IS201

Foundation of Information Systems

Prepared by

Dr. Samah Ahmed Zaki Hassan

□

Index

CHAPTER 1: FOUNDATION CONCEPTS OF INFORMATION SYSTEMS

Index

CHAPTER 2: GLOBAL E-BUSINESS AND COLLABORATION

CHAPTER 3: SECURING INFORMATION SYSTEMS

Index

CHAPTER 4: ENHENCING DECISION MAKING

CHAPTER 5: DATA RESOURCE MANAGEMENT

CHAPTER 1
Foundation Concepts of Information Systems

1.1 Information Technology Definition

Information technology is one of many tools managers use to cope with change. ***Information Technology (IT)*** consists of:

> all the hardware and software that a firm needs to use in order to achieve its business objectives.

This includes not only computer machines, storage devices, and handheld mobile devices, but also software, such as the Windows or Linux operating systems, the Microsoft Office desktop productivity suite, and the many thousands of computer programs that can be found in a typical large firm. "Information systems" are more complex and can be best be understood by looking at them from both a technology and a business perspective.

1.1.1 Information Technology Infrastructure

Computer hardware, Computer software, Data management technology, Networking and telecommunications technology, along with the people required to run and manage them, represent resources that can be shared throughout the organization and constitute the firm's information technology (IT) infrastructure. The IT infrastructure provides the foundation, or platform, on which the firm can build its specific information systems. Each organization must carefully design and manage its IT infrastructure so that it has the set of technology services it needs for the work it wants to accomplish with information systems.

1.1.1.1 Computer Hardware

Computer hardware is the physical equipment used for input, processing, and output activities in an information system. It consists of the following: computers of various sizes and shapes (including mobile handheld devices); various input, output, and storage devices; and telecommunications devices that link computers together.

1.1.1.2 Computer Software

Computer software consists of the detailed, preprogrammed instructions that control and coordinate the computer hardware components in an information system.

1.1.1.3 Data Management Technology

Data management technology consists of the software governing the organization of data and access methods on physical storage media.

1.1.1.4 Networking and Telecommunications Technology

Networking and telecommunications technology, consisting of both physical devices and software, links the various pieces of hardware and transfers data from one physical location to another. Computers and communications equipment can be connected in networks for sharing voice, data, images, sound, and video. A ***network*** links two or more computers to share data or resources, such as a printer.

- **Internet and World Wide Web**

The world's largest and most widely used network is the ***Internet***. The majority of Internet services are available to any business or consumer that has access to the Internet. The Internet is a global "network of networks" that uses universal standards to connect millions of different networks with billion users around the world.

The ***World Wide Web (WWW)*** is a service provided by the Internet that uses universally accepted standards for storing, retrieving, formatting, and displaying information in a page format on the Internet. Web pages contain text, graphics, animations, sound, and video and are linked to other Web pages. By clicking on highlighted words or buttons on a Web page, you can link to related pages to find additional information and links to other locations on the Web. The Web can serve as the foundation for new kinds of information systems such as UPS's Web-based package tracking system described in the following Interactive Session.

- **Internet, Intranet and Extranet**

For most business firms today, using Internet technology is both a business necessity and a competitive advantage. The ***Internet*** has created a new “universal” technology platform on which to build new products, services, strategies, and business models. This same technology platform has internal uses, providing the connectivity to link different systems and networks within the firm. However, many e-business applications that access sensitive company information require access to be limited to qualified individuals or partners. If information is restricted to employees inside an organization, this is an intranet. Internal corporate networks based on Internet technology are called ***intranets***. In other words, The intranet is defined as a private network within a single company using Internet standards to enable employees to access and share information using web publishing technology. In other words, it is a corporate or government internal network that uses Internet tools, such as Web browsers and Internet protocols. If access to an organization’s web services is extended to some others, but not everyone beyond the organization, this is an ***extranet***. Private intranets extended to authorized users outside the organization are called extranets, and firms use such networks to coordinate their activities with other firms for making purchases, collaborating on design, and other interorganizational work. Whenever users log on to an Internet service such as that for an e-retailer or online news site, this is effectively an extranet arrangement, although the term is most often used to mean a business-to-business application. The extranet is defined as a service provided through Internet and web technology delivered by extending an intranet beyond a company to customers, suppliers and collaborators. In other words, it is a network that uses Internet technology to link intranets of several organizations in a secure manner. Figure 1.1, shows The relationship between intranets, extranets and the Internet.

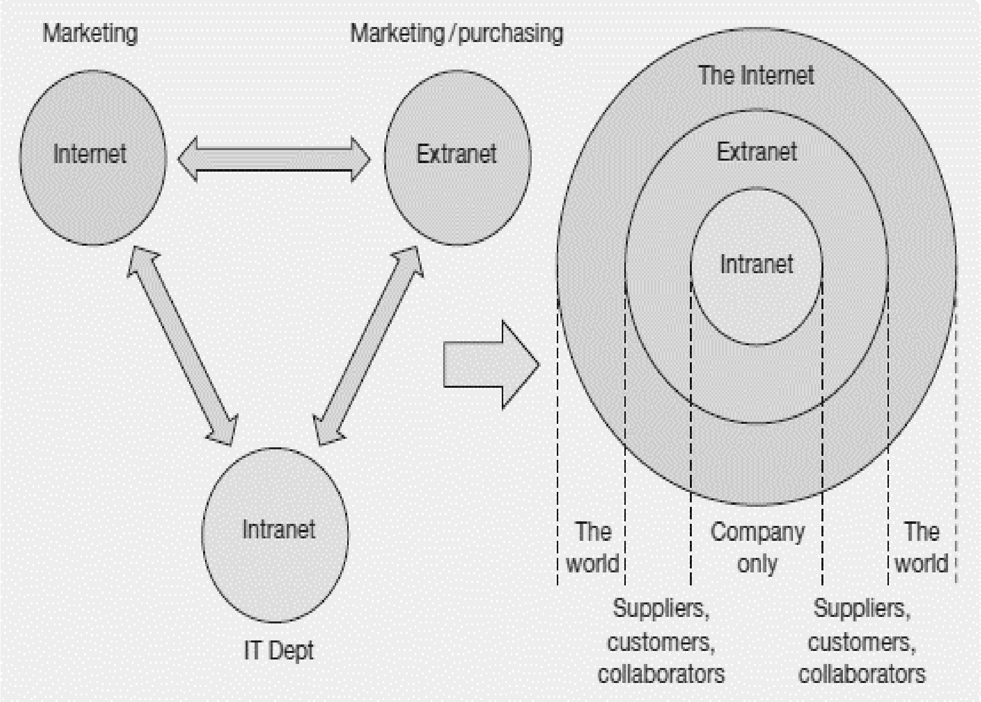


Figure 1.1: The Relationship between Intranets, Extranets and the Internet

1.2 Information System Definition

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.

Information systems contain information about significant people, places, and things within the organization or in the environment surrounding it. ***Information*** means data that have been shaped into a form that is meaningful and useful to human beings. ***Data***, in contrast, are streams of raw facts representing events occurring in organizations or the physical environment before they have been organized and arranged into a form that people can understand and use. For example, raw data from a supermarket checkout counter can be processed and organized to produce meaningful information, such as the total unit sales of dish detergent or the total sales revenue from dish detergent for a specific store or sales territory. People rely on modern information systems to communicate with one another using a variety of physical devices *(hardware),* information processing instructions and procedures *(software),* communications channels *(networks),* and stored data *(data resources).*

A simple definition of an ***Information System (IS),*** Figure 1.2, is:

> any organized combination of people, hardware, software, communications networks, data resources, and policies and procedures that stores, retrieves, transforms, and disseminates information in an organization.

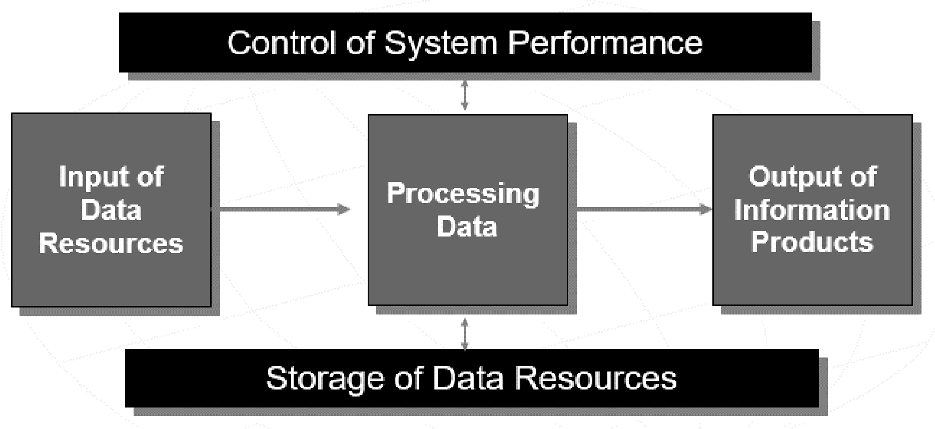

Control of System Performance
Input of Data Resources
Processing Data
Output of Information Products
Storage of Data Resources

Figure 1.2 : An Information System

1.3 Information System Activities

An Information System (IS) contains information about an organization and its surrounding environment. Three basic 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, Figure 1.3. ***Input*** captures or collects raw data from within the organization or from its external environment. ***Processing*** converts this raw input into a 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, correct, and/or refine the input stage. Environmental actors, such as customers, suppliers, competitors, stockholders, and regulatory agencies, interact with the organization and its information systems.

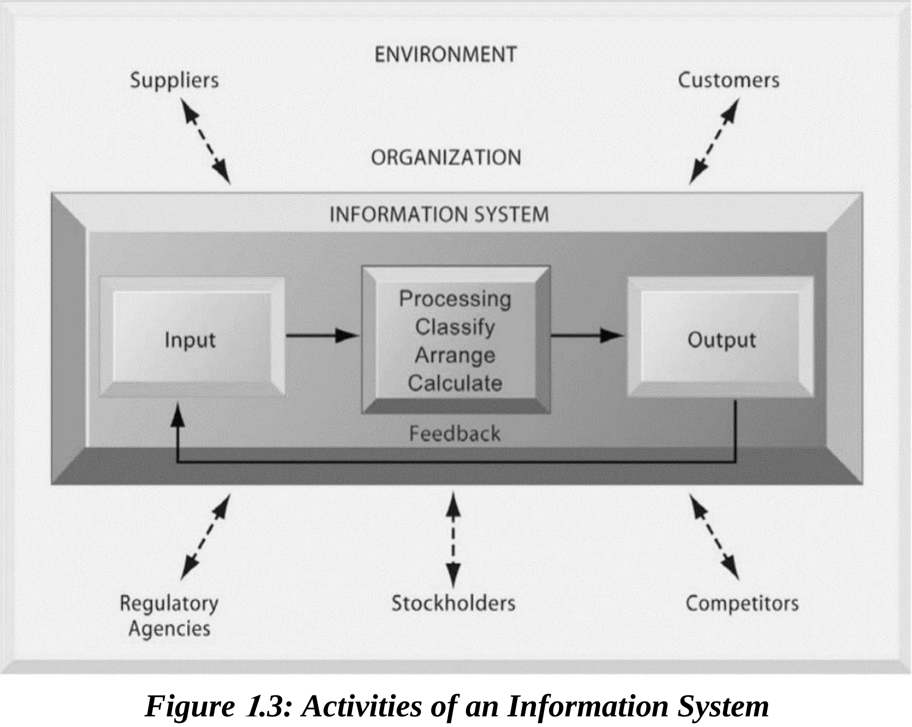


Figure 1.3: Activities of an Information System

Table 1.1 Shows basic activities of information systems' business examples.

Table 1.1: Activities of Information Systems

Activity	Example
Input.	Optical scanning of bar-coded tags on merchandise.
Processing.	Calculating employee pay, taxes, and other payroll deductions.
Output.	Producing reports and displays about sales performance.
Storage.	Maintaining records on customers, employees, and products.
Control.	Generating audible signals to indicate proper entry of sales data.

1.4 Information Systems Components

Figure 1.4 illustrates an information system model that expresses a fundamental conceptual framework for the major components and activities of information systems. An information system depends on the resources of ***people*** (end users and IS specialists), ***hardware*** (machines and media), ***software*** (programs and procedures), data (data and knowledge bases), and ***networks*** (communications media and network support) to perform input, processing, output, ***storage***, and ***control activities*** that transform data resources into information products.

This information system model highlights the relationships among the components and activities of information systems. It also provides a framework that emphasizes four major concepts that can be applied to all types of information systems:

- People, hardware, software, data, and networks are the basic resources of information systems.
- People resources include end users and IS specialists, hardware resources consist of machines and media, software resources include both programs and procedures, data resources include data and knowledge bases, and network resources include communications media and networks.
- Data resources are transformed by information processing activities into a variety of information products for end users.
- Information processing consists of the system activities of input, processing, output, storage, and control.

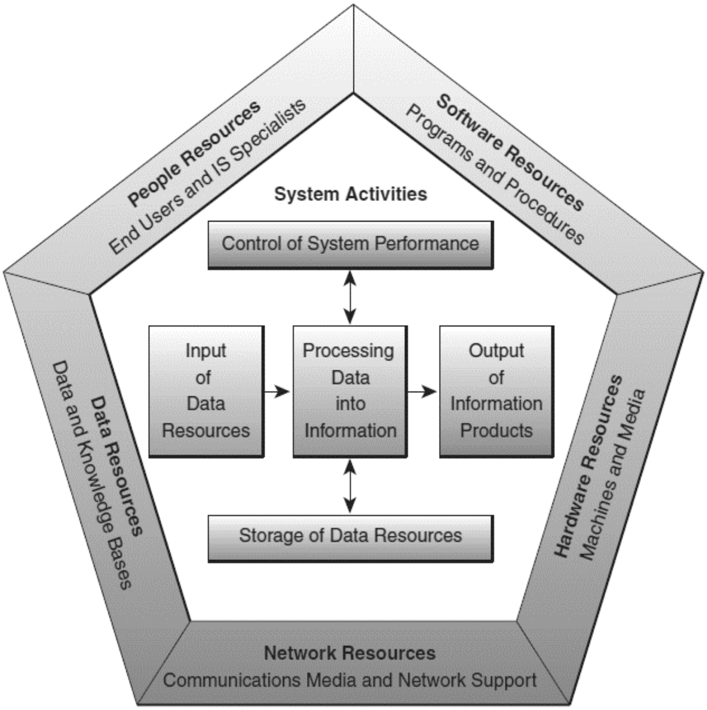


Figure 1.4: The components of an information system.

Table 1.2 shows some examples of information system resources and products.

Table 1.2: Information System Resources and Products

Resource/ Product	Example
People Resources	- **Specialists,** systems analysts, software developers, systems operators. - **End Users,** anyone else who uses information systems.
Hardware Resources	- **Machines,** computers, video monitors, magnetic disk drives, printers, optical scanners. - **Media,** floppy disks, magnetic tape, optical disks, plastic cards, paper forms, removable storage media.
Software Resources	- **Programs,** operating system programs, spreadsheet programs, word processing programs, payroll programs. - **Procedures,** data entry procedures, error correction procedures, paycheck distribution procedures.

Data Resources	- Product descriptions, customer records, employee files, inventory databases.
Network Resources	- Communications media, communications processors, network access, control software.
Information Products	- Management reports and business documents using text and graphics displays, audio responses, and paper forms.

1.5 The Fundamental Roles of IS In Business

There are three fundamental reasons for all business applications of information technology. They are found in the three vital roles that information systems can perform for a business enterprise:

- Support of business processes and operations.
- Support of decision making by employees and managers.
- Support of strategies for competitive advantage.

Figure 1.5 illustrates how these fundamental roles interact in a typical organization.

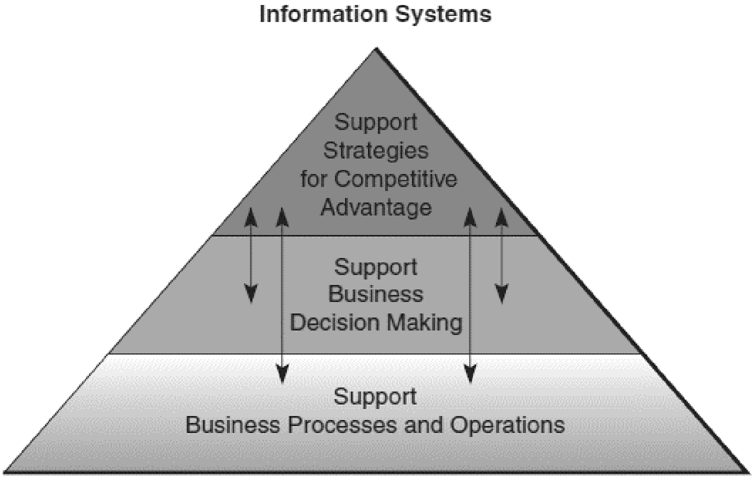

Information Systems
Support Strategies for Competitive Advantage
Support Business Decision Making
Support Business Processes and Operations

Figure 1.5: Business Applications of Information Systems Roles.

At any given moment, information systems designed to support business processes and operations may also be providing data to, or accepting data from, systems focused on business decision making or achieving competitive advantage. The same is true for the other two fundamental roles of IS. Today's organizations are constantly striving to achieve integration of their systems to allow information to flow freely through them, which adds even greater flexibility and business support than any of the individual system roles could provide.

1.5.1 Support of Business Processes and Operations.

As a consumer, you regularly encounter information systems that support the business processes and operations at the many retail stores where you shop. For example, most retail stores now use ***computer-based information systems*** to help their employees record customer purchases, keep track of inventory, pay employees, buy new merchandise, and evaluate sales trends. Store operations would grind to a halt without the support of such information systems.

1.5.2 Support of Business Decision Making.

Information systems also help store managers and other business professionals make better decisions. For example, decisions about what lines of merchandise need to be added or discontinued and what kind of investments they require are typically made after an analysis provided by computer-based information systems. This function not only supports the decision making of store managers, buyers, and others, but also helps them look for ways to gain an advantage over other retailers in the competition for customers.

1.5.3 Support of Strategies for Competitive Advantage.

Gaining a strategic advantage over competitors requires the innovative application of information technologies. For example, store management might make a decision to install touch-screen kiosks in all stores, with links to the e-commerce Web site for online shopping. This offering might attract new customers and build customer loyalty because of the ease of shopping and buying merchandise provided by such information systems. Thus, strategic information systems can help provide products and services that give a business a comparative advantage over its competitors.

1.6 Managerial Levels of Business Organizations

Organizations have a structure that is composed of different levels and specialties. Their structures reveal a clear-cut division of labor. Authority and responsibility in a business firm are organized as a hierarchy, or a pyramid structure. The upper levels of the hierarchy consist of managerial, professional, and technical employees, whereas the lower levels consist of operational personnel.

Business organizations are hierarchies consisting of three principal levels: senior management, middle management, and operational management, Figure 1.6. Information systems serve each of these levels. Scientists and knowledge workers often work with middle management.

