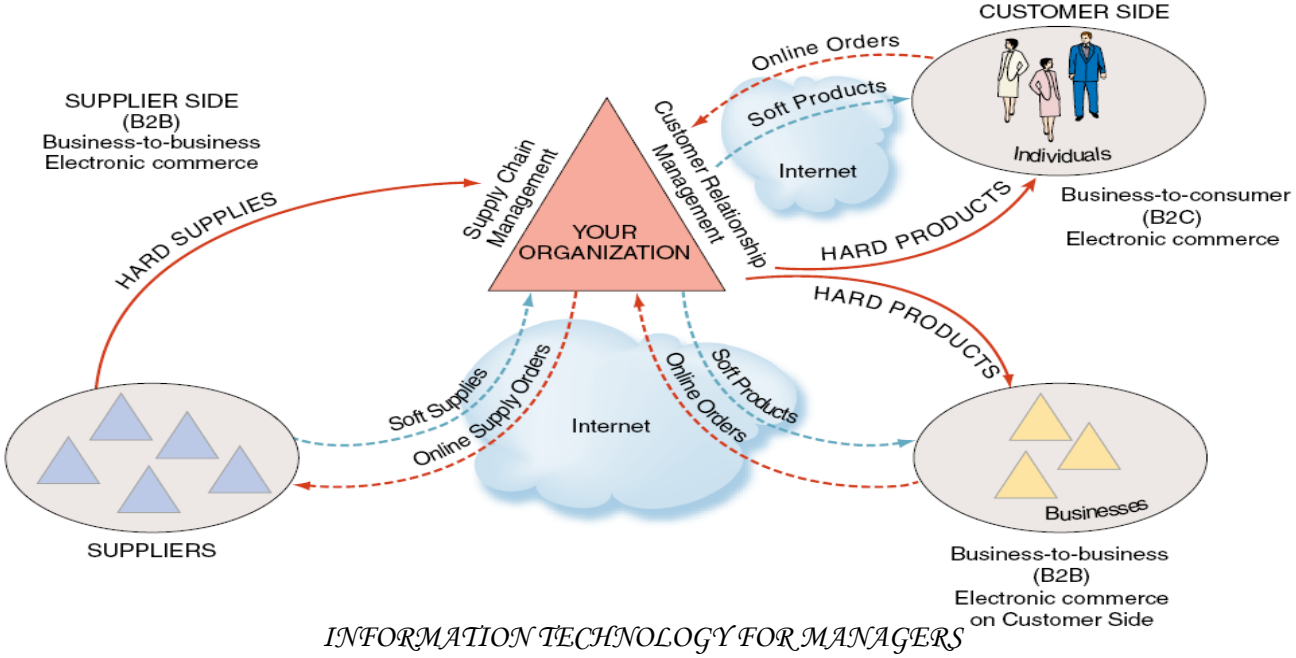


Figure 8: Information flows outside organization in inter-organizational information systems

Another example is the worldwide airline reservation system, which is composed of several systems belonging to different airlines. Thousands of travel agents and hundreds of airlines are connected to it. Those that support international or global operations may be especially complex. Inter-organizational information systems play a major role in e-commerce and other web-based e-government information systems applications.

2. Classification by Mode of Data Processing

- Batch Processing Systems: The transactions are collected as they occur, but processed periodically, say, once a day or week.
- On-line Batch Systems: The transaction information is captured by on-line data-entry devices and logged on the system, but it is processed periodically as in batch processing systems.
- On-line Real-time Systems: The transaction data capture as well as their processing in order to update records (and generate reports) is carried out in real-time as the transaction is taking place.

3. Classification by System Objectives

- Transaction Processing Systems (TPS): Their objective is to process transactions in order to update records and generate reports, i.e., to perform score-keeping functions.
- Process Control System (PCS): These systems are designed to make routine decision that control operational processes.
- Decision Support Systems (DSS): Their objective is to support the managerial decisions. Usually, these systems are based on a model of the

decision-making domain, and utilize techniques from management science, finance or other functional areas of business in order to build such models. These systems are also used often for attention-directing purposes, i.e., for directing the attention of managers to a problematic aspect of operations.

- Expert Systems (ES): These systems incorporate expertise in order to aid managers in diagnosing problems or in problem solving.
- Executive Information System (EIS): These are MIS tailored to the strategic information needs of the top managers.
- Business Information Systems (BIS): As a future managerial end user, it is very important to realize that information systems directly support both operations and management activities in business functions of accounting, finance, human resource management, marketing, and operations management. Such business information systems are needed by all business functions.