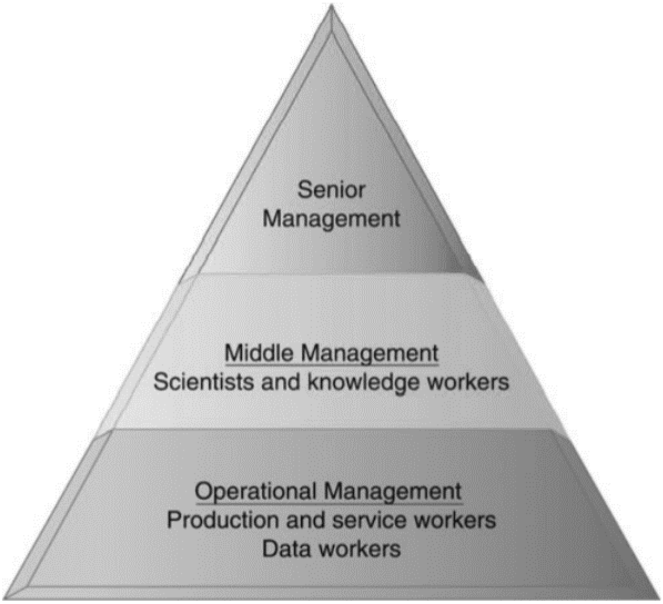


Figure 1.6: Levels of Business Organizations

1.6.1 Senior Executives

Senior management makes long-range strategic decisions about products and services as well as ensures financial performance of the firm. They face many unstructured decision situations, such as establishing the firm’s five- or ten-year goals or deciding new markets to enter. Answering the question “Should we enter a new market?” would require access to news, government reports, and industry views as well as high-level summaries of firm performance. However, the answer would also require senior managers to use their own best judgment and poll other managers for their opinions.

1.6.2 Middle Management

Middle management carries out the programs and plans of senior management. They faces more structured decision scenarios but their decisions may include unstructured components. A typical middle-level management decision might be “Why is the reported order fulfillment report showing a decline over the past six months at a distribution center in Minneapolis?” This middle manager will obtain a report from the firm’s enterprise system or distribution management system on order activity and operational efficiency at the Minneapolis distribution center. This is the structured part of the decision. But before arriving at an answer, this middle manager will have to interview employees and gather more unstructured information from external sources about local economic conditions or sales trends.

1.6.3 Operational Management

Operational management is responsible for monitoring the daily activities of the business. As rank-and-file employees, they tend to make more structured decisions. For example, a supervisor on an assembly line has to decide whether an hourly paid worker is entitled to overtime pay. If the employee worked more than eight hours on a particular day, the supervisor would routinely grant overtime pay for any time beyond eight hours that was clocked on that day.

Knowledge workers, such as engineers, scientists, or architects, design products or services and create new knowledge for the firm, whereas ***data workers***, such as secretaries or clerks, assist with scheduling and communications at all levels of the firm. ***Production or service workers*** actually produce the product and deliver the service.

1.7 Types of Information Systems

Information systems are developed for different purposes, depending on the needs of human users and the business and to perform a wide variety of related tasks or just a single task, for example, several types of information systems can be classified according to managerial levels or either as operations or management information systems.

1.7.1 According to Managerial Levels

Transaction processing systems (TPS) function at the operational level of the organization; office automation systems (OAS) and knowledge work systems (KWS) support work at the knowledge level. Higher-level systems include management information systems (MIS) and decision support systems (DSS). Expert systems apply the expertise of decision makers to solve specific, structured problems. On the strategic level of management we find executive support systems (ESS). Group decision support systems (GDSS) and the more generally described computer-supported collaborative work systems (CSCWS) aid group-level decision making of a semistructured or unstructured variety. The variety of information systems that analysts may develop is shown in Figure 1.9.

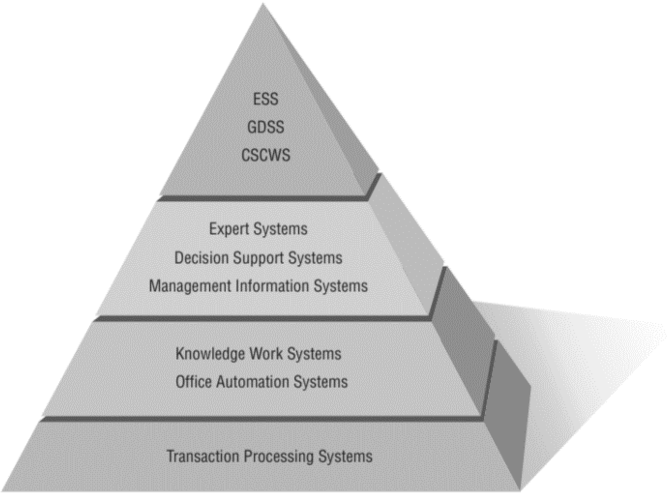

ESS
GDSS
CSCWS
Expert Systems
Decision Support Systems
Management Information Systems
Knowledge Work Systems
Office Automation Systems
Transaction Processing Systems

Figure 1.7: Types of Information Systems

Notice that the figure presents these systems from the bottom up, indicating that the operational, or lowest, level of the organization is supported by TPS, and the strategic, or highest, level of semistructured and unstructured decisions is supported by ESS, GDSS, and CSCWS at the top.

1.7.1.1 Transaction Processing Systems

Transaction Processing Systems (TPS) are computerized information systems that were developed to process large amounts of data for routine business transactions such as payroll and inventory. A TPS eliminates the tedium of necessary operational transactions and reduces the time once required to perform them manually, although people must still input data to computerized systems.

Transaction processing systems are boundary-spanning systems that permit the organization to interact with external environments. Because managers look to the data generated by the TPS for up-to-the-minute information about what is happening in their companies, it is essential to the day-to-day operations of business that these systems function smoothly and without interruption.

1.7.1.2 Office Automation Systems and Knowledge Work Systems

At the knowledge level of the organization are two classes of systems. ***Office Automation Systems (OAS)*** support data workers, who do not usually create new knowledge but rather analyze information to transform data or manipulate it in some way before sharing it with, or formally disseminating it throughout, the organization and, sometimes, beyond. Familiar aspects of OAS include word processing, spreadsheets, desktop publishing, electronic scheduling, and communication through voice mail, email (electronic mail), and teleconferencing.

Knowledge Work Systems (KWS) support professional workers such as scientists, engineers, and doctors by aiding them in their efforts to create new knowledge (often in teams) and by allowing them to contribute it to their organization or to society at large.

1.7.1.3 Management Information Systems

Management Information Systems (MIS) do not replace transaction processing systems; rather, all MIS include transaction processing. MIS are computerized information systems that work because of the purposeful interaction between people and computers. By requiring people, software, and hardware to function in concert, management information systems support users in accomplishing a broader spectrum of organizational tasks than transaction processing systems, including decision analysis and decision making.

To access information, users of the management information system share a common database. The database stores both data and models that help the user interact with, interpret, and apply that data. Management information systems output information that is used in decision making. A management information system can also help integrate some of the computerized information functions of a business.

1.7.1.4 Decision Support Systems

A higher-level class of computerized information systems is ***Decision Support Systems (DSS)***. DSS are similar to the traditional management information system because they both depend on a database as a source of data. A decision support system departs from the traditional management information system because it emphasizes the support of decision making in all its phases, although the actual decision is still the exclusive province of the decision maker. Decision support systems are more closely tailored to the person or group using them than is a traditional management information system. Sometimes they are discussed as systems that focus on business intelligence.

1.7.1.5 Artificial Intelligence and Expert Systems

Artificial Intelligence (AI) can be considered the overarching field for expert systems. The general thrust of AI has been to develop machines that behave intelligently. Two avenues of AI research are (1) understanding natural language and (2) analyzing the ability to reason through a problem to its logical conclusion. Expert systems use the approaches of AI reasoning to solve the problems put to them by business (and other) users.

Expert systems are a very special class of information system that has been made practicable for use by business as a result of widespread availability of hardware and software such as personal computers (PCs) and expert system shells. An expert system (also called a knowledgebased system) effectively captures and uses the knowledge of a human expert or experts for solving a particular problem experienced in an organization. Notice that unlike DSS, which leave the ultimate judgment to the decision maker, an expert system selects the best solution to a problem or a specific class of problems.

The basic components of an expert system are the knowledge base, an inference engine connecting the user with the system by processing queries via languages such as structured query language (SQL), and the user interface. People called knowledge engineers capture the expertise of experts, build a computer system that includes this expert knowledge, and then implement it.

1.7.1.6 Group Decision Support Systems and Computer–Supported Collaborative Work Systems

Organizations are becoming increasingly reliant on groups or teams to make decisions together. When groups make semistructured or unstructured decisions, a group decision support system may afford a solution. ***Group Decision Support Systems (GDSS)***, which are used in special rooms equipped in a number of different configurations, permit group members to interact with electronic support—often in the form of specialized software—and a special group facilitator. Group decision support systems are intended to bring a group together to solve a problem with the help of various supports such as polling, questionnaires, brainstorming, and scenario creation. GDSS software can be designed to minimize typical negative group behaviors such as lack of participation due to fear of reprisal for expressing an unpopular or contested viewpoint, domination by vocal group members, and "group think" decision making. Sometimes GDSS are discussed under the more general term ***Computer-Supported Collaborative Work Systems(CSCWS)***, which might include software support called groupware for team collaboration via networked computers. Group decision support systems can also be used in a virtual setting.

1.7.1.7 Executive Support Systems

When executives turn to the computer, they are often looking for ways to help them make decisions on the strategic level. ***Executive Support Systems (ESS)*** help executives organize their interactions with the external environment by providing graphics and communications technologies in accessible places such as boardrooms or personal corporate offices. Although ESS rely on the information generated by TPS and MIS, executive support systems help their users address unstructured decision problems, which are not application specific, by creating an environment that helps them think about strategic problems in an informed way. ESS extend and support the capabilities of executives, permitting them to make sense of their environments.

1.7.2 According to Operations or Management Information Systems

Several types of information systems can be classified either as operations or management information systems. Figure 1.10 illustrates this conceptual classification of information systems applications. Information systems are categorized this way to spotlight the major role each plays in the operations and management of a business. Note, however, that there are many subcategories of information systems, and each plays an essential role in either the operation of the business or the execution of its chosen strategy. Let's look briefly at some examples of such information systems categories.

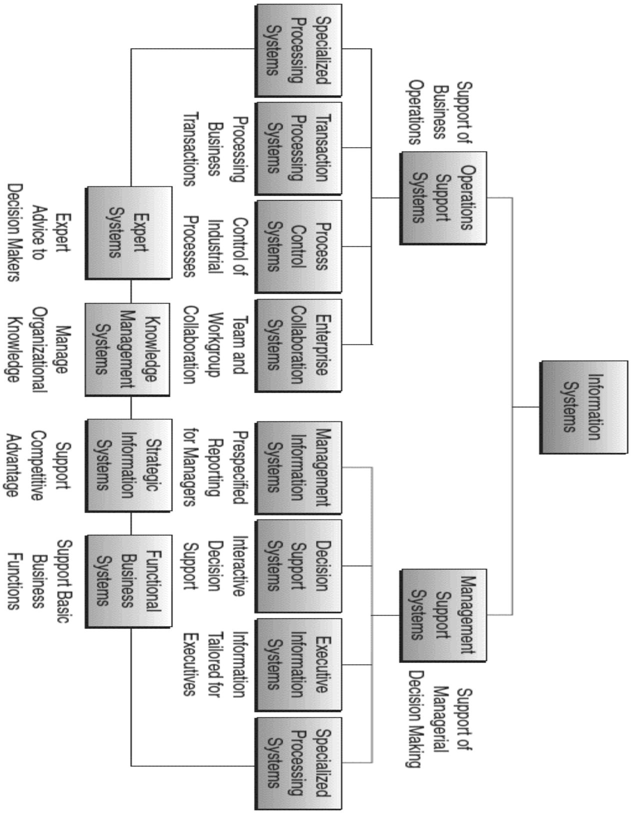

Information Systems
Operations Support Systems
Support of Business Operations
Management Support Systems
Support of Managerial Decision Making
Transaction Processing Systems
Processing Business Transactions
Process Control Systems
Control of Industrial Processes
Enterprise Collaboration Systems
Team and Workgroup Collaboration
Management Information Systems
Prespecified Reporting for Managers
Decision Support Systems
Interactive Decision Support
Executive Information Systems
Information Tailored for Executives
Specialized Processing Systems
Expert Systems
Expert Advice to Decision Makers
Knowledge Management Systems
Manage Organizational Knowledge
Strategic Information Systems
Support Competitive Advantage
Functional Business Systems
Support Basic Business Functions
Specialized Processing Systems

Figure 1.8: Operations and management classifications of Information Systems.

1.7.2.1 Operations Support Systems

Information systems have always been needed to process data generated by, and used in, business operations. Such ***operations support systems*** produce a variety of information products for internal and external use; however, they do not emphasize the specific information products that can best be used by managers. Further processing by management information systems is usually required. The role of a business firm’s operations support systems is to process business transactions, control industrial processes, support enterprise communications and collaborations, and update corporate databases efficiently.

- **Transaction processing systems**

Transaction processing systems(TPSs) are important examples of operations support systems that record and process the data resulting from business transactions. They process transactions in two basic ways. In ***batch processing***, transactions data are accumulated over a period of time and processed periodically. In ***real-time (or online) processing***, data are processed immediately after a transaction occurs. For example, point-of-sale (POS) systems at many retail stores use electronic cash register terminals to capture and transmit sales data electronically over telecommunications links to regional computer centers for immediate (real-time) or nightly (batch) processing.

- **Process Control Systems**

Process control systems monitor and control physical processes. For example, a petroleum refinery uses electronic sensors linked to computers to monitor chemical processes continually and make instant (real-time) adjustments that control the refinery process.

- **Enterprise Collaboration Systems**

Enterprise Collaboration Systems enhance team and workgroup communications and productivity and include applications that are sometimes called office automation systems. For example, knowledge workers in a project team may use e-mail to send and receive e-messages or use videoconferencing to hold e-meetings to coordinate activities.

The following table shows A summary of operations support systems.

Table 1.3: A summary of operations support systems.

System	Description with examples
Transaction Processing Systems (TPS)	Process data resulting from business transactions, update operational databases, and produce business documents. Examples: sales and inventory processing systems.
Process Control Systems.	Monitor and control industrial processes. Examples: petroleum refining and power generation systems.
Enterprise Collaboration Systems.	Support team, workgroup, and enterprise communications and collaborations. Examples: e-mail, chat, and videoconferencing groupware systems.

1.7.2.2 Management Support Systems

When information system applications focus on providing information and support for effective decision making by managers, they are called ***Management Support Systems***. Providing information and support for decision making by all types of managers and business professionals is a complex task. Conceptually, several major types of information systems support a variety of decision-making responsibilities, *Table 1.6*.

Table 1.4: A summary of management support systems.

System	Discription and examples
Management information systems (MIS).	Provide information in the form of prespecified reports and displays to support business decision making. Examples: sales analysis, production performance, and cost trend reporting systems.
Decision support systems (DSS).	Provide interactive ad hoc support for the decision-making processes of managers and other business professionals. Examples: product pricing, profitability forecasting, and risk analysis systems.
Executive information systems (ESS).	Provide critical information from MIS, DSS, BI, and other sources tailored to the information needs of executives. Examples: systems for easy access to analyses of business performance, actions of competitors, and economic developments to support strategic planning.

- **Management Information Systems**

Management Information Systems (MIS) provide information in the form of reports and displays to managers and many business professionals. They are the most common form of information system in an organization. For example, sales managers may use their networked computers and Web browsers to receive

access their corporate intranet for daily sales analysis reports that evaluate sales made by each salesperson.

- **Decision support systems (DSS)**

Decision support systems (DSS) give direct computer support to managers during the decision-making process. These types of systems fall under the business intelligence or business analytics umbrella. For example, an advertising manager may use a DSS to perform a what-if analysis as part of the decision to determine how to spend advertising dollars. A production manager may use a DSS to decide how much product to manufacture, based on the expected sales associated with a future promotion and the location and availability of the raw materials necessary to manufacture the product.

- **Executive information systems (EIS)**

Executive Information Systems (EIS) provide critical information from a wide variety of internal and external sources in easy-to-use displays to executives and managers. Think of an EIS as a "30,000-foot-high view of the organization." For example, top executives may use touch-screen terminals for an instant view of text and graphics displays that highlight key areas of organizational and competitive performance.

1.7.3 Other Classifications of Information Systems

Several other categories of information systems can support either operations or management applications. For example, ***Expert Systems*** can provide expert advice for operational chores like equipment diagnostics or managerial decisions such as loan portfolio management. IBM's famous supercomputer, Watson, is an example of an expert system that can translate text input and use a complex search algorithm to find answers to questions. ***Knowledge Management Systems*** are knowledge-based information systems that support the creation, organization, and dissemination of business knowledge to employees and managers throughout a company. Information systems that focus on operational and managerial applications in support of basic business functions such as accounting or marketing are known as ***functional business systems***. Finally, ***Strategic Information Systems*** apply information technology to a firm's products, services, or business processes to help it gain a strategic advantage over its competitors.

Table 1.5: A Summary of Other Categories of Information Systems.

System	Discription and examples
Expert Systems.	Knowledge-based systems that provide expert advice and act as expert consultants to users. Examples: credit application advisor, process monitor, and diagnostic maintenance systems.
Knowledge Management Systems.	Knowledge-based systems that support the creation, organization, and dissemination of business knowledge within the enterprise. Examples: intranet access to best business practices, sales proposal strategies, and customer problem resolution systems.
Strategic Information Systems.	Support operations or management processes that provide a firm with strategic products, services, and capabilities for competitive advantage. Examples: online stock trading, shipment tracking, and e-commerce Web systems.
Functional Business Systems.	Support a variety of operational and managerial applications of the basic business functions of a company. Examples: information systems that support applications in accounting, finance, marketing, operations management, and human resource management.

It is also important to realize that business applications of information systems in the real world are typically integrated combinations of the several types of information systems just mentioned. That is because conceptual classifications of information systems are designed to emphasize the many different roles of information systems. In practice, these roles are combined into integrated or ***cross-functional informational systems*** that provide a variety of functions. Thus, most information systems are designed both to produce information and to support decision making for various levels of management and business functions, as well as perform record-keeping and transaction-processing chores. Whenever you analyze an information system, you probably see that it provides information for a variety of managerial levels and business functions. The enterprise resource planning systems are examples of information systems that combine virtually all of the processes of an organization into a single system that spans all organizational boundaries. It’s like one big information system that runs the whole organization.

CHAPTER 2
Global E-business and Collaboration

In order to operate, businesses must deal with many different pieces of information about suppliers, customers, employees, invoices and payments, and of course their products and services. They must organize work activities that use this information to operate efficiently and enhance the overall performance of the firm. Information systems make it possible for firms to manage all their information, make better decisions, and improve the execution of their business processes.

2.1 Business processes

Business processes, refer to the manner in which work is organized, coordinated, and focused to produce a valuable product or service. Business processes are the collection of activities required to produce a product or service. These activities are supported by flows of material, information, and knowledge among the participants in business processes. Business processes also refer to the unique ways in which organizations coordinate work, information, and knowledge, and the ways in which management chooses to coordinate work.

To a large extent, the performance of a business firm depends on how well its business processes are designed and coordinated. A company's business processes can be a source of competitive strength if they enable the company to innovate or to execute better than its rivals. Business processes can also be liabilities if they are based on outdated ways of working that impede organizational responsiveness and efficiency. Table 2.1 describes some typical business processes for each of the functional areas of business.

Table 2.1: Examples of Functional Business Processes.

Functional Area	Business Process
Manufacturing and production	- Assembling the product - Checking for quality - Producing bills of materials
Sales and marketing	- Identifying customers - Making customers aware of the product - Selling the product

Finance and accounting	- Paying creditors - Creating financial statements - Managing cash accounts
Human resources	- Hiring employees - Evaluating employees’ job performance - Enrolling employees in benefits plans

2.2 E−Business, E−Commerce, and E−Government

Systems and technologies are transforming firms’ relationships with customers, employees, suppliers, and logistic partners into digital relationships using networks and the Internet. Business is now enabled by or based upon digital networks, so the terms “electronic business” and “electronic commerce” are used frequently.