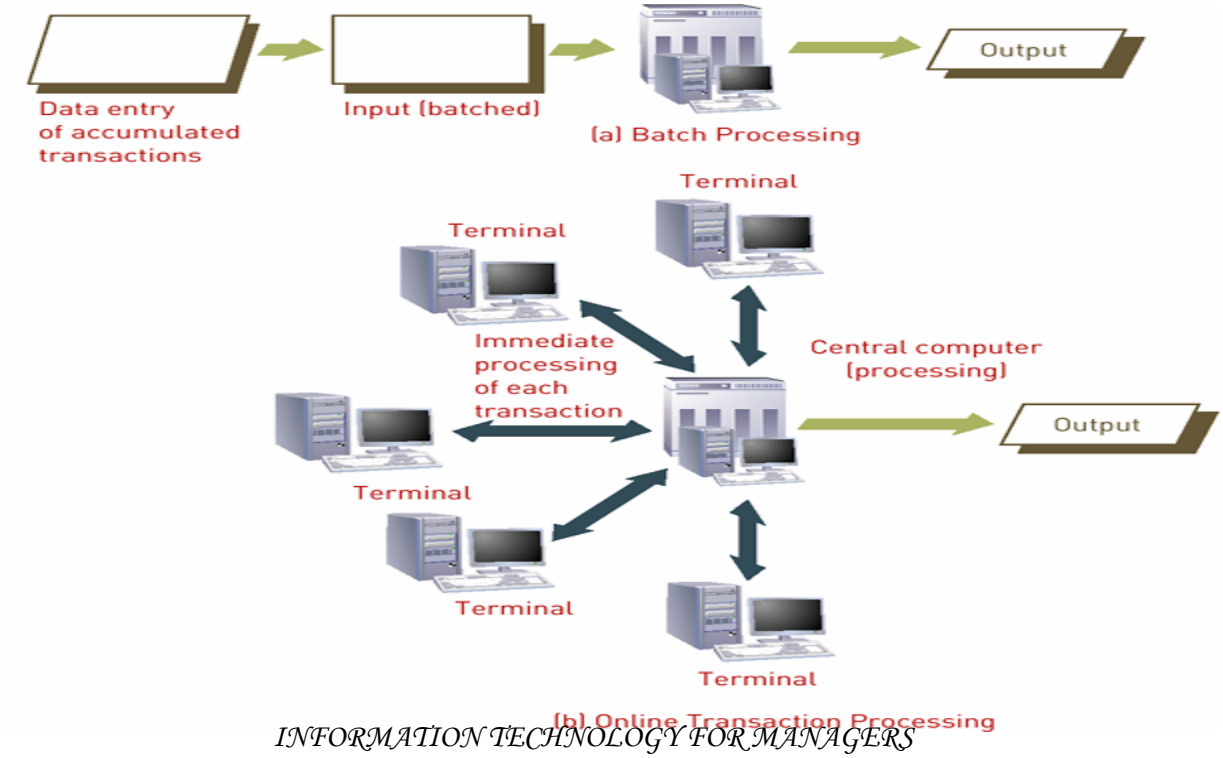


Figure 9: Modes of data processing

4. Classification by the Type of Support Provided

Another way to classify information systems is according to the type of support they provide, regardless of the functional area. For example, an information system can support office workers in almost any functional area. Likewise, managers working from various geographical locations can be supported by a computerized decision-making system.

Clerical workers, who support managers at all levels of the organization, include bookkeepers, secretaries, electronic file clerks, and insurance claim processors. Lower-level managers handle the day-to-day operations of the organization, making routine decisions such as assigning tasks to employees and placing purchase orders. Middle managers make tactical decisions, which deal with activities such as short-term planning, organizing, and control.

Knowledge workers are professional employees such as financial and marketing analysts, engineers, lawyers, and accountants. All knowledge workers are experts in a particular subject area. They create information and knowledge, which they integrate into the business. Knowledge workers act as advisors to middle managers and executives.

Finally, executives make decisions that deal with situations that can significantly change the manner in which business is done. Examples of executive decisions are introducing a new product line, acquiring other businesses, and relocating operations to a foreign country.

Office automation systems (OAS's) typically support the clerical staff, lower and middle managers, and knowledge workers. These employees use OAS to develop documents (word processing and desktop publishing

software), schedule resources (electronic calendars), and communicate (e-mail, voice mail, videoconferencing, and groupware).