Electronic business, or e-business, refers to the use of digital technology and the Internet to execute the major business processes in the enterprise. E-business includes activities for the internal management of the firm and for coordination with suppliers and other business partners. By E-business, all kinds of business are conducted online, such as servicing customers, collaborating with business partners, delivering e-learning, and conducting electronic transactions within an organization. It is simply defined as the transformation of key business processes through the use of Internet technologies. It also considered as all electronically mediated information exchanges, both within an organization and with external stakeholders supporting the range of business processes.

Electronic commerce, or e-commerce, is the part of e-business that deals with the buying and selling of goods and services over the Internet; in othor words it, refers to using the Internet and intranets to purchase, sell, transport, or trade data, goods, or services. people immediately think of consumer retail purchases from companies such as Amazon. But e-commerce involves much more than electronically mediated financial transactions between organizations and customers. E-commerce should be considered as all electronically mediated transactions between an organization and any third party it deals with. By this definition, non-financial transactions such as customer requests for further information would also be considered to be part of e-commerce. So, EC is not solely restricted to the actual buying and selling of products, but also includes pre-sale and post-sale activities across the supply chain. It also encompasses activities supporting those market transactions, such as advertising, marketing, customer support, security, delivery, and payment. E-commerce is facilitated by a range of digital technologies that enable electronic communications. These technologies include Internet communications through web sites and e-mail as well as other digital media such as wireless or mobile and media for delivering digital television such as cable and satellite.

The technologies associated with e-business have also brought about similar changes in the public sector. Governments on all levels are using Internet technology to deliver information and services to citizens, employees, and businesses with which they work. ***E-government*** refers to the application of the Internet and networking technologies to digitally enable government and public sector agencies' relationships with citizens, businesses, and other arms of government. In addition to improving delivery of government services, e-government makes government operations more efficient and also empowers citizens by giving them easier access to information and the ability to network electronically with other citizens. For example, citizens in some states can renew their driver's licenses or apply for unemployment benefits online, and the Internet has become a powerful tool for instantly mobilizing interest groups for political action and fund-raising.

2.3 Types of E-Business Models

E-Business models can generally be categorized into the 9 categories as shown in the following table.

Table 2.2: Types of E-business Model

	Consumer	Business	Government
Consumer	**(C2C)**	**(C2B)**	**(C2G)**
Business	**(B2C)**	**(B2B)**	**(B2G)**
Government	**(G2C)**	**(G2B)**	**(G2G)**

2.3.1 Consumer – to – Consumer (C2C)

Using this business model helps consumers, for example, to sell their assets like residential property, cars, motorcycles, etc., or rent a room by publishing their information on the website. Website may or may not charge the consumer for its services. Another consumer may choose to buy the product of the first customer by viewing the post/advertisement on the website.

2.3.2 Consumer – to – Business (C2B)

In this model, a consumer approaches a website showing multiple business organizations for a particular service. The consumer places an estimate of amount he/she wants to spend for a particular service. For example, the comparison of interest rates of personal loan/car loan provided by various banks via websites. A business organization who fulfills the consumer's requirement within the specified budget, approaches the customer and provides its services.

2.3.3 Consumer – to – Government (C2G)

Occurs when an individual sells products and services to a government entity. It also allows consumers to provide feedback or ask for information about government authority from the public sector. When consumers pay an electricity bill via the government website, it is a favorite E-business model. Hence, the C2G model of business allows consumers to reach higher authorities without going around in circles.

2.3.4 Business – to – Consumer (B2C)

A website following the B2C business model sells its products directly to a customer. A customer can view the products shown on the website. The customer can choose a product and order the same. The website will then send a notification to the business organization via email and the organization will dispatch the product/goods to the customer.

2.3.5 Business – to – Business (B2B)

A website following the B2B business model sells its products to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the endproduct to the final customer who comes to buy the product at one of its retail outlets.

2.3.6 Business – to – Government (B2G)

B2G model is a variant of B2B model. Such websites are used by governments to trade and exchange information with various business organizations. Such websites are accredited by the government and provide a medium to businesses to submit application forms to the government.

2.3.7 Government – to – Consumer/Citizen (G2C)

Governments use G2C model websites to approach citizen in general. Such websites support auctions of vehicles, machinery, or any other material. Such website also provides services like registration for birth, marriage or death certificates. The main objective of G2C websites is to reduce the average time for fulfilling citizen’s requests for various government services.

2.3.8 Government – to – Business (G2B)

Governments use B2G model websites to approach business organizations. Such websites support auctions, tenders, and application submission functionalities.

2.3.9 Government – to – Government (G2G)

It is the online non-commercial interaction and electronic sharing of data and/or information systems between Government organizations, agencies, departments, and authorities. The goal of G2G is to support e-government initiatives by improving communication, data access and data sharing.

2.4 Web 2.0

Web 2.0 is the second generation of Internet-based tools and services that enables users to easily generate new services and content, share media, and communicate and collaborate online, in innovative ways. If you have shared photos over the Internet at Flickr or another photo site, posted a video to YouTube, created a blog, used Wikipedia, or added a widget to your Facebook page, you've used some of these Web 2.0 services.

Web 2.0 has four defining features: ***interactivity***, ***real-time user control, social participation (sharing),*** and ***user-generated content***. The technologies and services behind these features include cloud computing, software mashups and widgets, blogs, RSS, wikis, and social networks.

Behind the label 'Web 2.0' lies a bewildering range of interactive tools and social communications techniques like those we have just men tioned such as blogs, podcasts and social networks which have engaged many web users. These are aimed at increasing user participation and interaction on the web. With the widespread adoption of high-speed broadband in many countries, rich media experiences are increasingly used to engage customers with the hope they will have a viral effect, i.e. they will be discussed online or offline and more people will become aware of or interact with the brand campaign.

Web 2.0 is defined as a collection of web services that facilitate interaction of web users with sites to create usergenerated content and encourage behaviours such as community or social network participation, mashups, content rating, use of widgets and tagging.

Web 2.0 uses dozens of tools such as wikis, RSS feeds, blogs, and microblogs (e.g., Twitter). In microblogging you can transmit short messages to a list of recipients via the Internet and wireless or wireline devices. Twitter became a major Web 2.0 tool with diversified business applications.

With Web 2.0, the Web is not just a collection of destination sites, but a source of data and services that can be combined to create applications users need. Web 2.0 tools and services have fueled the creation of social networks and other online communities where people can interact with one another in the manner of their choosing.

2.4.1 Mashups and Widget

Mashups and widgets are software services that enable users and system developers to mix and match content or software components to create something entirely new. For example, Yahoo’s photo storage and sharing site Flickr combines photos with other information about the images provided by users and tools to make it usable within other programming environments.

Mashups are defined as web sites, pages or widgets that combine the content or functionality of one web site or data source with another to create something offering a different type of value to web users from the separate types of content or functionality.

A Widget is a badge or button incorporated into a site or social network space by its owner, with content or services typically served from another site making widgets effectively a mini-software application or web service. Content can be updated in real time since the widget interacts with the server each time it loads.

2.4.2 Blogs

A blog, the popular term for a Weblog, is a personal Web site that typically contains a series of chronological entries (newest to oldest) by its author, and links to related Web pages. The blog may include a ***blogroll*** (a collection of links to other blogs) and ***trackbacks*** (a list of entries in other blogs that refer to a post on the first blog). Most blogs allow readers to post comments on the blog entries as well. The act of creating a blog is often referred to as “***blogging***”. Blogs allow visitors to add comments to the original content, but they do not allow visitors to change the original posted material.

2.4.3 Feed or RSS Fee

RSS, which stands for ***Rich Site Summary*** or ***Really Simple Syndication***, syndicates Web site content so that it can be used in another setting. RSS technology pulls specified content from Web sites and feeds it automatically to users’ computers, where it can be stored for later viewing.

To receive an RSS information feed, you need to install aggregator or news reader software that can be downloaded from the Web. (Most current Web browsers include RSS reading capabilities.) Alternatively, you can establish an account with an aggregator Web site. You tell the aggregator to collect all updates from a given Web page, or list of pages, or gather information on a given subject by conducting Web searches at regular intervals. Once subscribed, you automatically receive new content as it is posted to the specified Web site.

2.4.4 Wikis

Wikis are collaborative Web sites where visitors can add, delete, or modify content on the site, including the work of previous authors. Wiki comes from the Hawaiian word for “quick”.

Wiki software typically provides a template that defines layout and elements common to all pages, displays user-editable software program code, and then renders the content into an HTML-based page for display in a Web browser. Some wiki software allows only basic text formatting, whereas other tools allow the use of tables, images, or even interactive elements, such as polls or games. Most wikis provide capabilities for monitoring the work of other users and correcting mistakes.

2.4.5 Social Networking

Social networking sites enable users to build communities of friends and professional colleagues. Members each typically create a "profile," a Web page for posting photos, videos, MP3 files, and text, and then share these profiles with others on the service identified as their "friends" or contacts. Social networking sites are highly interactive, offer real-time user control, rely on user-generated content, and are broadly based on social participation and sharing of content and opinions. Leading social networking sites include Facebook, MySpace, and LinkedIn (for professional contacts).

2.5 Web 3.0

Web 1.0 solved the problem of obtaining access to information. ***Web 2.0*** solved the problem of sharing that information with others, and building new Web experiences. ***Web 3.0*** is the promise of a future Web where all this digital information, all these contacts, can be woven together into a single meaningful experience. Web 3.0 is the third generation of internet services for websites and applications that will focus on using a machine-based understanding of data to provide a data-driven and semantic web. The ultimate goal of Web 3.0 is to create more intelligent, connected and open websites.

Sometimes this is referred to as the Semantic Web. "Semantic" refers to meaning. Most of the Web's content today is designed for humans to read and for computers to display, not for computer programs to analyze and manipulate. Search engines can discover when a particular term or keyword appears in a Web document, but they do not really understand its meaning or how it relates to other information on the Web.

The ***Semantic Web*** is a collaborative effort led by the World Wide Web Consortium to add a layer of meaning atop the existing Web to reduce the amount of human involvement in searching for and processing Web information.

The basis of the Web 3.0 are semantic markup and web services. ***Semantic markup*** refers to the communication gap between human web users and computerized applications. One of the largest organizational challenges of presenting information on the web was that web applications weren't able to provide context to data, and, therefore, didn't really understand what was relevant and what was not.

A **web service** is a software system designed to support computer-to-computer interaction over the Internet. Currently, thousands of web services are available. However, in the context of Web 3.0, they take center stage. By combining a semantic markup and web services, the Web 3.0 promises the potential for applications that can speak to each other directly, and for broader searches for information through simpler interfaces. Figure 2.1 and Table 2.3 show the difference between Web 1.0, Web 2.0, and Web 3.0.

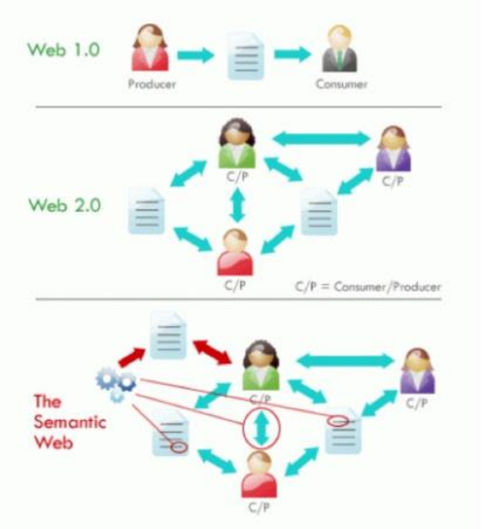
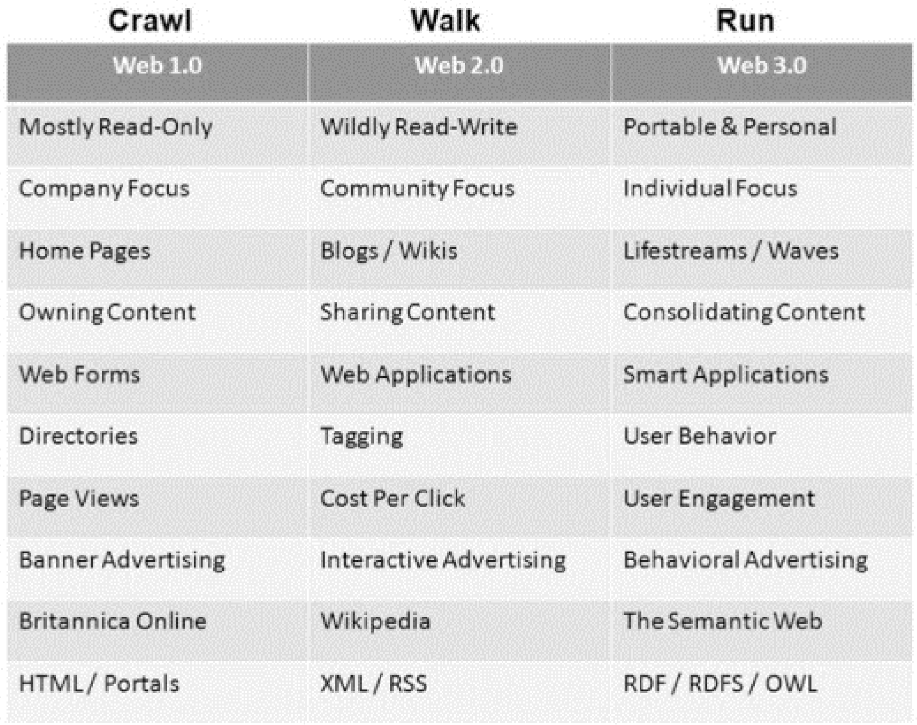


Figure 2.1: The Difference between Web 1.0, Web 2.0, and Web 3.0.

Table 2.3: The Difference between Web 1.0, Web 2.0, and Web 3.0.



Crawl	Walk	Run
Web 1.0	Web 2.0	Web 3.0
Mostly Read-Only	Wildly Read-Write	Portable & Personal
Company Focus	Community Focus	Individual Focus
Home Pages	Blogs / Wikis	Lifestreams / Waves
Owning Content	Sharing Content	Consolidating Content
Web Forms	Web Applications	Smart Applications
Directories	Tagging	User Behavior
Page Views	Cost Per Click	User Engagement
Banner Advertising	Interactive Advertising	Behavioral Advertising
Britannica Online	Wikipedia	The Semantic Web
HTML / Portals	XML / RSS	RDF / RDFS / OWL

2.6 Web 4.0

The next step is not realy a new version, but is a alternate version of what we already have. Web needed to adapt to it's mobile surroundings. Web 4.0 connects all devices in the real and virtual world in real-time.

The web 4.0 is also known as the "Symbiotic Web". The idea being the symbiotic web is that once the metadata are organized (web 3.0), human and machines can interact in symbiosis. Meaning that we would be able to build more powerful interfaces like mind controlled interfaces for example.

2.7 Web 5.0

Although Web 5.0 still is in developing mode and the true shape is still forming, first signals are in that Web 5.0 will be about a linked web which communicates with us like we communicate with each other (like a personal assistant). Web 5.0 is called “symbiotic” web. This Web will be very powerful and fully executing. Web 5.0 will be the read-write-execution-concurrency web.

Web 5.0 will be about the (emotional) interaction between humans and computers. The interaction will become a daily habit for a lot of people based on neurotechnology. For the moment web is “emotionally” neutral, which means web does not perceive the users feel and emotions. This will change with web 5.0 – emotional web. As an example, a web site which maps emotions of people. With headphones on, users will interact with content that interacts with their emotions or changes in facial recognition.

2.8 The Information Systems Department

In all but the smallest of firms, the information systems department is the formal organizational unit responsible for information technology services. ***The information systems department*** is responsible for maintaining the hardware, software, data storage, and networks that comprise the firm’s IT infrastructure. The information systems department consists of specialists, such as programmers, systems analysts, project leaders, and information systems managers.

Programmers are highly trained technical specialists who write the software instructions for computers. ***Systems analysts*** constitute the principal liaisons between the information systems groups and the rest of the organization. It is the systems analyst’s job to translate business problems and requirements into information requirements and systems. ***Information systems managers*** are leaders of teams of programmers and analysts, project managers, physical facility managers, telecommunications managers, or database specialists. They are also managers of computer operations and data entry staff. Also, external specialists, such as hardware vendors and manufacturers, software firms, and consultants, frequently participate in the day-to-day operations and long-term planning of information systems.

In many companies, the information systems department is headed by a ***Chief Information Officer (CIO)***. The CIO is a senior manager who oversees the use of information technology in the firm. Today's CIOs are expected to have a strong business background as well as information systems expertise and to play a leadership role in integrating technology into the firm's business strategy. Large firms today also have positions for a chief security officer, chief knowledge officer, and chief privacy officer, all of whom work closely with the CIO.

The ***Chief Security Officer (CSO)*** is in charge of information systems security for the firm and is responsible for enforcing the firm's information security policy. (Sometimes this position is called the ***Chief Information Security Officer [CISO]*** where information systems security is separated from physical security.) The CSO is responsible for educating and training users and information systems specialists about security, keeping management aware of security threats and breakdowns, and maintaining the tools and policies chosen to implement security.

Information systems security and the need to safeguard personal data have become so important that corporations collecting vast quantities of personal data have established positions for a ***Chief Privacy Officer (CPO)***. The CPO is responsible for ensuring that the company complies with existing data privacy laws.

The ***Chief Knowledge Officer (CKO)*** is responsible for the firm's knowledge management program. The CKO helps design programs and systems to find new sources of knowledge or to make better use of existing knowledge in organizational and management processes.

End users are representatives of departments outside of the information systems group for whom applications are developed. These users are playing an increasingly large role in the design and development of information systems.

2.9 Ethical and Social Issues Related to Systems

Ethics refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors. Information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights, and obligations. Like other technologies, such as steam engines, electricity, the telephone, and the radio, information technology can be used to achieve social progress, but it can also be used to commit crimes and threaten cherished social values. The development of information technology will produce benefits for many and costs for others.

Ethical issues in information systems have been given new urgency by the rise of the Internet and electronic commerce. Internet and digital firm technologies make it easier than ever to assemble, integrate, and distribute information, unleashing new concerns about the appropriate use of customer information, the protection of personal privacy, and the protection of intellectual property.

Other pressing ethical issues raised by information systems include establishing accountability for the consequences of information systems, setting standards to safeguard system quality that protects the safety of the individual and society, and preserving values and institutions considered essential to the quality of life in an information society. When using information systems, it is essential to ask, “What is the ethical and socially responsible course of action?”

2.10 Ethical, Social, and Political Issues

Ethical, social, and political issues are closely linked. The ethical dilemma you may face as a manager of information systems typically is reflected in social and political debate. One way to think about these relationships is given in Figure 1.2. The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: (1) information rights and obligations, (2) property rights and obligations, (3) system quality, (4) quality of life, and (5) accountability and control.