Table 2: Types of Organizational Information Systems

Type of System	Function	Example
Functional area IS	Support the activities within specific functional area.	System for processing payroll
Transaction processing system	Process transaction data from business events.	Wal-Mart checkout point-of-sale terminal
Enterprise resource planning system	Integrate all functional areas of the organization.	Oracle, SAP
Office automation system	Support daily work activities of individuals and groups.	Microsoft Office
Management information system	Produce reports summarized from transaction data, usually in one functional area.	Report on total sales for each customer
Decision support system	Provide access to data and analysis tools.	"What-if" analysis of changes in budget
Expert system	Mimic human expert in a particular area and make a decision.	Credit card approval analysis
Executive information system	Present structured, summarized information about aspects of business important to executives.	Status of production by product
Supply chain management system	Manage flows of products, services, and information among organizations.	Wal-Mart Retail Link system connecting suppliers to Wal-Mart
Electronic commerce system	Enable transactions among organizations and between organizations and customers.	www.dell.com

Relationships between Information Systems and Organizations

Because there are different interests, specialties, and levels in an organization, there are different kinds of systems. No single system can provide all the information an organization needs. Figure (13) illustrates one way to depict the kinds of systems found in an organization. In the illustration, the organization is divided into strategic, management, and operational levels and then is further divided into functional areas, such as sales and marketing, manufacturing and production, finance and accounting, and human resources. Systems are built to serve these different organizational interests.

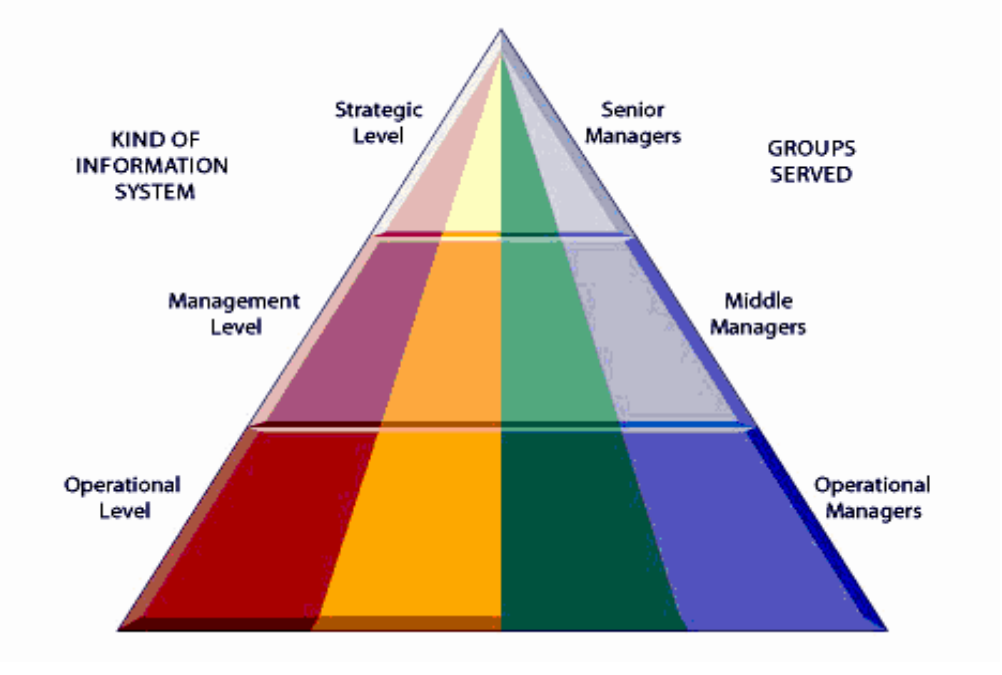


Figure: 13 Types of information systems

Different Kinds of Systems

Three main categories of information systems serve different organizational levels: operational-level systems, management-level systems, and strategic-level systems.

- **Operational-level systems:** support operational activities by keeping track of the elementary activities and transactions of the organization, such as assigning employees to tasks and recording the number of hours they work, or placing a purchase order. Operational activities are short-term in nature. The information systems that support them are mainly. Operational systems are used by supervisors (first-line managers), operators, and clerical employees. The principal purpose of systems at this level is to answer routine questions and to track the flow of transactions through the organization. How many parts are in inventory? What happened to Mr. Williams's payment? To answer these kinds of questions, information generally must be easily available, current, and accurate. Examples of operational-level systems include a system to record bank deposits from ATM (Automatic Teller Machines) or one that tracks the number of hours worked each day by employees on a factory floor.

- **Management-level systems:** serve the monitoring, controlling, decision-making, and administrative activities of middle managers. The principal question addressed by such systems is this: Are things working well? Management-level systems typically provide periodic reports rather than instant information on operations. Some management-level systems

support no routine decision making. They tend to focus on less-structured decisions for which information requirements are not always clear. These systems often answer "what-if" questions: What would be the impact on production schedules if we were to double sales in the next month? What would happen to our return on investment if a factory schedule were delayed for six months? Answers to these questions frequently require new data from outside the organization, as well as data from inside that cannot be easily drawn from existing operational-level systems. Management-level systems are broader in scope than operational-level systems, but like operational systems, they use mainly internal sources of data. They provide the types of support shown in Table 4.