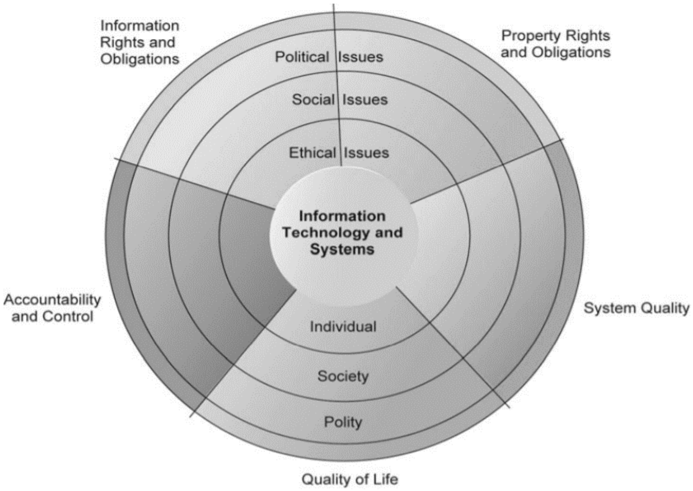

Information Rights and Obligations
Property Rights and Obligations
Political Issues
Social Issues
Ethical Issues
Information Technology and Systems
Accountability and Control
System Quality
Individual
Society
Polity
Quality of Life

Figure 2.2: The Relationship between Ethical, Social, and Political Issues In An Information Society

Imagine society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organizations) have developed well-honed rules of behavior, and these are supported by laws developed in the political sector that prescribe behavior and promise sanctions for violations. Now toss a rock into the center of the pond. What happens? Ripples, of course.

2.10.1 Moral Dimensions of The Information Age

The major ethical, social, and political issues raised by information systems include the following moral dimensions:

1) ***Information rights and obligations***. What information rights do individuals and organizations possess with respect to themselves? What can they protect?

2) ***Property rights and obligations***. How will traditional intellectual property rights be protected in a digital society in which tracing and

accounting for ownership are difficult and ignoring such property rights is so easy?

3) ***Accountability and control***. Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?

4) ***System quality***. What standards of data and system quality should we demand to protect individual rights and the safety of society?

5) ***Quality of life***. What values should be preserved in an information- and knowledge-based society? Which institutions should we protect from violation? Which cultural values and practices are supported by the new information technology?

2.11 Ethics In An Information Society

Ethics is a concern of humans who have freedom of choice. Ethics is about individual choice: When faced with alternative courses of action, what is the correct moral choice? What are the main features of ethical choice?

2.11.1 Responsibility, Accountability, and Liability

Ethical choices are decisions made by individuals who are responsible for the consequences of their actions. ***Responsibility*** is a key element of ethical action. Responsibility means that you accept the potential costs, duties, and obligations for the decisions you make. ***Accountability*** is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action, and who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action. ***Liability*** extends the concept of responsibility further to the area of laws. Liability is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. ***Due process*** is a related feature of law-governed societies and is a process in which laws are known and understood, and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.

These basic concepts form the underpinning of an ethical analysis of information systems and those who manage them. First, information technologies are filtered through social institutions, organizations, and individuals. Systems do not have impacts by themselves. Whatever information system impacts exist are products of institutional, organizational, and individual actions and behaviors. Second, responsibility for the consequences of technology falls clearly on the institutions, organizations, and individual managers who choose to use the technology. Using information technology in a socially responsible manner means that you can and will be held accountable for the consequences of your actions. Third, in an ethical, political society, individuals and others can recover damages done to them through a set of laws characterized by due process.

2.12Privacy

Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Claims to privacy are also involved at the workplace: Millions of employees are subject to electronic and other forms of high-tech surveillance. Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective.

2.12.1 Internet Challenges to Privacy

Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it.

It is possible to record many online activities, including what searches have been conducted, which Web sites and Web pages have been visited, the online content a person has accessed, and what items that person has inspected or purchased over the Web. Tools to monitor visits to the World Wide Web have become popular because they help businesses determine who is visiting their Web sites and how to better target their offerings. (Some firms also monitor the Internet usage of their employees to see how they are using company network resources.) The commercial demand for this personal information is virtually insatiable. Web sites can learn the identities of their visitors if the visitors voluntarily register at the site. Web sites can also capture information about visitors without their knowledge using cookie technology.

Cookies are small text files deposited on a computer hard drive when a user visits Web sites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past. It may also update the cookie, depending on the activity during the visit. In this way, the site can customize its contents for each visitor's interests.

Marketers use Web beacons as another tool to monitor online behavior. ***Web beacons***, also called ***Web bugs***, are tiny objects invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending e-mail. The Web beacon captures and transmits information such as the IP address of the user's computer, the time a Web page was viewed and for how long, the type of Web browser that retrieved the beacon, and previously set cookie values. Web beacons are placed on popular Web sites by "third party" firms who pay the Web sites a fee for access to their audience.

Other ***spyware*** can secretly install itself on an Internet user's computer by piggybacking on larger applications. Once installed, the spyware calls out to Web sites to send banner ads and other unsolicited material to the user, and it can also report the user's movements on the Internet to other computers.

CHAPTER 3
Securing Information Systems

3.1 SYSTEM VULNERABILITY AND ABUSE

Computer systems had been penetrated by outsiders, who perhaps stole or destroyed valuable data, including confidential data. If too much data were destroyed or divulged, your business might never be able to operate!

In short, if you operate a business today, you need to make security and control a top priority. ***Security*** refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems. ***Controls*** are methods, policies, and organizational procedures that ensure the safety of the organization's assets; the accuracy and reliability of its records; and operational adherence to management standards.

When large amounts of data are stored in electronic form, they are vulnerable to many more kinds of threats than when they existed in manual form. Through communications networks, information systems in different locations are interconnected. The potential for unauthorized access, abuse, or fraud is not limited to a single location but can occur at any access point in the network. Figure 3.1 illustrates the most common threats against contemporary information systems. They can stem from technical, organizational, and environmental factors compounded by poor management decisions. In the multi-tier client/server computing environment illustrated here, vulnerabilities exist at each layer and in the communications between the layers. Users at the client layer can cause harm by introducing errors or by accessing systems without authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter messages without authorization. Radiation may disrupt a network at various points as well. Intruders can launch denial-ofservice attacks or malicious software to disrupt the operation of Web sites. Those capable of penetrating corporate systems can destroy or alter corporate data stored in databases or files.

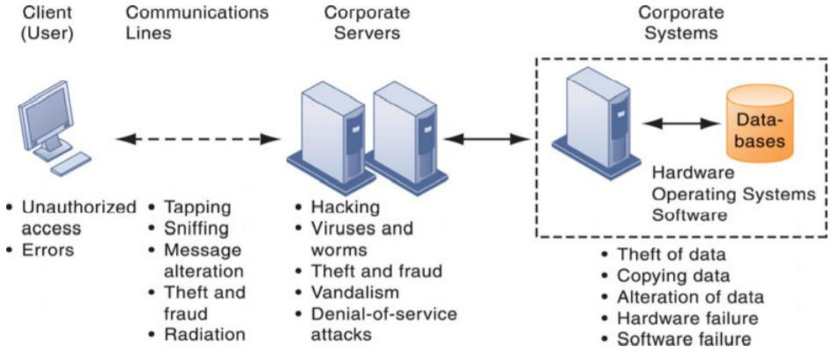


Figure 3.1: Contemporary Security Challenges and Vulnerabilities.

The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

3.2 Malicious Software

Malicious software programs are referred to as ***malware*** and include a variety of threats, such as computer viruses, worms, Trojan horses, SQL injection attacks and spyware. The following susections discuss those terms in details.

3.2.1 virus

A computer virus is a rogue software program that attaches itself to other software programs or data files in order to be executed, usually without user knowledge or permission. Most computer viruses deliver a "payload." The payload may be relatively simple, such as the instructions to display a message or image, or it may be highly destructive, such as destroying programs or data, clogging computer memory, reformatting a computer's hard drive, or causing programs to run improperly. Viruses typically spread from computer to computer when humans take an action, such as sending an e-mail attachment or copying an infected file.

3.2.2 Worms

Most recent attacks have come from worms, which are independent computer programs that copy themselves from one computer to other computers over a network. (Unlike viruses, they can operate on their own without attaching to other computer program files and rely less on human behavior in order to spread from computer to computer. This explains why computer worms spread much more rapidly than computer viruses.) Worms destroy data and programs as well as disrupt or even halt the operation of computer networks.

Over the past decade, worms and viruses have caused billions of dollars of damage to corporate networks, e-mail systems, and data. Table 3.1 describes the characteristics of some of the most harmful worms and viruses that have appeared.

Table 3.1: EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Conficker (aka Downadup, Downup)	Worm	First detected in November 2008. Uses flaws in Windows software to take over machines Downadup, and link them into a virtual computer that can be commanded remotely. Has more than 5 Downup) million computers worldwide under its control. Difficult to eradicate.
Storm	Worm/ Trojan horse	First identified in January 2007. Spreads via e-mail spam with a fake attachment. Trojan horse Infected up to 10 million computers, causing them to join its zombie network of computers engaged in criminal activity.
Sasser.ftp	Worm	First appeared in May 2004. Spread over the Internet by attacking random IP addresses. Causes computers to continually crash and reboot, and infected computers to search for more victims. Affected millions of computers worldwide, disrupting British Airways flight check-ins, operations of British coast guard stations, Hong Kong hospitals, Taiwan post office branches, and Australia’s Westpac Bank. Sasser and its variants caused an estimated $14.8 billion to $18.6 billion in damages worldwide.

MyDoom.A	Worm	First appeared on January 26, 2004. Spreads as an e-mail attachment. Sends e-mail to addresses harvested from infected machines, forging the sender's address. At its peak this worm lowered global Internet performance by 10 percent and Web page loading times by as much as 50 percent. Was programmed to stop spreading after February 12, 2004.
Sobig.F	Worm	First detected on August 19, 2003. Spreads via e-mail attachments and sends massive amounts of mail with forged sender information. Deactivated itself on September 10, 2003, after infecting more than 1 million PCs and doing $5 to $10 billion in damage
ILOVEYOU	Virus	First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overwrites music, image, and other files with a copy of itself and did an estimated $10 billion to $15 billion in damage.
Melissa	Macro virus/ Worm	First appeared in March 1999. Word macro script mailing infected Word file to first 50 worm entries in user's Microsoft Outlook address book. Infected 15 to 29 percent of all business PCs, causing $300 million to $600 million in damage.

3.2.3 Trojan horse

A Trojan horse is a software program that appears to be benign but then does something other than expected, such as the Zeus Trojan described in the chapter-opening case. The Trojan horse is not itself a virus because it does not replicate, but it is often a way for viruses or other malicious code to be introduced into a computer system. The term Trojan horse is based on the huge wooden horse used by the Greeks to trick the Trojans into opening the gates to their fortified city during the Trojan War. Once inside the city walls, Greek soldiers hidden in the horse revealed themselves and captured the city.

3.2.4 SQL injection attacks

At the moment, SQL injection attacks are the largest malware threat. SQL injection attacks take advantage of vulnerabilities in poorly coded Web application software to introduce malicious program code into a company's systems and networks. These vulnerabilities occur when a Web application fails to properly validate or filter data entered by a user on a Web page, which might occur when ordering something online. An attacker uses this input validation error to send a rogue SQL query to the underlying database to access the database, plant malicious code, or access other systems on the network. Large Web applications have hundreds of places for inputting user data, each of which creates an opportunity for an SQL injection attack.

A large number of Web-facing applications are believed to have SQL injection vulnerabilities, and tools are available for hackers to check Web applications for these vulnerabilities. Such tools are able to locate a data entry field on a Web page form, enter data into it, and check the response to see if shows vulnerability to a SQL injection.

3.2.5 Spyware

Some types of spyware also act as malicious software. These small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising. Thousands of forms of spyware have been documented.

Many users find such spyware annoying and some critics worry about its infringement on computer users' privacy. Some forms of spyware are especially nefarious. ***Keyloggers*** record every keystroke made on a computer to steal serial numbers for software, to launch Internet attacks, to gain access to e-mail accounts, to obtain passwords to protected computer systems, or to pick up personal information such as credit card numbers. Other spyware programs reset Web browser home pages, redirect search requests, or slow performance by taking up too much memory.

3.3 Hackers and Computer Crime

A ***hacker*** is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term ***cracker*** is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker are used interchangeably. Hackers and crackers gain unauthorized access by finding weaknesses in the security protections employed by Web sites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use.

Hackers activities have broadened beyond mere system intrusion to include theft of goods and information, as well as system damage and cybervandalism, the intentional disruption, defacement, or even destruction of a Web site or corporate information system.

3.3.1 Spoofing and Sniffing

Hackers attempting to hide their true identities often spoof, or misrepresent, themselves by using fake e-mail addresses or masquerading as someone else. ***Spoofing*** also may involve redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination. For example, if hackers redirect customers to a fake Web site that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business as well as sensitive customer information from the true site. We provide more detail on other forms of spoofing in our discussion of computer crime.

A ***sniffer*** is a type of overhearing program that monitors information traveling over a network. When used legitimately, sniffers help identify potential network trouble spots or criminal activity on networks, but when used for criminal purposes, they can be damaging and very difficult to detect. Sniffers enable hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports.

3.3.2 Denial−of−Service Attacks

In a ***Denial-of-Service (DoS) attack***, hackers flood a network server or Web server with many thousands of false communications or requests for services to crash the network. The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests. ***A distributed denial-of-service (DDoS) attack*** uses numerous computers to flood and overpower the network from numerous launch points.

Although DoS attacks do not destroy information or access restricted areas of a company's information systems, they often cause a Web site to shut down, making it impossible for legitimate users to access the site. For busy e-commerce sites, these attacks are costly.

Perpetrators of DoS attacks often use thousands of "***zombie***" PCs infected with malicious software without their owners' knowledge and organized into a ***botnet***. Hackers create these botnets by infecting other people's computers with bot malware that opens a back door through which an attacker can give instructions. The infected computer then becomes a slave, or zombie, serving a master computer belonging to someone else. Once a hacker infects enough computers, her or she can use the amassed resources of the botnet to launch DDos attacks, phishing campaigns, or unsolicited "spam" e-mail.

3.3.3 Computer Crime

Most hacker activities are criminal offenses, and the vulnerabilities of systems we have just described make them targets for other types of computer crime as well.

Computer crime is defined by the U.S. Department of Justice as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution". The most economically damaging kinds of computer crime are DoS attacks, introducing viruses, theft of services, and disruption of computer systems.

Computer as a target of crime

- Accessing a computer system without authority.
- Knowingly accessing a protected computer to commit fraud.
- Threatening to cause damage to a protected computer.
- Intentionally accessing a protected computer and causing damage, negligently or deliberately.
- Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer.

Computer as an instrument of crime

- Theft of trade secrets.
- Using e-mail for threats or harassment.
- Transmitting or possessing child pornography using a computer.
- Intentionally attempting to intercept electronic communication.
- Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video.
- Illegally accessing stored electronic communications, including e-mail and voice mail.

3.3.4 Click Fraud

When you click on an ad displayed by a search engine, the advertiser typically pays a fee for each click, which is supposed to direct potential buyers to its products. ***Click fraud*** occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase. Click fraud has become a serious problem at Google and other Web sites that feature pay-per-click online advertising.

Some companies hire third parties (typically from low-wage countries) to fraudulently click on a competitor’s ads to weaken them by driving up their marketing costs. Click fraud can also be perpetrated with software programs doing the clicking, and botnets are often used for this purpose. Search engines such as Google attempt to monitor click fraud but have been reluctant to publicize their efforts to deal with the problem.

3.3.5 Global Threats: Cyberterrorism and Cyberwarfare

The cybercriminal activities, launching malware, denial-ofservice attacks, and phishing probes, are borderless. The global nature of the Internet makes it possible for cybercriminals to operate, and to do harm, anywhere in the world.

The vulnerabilities of the Internet or other networks make digital networks easy targets for digital attacks by terrorists, foreign intelligence services, or other groups seeking to create widespread disruption and harm. Such cyberattacks might target the software that runs electrical power grids, air traffic control systems, or networks of major banks and financial institutions.

3.3.6 Internal Threats: Employees

Employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization’s systems without leaving a trace.

Studies have found that user lack of knowledge is the single greatest cause of network security breaches. Many employees forget their passwords to access computer systems or allow co-workers to use them, which compromises the system. Malicious intruders seeking system access sometimes trick employees into revealing their passwords by pretending to be legitimate members of the company in need of information. This practice is called **social *engineering***.

Both end users and information systems specialists are also a major source of errors introduced into information systems. End users introduce errors by entering faulty data or by not following the proper instructions for processing data and using computer equipment. Information systems specialists may create software errors as they design and develop new software or maintain existing programs.

3.4 Software Vulnerability

Software errors pose a constant threat to information systems, causing untold losses in productivity. Growing complexity and size of software programs, coupled with demands for timely delivery to markets, have contributed to an increase in software flaws or vulnerabilities.

3.4.1 Bugs

A major problem with software is the presence of hidden ***bugs*** or program code defects. Studies have shown that it is virtually impossible to eliminate all bugs from large programs. The main source of bugs is the complexity of decision-making code. A relatively small program of several hundred lines will contain tens of decisions leading to hundreds or even thousands of different paths. Important programs within most corporations are usually much larger, containing tens of thousands or even millions of lines of code, each with many times the choices and paths of the smaller programs.

Zero defects cannot be achieved in larger programs. Complete testing simply is not possible. Fully testing programs that contain thousands of choices and millions of paths would require thousands of years. Even with rigorous testing, you would not know for sure that a piece of software was dependable until the product proved itself after much operational use.

To correct software flaws once they are identified, the software vendor creates small pieces of software called ***patches*** to repair the flaws without disturbing the proper operation of the software. It is up to users of the software to track these vulnerabilities, test, and apply all patches. This process is called ***patch management***.

Because a company's IT infrastructure is typically laden with multiple business applications, operating system installations, and other system services, maintaining patches on all devices and services used by a company is often time-consuming and costly. Malware is being created so rapidly that companies have very little time to respond between the time a vulnerability and a patch are announced and the time malicious software appears to exploit the vulnerability.

The need to respond so rapidly to the torrent of security vulnerabilities even creates defects in the software meant to combat them, including popular antivirus products.

3.5 Establishing A Framework For Security And Control

Even with the best security tools, your information systems won’t be reliable and secure unless you know how and where to deploy them. You’ll need to know where your company is at risk and what controls you must have in place to protect your information systems. You’ll also need to develop a security policy and plans for keeping your business running if your information systems aren’t operational.

3.5.1 Information Systems Controls

Information systems controls are both manual and automated and consist of both general controls and application controls.

3.5.1.1 General Controls

General controls govern the design, security, and use of computer programs and the security of data files in general throughout the organization’s information technology infrastructure. On the whole, general controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over implementation of system processes, and administrative controls. Table 3.2 describes the functions of each of these controls.

Table 3.2 General Controls

Type of general control	Description
Software controls	Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.
Hardware controls	Ensure that computer hardware is physically secure, and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed.
Administrative controls	Formalize standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

3.5.1.2 Application controls

Application controls are specific controls unique to each computerized application, such as payroll or order processing. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application. Application controls can be classified as *(1) input controls, (2) processing controls,* and *(3) output controls*. Input controls check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling. Processing controls establish that data are complete and accurate during updating. Output controls ensure that the results of computer processing are accurate, complete, and properly distributed. You can find more detail about application and general controls in our Learning Tracks.

3.5.2 Risk Assessment

Before your company commits resources to security and information systems controls, it must know which assets require protection and the extent to which these assets are vulnerable.

A ***risk assessment*** helps answer these questions and determine the most cost-effective set of controls for protecting assets. A risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled. Not all risks can be anticipated and measured, but most businesses will be able to acquire some understanding of the risks they face. Business managers working with information systems specialists should try to determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage.

Once the risks have been assessed, system builders will concentrate on the control points with the greatest vulnerability and potential for loss. In this case, controls should focus on ways to minimize the risk of power failures and user errors because anticipated annual losses are highest for these areas.

3.5.3 Security Policy

Once you've identified the main risks to your systems, your company will need to develop a security policy for protecting the company's assets. A security policy consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals. What are the firm's most important information assets? Who generates and controls this information in the firm? What existing security policies are in place to protect the information? What level of risk is management willing to accept for each of these assets? Is it willing, for instance, to lose customer credit data once every 10 years? Or will it build a security system for credit card data that can withstand the once-in-a-hundred-year disaster? Management must estimate how much it will cost to achieve this level of acceptable risk.

The security policy drives policies determining acceptable use of the firm's information resources and which members of the company have access to its information assets. An ***acceptable use policy (AUP)*** defines acceptable uses of the firm's information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet. The policy should clarify company policy regarding privacy, user responsibility, and personal use of company equipment and networks. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance.

Security policy also includes provisions for identity management. ***Identity management*** consists of business processes and software tools for identifying the valid users of a system and controlling their access to system resources. It includes policies for identifying and authorizing different categories of system users, specifying what systems or portions of systems each user is allowed to access, and the processes and technologies for authenticating users and protecting their identities.

3.5.4 Disaster Recovery and Business Continuity Planning

If you run a business, you need to plan for events, such as power outages, floods, earthquakes, or terrorist attacks that will prevent your information systems and your business from operating. ***Disaster recovery planning*** devises plans for the restoration of computing and communications services after they have been disrupted. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.

Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down.

Business managers and information technology specialists need to work together on both types of plans to determine which systems and business processes are most critical to the company. They must conduct a business impact analysis to identify the firm's most critical systems and the impact a systems outage would have on the business. Management must determine the maximum amount of time the business can survive with its systems down and which parts of the business must be restored first.

3.5.5 The Role of Auditing

How does management know that information systems security and controls are effective? To answer this question, organizations must conduct comprehensive and systematic audits. An ***MIS audit*** examines the firm's overall security environment as well as controls governing individual information systems. The auditor should trace the flow of sample transactions through the system and perform tests, using, if appropriate, automated audit software. The MIS audit may also examine data quality.

Security audits review technologies, procedures, documentation, training, and personnel. A thorough audit will even simulate an attack or disaster to test the response of the technology, information systems staff, and business employees.

The audit lists and ranks all control weaknesses and estimates the probability of their occurrence. It then assesses the financial and organizational impact of each threat. Management is expected to devise a plan for countering significant weaknesses in controls.

3.6 Technologies and Tools for Protecting Information Resources

Businesses have an array of technologies for protecting their information resources. They include tools for managing user identities, preventing unauthorized access to systems and data, ensuring system availability, and ensuring software quality.

3.6.1 Identity Management and Authentication

Large and midsize companies have complex IT infrastructures and many different systems, each with its own set of users. Identity management software automates the process of keeping track of all these users and their system privileges, assigning each user a unique digital identity for accessing each system. It also includes tools for authenticating users, protecting user identities, and controlling access to system resources.

3.6.1.1 Authentication

To gain access to a system, a user must be authorized and authenticated. ***Authentication*** refers to the ability to know that a person is who he or she claims to be. Authentication is often established by using ***passwords*** known only to authorized users. An end user uses a password to log on to a computer system and may also use passwords for accessing specific systems and files. However, users often forget passwords, share them, or choose poor passwords that are easy to guess, which compromises security. Password systems that are too rigorous hinder employee productivity. When employees must change complex passwords frequently, they often take shortcuts, such as choosing passwords that are easy to guess or writing down their passwords at their workstations in plain view. Passwords can also be “sniffed” if transmitted over a network or stolen through social engineering.

3.6.1.2 Tokens and smart cards

New authentication technologies, such as tokens, smart cards, and biometric authentication, overcome some of these problems. A ***token*** is a physical device, similar to an identification card, that is designed to prove the identity of a single user. Tokens are small gadgets that typically fit on key rings and display passcodes that change frequently. A ***smart card*** is a device about the size of a credit card that contains a chip formatted with access permission and other data. (Smart cards are also used in electronic payment systems.) A reader device interprets the data on the smart card and allows or denies access.

3.6.1.3 Biometric Authentication

Biometric authentication uses systems that read and interpret individual human traits, such as fingerprints, irises, and voices, in order to grant or deny access. Biometric authentication is based on the measurement of a physical or behavioral trait that makes each individual unique. It compares a person's unique characteristics, such as the fingerprints, face, or retinal image, against a stored profile of these characteristics to determine whether there are any differences between these characteristics and the stored profile. If the two profiles match, access is granted. Fingerprint and facial recognition technologies are just beginning to be used for security applications, with many PC laptops equipped with fingerprint identification devices and several models with builtin webcams and face recognition software.

3.6.2 Firewalls, Intrusion Detection Systems, and Antivirus Software

Without protection against malware and intruders, connecting to the Internet would be very dangerous. Firewalls, intrusion detection systems, and antivirus software have become essential business tools.

3.6.2.1 Firewalls

Firewalls prevent unauthorized users from accessing private networks. A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. It is generally placed between the organization's private internal networks and distrusted external networks, such as the Internet, although firewalls can also be used to protect one part of a company's network from the reste of the network. The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic, Figure 3.2.

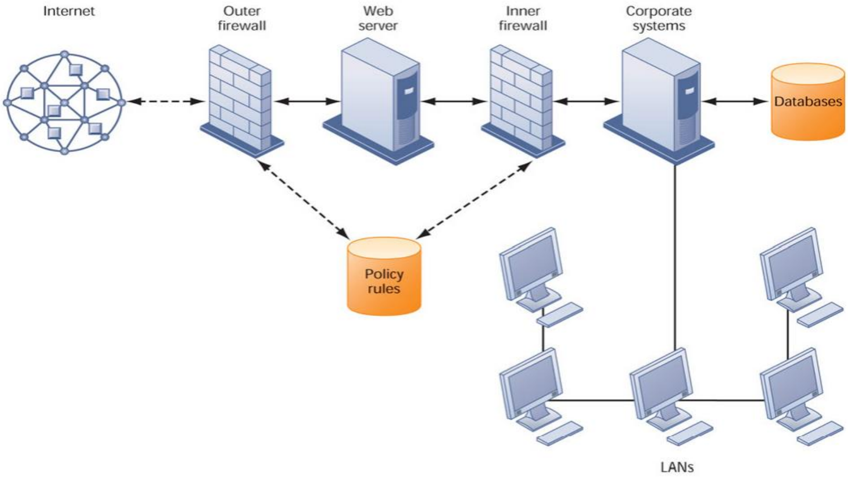


Figure 3.2: A Corporate Firewall.

The firewall acts like a gatekeeper who examines each user's credentials before access is granted to a network. The firewall identifies names, IP addresses, applications, and other characteristics of incoming traffic. It checks this information against the access rules that have been programmed into the system by the network administrator. The firewall prevents unauthorized communication into and out of the network.

In large organizations, the firewall often resides on a specially designated computer separate from the rest of the network, so no incoming request directly accesses private network resources. There are a number of firewall screening technologies, including static packet filtering, stateful inspection, Network Address Translation, and application proxy filtering. They are frequently used in combination to provide firewall protection.

Packet filtering examines selected fields in the headers of data packets flowing back and forth between the trusted network and the Internet, examining individual packets in isolation. This filtering technology can miss many types of attacks. ***Stateful inspection*** provides additional security by determining whether packets are part of an ongoing dialogue between a sender and a receiver. It sets up state tables to track information over multiple packets. Packets are accepted or rejected based on whether they are part of an approved conversation or whether they are attempting to establish a legitimate connection.

Network Address Translation (NAT) can provide another layer of protection when static packet filtering and stateful inspection are employed. NAT conceals the IP addresses of the organization's internal host computer(s) to prevent sniffer programs outside the firewall from ascertaining them and using that information to penetrate internal systems.

Application proxy filtering examines the application content of packets. A proxy server stops data packets originating outside the organization, inspects them, and passes a proxy to the other side of the firewall. If a user outside the company wants to communicate with a user inside the organization, the outside user first "talks" to the proxy application and the proxy application communicates with the firm's internal computer. Likewise, a computer user inside the organization goes through the proxy to talk with computers on the outside.

To create a good firewall, an administrator must maintain detailed internal rules identifying the people, applications, or addresses that are allowed or rejected. Firewalls can deter, but not completely prevent, network penetration by outsiders and should be viewed as one element in an overall security plan.

3.6.2.2 Intrusion Detection Systems

In addition to firewalls, commercial security vendors now provide intrusion detection tools and services to protect against suspicious network traffic and attempts to access files and databases. ***Intrusion detection systems*** feature full-time monitoring tools placed at the most vulnerable points or "hot spots" of corporate networks to detect and deter intruders continually. The system generates an alarm if it finds a suspicious or anomalous event. Scanning software looks for patterns indicative of known methods of computer attacks, such as bad passwords, checks to see if important files have been removed or modified, and sends warnings of vandalism or system administration errors. Monitoring software examines events as they are happening to discover security attacks in progress. The intrusion detection tool can also be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

3.6.2.3 Antivirus and Antispyware Software

Defensive technology plans for both individuals and businesses must include antivirus protection for every computer. ***Antivirus software*** is designed to check computer systems and drives for the presence of computer viruses. Often the software eliminates the virus from the infected area. However, most antivirus software is effective only against viruses already known when the software was written. To remain effective, the antivirus software must be continually updated. Antivirus products are available for many different types of mobile and handheld devices in addition to servers, workstations, and desktop PCs.

Leading antivirus software vendors, such as McAfee, Symantec, and Trend Micro, have enhanced their products to include protection against spyware. Antispyware software tools such as Ad-Aware, Spybot S&D, and Spyware Doctor are also very helpful.

3.6.2.4 Unified Threat Management Systems

To help businesses reduce costs and improve manageability, security vendors have combined into a single appliance various security tools, including firewalls, virtual private networks, intrusion detection systems, and Web content filtering and antispam software. These comprehensive security management products are called ***unified threat management (UTM)*** systems. Although initially aimed at small and medium-sized businesss, UTM products are available for all sizes of networks. Leading UTM vendors include Crossbeam, Fortinent, and Check Point, and networking vendors such as Cisco Systems and Juniper Networks provide some UTM capabilities in their equipment.

3.6.3 Securing Wireless Networks

Despite its flaws, WEP provides some margin of security if Wi-Fi users remember to activate it. A simple first step to thwart hackers is to assign a unique name to your network's SSID and instruct your router not to broadcast it. Corporations can further improve Wi-Fi security by using it in conjunction with virtual private network (VPN) technology when accessing internal corporate data.

In June 2004, the Wi-Fi Alliance industry trade group finalized the 802.11i specification (also referred to as Wi-Fi Protected Access 2 or WPA2) that replaces WEP with stronger security standards. Instead of the static encryption keys used in WEP, the new standard uses much longer keys that continually change, making them harder to crack. It also employs an encrypted authentication system with a central authentication server to ensure that only authorized users access the network.

3.6.3.1 Encryption and Public Key Infrastructure

Many businesses use encryption to protect digital information that they store, physically transfer, or send over the Internet. ***Encryption*** is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver. Data are encrypted by using a secret numerical code, called an encryption key, that transforms plain data into cipher text. The message must be decrypted by the receiver.

Two methods for encrypting network traffic on the Web are SSL and S-HTTP. ***Secure Sockets Layer (SSL)*** and its successor ***Transport Layer Security (TLS)*** enable client and server computers to manage encryption and decryption activities as they communicate with each other during a secure Web session. ***Secure Hypertext Transfer Protocol (S-HTTP)*** is another protocol used for encrypting data flowing over the Internet, but it is limited to individual messages, whereas SSL and TLS are designed to establish a secure connection between two computers.

The capability to generate secure sessions is built into Internet client browser software and servers. The client and the server negotiate what key and what level of security to use. Once a secure session is established between the client and the server, all messages in that session are encrypted.

There are two alternative methods of encryption: symmetric key encryption and public key encryption. In ***symmetric key encryption***, the sender and receiver establish a secure Internet session by creating a single encryption key and sending it to the receiver so both the sender and receiver share the same key. The strength of the encryption key is measured by its bit length, a typical key will be 128 bits long (a string of 128 binary digits).

The problem with all symmetric encryption schemes is that the key itself must be shared somehow among the senders and receivers, which exposes the key to outsiders who might just be able to intercept and decrypt the key. A more secure form of encryption called ***Asymmetric key encryption or public key encryption*** uses two keys: one shared (or public) and one totally private as shown in Figure 3.3. The keys are mathematically related so that data encrypted with one key can be decrypted using only the other key. To send and receive messages, communicators first create separate pairs of private and public keys. The public key is kept in a directory and the private key must be kept secret. The sender encrypts a message with the recipient's public key. On receiving the message, the recipient uses his or her private key to decrypt it.

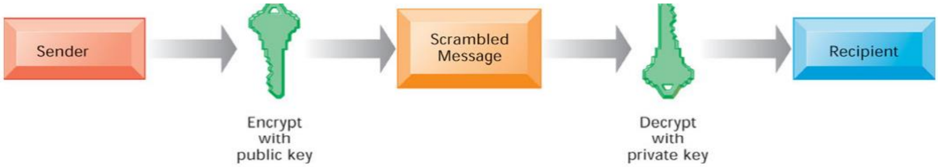


Figure 3.3: Public Key Encryption

A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.

Digital certificates are data files used to establish the identity of users and electronic assets for protection of online transactions, Figure 3.4. A digital certificate system uses a trusted third party, known as a ***certificate authority*** (CA, or certification authority), to validate a user's identity. Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication. There are many CAs in the United States and around the world, including VeriSign, IdenTrust, and Australia's KeyPost.

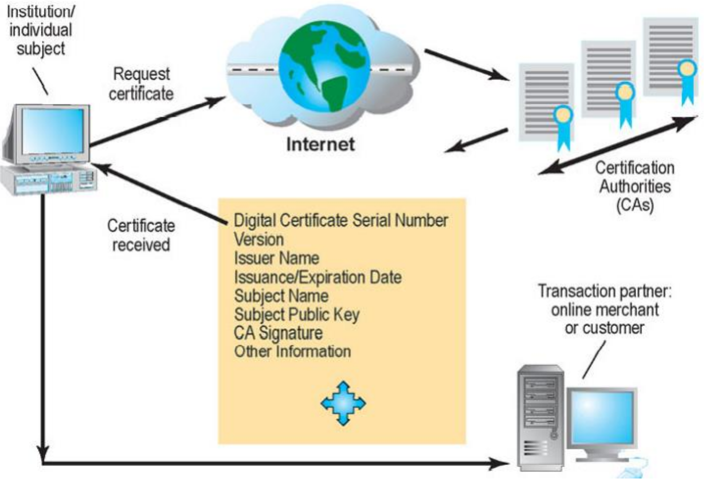


Figure 3.4: Digital Certificates

The CA verifies a digital certificate user's identity offline. This information is put into a CA server, which generates an encrypted digital certificate containing owner identification information and a copy of the owner's public key. The certificate authenticates that the public key belongs to the designated owner. The CA makes its own public key available publicly either in print or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it was issued by the CA, and then obtains the sender's public key and identification information contained in the certificate. Using this information, the recipient can send an encrypted reply. The digital certificate system would enable, for example, a credit card user and a merchant to validate that their digital certificates were issued by an authorized and trusted third party before they exchange data. Public key infrastructure (PKI), the use of public key cryptography working with a CA, is now widely used in e-commerce.

3.6.4 Ensuring System Availability

As companies increasingly rely on digital networks for revenue and operations, they need to take additional steps to ensure that their systems and applications are always available. Firms such as those in the airline and financial services industries with critical applications requiring online transaction processing have traditionally used fault-tolerant computer systems for many years to ensure 100-percent availability. In ***online transaction processing***, transactions entered online are immediately processed by the computer. Multitudinous changes to databases, reporting, and requests for information occur each instant.

Fault-tolerant computer systems contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service. Fault-tolerant computers use special software routines or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device. Parts from these computers can be removed and repaired without disruption to the computer system.

Fault tolerance should be distinguished from high-availability computing. Both fault tolerance and high-availability computing try to minimize downtime. ***Downtime*** refers to periods of time in which a system is not operational. However, high-availability computing helps firms recover quickly from a system crash, whereas fault tolerance promises continuous availability and the elimination of recovery time altogether.

High-availability computing environments are a minimum requirement for firms with heavy e-commerce processing or for firms that depend on digital networks for their internal operations. High-availability computing requires backup servers, distribution of processing across multiple servers, high-capacity storage, and good disaster recovery and business continuity plans. The firm's computing platform must be extremely robust with scalable processing power, storage, and bandwidth.

Researchers are exploring ways to make computing systems recover even more rapidly when mishaps occur, an approach called ***recovery-oriented computing***. This work includes designing systems that recover quickly, and implementing capabilities and tools to help operators pinpoint the sources of faults in multi-component systems and easily correct their mistakes.

3.6.5 Controlling Network Traffic: Deep Packet Inspection

Have you ever tried to use your campus network and found it was very slow? It may be because your fellow students are using the network to download music or watch YouTube. Bandwith-consuming applications such as file-sharing programs, Internet phone service, and online video are able to clog and slow down corporate networks, degrading performance. For example, Ball Sate University in Muncie, Indiana, found its network had slowed because a small minority of students were using peer-to-peer file-sharing programs to download movies and music.

A technology called ***deep packet inspection (DPI)*** helps solve this problem. DPI examines data files and sorts out low-priority online material while assigning higher priority to business-critical files. Based on the priorities established by a network's operators, it decides whether a specific data packet can continue to its destination or should be blocked or delayed while more important traffic proceeds. Using a DPI system from Allot Communications, Ball State was able to cap the amount of file-sharing traffic and assign it a much lower priority. Ball State's preferred network traffic speeded up.

3.6.6 Security Outsourcing

Many companies, especially small businesses, lack the resources or expertise to provide a secure high-availability computing environment on their own. They can outsource many security functions to ***Managed Security Service Providers (MSSPs)*** that monitor network activity and perform vulnerability testing and intrusion detection. SecureWorks and Symantec are leading providers of MSSP services.

3.7 Ensuring Software Quality

In addition to implementing effective security and controls, organizations can improve system quality and reliability by employing software metrics and rigorous software testing. ***Software metrics*** are objective assessments of the system in the form of quantified measurements. Ongoing use of metrics allows the information systems department and end users to jointly measure the performance of the system and identify problems as they occur. Examples of software metrics include the number of transactions that can be processed in a specified unit of time, online response time, the number of payroll checks printed per hour, and the number of known bugs per hundred lines of program code. For metrics to be successful, they must be carefully designed, formal, objective, and used consistently.

Early, regular, and thorough testing will contribute significantly to system quality. Many view testing as a way to prove the correctness of work they have done. In fact, we know that all sizable software is riddled with errors, and we must test to uncover these errors.

Good testing begins before a software program is even written by using a ***walkthrough***, a review of a specification or design document by a small group of people carefully selected based on the skills needed for the particular objectives being tested. Once developers start writing software programs, coding walkthroughs also can be used to review program code. However, code must be tested by computer runs. When errors are discovered, the source is found and eliminated through a process called ***debugging***.

3.8 Establishing An Information Policy

Every business, large and small, needs an information policy. Your firm's data are an important resource, and you don't want people doing whatever they want with them. You need to have rules on how the data are to be organized/maintained, and who is allowed to view/change data.

An ***information policy*** specifies the organization's rules for sharing, disseminating, acquiring, standardizing, classifying, and inventorying information. Information policy lays out specific procedures and accountabilities, identifying which users and organizational units can share information, where information can be distributed, and who is responsible for updating and maintaining the information. For example, a typical information policy would specify that only selected members of the payroll and human resources department would have the right to change and view sensitive employee data, such as an employee's salary or social security number, and that these departments are responsible for making sure that such employee data are accurate.