Table: 4 Supports provided by MIS

Support Provided by MISs for Managerial Activities	
Task	**MIS Support**
Statistical summaries	Summaries of new data (e.g., daily production by item, monthly electricity usage).
Exception reports	Comparison of actual performances to standards (or target). Highlight only deviations from a threshold (e.g., above or below 5%).
Periodic reports	Generated at predetermined intervals.
Ad-hoc reports	Generated as needed, on demand. These can be routine reports or special ones.
Comparative analysis and early detection of problems	Comparison of performance to metrics or standards. Includes analysis such as trends and early detection of changes.
Projections	Projection of future sales, cash flows, market share, etc.
Automation of routine decision	Standard modeling techniques applied to routine decisions such as when and how much to order or how to schedule work.
Connection and collaboration	Internal and external Web-based messaging systems, e-mail, voice mail, and groupware

- **Strategic-level systems**: help senior management address strategic issues and long-term trends, both in the firm and in the external environment. Strategic activities are basically decisions that deal with situations that significantly may change the manner in which business is done. Traditionally, strategic decisions involved only long-range planning. A long-range planning document traditionally outlines strategies and plans for the next five or even 10 years. From this plan, companies derive their shorter-range planning, budgeting, and resource allocation. In the digital economy, the planning period has been dramatically reduced to one or two years, or even months.

Transaction Processing Systems

Transaction processing systems (TPS's) were among the earliest computerized systems. Their primary purpose is to record, process, validate, and store transactions that take place in the various functional areas of a business for future retrieval and use.

Transaction processing systems are cross-functional information systems that process data resulting from the occurrence of business transactions, such as sales, purchases, deposits, withdrawals, refunds, and payments. A TPS is also acts as main link between the organization and external entities, such as customers' suppliers, distributors, and regulatory agencies

Transaction processing systems serve the operational level of the organization. It is a computerized system that performs and records the daily routine transactions necessary to manage business; they serve the organization's operational level. The principal purpose of systems at this level is to answer routine questions and to track the flow of transactions through the organization. Examples are hotel reservation systems, payroll, employee record keeping, and shipping. At the operational level, tasks, resources, and goals are ***predefined and highly structured***. The decision to grant credit to a customer, for instance, is made by a lower level supervisor according to predefined criteria. All that must be determined is whether the customer meets the criteria. Figure (14) depicts a payroll TPS, which is a typical accounting transaction processing system found in most firms. A payroll system keeps track of the money paid to employees. The master file is composed of discrete pieces of information (such as a name, address, or employee number) called data elements. Data are keyed into the system,

updating the data elements. The elements on the master file are combined in different ways to make up reports of interest to management and government agencies and to send paychecks to employees. These TPS can generate other report combinations of existing data elements.