If you are in a small business, the information policy would be established and implemented by the owners or managers. In a large organization, managing and planning for information as a corporate resource often requires a formal data administration function. ***Data administration*** is responsible for the specific policies and procedures through which data can be managed as an organizational resource. These responsibilities include developing information policy, planning for data, overseeing logical database design and data dictionary development, and monitoring how information systems specialists and end-user groups use data.

You may hear the term ***data governance*** used to describe many of these activities. Promoted by IBM, data governance deals with the policies and processes for managing the availability, usability, integrity, and security of the data employed in an enterprise, with special emphasis on promoting privacy, security, data quality, and compliance with government regulations.

A large organization will also have a database design and management group within the corporate information systems division that is responsible for defining and organizing the structure and content of the database, and maintaining the database. In close cooperation with users, the design group establishes the physical database, the logical relations among elements, and the access rules and security procedures. The functions it performs are called ***database administration***.

3.8.1 Ensuring Data Quality

A well-designed database and information policy will go a long way toward ensuring that the business has the information it needs. However, additional steps must be taken to ensure that the data in organizational databases are accurate and remain reliable.

If a database is properly designed and enterprise-wide data standards established, duplicate or inconsistent data elements should be minimal. Most data quality problems, however, such as misspelled names, transposed numbers, or incorrect or missing codes, stem from errors during data input.

Before a new database is in place, organizations need to identify and correct their faulty data and establish better routines for editing data once their database is in operation. Analysis of data quality often begins with a ***data quality audit***, which is a structured survey of the accuracy and level of completeness of the data in an information system. Data quality audits can be performed by surveying entire data files, surveying samples from data files, or surveying end users for their perceptions of data quality.

Data cleansing, also known as ***data scrubbing***, consists of activities for detecting and correcting data in a database that are incorrect, incomplete, improperly formatted, or redundant. Data cleansing not only corrects errors but also enforces consistency among different sets of data that originated in separate information systems. Specialized data-cleansing software is available to automatically survey data files, correct errors in the data, and integrate the data in a consistent company-wide format.

CHAPTER 4
ENHENCING DECISION MAKING

4.1 Decision Making and Information Systems

Decision making in businesses used to be limited to management. Today, lower-level employees are responsible for some of these decisions, as information systems make information available to lower levels of the business. But what do we mean by better decision making? How does decision making take place in businesses and other organizations?

4.1.1 Types of Decisions

Section 1.6 showed that there are different managerial levels in an organization. Each of these levels has different information requirements for decision support and responsibility for different types of problems and decisions, Figure 4.1. Decisions are classified as structured, semistructured, and unstructured.

- ***Unstructured decisions*** are those in which the decision maker must provide judgment, evaluation, and insight to solve the problem. Each of these decisions is novel, important, and nonroutine, and there is no well-understood or agreed-on procedure for making them.
- ***Structured decisions***, are repetitive and routine, they involve a definite **preprogrammed** procedure for handling them so that they do not have to be treated each time as if they were new.
- ***Semistructured decisions***, have elements of both types of decisions where only part of the problem has a clear-cut answer provided by an accepted procedure. In general, structured decisions are more prevalent at lower organizational levels, whereas unstructured problems are more common at higher levels of the firm.

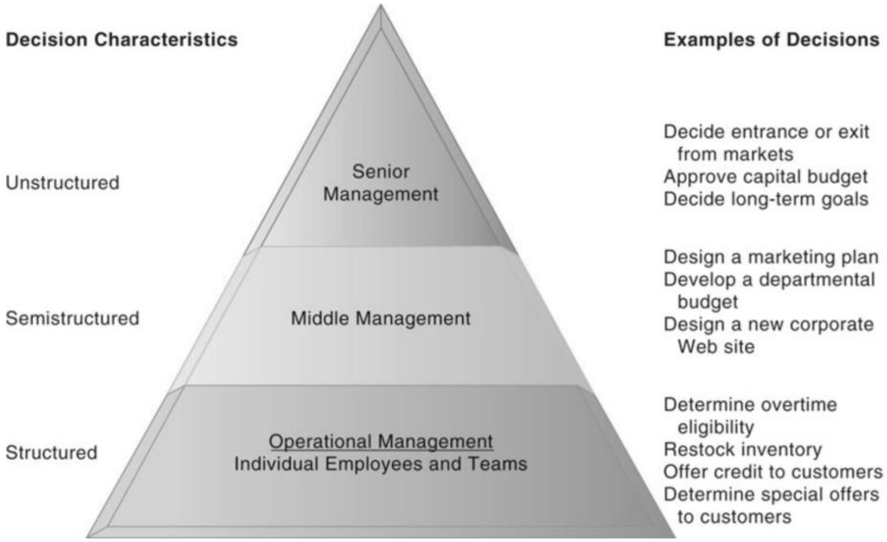


Figure 4.1: Types of Decisions and Information Requirements

Senior executives face many unstructured decision situations, such as establishing the firm's five- or ten-year goals or deciding new markets to enter. Answering the question "Should we enter a new market?" would require access to news, government reports, and industry views as well as high-level summaries of firm performance. However, the answer would also require senior managers to use their own best judgment and poll other managers for their opinions.

Middle management faces more structured decision scenarios but their decisions may include unstructured components. A typical middle-level management decision might be "Why is the reported order fulfillment report showing a decline over the past six months at a distribution center in Minneapolis?" This middle manager will obtain a report from the firm's enterprise system or distribution management system on order activity and operational efficiency at the Minneapolis distribution center. This is the structured part of the decision. But before arriving at an answer, this middle manager will have to interview employees and gather more unstructured information from external sources about local economic conditions or sales trends.

Operational management and rank-and-file employees tend to make more structured decisions. For example, a supervisor on an assembly line has to decide whether an hourly paid worker is entitled to overtime pay. If the employee worked more than eight hours on a particular day, the supervisor would routinely grant overtime pay for any time beyond eight hours that was clocked on that day.

4.1.2 The Decision−Making Process

Making a decision is a multistep process. There are four different stages in decision making: intelligence, design, choice, and implementation, Figure 2.2.

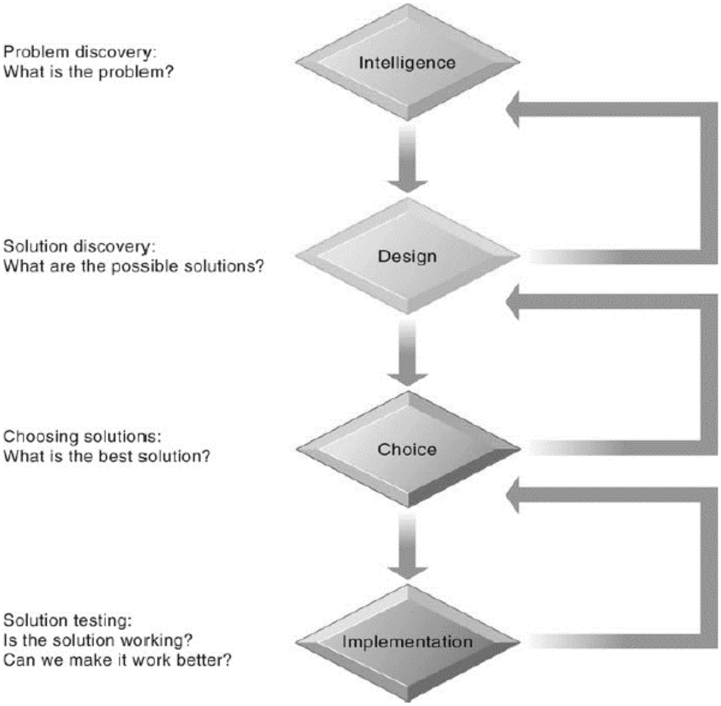


Figure 2.2: Stages in Decision Making.

- ***<u>Intelligence</u>*** consists of discovering, identifying, and understanding the problems occurring in the organization—why a problem exists, where, and what effects it is having on the firm.

- ***Design*** involves identifying and exploring various solutions to the problem.
- ***Choice*** consists of choosing among solution alternatives.
- ***Implementation*** involves making the chosen alternative work and continuing to monitor how well the solution is working.

The Figure shows that you can return to an earlier stage in the decision-making process and repeat it if necessary.

4.1.3 Managerial Roles

Managers play key roles in organizations. Their responsibilities range from making decisions, to writing reports, to attending meetings, to arranging birthday parties. ***Managerial roles*** are expectations of the activities that managers should perform in an organization. We are able to better understand managerial functions and roles by examining classical and contemporary models of managerial behavior.

4.1.3.1 Classical and Behavioral Model

The ***classical model of management***, which describes what managers do. Early writers first described the five classical functions of managers as planning, organizing, coordinating, deciding, and controlling. This description of management activities dominated management thought for a long time, and it is still popular today.

The classical model describes formal managerial functions but does not address what exactly managers do when they plan, decide things, and control the work of others. For this, we must turn to the work of contemporary behavioral scientists who have studied managers in daily action.

The ***Behavioral models*** state that the actual behavior of managers appears to be less systematic, more informal, less reflective, more reactive, and less well organized than the classical model would have us believe.

Observers find that managerial behavior actually has five attributes that differ greatly from the classical description. First, managers perform a great deal of work at an unrelenting pace, with no break in their pace. Second, managerial activities are fragmented; most activities last for less than nine minutes, and only 10 percent of the activities exceed one hour in duration. Third, managers prefer current, specific, and ad hoc information (printed information often will be too old). Fourth, they prefer oral forms of communication to written forms because oral media provide greater flexibility, require less effort, and bring a faster response. Fifth, managers give high priority to maintaining a diverse and complex web of contacts that acts as an informal information system and helps them execute their personal agendas and short/long-term goals.

4.1.3.2 Interpersonal, Informational, and Decisional Models

By analyzing managers' day-to-day behavior, it is found that managers' behaviors could be classified into 10 managerial roles, whitch fell into three categories: interpersonal, informational, and decisional.

Interpersonal Roles. Managers act as figureheads for the organization when they represent their companies to the outside world and perform symbolic duties, such as giving out employee awards, in their interpersonal role. Managers act as leaders, attempting to motivate, counsel, and support subordinates. Managers also act as contacts between various organizational levels; within each of these levels, they serve as contacts among the members of the management team. Managers provide time and favors, which they expect to be returned.

Informational Roles. In their informational role, managers act as the nerve centers of their organizations, receiving the most concrete, up-to-date information and redistributing it to those who need to be aware of it. Managers are therefore information disseminators and spokespersons for their organizations.

Decisional Roles. Managers make decisions. In their decisional role, they act as business mans by initiating new kinds of activities; they handle disturbances arising in the organization; they allocate resources to staff members who need them; and they negotiate conflicts and mediate between conflicting groups.

4.1.4 Real–World Decision Making

We now see that information systems are not helpful for all managerial roles. And in those managerial roles where information systems might improve decisions, investments in information technology do not always produce positive results. There are three main reasons: information quality, management filters, and organizational culture.

4.1.4.1 Information Quality

High-quality decisions require high-quality information. Table 2.1 describes information quality dimensions that affect the quality of decisions. If the output of information systems does not meet these quality criteria, decision-making will suffer.

Table 2.1 Describes Information Quality Dimensions That Affect The Quality Of Decisions

Quality dimension	Description
Accuracy	Do the data represent reality?
Integrity	Are the structure of data and relationships among the entities and attributes consistent?
Consistency	Are data elements consistently defined?
Completeness	Are all the necessary data present?
Validity	Do data values fall within defined ranges?
Timeliness	Area data available when needed?
Accessibility	Are the data accessible, comprehensible, and usable?

4.1.4.2 Management Filters.

Even with timely, accurate information, some managers make bad decisions. Managers (like all human beings) absorb information through a series of filters to make sense of the world around them. Managers have selective attention, focus on certain kinds of problems and solutions, and have a variety of biases that reject information that does not conform to their prior conceptions.

4.1.4.3 Organizational Inertia and Politics.

Organizations are bureaucracies with limited capabilities and competencies for acting decisively. When environments change and businesses need to adopt new business models to survive, strong forces within organizations resist making decisions calling for major change. Decisions taken by a firm often represent a balancing of the firm's various interest groups rather than the best solution to the problem.

Studies of business restructuring find that firms tend to ignore poor performance until threatened by outside takeovers, and they systematically blame poor performance on external forces beyond their control such as economic conditions (the economy), foreign competition, and rising prices, rather than blaming senior or middle management for poor business judgment.

4.2 Business Intelligence

When we think of humans as intelligent beings we often refer to their ability to take in data from their environment, understand the meaning and significance of the information, and then act appropriately.

Business intelligence is a term used by hardware and software vendors and information technology consultants to describe the infrastructure for warehousing, integrating, reporting, and analyzing data that comes from the business environment. The foundation infrastructure collects, stores, cleans, and makes relevant information available to managers using ***databases***, ***data warehouses***, and ***data marts***.

A ***Databases (DB)*** is an organized collection of data, generally stored an accessed electronically from a computer system. It is usually controlled by a ***Database Management System (DBMS)***. Together, the data and the DBMS, along with the applications that are associated with them, are referred to as a ***Database System (DBS)***.

A ***Data Warehouse (DW)*** is a system used for reporting and data analysis. It is considered a core component of BI. DWs are central repositories of integrated data from one or more disparate sources. They store current and historical data in one single place that are used for creating analytical reports for workers throughout the enterprise.

A ***Data Mart (DM)*** is a structure/access pattern specific to data warehouse environments, used to retrieve client-fcing data. The data mart is a subset of the data warehouse and is usually oriented to a specific business line or team. Whereas data warehouses have an enterprise-wide depth, the information in data marts pertains to a single department and focused on a single subject.

Business analytics is also a vendor-defined term that focuses more on tools and techniques for analyzing and understanding data using ***online analytical processing (OLAP)***, statistics, models, and data mining.

Business intelligence and analytics are products defined by technology vendors and consulting firms. They consist of hardware and software suites sold primarily by large system vendors. They are about integrating all the information streams produced by a firm into a single, coherent enterprise-wide set of data, and then, using modeling, statistical analysis tools (like normal distributions, correlation and regression analysis, Chi square analysis, forecasting, and cluster analysis), and data mining tools (pattern discovery and machine learning), to make sense out of all these data so managers can make better decisions and better plans, or at least know quickly when their firms are failing to meet planned targets. The largest five providers of these products are SAP, Oracle, IBM, SAS Institute, and Microsoft.

4.2.1 The Business Intelligence Environment

Business intelligence and analytics requires a strong database foundation, a set of analytic tools, and an involved management team that can ask intelligent questions and analyze data. Figure 2.3 gives an overview of a business intelligence environment, highlighting the kinds of hardware, software, and management capabilities that the major vendors offer and that firms develop over time. There are six elements in this business intelligence environment:

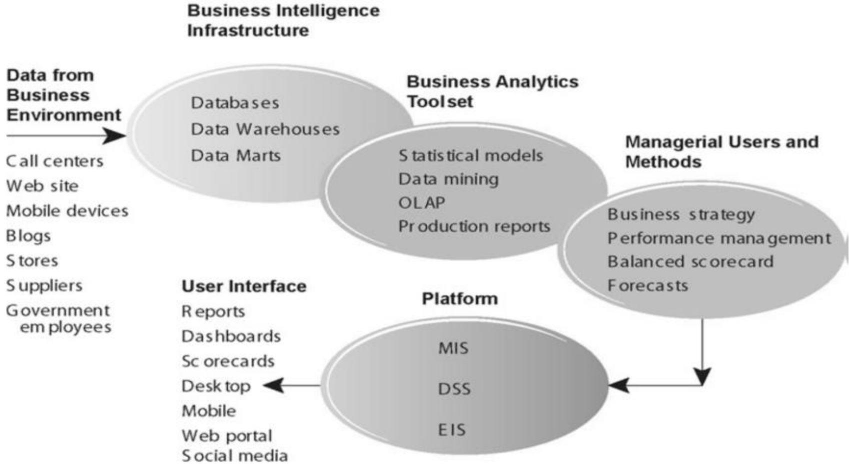


Figure 2.3: Business Intelligence Environment.

1- ***Data from the business environment:*** Businesses must deal with both structured and unstructured data from many different sources, including mobile devices and the Internet. The data need to be integrated and organized so that they can be analyzed and used by human decision makers.

2- ***Business intelligence infrastructure:*** The underlying foundation of business intelligence is a powerful database system that captures all the relevant data to operate the business. The data may be stored in transactional databases or combined and integrated into an enterprise-data warehouse or series of interrelated data marts.

3- ***Business analytics toolset:*** A set of software tools are used to analyze data and produce reports, respond to questions posed by managers, and track the progress of the business using key indicators of performance.

4- ***Managerial users and methods:*** Business intelligence hardware and software are only as intelligent as the human beings who use them. Managers impose order on the analysis of data using a variety of managerial methods that define strategic business goals and specify how progress will be measured. These include business performance management and balanced scorecard approaches focusing on key performance indicators and industry strategic analyses focusing on changes in the general business environment, with special attention to competitors. Without strong senior management oversight, business analytics can produce a great deal of information, reports, and online screens that focus on the wrong matters and divert attention from the real issues. You need to remember that, so far, only humans can ask intelligent questions.

5- ***Delivery platform—MIS, DSS, ESS.*** The results from business intelligence and analytics are delivered to managers and employees in a variety of ways, depending on what they need to know to perform their jobs. MIS, DSS, and ESS, which we introduced in Chapter 1, deliver information and knowledge to different people and levels in the firm—operational employees, middle managers, and senior executives. In the past, these systems could not share data and operated as independent systems. Today, one suite of hardware and software tools in the form of a business intelligence and analytics package is able to integrate all this information and bring it to managers' desktop or mobile platforms.

6- ***User interface:*** Business people are no longer tied to their desks and desktops. They often learn quicker from a visual representation of data than from a dry report with columns and rows of information. Today's business analytics software suites emphasize visual techniques such as dashboards and scorecards. They also are able to deliver reports on Blackberrys, iPhones, and other mobile handhelds as well as on the firm's Web portal. BA software is adding capabilities to post information on Twitter, Facebook, or internal social media to support decision making in an online group setting rather than in a face-to-face meeting.

4.2.2 Business Intelligence and Analytics Capabilities

Business intelligence and analytics promise to deliver correct, nearly real-time information to decision makers, and the analytic tools help them quickly understand the information and take action. There are analytic functionalities that BI systems deliver to achieve these ends:

1- ***Production reports.*** These are predefined reports based on industry-specific requirements.

2- ***Parameterized reports.*** Users enter several parameters as in a pivot table to filter data and isolate impacts of parameters. For instance, you might want to enter region and time of day to understand how sales of a product vary by region and time.

3- ***Dashboards/scorecards.*** These are visual tools for presenting performance data defined by users

4- ***Ad hoc query/search/report creation.*** These allow users to create their own reports based on queries and searches

5- ***Drill down.*** This is the ability to move from a high-level summary to a more detailed view

6- ***Forecasts, scenarios, models.*** These include the ability to perform linear forecasting, what-if scenario analysis, and analyze data using standard statistical tools.

4.3 Decision Support for Different Management Levels

4.3.1 Support for Operational And Middle Management

Operational and middle management are generally charged with monitoring the performance of key aspects of the business, ranging from the down-time of machines on a factory floor, to the daily or even hourly sales at franchise food stores, to the daily traffic at a company’s Web site. Most of the decisions they make are fairly structured. Management information systems (MIS) are typically used by middle managers to support this type of decision making, and their primary output is a set of routine production reports based on data extracted and summarized from the firm's underlying transaction processing systems (TPS). Increasingly, middle managers receive these reports online on the company portal, and are able to interactively query the data to find out why events are happening. To save even more analysis time, managers turn to exception reports, which highlight only exceptional conditions, such as when the sales quotas for a specific territory fall below an anticipated level or employees have exceeded their spending limits in a dental care plan.

4.3.2 Support for Semistructured Decisions

Some managers are "super users" and keen business analysts who want to create their own reports, and use more sophisticated analytics and models to find patterns in data, to model alternative business scenarios, or to test specific hypotheses. ***Decision support systems (DSS)*** are the BI delivery platform for this category of users, with the ability to support semi-structured decision making.

DSS rely more heavily on modeling than MIS, using mathematical or analytical models to perform what-if or other kinds of analysis. ***"What-if" analysis***, working forward from known or assumed conditions, allows the user to vary certain values to test results to predict outcomes if changes occur in those values. What happens if we raise product prices by 5 percent or increase the advertising budget by $1 million? ***Sensitivity analysis*** models ask what-if questions repeatedly to predict a range of outcomes when one or more variables are changed multiple times. ***Backward sensitivity analysis*** helps decision makers with ***goal seeking***: If I want to sell 1 million product units next year, how much must I reduce the price of the product?

Spreadsheets have a similar feature for multidimensional analysis called a ***pivot table***, which manager "super users" and analysts employ to identify and understand patterns in business information that may be useful for semistructured decision making.

4.3.3 Support for Senior Management

The leading methodology for understanding the really important information needed by a firm's executives is called the ***balanced scorecard method***. The balanced score card is a framework for operationalizing a firm's strategic plan by focusing on measurable outcomes on four dimensions of firm performance: financial, business process, customer, and learning and growth, Figure 4.2.

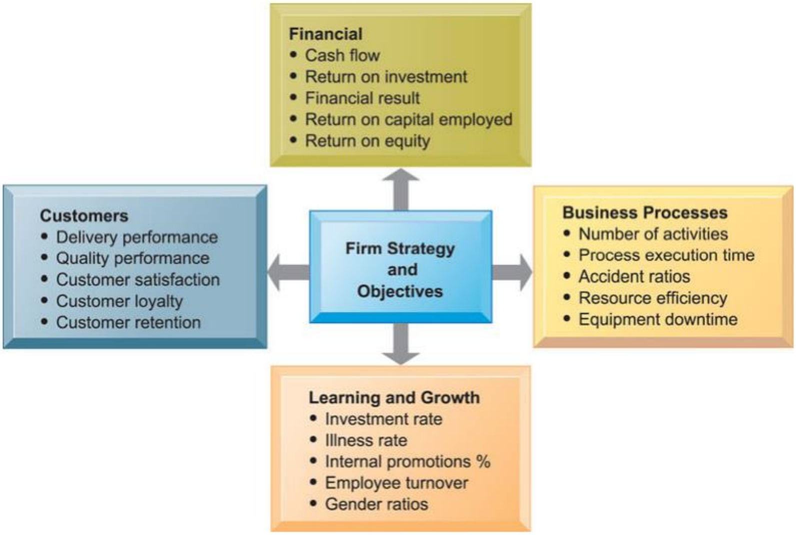


Figure 4.2: The Balanced Scorecard Framework

In the balanced scorecard framework, the firm's strategic objectives are operationalized along four dimensions: financial, business process, customer, and learning and growth. Each dimension is measured using several ***key performance indicators (KPIs)***.

Performance on each dimension is measured using KPIs, which are the measures proposed by senior management for understanding how well the firm is performing along any given dimension. For instance, one key indicator of how well an online retail firm is meeting its customer performance objectives is the average length of time required to deliver a package to a consumer. If your firm is a bank, one KPI of business process performance is the length of time required to perform a basic function like creating a new customer account.

The balanced scorecard framework is thought to be “balanced” because it causes managers to focus on more than just financial performance. In this view, financial performance is past history, the result of past actions, and managers should focus on the things they are able to influence today, such as business process efficiency, customer satisfaction, and employee training. Once a scorecard is developed by consultants and senior executives, the next step is automating a flow of information to executives and other managers for each of the key performance indicators. There are literally hundreds of consulting and software firms that offer these capabilities, which are described below. Once these systems are implemented, they are often referred to as ESS.

Another closely related popular management methodology is ***business performance management (BPM)***. BPM attempts to systematically translate a firm’s strategies (e.g., differentiation, low-cost producer, market share growth, and scope of operation) into operational targets. Once the strategies and targets are identified, a set of KPIs are developed that measure progress towards the targets. The firm’s performance is then measured with information drawn from the firm’s enterprise database systems. BPM uses the same ideas as balanced scorecard but with a stronger strategy flavor.

Corporate data for contemporary ESS are supplied by the firm’s existing enterprise applications (enterprise resource planning, supply chain management, and customer relationship management). ESS also provide access to news services, financial market databases, economic information, and whatever other external data senior executives require. ESS also have significant ***drill-down*** capabilities if managers need more detailed views of data.

4.4 Tools for Business Intelligence

Business intelligence tools enable users to analyze data to see new patterns, relationships, and insights that are useful for guiding decision making. Principal tools for business intelligence include software for database querying and reporting, tools for multidimensional data analysis (online analytical processing), and tools for data mining.

4.4.1 Online Analytical Processing (OLAP)

Online Analytical Processing (OLAP) supports multidimensional data analysis, enabling users to view the same data in different ways using multiple dimensions. Suppose your company sells four different products, which are nuts, bolts, washers, and screws, in the East, West, and Central regions. If you wanted to ask a fairly straightforward question, such as how many washers were sold during the past quarter, you could easily find the answer by querying your sales database. But what if you wanted to know how many washers sold in each of your sales regions and compare actual results with projected sales?. Each aspect of information, for example product, pricing, cost, region, or time period, represents a different dimension. So, a product manager could use a multidimensional data analysis tool to learn how many washers were sold in the East in June, how that compares with the previous month and the previous June, and how it compares with the sales forecast. OLAP enables users to obtain online answers to ad hoc questions such as these in a fairly rapid amount of time, even when the data are stored in very large databases for multiple years.

Figure 4.3 shows a multidimensional model that could be created to represent products, regions, actual sales, and projected sales. A matrix of actual sales can be stacked on top of a matrix of projected sales to form a cube with six faces. If you rotate the cube 90 degrees one way, the face showing will be product versus actual and projected sales. If you rotate the cube 90 degrees again, you will see region versus actual and projected sales. If you rotate 180 degrees from the original view, you will see projected sales and product versus region. Cubes can be nested within cubes to build complex views of data. A company would use either a specialized multidimensional database or a tool that creates multidimensional views of data in relational databases.

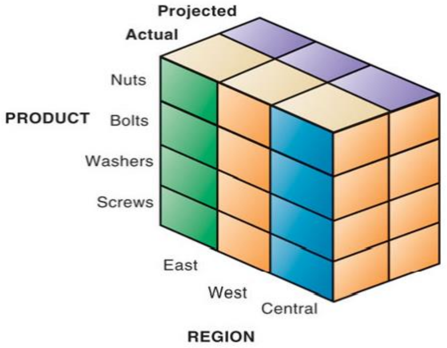


Figure 4.3: Multidimensional Data Model

4.4.1.1 OLTP vs. OLAP

OLTP and OLAP: The two terms look similar but refer to different kinds of systems. ***Online Transaction Processing (OLTP)*** captures, stores, and processes data from transactions in real time. ***Online Analytical Processing (OLAP)*** uses complex queries to analyze aggregated historical data from OLTP systems.

An OLTP system captures and maintains transaction data in a database. Each transaction involves individual database records made up of multiple fields or columns. Examples include banking and credit card activity or retail checkout scanning. In OLTP, the emphasis is on fast processing, because OLTP databases are read, written, and updated frequently. If a transaction fails, built-in system logic ensures data integrity.

OLAP applies complex queries to large amounts of historical data, aggregated from OLTP databases and other sources, for data mining, analytics, and business intelligence projects. In OLAP, the emphasis is on response time to these complex queries. Each query involves one or more columns of data aggregated from many rows. Examples include year-over-year financial performance or marketing lead generation trends. OLAP databases and data warehouses give analysts and decision-makers the ability to use custom reporting tools to turn data into information. Query failure in OLAP does not interrupt or delay transaction processing for customers, but it can delay or impact the accuracy of business intelligence insights.

OLTP provides an immediate record of current business activity, while OLAP generates and validates insights from that data as it's compiled over time. That historical perspective empowers accurate forecasting, but as with all business intelligence, the insights generated with OLAP are only as good as the data pipeline from which they emanate. Table 4.1 compares between OLTP and OLAP.

Table 4.1: OLTP vs OLAP

	OLTP	**OLAP**
Characteristics	Handles a large number of small transactions	Handles large volumes of data with complex queries
Query types	Simple standardized queries	Complex queries
Operations	Based on INSERT, UPDATE, DELETE commands	Based on SELECT commands to aggregate data for reporting
Response time	Milliseconds	Seconds, minutes, or hours depending on the amount of data to process
Design	Industry-specific, such as retail, manufacturing, or banking	Subject-specific, such as sales, inventory, or marketing
Source	Transactions	Aggregated data from transactions
Purpose	Control and run essential business operations in real time	Plan, solve problems, support decisions, discover hidden insights
Data updates	Short, fast updates initiated by user	Data periodically refreshed with scheduled, long-running batch jobs
Space requirements	Generally small if historical data is archived	Generally large due to aggregating large datasets
Backup and recovery	Regular backups required to ensure business continuity and meet legal and governance requirements	Lost data can be reloaded from OLTP database as needed in lieu of regular backups

Productivity	Increases productivity of end users	Increases productivity of business managers, data analysts, and executives
Data view	Lists day-to-day business transactions	Multi-dimensional view of enterprise data
User examples	Customer-facing personnel, clerks, online shoppers	Knowledge workers such as data analysts, business analysts, and executives
Database design	Normalized databases for efficiency	Denormalized databases for analysis

4.4.2 Data Mining

Traditional database queries answer such questions as, "How many units of product number 403 were shipped in February 2010?" OLAP, or multidimensional analysis, supports much more complex requests for information, such as "Compare sales of product 403 relative to plan by quarter and sales region for the past two years." With OLAP and query-oriented data analysis, users need to have a good idea about the information for which they are looking.

Data mining is more discovery-driven. Data mining provides insights into corporate data that cannot be obtained with OLAP by finding hidden patterns and relationships in large databases and inferring rules from them to predict future behavior. The patterns and rules are used to guide decision making and forecast the effect of those decisions. The types of information obtainable from data mining include associations, sequences, classifications, clusters, and forecasts.

- ***Associations*** are occurrences linked to a single event. For instance, a study of supermarket purchasing patterns might reveal that, when corn chips are purchased, a cola drink is purchased 65 percent of the time, but when there is a promotion, cola is purchased 85 percent of the time. This information helps managers make better decisions because they have learned the profitability of a promotion.
- In ***sequences***, events are linked over time. We might find, for example, that if a house is purchased, a new refrigerator will be

purchased within two weeks 65 percent of the time, and an oven will be bought within one month of the home purchase 45 percent of the time.

- ***Classification*** recognizes patterns that describe the group to which an item belongs by examining existing items that have been classified and by inferring a set of rules. For example, businesses such as credit card or telephone companies worry about the loss of steady customers. Classification helps discover the characteristics of customers who are likely to leave and can provide a model to help managers predict who those customers are so that the managers can devise special campaigns to retain such customers.
- ***Clustering*** works in a manner similar to classification when no groups have yet been defined. A data mining tool can discover different groupings within data, such as finding affinity groups for bank cards or partitioning a database into groups of customers based on demographics and types of personal investments.
- Although these applications involve predictions, ***forecasting*** uses predictions in a different way. It uses a series of existing values to forecast what other values will be. For example, forecasting might find patterns in data to help managers estimate the future value of continuous variables, such as sales figures. ***Predictive analytics*** use data mining techniques, historical data, and assumptions about future conditions to predict outcomes of events, such as the probability a customer will respond to an offer or purchase a specific product.

4.4.3 Text Mining and Web Mining

Business intelligence tools deal primarily with data that have been structured in databases and files. However, ***unstructured data***, most in the form of text files, is believed to account for over 80 percent of an organization’s useful information. E-mail, memos, call center transcripts, survey responses, legal cases, patent descriptions, and service reports are all valuable for finding patterns and trends that will help employees make better business decisions.

Text mining tools are now available to help businesses analyze unstructured data. These tools are able to extract key elements from large unstructured data sets, discover patterns and relationships, and summarize the information. Businesses might turn to text mining to analyze transcripts of calls to customer service centers to identify major service and repair issues.

The Web is another rich source of valuable information, some of which can now be mined for patterns, trends, and insights into customer behavior. The discovery and analysis of useful patterns and information from the World Wide Web is called ***Web mining***. Businesses might turn to Web mining to help them understand customer behavior, evaluate the effectiveness of a particular Web site, or quantify the success of a marketing campaign. For instance, marketers use Google Trends and Google Insights for Search services, which track the popularity of various words and phrases used in Google search queries, to learn what people are interested in and what they are interested in buying.

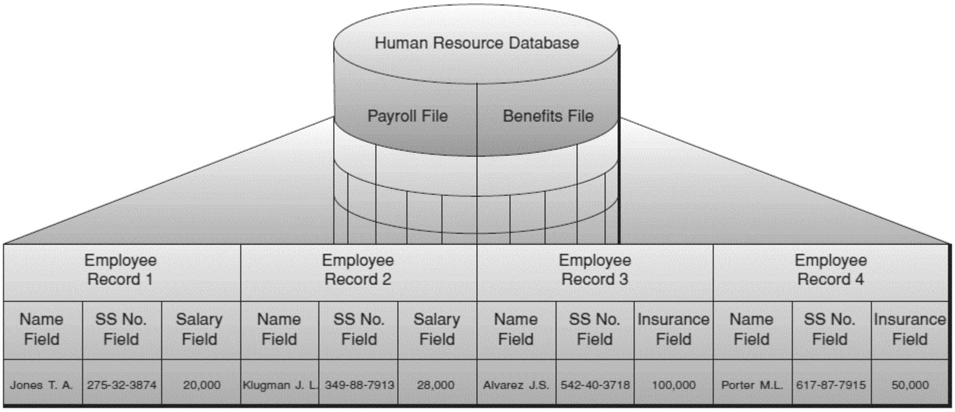
Web mining looks for patterns in data through content mining, structure mining, and usage mining. ***Web content mining*** is the process of extracting knowledge from the content of Web pages, which may include text, image, audio, and video data. ***Web structure mining*** extracts useful information from the links embedded in Web documents. For example, links pointing to a document indicate the popularity of the document, while links coming out of a document indicate the richness or perhaps the variety of topics covered in the document. ***Web usage mining*** examines user interaction data recorded by a Web server whenever requests for a Web site's resources are received. The usage data records the user's behavior when the user browses or makes transactions on the Web site and collects the data in a server log. Analyzing such data can help companies determine the value of particular customers, cross marketing strategies across products, and the effectiveness of promotional campaigns.

CHAPTER 5

Data Resource Management

5.1 Fundamental Data Concepts

Before we go any further, let’s discuss some fundamental concepts about how data are organized in information systems. A conceptual framework of several levels of data has been devised that differentiates among different groupings, or elements, of data. Thus, data may be logically organized into characters, fields, records, files, and databases , just as writing can be organized into letters, words, sentences, paragraphs, and documents. Examples of these logical data elements are shown in Figure 5.1.

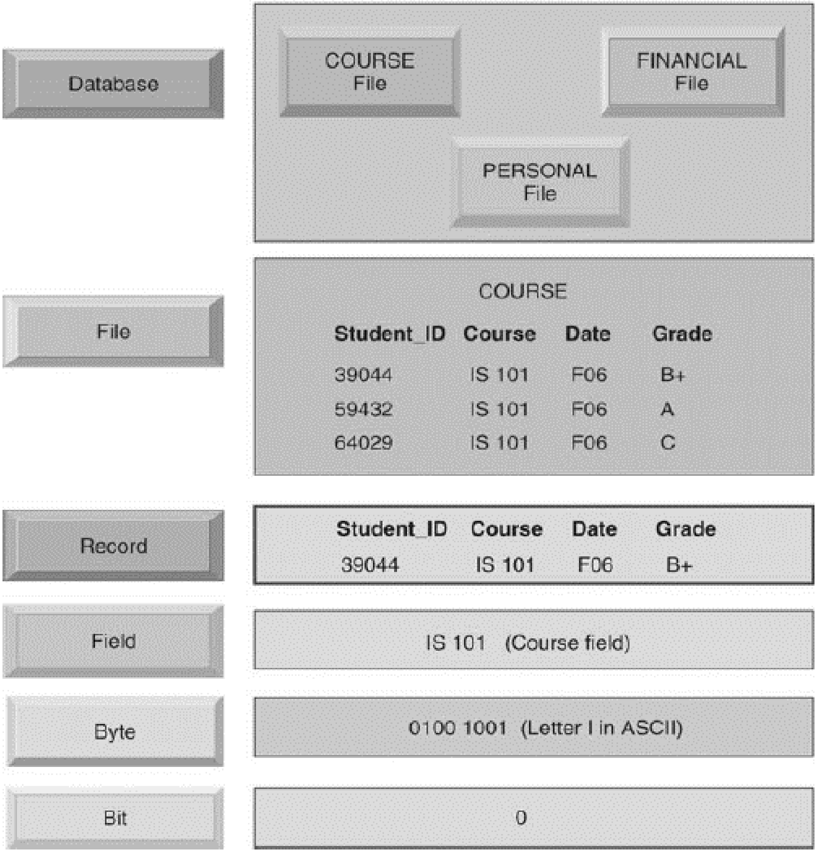


Employee Record 1			Employee Record 2			Employee Record 3			Employee Record 4		
Name Field	SS No. Field	Salary Field	Name Field	SS No. Field	Salary Field	Name Field	SS No. Field	Insurance Field	Name Field	SS No. Field	Insurance Field
Jones T. A.	275-32-3874	20,000	Klugman J. L.	349-88-7913	28,000	Alvarez J.S.	542-40-3718	100,000	Porter M.L.	617-87-7915	50,000

***Figure 5.1*: Examples of the logical data elements in information systems**

A computer system organizes data in a hierarchy that starts with bits and bytes and progresses to fields, records, files, and databases. A bit represents the smallest unit of data a computer can handle. A group of bits, called a byte, represents a single character, which can be a letter, a number, or another symbol. A grouping of characters into a word, a group of words, or a complete number (such as a person’s name or age) is called a field. A group of related fields, such as the student’s name, the course taken, the date, and the grade, comprises a record; a group of records of the sametype is called a file.

For example, the records in Figure 5.2 could constitute a student course file. A group of related files makes up a **database**. The student course file illustrated in Figure 5.2 could be grouped with files on students' personal histories and financial backgrounds to create a student database. A record describes an entity. An **entity** is a person, place, thing, or event on which we store and maintain information. Each characteristic or quality describing a particular entity is called an **attribute**. For example, Student_ID, Course, Date, and Grade are attributes of the entity COURSE. The specific values that these attributes can have are found in the fields of the record describing the entity COURSE.



Student_ID	Course	Date	Grade
39044	IS 101	F06	B+
59432	IS 101	F06	A
64029	IS 101	F06	C

Student_ID	Course	Date	Grade
39044	IS 101	F06	B+

Figure 5.2: A computer system organizes data in a hierarchy.

The following subsections discuss the data hierarchy.