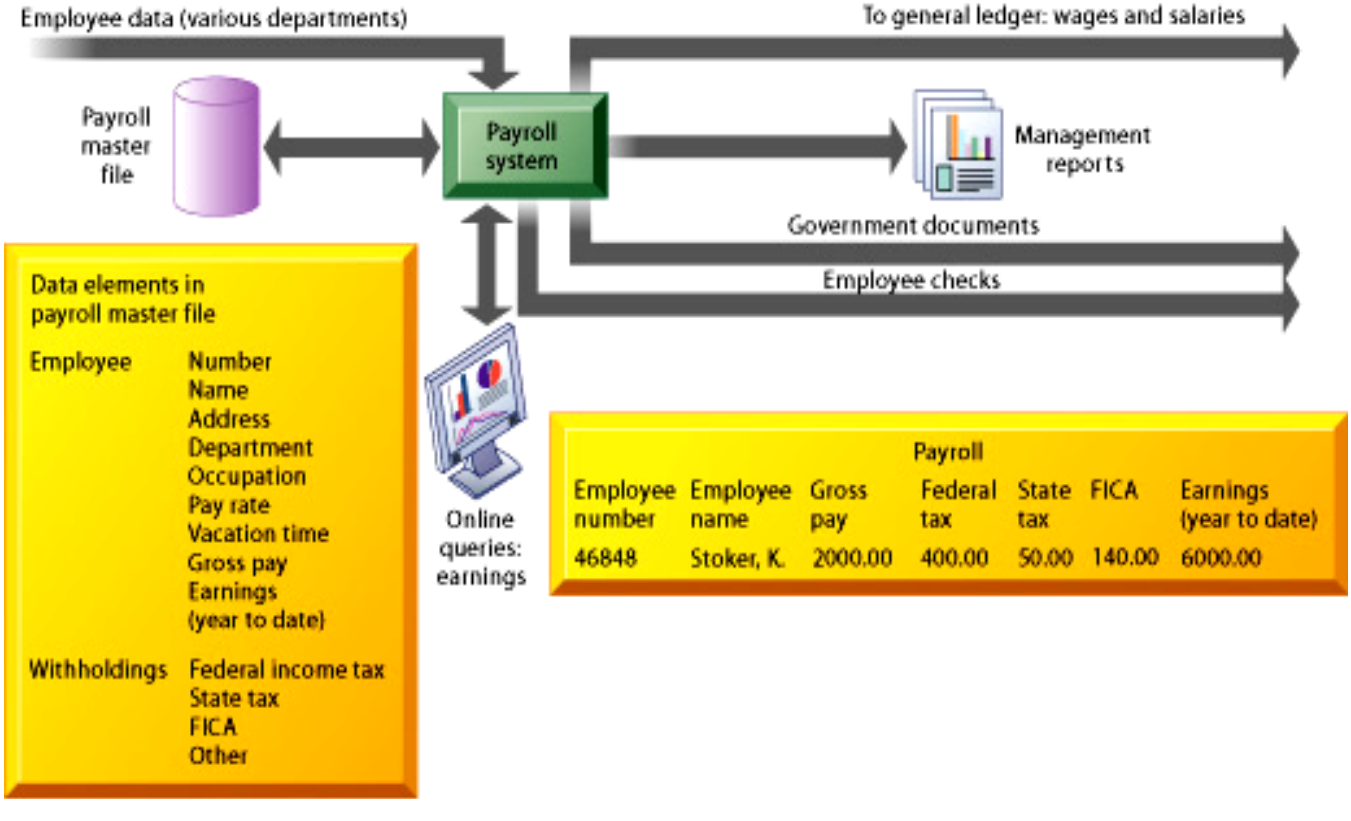


Figure: 14 A symbolic representation for a payroll TPS

A payroll system is a typical accounting TPS that processes transactions such as employee time cards and changes in employee salaries and deductions. It keeps track of money paid to employees, withholding tax, and paychecks.

Types of Transaction Processing System (TPS's)

1. **On-line system:** involves a direct connection between operator and the TPS program. They provide immediate result and used to process a single transaction at a time. Ex: an order arrives by telephone call; it is processed at that moment and the result are produced.
2. **Batch-processing system:** This is a second type of TPS, where transactions are grouped together and processed as a unit. Example: cheque processing system in a bank.

Types of Transactions:

1. **Internal Transactions:** Those transactions, which are internal to the company and are related with the internal working of any organization. For example Recruitment Policy, Promotion Policy, Production policy etc.
2. **External Transactions:** Those transactions, which are external to the organization and are related with the external sources, are regarded as External Transaction. For example sales, purchase etc.

TPS Properties:

1. **Consistency**: The transaction is a correct transformation of the state. This means that the transaction is a correct program.
2. **Isolation**: Even though transactions execute concurrently, it appears to the outside observer as if they execute in some serial order. Isolation is required to guarantee consistent input, which is needed for a consistent program to provide consistent output.

3. **Reliability**: TPS system is designed to ensure that all transactions are entered in sequential and systematic manner.
4. **Standardization**: Transactions must be processed in the same way each time to maximize efficiency and effectiveness.
5. **Controlled Access**: Since TPS also contains confidential matters or data; it acts as powerful tool for the organization. Hence access must be restricted.

Objectives (Goals) of TPS

1. Process data generated by and about transactions.
2. Maintain a high degree of accuracy.
3. Ensure data and information integrity and accuracy.
4. Produce timely documents and reports.
5. Increase labor efficiency.
6. Help provide increased and enhanced service.
7. Help build and maintain customer loyalty.
8. Achieve competitive advantage.

Major Characteristics of TPS

1. TPS handles data which shows the results of various activities on historical basis i.e., activities which have already happened.
2. It is relevant to all functional areas inside organization i.e. (production, marketing, finance and human resources) because each area has some kind of transaction.
3. TPS helps to assess the organizational performance.
4. The sources of data are mostly internal, and the output is intended mainly for an internal audience.

5. The TPS processes information on a regular basis: daily, weekly, monthly, annually etc.
6. It provides high processing speed to handle the high volume of data.
7. Input and output data are structured (i.e., standardized).
8. A high level of accuracy, data integrity, and security is needed which is provided by TPS.

Transaction Processing Activities

1. Data collection: Capturing data necessary for the transaction.
2. Data editing: Check validity and completeness of data.
3. Data correction: Correct the wrong data.
4. Data manipulation: Calculate, summarize, Process data.
5. Data storage: Update transactions (on Databases).
6. Document production and reports: Create end result reports.

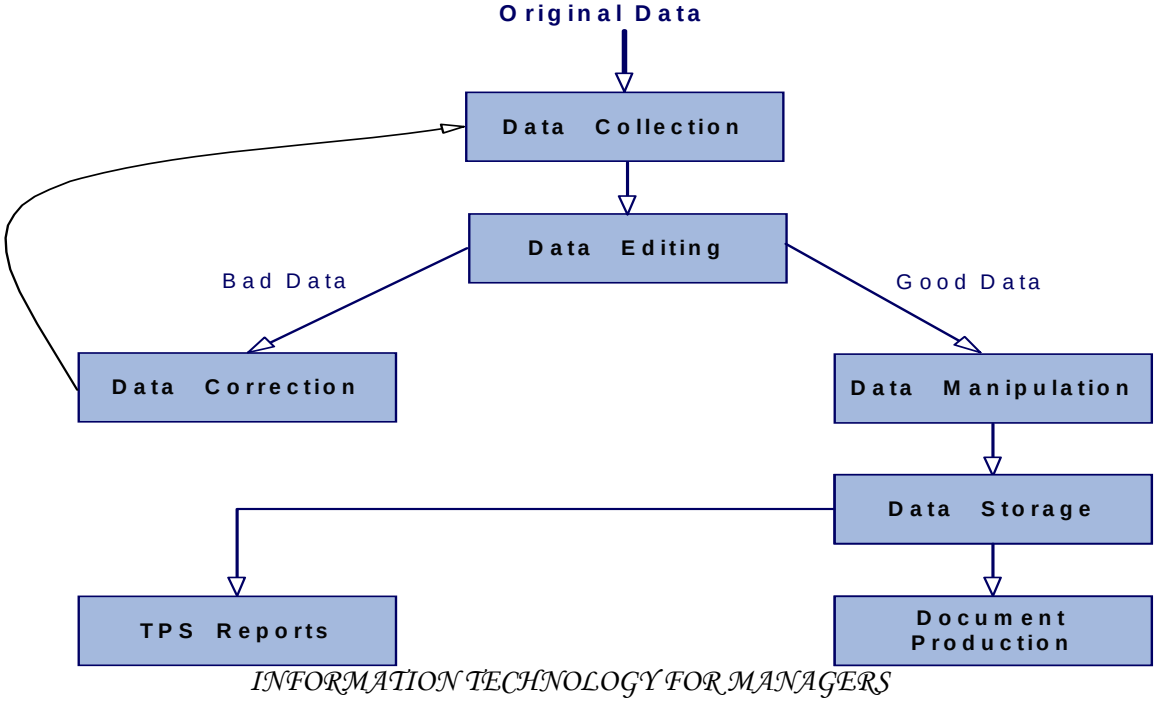


Figure 15: Transaction Processing Activities

COMPUTER SECURITY

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).

• **Confidentiality:** This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

• **Integrity:** This term covers two related concepts:

Data integrity: Assures that information and programs are changed only in specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

• **Availability:** Assures that systems work promptly and service is not denied to authorized users.

The Challenges of Computer Security

Computer and network security is both fascinating and complex. Some of the reasons follow:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, non-repudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

3. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].

5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

8. Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.

9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

The OSI security architecture is useful to managers as a way of organizing the task of providing security. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

• **Security attack:** Any action that compromises the security of information owned by an organization.

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

• **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

SECURITY ATTACKS

A useful means of classifying security attacks is in terms of *passive attacks* and *active attacks.*

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

An active attack attempts to alter system resources or affect their operation.

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

The **release of message contents: A** telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

A second type of passive attack is **traffic analysis:** If we had encryption protection in place, an

Opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect . For example, a message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *accounts.*"

The **denial of service** prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

SECURITY SERVICES

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

- ✓ **AUTHENTICATION:** The assurance that the communicating entity is the one that it claims to be.

  Peer Entity Authentication: Used in association with a logical connection to provide confidence in the identity of the entities connected.

  Data-Origin Authentication: In a connectionless transfer, provides assurance that the source of received data is as claimed.
- ✓ **ACCESS CONTROL:** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
- ✓ **DATA CONFIDENTIALITY:** The protection of data from unauthorized disclosure.

  Connection Confidentiality: The protection of all user data on a connection.

  Connectionless Confidentiality: The protection of all user data in a single data block

  Selective-Field Confidentiality: The confidentiality of selected fields within the user data on a connection or in a single data block.

  Traffic-Flow Confidentiality: The protection of the information that might be derived from observation of traffic flows.
- ✓ **DATA INTEGRITY :** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

  Connection Integrity with Recovery: Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

  Connection Integrity without Recovery: As above, but provides only detection without recovery.