5.1.1 Character

The most basic logical data element is the character, which consists of a single alphabetic, numeric, or other symbol. You might argue that the bit or byte is a more elementary data element, but remember that those terms refer to the physical storage elements provided by the computer hardware. Using that understanding, one way to think of a character is that it is a byte used to represent a particular character. In other words, bits and bytes are the method by which a computer- based system represents data. They are not the data, just the way a computer stores the data. As such, from a user's point of view (i.e., from a logical as opposed to a physical or hardware view of data), a character is the most basic element of data that can be observed and manipulated.

5.1.2 Field

The next higher level of data is the field, or data item. A field consists of a grouping of related characters. For example, the grouping of alphabetic characters in a person's name may form a name field (or typically, last name, first name, and middle initial fields), and the grouping of numbers in a sales amount forms a sales amount field. Specifically, a data field represents an ***attribute*** (a characteristic or quality) of some ***entity*** (object, person, place, or event). For example, an employee's salary is an attribute that is a typical data field used to describe an entity who is an employee of a business. Generally speaking, fields are organized such that they represent some logical order, for example, last_name, first_name, address, city, state, and zip code. Fields are everywhere you look, especially on the Internet!

5.1.3 Record

All of the fields used to capture, organize, and store the attributes of an entity are grouped to form a record . Thus, a record represents a collection of attributes that describe a single instance of an entity. An example is a person's payroll record, which consists of data fields describing attributes such as the person's name, Social Security number, and rate of pay. This record will serve to uniquely describe that person and only that person. Other payroll records may be similar, but none will be exactly the same. Fixed-length records contain a fixed number of fixed-length data fields and, therefore, a predetermined maximum number of characters. Variable-length records contain a variable number of fields and field lengths and, therefore, can be any length. Another way of looking at a record is that it represents a single instance of an entity. Each record in an employee file describes one specific employee.

Normally, the first field in a record is used to store some type of unique identifier for the record. This unique identifier is called the ***primary key***. The value of a primary key can be anything that will serve to uniquely identify one instance of an entity and distinguish it from another. For example, if we wanted to uniquely identify a single student from a group of related students, we could use a student ID number as a primary key. As long as no one shared the same student ID number, we would always be able to identify the record of that student. If no specific data can be found to serve as a primary key for a record, the database designer can simply assign a record a unique sequential number so that no two records will ever have the same primary key. The important thing about a primary key is that it must be unique, and the manner in which a primary key is created must be consistent for the entire data file.

5.1.4 File

A group of related records is a data file (sometimes referred to as a table or flat file). When it is independent of any other files related to it, a single table may be referred to as a flat file . As a point of accuracy, the term flat file may be defined either narrowly or more broadly. Strictly speaking, a flat file database should consist of nothing but data and delimiters (things that separate the fields from each other). More broadly, the term refers to any database that exists in a single file in the form of rows and columns, with no relationships or links between records and fields except the table structure. Regardless of the name used, any grouping of related records in tabular (row-andcolumn form) is called a file . Thus, an employee file would contain the records of the employees of a firm. Files are frequently classified (named) by the application for which they are primarily used, such as a payroll file or an inventory file, or the type of data they contain, such as a document file or a graphical image file. Files are also classified by their permanence, for example, a payroll master file versus a payroll weekly transaction file . A transaction file, therefore, would contain records of all transactions occurring during a period and might be used periodically to update the permanent records contained in a master file. A history file is an obsolete transaction or master file retained for backup purposes or for long-term historical storage, called archival storage**.**

5.1.5 Database

A database is an integrated collection of logically related data elements. A database consolidates records previously stored in separate files into a common pool of data elements that provides data for many applications. The data stored in a database are independent of the application programs using them and of the type of storage devices on which they are stored. Thus, databases contain data elements describing entities and relationships among entities.

5.2 Problems With The Traditional File Environment

The resulting problems are data redundancy and inconsistency, program-data dependence, inflexibility, poor data security, and an inability to share data among applications.

- ***Data redundancy*** is the presence of duplicate data in multiple data files so that the same data are stored in more than place or location. Data redundancy occurs when different groups in an organization independently collect the same piece of data and store it independently of each other. Data redundancy wastes storage resources and also leads to data inconsistency.
- ***Data inconsistency***, where the same attribute may have different values. For example, in instances of the entity COURSE, the Date may be updated in some systems but not in others. The same attribute, Student_ID, may also have different names in different

systems throughout the organization. Some systems might use Student_ID and others might use ID, for example. Additional confusion might result from using different coding systems to represent values for an attribute. For instance, the sales, inventory, and manufacturing systems of a clothing retailer might use different codes to represent clothing size. One system might represent clothing size as "extra large," whereas another might use the code "XL" for the same purpose. The resulting confusion would make it difficult for companies to create customer relationship management, supply chain management, or enterprise systems that integrate data from different sources.

- ***Program-data dependence*** refers to the coupling of data stored in files and the specific programs required to update and maintain those files such that changes in programs require changes to the data. Every traditional computer program has to describe the location and nature of the data with which it works. In a traditional file environment, any change in a software program could require a change in the data accessed by that program. One program might be modified from a five-digit to a nine-digit ZIP code. If the original data file were changed from five-digit to nine-digit ZIP codes, then other programs that required the five-digit ZIP code would no longer work properly. Such changes could cost millions of dollars to implement properly.
- ***Lack of Flexibility*** A traditional file system can deliver routine scheduled reports after extensive programming efforts, but it cannot deliver ad hoc reports or respond to unanticipated information requirements in a timely fashion. The information required by ad hoc requests is somewhere in the system but may be too expensive to retrieve. Several programmers might have to work for weeks to put together the required data items in a new file.
- ***Poor Security*** Because there is little control or management of data, access to and dissemination of information may be out of

control. Management may have no way of knowing who is accessing or even making changes to the organization’s data.

- ***Lack of Data Sharing and Availability*** Because pieces of information in different files and different parts of the organization cannot be related to one another, it is virtually impossible for information to be shared or accessed in a timely manner. Information cannot flow freely across different functional areas or different parts of the organization. If users find different values of the same piece of information in two different systems, they may not want to use these systems because they cannot trust the accuracy of their data.

5.3 Database Management Systems

A database management system (DBMS) is software that permits an organization to centralize data, manage them efficiently, and provide access to the stored data by application programs. The DBMS acts as an interface between application programs and the physical data files. When the application program calls for a data item, such as gross pay, the DBMS finds this item in the database and presents it to the application program. Using traditional data files, the programmer would have to specify the size and format of each data element used in the program and then tell the computer where they were located.

The DBMS relieves the programmer or end user from the task of understanding where and how the data are actually stored by separating the logical and physical views of the data. The logical view presents data as they would be perceived by end users or business specialists, whereas the physical view shows how data are actually organized and structured on physical storage media.

The database management software makes the physical database available for different logical views required by users. For example, for the human resources database illustrated in Figure 5.3, a benefits specialist might require a view consisting of the employee’s name, social security number, and health insurance coverage. A payroll department member might need data such as the employee's name, social security number, gross pay, and net pay. The data for all these views are stored in a single database, where they can be more easily managed by the organization.

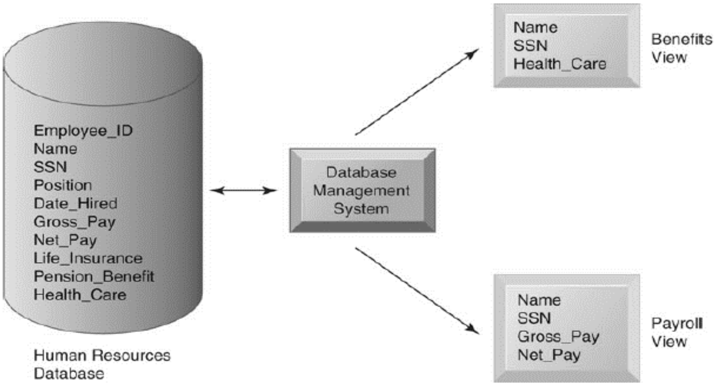


Figure 5.3: Human Resources Database With Multiple Views

5.3.1 How a DBMS Solves the Problems of the Traditional File Environment

A DBMS reduces data redundancy and inconsistency by minimizing isolated files in which the same data are repeated. The DBMS may not enable the organization to eliminate data redundancy entirely, but it can help control redundancy. Even if the organization maintains some redundant data, using a DBMS eliminates data inconsistency because the DBMS can help the organization ensure that every occurrence of redundant data has the same values. The DBMS uncouples programs and data, enabling data to stand on their own. Access and availability of information will be increased and program development and maintenance costs reduced because users and programmers can perform ad hoc queries of data in the database. The DBMS enables the organization to centrally manage data, their use, and security.

5.4 Database Structures

The relationships among the many individual data elements stored in databases are based on one of several logical data structures, or models.

Database management system (DBMS) packages are designed to use a specific data structure to provide end users with quick, easy access to information stored in databases. Five fundamental database structures are the hierarchical, network, relational, object-oriented, and multidimensional models.

5.4.1 Hierarchical Structure

Early mainframe DBMS packages used the hierarchical structure, in which the relationships between records form a hierarchy or treelike structure. In the traditional hierarchical model, all records are dependent and arranged in multilevel structures, consisting of one root record and any number of subordinate levels. Thus, all of the relationships among records are one-to-many because each data element is related to only one element above it. The data element or record at the highest level of the hierarchy (the department data element in this illustration) is called the root element. Any data element can be accessed by moving progressively downward from a root and along the branches of the tree until the desired record (e.g., the employee data element) is located. Simplified illustrations of the Hierarchical database structures are shown in Figure 5.4.

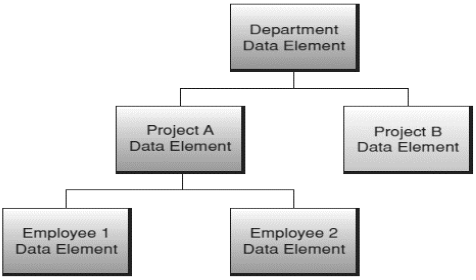


Figure 5.4: Hierarchical Structure

5.4.2 Network Structure

The network structure can represent more complex logical relationships and is still used by some mainframe DBMS packages. It allows many-to-many relationships among records; that is, the network model can access a data element by following one of several paths because any data element or record can be related to any number of other data elements. For example, in Figure 5.4, departmental records can be related to more than one employee record, and employee records can be relaed to more than one project record. Thus, you could locate all employee records for a particular department or all project records related to a particular employee.

It should be noted that neither the hierarchical nor the network data structures are commonly found in the modern organization. The next data structure we discuss, the relational data structure, is the most common of all and serves as the foundation for most modern databases in organizations. Simplified illustrations of the Hierarchical database structures are shown in Figure 5.5.

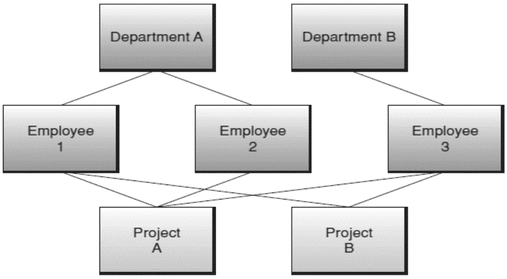
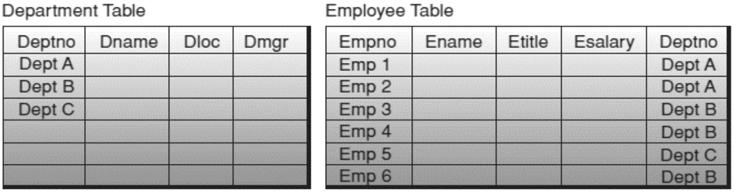


Figure 5.5: Network Structure

5.4.3 Relational Structure

The relational model is the most widely used of the three database structures. It is used by most microcomputer DBMS packages, as well as by most midrange and mainframe systems. In the relational model, all data elements within the database are viewed as being stored in the form of simple two-dimensional tables, sometimes referred to as ***relations*** . The tables in a relational database are flat files that have rows and columns. Each row represents a single record in the file, and each column represents a field. The major difference between a flat file and a database is that a flat file can only have data attributes specified for one file. In contrast, a database can specify data attributes for multiple files simultaneously and can relate the various data elements in one file to those in one or more other files.

Figure 5.6 illustrates the relational database model with two tables representing some of the relationships among departmental and employee records. Other tables, or relations, for this organization's database might represent the data element relationships among projects, divisions, product lines, and so on. Database management system packages based on the relational model can link data elements from various tables to provide information to users.



Department Table

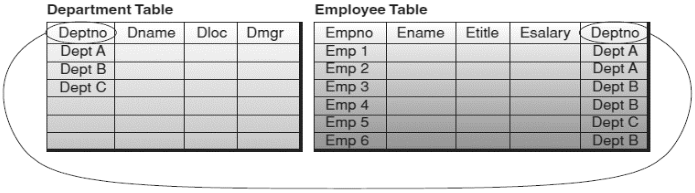
Deptno	Dname	Dloc	Dmgr
Dept A			
Dept B			
Dept C			

Employee Table

Empno	Ename	Etitle	Esalary	Deptno
Emp 1				Dept A
Emp 2				Dept A
Emp 3				Dept B
Emp 4				Dept B
Emp 5				Dept C
Emp 6				Dept B

Figure 5.6: Relational Structure

For example, a manager might want to retrieve and display an employee's name and salary from the employee table in Figure 5.6, as well as the name of the employee's department from the department table, by using their common department number field (Deptno) to link or join the two tables. See Figure 5.7. The relational model can relate data in any one file with data in another file if both files share a common data element or field. Because of this, information can be created by retrieving data from multiple files even if they are not all stored in the same physical location.



Department Table

Deptno	Dname	Dloc	Dmgr
Dept A			
Dept B			
Dept C			

Employee Table

Empno	Ename	Etitle	Esalary	Deptno
Emp 1				Dept A
Emp 2				Dept A
Emp 3				Dept B
Emp 4				Dept B
Emp 5				Dept C
Emp 6				Dept B

Figure 5.7: Join Tables in Relational Database.

5.4.3.1 Relational Operations

Three basic operations can be performed on a relational database to create useful setsof data. The ***select*** operation is used to create a subset of records that meet a stated criterion. For example, a select operation might be used on an employee database to create a subset of records containing all employees who make more than $30,000 per year and who have been with the company more than three years. Another way to think of the select operation is that it temporarily creates a table whose rows have records that meet only the selection criteria.

The ***join*** operation can be used to combine two or more tables temporarily so that a user can see relevant data in a form that looks like it is all in one big table. Using this operation, a user can ask for data to be retrieved from multiple files or databases without having to go to each one separately. This allows multiple data sets from multiple (and often unrelated) locations to be brought together and analyzed.

Finally, the ***project*** operation is used to create a subset of the columns contained in the temporary tables created by the select and join operations. Just as the select operation creates a subset of records that meet stated criteria, the project operation creates a subset of the columns, or fields, that the user wants to see. Using a project operation, the user can decide not to view all of the columns in the table, but instead to view only those that have the data necessary to answer a particular question or construct a specific report.

5.4.4 Multidimensional Structure

The multidimensional model is a variation of the relational model that uses multidimensional structures to organize data and express the relationships between data. You can visualize multidimensional structures as cubes of data and cubes within cubes of data. Each side of the cube is considered a dimension of the data. Figure 5.8 is an example that shows that each dimension can represent a different category, such as product type, region, sales channel, and time.

Each cell within a multidimensional structure contains aggregated data related to elements along each of its dimensions. For example, a single cell may contain the total sales for a product in a region for a specific sales channel in a single month. A major benefit of multidimensional databases is that they provide a compact and easy-tounderstand way to visualize and manipulate data elements that have many interrelationships. So multidimensional databases have become the most popular database structure for the analytical databases that support online analytical processing (OLAP) applications, in which fast answers to complex business queries are expected.

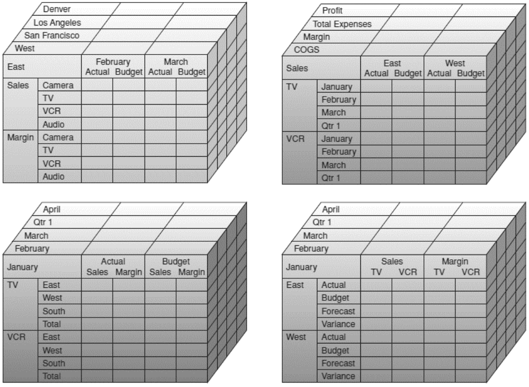


Figure 5.8: A Multidimensional Database

5.4.5 Object–Oriented Structure

The object-oriented model is considered one of the key technologies of a new generation of multimedia Web-based applications. As Figure 5.9 illustrates, an object consists of data values describing the attributes of an entity, plus the operations that can be performed upon the data. This encapsulation capability allows the object-oriented model to handle complex types of data (graphics, pictures, voice, and text) more easily than other database structures.

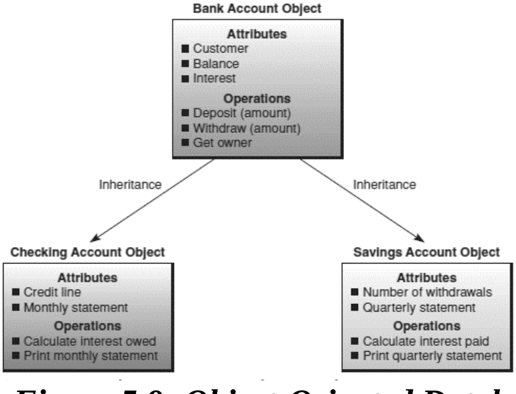


Figure 5.9: Object-Oriented Database

5.5 Databases in the Cloud

Cloud computing providers offer database management services, but these services typically have less functionality than their on-premises counterparts. At the moment, the primary customer base for cloud-based data management consists of Webfocused start-ups or small to medium-sized businesses looking for database capabilities at a lower price than a standard relational DBMS.

Amazon Web Services has both a simple non-relational database called SimpleDB and a Relational Database Service, which is based on an online implementation of the MySQL open source DBMS. Amazon Relational Database Service (Amazon RDS) offers the full range of capabilities of MySQL. Pricing is based on usage. There are also charges for the volume of data stored, the number of input-output requests, the amount of data written to the database, and the amount of data read from the database.

Amazon Web Services additionally offers Oracle customers the option to license Oracle Database 11g, Oracle Enterprise Manager, and Oracle Fusion Middleware to run on the Amazon EC2 (Elastic Cloud Compute) platform. Microsoft SQL Azure Database is a cloud-based relational database service based on Microsoft's SQL Server DBMS. It provides a highly available, scalable database service hosted by Microsoft in the cloud. SQL Azure Database helps reduce costs by integrating with existing software tools and providing symmetry with on-premises and cloud databases.

TicketDirect, which sells tickets to concerts, sporting events, theater performances, and movies in Australia and New Zealand, adopted the SQL Azure Database cloud platform in order to improve management of peak system loads during major ticket sales. It migrated its data to the SQL Azure database. By moving to a cloud solution, TicketDirect is able to scale its computing resources in response to real-time demand while keeping costs low.

References

[1] Management Information Systems: Managing The Digital Firm, Laudon, KC., And Laudon, JP, 12th Edition, 2012.

[2] Management Information Systems, O’Brien, JA and Marakas, GM, 10th Edition, 2007.

[3] Introduction To Information Systems, O’Brien, JA and Marakas, GM, 10th Edition, 16th Edition, 2011.

[4] Fundamentals of Database System, R. Elmasri, 7th Edition, 2016.

[5] Systems Analysis And Design, KENDALL, KE., and KENDALL, JE., 8th Edition, 2006.