  Selective-Field Connection Integrity: Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

  Connectionless Integrity: Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

  Selective-Field Connectionless Integrity: Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.
- ✓ **NONREPUDIATION:** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

  Nonrepudiation, Origin: Proof that the message was sent by the specified party.

  Nonrepudiation, Destination: Proof that the message was received by the specified party.

SECURITY MECHANISMS

The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment: The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control: A variety of mechanisms that enforce access rights to resources.

Data Integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control: Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization: The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality: That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection: Detection of security-relevant events.

Security Audit Trail: Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery: Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Types of Computer Crime

Computer crime, or *cybercrime*, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.

The term *cybercrime* has a connotation of the use of networks specifically, whereas *computer crime* may or may not involve networks.

The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity, as follows:

• **Computers as targets:** This form of crime targets a computer system, to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server.

This form of crime involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability.

• **Computers as storage devices:** Computers can be used to further unlawful activity by using a computer or a computer device as a passive storage medium. For example, the computer can be used to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software).

• **Computers as communications tools:** Many of the crimes falling within this category are simply traditional crimes that are committed online. Examples include the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling.

A more specific list of crimes, shown in Table, is defined in the international Convention on Cybercrime

Illegal access

The access to the whole or any part of a computer system without right.

Illegal interception

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Data interference

The damaging, deletion, deterioration, alteration or suppression of computer data without right.

System interference

The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Misuse of devices

The production, sale, procurement for use, import, distribution or otherwise making available of:

i. A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above ;

ii. A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above ;

Computer-related forgery

The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Computer-related fraud

The causing of a loss of property to another person by:

a. Any input, alteration, deletion or suppression of computer data;

b. Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Offenses related to child pornography

a. Producing child pornography for the purpose of its distribution through a computer system;

b. Offering or making available child pornography through a computer system;

c. Distributing or transmitting child pornography through a computer system;

d. Procuring child pornography through a computer system for oneself or for another person;

e. Possessing child pornography in a computer system or on a computer-data storage medium.

Infringements of copyright and related rights

Top 10 Cyber Crime Prevention Tips

1. **Use Strong Passwords** Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.
2. **Secure your computer**

- ✓ **Activate your firewall** Firewalls are the first line of cyber defence; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
- ✓ **Use anti-virus/malware software** Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
- ✓ **Block spyware attacks** Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

3. **Be Social-Media Savvy** Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!
4. **Secure your Mobile Devices** Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.
5. **Install the latest operating system updates** Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.
6. **Protect your Data** Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.
7. **Secure your wireless network** Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.
8. **Protect your e-identity** Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you’ve enabled privacy settings (e.g. when accessing/using social networking sites).
9. **Avoid being scammed** Always think before you click on a link or file of unknown origin. Don’t feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.
10. **Call the right person for help** Don’t panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

A virus can be either transient or resident. A **transient** virus has a life that depends on the life of its host; the virus runs when its attached program executes and terminates when its attached program ends. (During its execution, the transient virus may have spread its infection to other programs.) A **resident** virus locates itself in memory; then it can remain active or be activated as a stand-alone program, even after its attached program ends.

A **Trojan horse** is malicious code that, in addition to its primary effect, has a second, non obvious malicious effect.

A **logic bomb** is a class of malicious code that "detonates" or goes off when a specified condition occurs. A **time bomb** is a logic bomb whose trigger is a time or date.

A **trapdoor** or **backdoor** is a feature in a program by which someone can access the program other than by the obvious, direct call, perhaps with special privileges. For instance, an automated bank teller program might allow anyone entering the number 990099 on the keypad to process the log of everyone's transactions at that machine. In this example, the trapdoor could be intentional, for maintenance purposes, or it could be an illicit way for the implementer to wipe out any record of a crime.

A **worm** is a program that spreads copies of itself through a network. The primary difference between a worm and a virus is that a worm operates through networks, and a virus can spread through any medium (but usually uses copied program or data files). Additionally, the worm spreads copies of itself as a stand-alone program, whereas the virus spreads copies of itself as a program that attaches to or embeds in other programs.

EMERGING TRENDS IN INFORMATION TECHNOLOGY:

CLOUD COMPUTING:

Cloud computing is Internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customers on a pay-as-you-use basis. All information that a digitized system has to offer is provided as a service in the cloud computing model.

Users can access these services available on the "Internet cloud" without having any previous know-how on managing the resources involved. Thus, users can concentrate more on their core business processes rather than spending time and gaining knowledge on resources needed to manage their business processes.

Cloud computing customers do not own the physical infrastructure; rather they rent the usage from a third-party provider. This helps them to avoid huge. They consume resources as a service and pay only for resources that they use. Most cloud computing infrastructures consist of services delivered through common centers and built on servers.

Sharing resources amongst can improve, as servers are not unnecessarily left idle, which can reduce costs significantly while increasing the speed of application development.

Types of Cloud Computing

Public cloud: Public clouds are made available to the general public by a service provider who hosts the cloud infrastructure.

Private cloud: Private cloud is cloud infrastructure dedicated to a particular organization. Private clouds allow businesses to host applications in the cloud, while addressing concerns regarding data security and control, which is often lacking in a public cloud environment.

Hybrid cloud: Hybrid Clouds are a composition of two or more clouds (private, community or public) that remain unique entities but are bound together offering the advantages of multiple deployment models.

Advantages of Cloud Computing

The following are some of the possible advantages of cloud computing:

Flexibility
Low Cost
Easier Management of Data and Information
Device Diversity
Increased Storage Capacity
Easy to Learn and Understand
Automatic Updating

ARITIFICIAL INTELLIGENCE

Artificial intelligence is the branch of computer science concerned with making computers behave like humans.

Artificial Intelligence is a way of **making a computer, a computer-controlled robot, or a software think intelligently**, in the similar manner the intelligent humans think.

AI is accomplished by studying how human brain thinks, and how humans learn, decide, and work while trying to solve a problem, and then using the outcomes of this study as a basis of developing intelligent software and systems.

Applications of AI

AI has been dominant in various fields such as:

- ✓ **Gaming**

AI plays crucial role in strategic games such as chess, poker, tic-tac-toe, etc., where machine can think of large number of possible positions based on heuristic knowledge.

- ✓ **Natural Language Processing**

It is possible to interact with the computer that understands natural language spoken by humans.

- ✓ **Expert Systems**

There are some applications which integrate machine, software, and special information to impart reasoning and advising. They provide explanation and advice to the users.

- ✓ **Vision Systems**

  These systems understand, interpret, and comprehend visual input on the computer. For example,

  - A spying aeroplane takes photographs which are used to figure out spatial information or map of the areas.
  - Doctors use clinical expert system to diagnose the patient.
  - Police use computer software that can recognize the face of criminal with the stored portrait made by forensic artist.

- ✓ **Speech Recognition**

  Some intelligent systems are capable of hearing and comprehending the language in terms of sentences and their meanings while a human talks to it. It can handle different accents, slang words, noise in the background, change in human's noise due to cold, etc.

- ✓ **Handwriting Recognition**

  The handwriting recognition software reads the text written on paper by a pen or on screen by a stylus. It can recognize the shapes of the letters and convert it into editable text.

- ✓ **Intelligent Robots**

  Robots are able to perform the tasks given by a human. They have sensors to detect physical data from the real world such as light, heat, temperature, movement, sound, bump, and pressure. They have efficient processors, multiple sensors and huge memory, to exhibit intelligence. In addition, they are capable of learning from their mistakes and they can adapt to the new environment.

4G TECHNOLOGIES

4G refers to the fourth generation of mobile technology. The first two generations were analog cell phones (1G) and digital phones (2G). The First-generation was introduced in 1981 and the second in 1992. The third-generation mobile networks, or 3G, was introduced in 2001.

The technologies that fall in the 4G categories are UMTS, OFDM, SDR, MIMO and WiMAX to some extent.

LTE Advanced: LTE refers to Long-Term Evolution. As the name suggests, it has matured over a long time to a state where changes in the specification are limited to corrections and bug fixes.

UMTS: UMTS refers to Universal Mobile Telecommunications System. UMTS supports maximum theoretical data transfer rates of 42 Mbit/s.

WiMAX: WiMAX refers to Worldwide Interoperability for Microwave Access.

MIMO: MIMO stands for Multiple-Input and Multiple-Output.

OFDM: OFDM stands for Orthogonal Frequency Division Multiplexing.

SDR: SDR stands for Software-Defined-Radio.

TELECOMMUTING

Telecommuting (also known as working from home, or e-commuting) is a work arrangement in which the employee works outside the office, often working from home or a location close to home (including coffee shops, libraries, and various other locations).

Rather than traveling to the office, the employee "travels" via telecommunication links, keeping in touch with coworkers and employers via telephone and email.

The worker may occasionally enter the office to attend meetings and touch base with the employer. However, with many options for distance conferencing, there may be no need to visit the office.

What Are the Benefits of Telecommuting?

There are many benefits to telecommuting. Telecommuting allows a worker greater freedom regarding his or her work hours and work location. This gives the employee more flexibility to balance work and personal obligations.

Often, working from home can actually make you more productive, because you do not have the distractions of an office space.

There are also many benefits to employers. Allowing workers to telecommute often makes them more productive, which benefits the company. Telecommuters are also likely to be happier in their jobs and are therefore more likely to stay with the company. Telecommuting even saves companies money in office expenses.