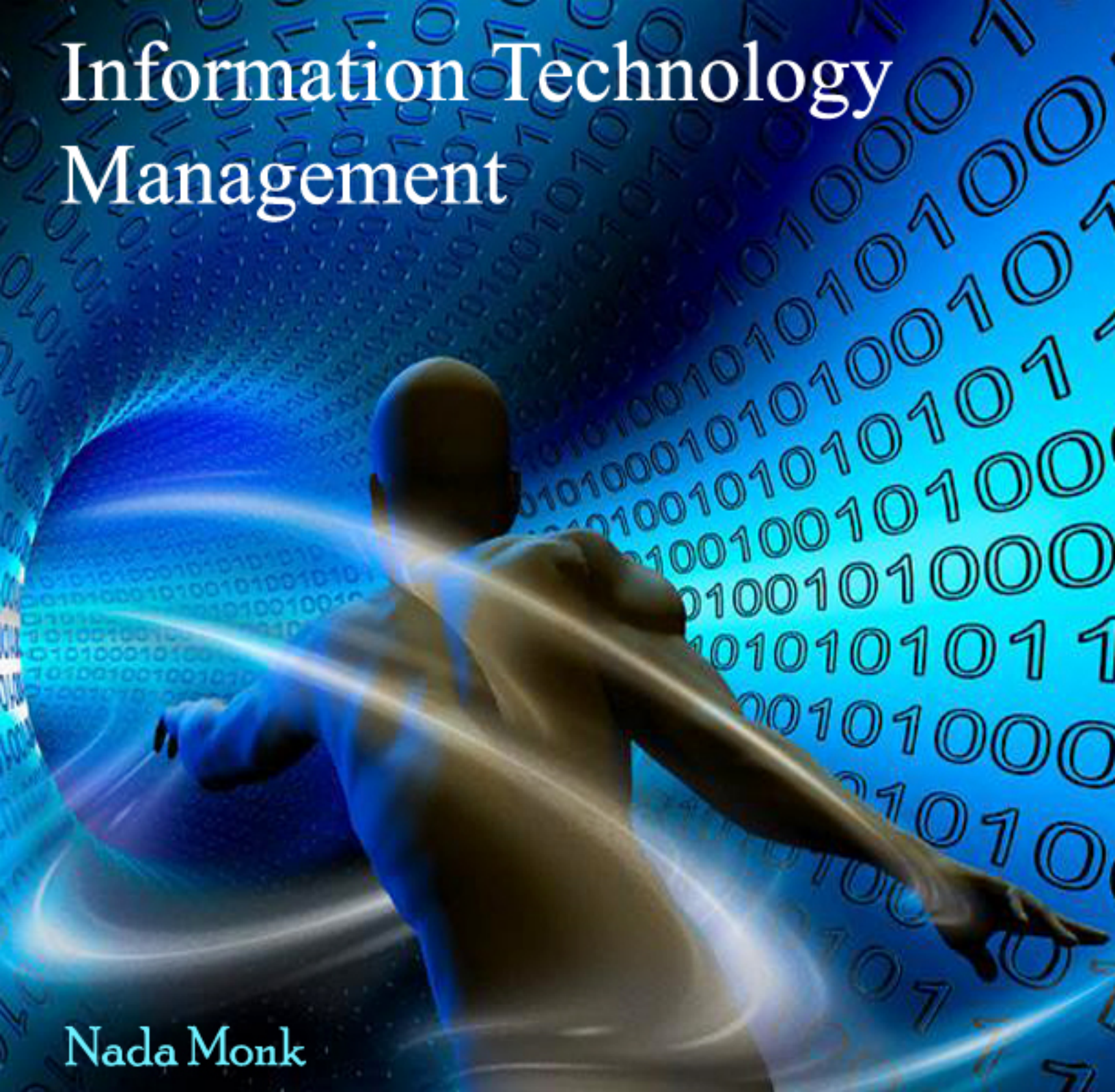
Information Technology Management



Nada Monk

First Edition, 2012

ISBN 978-81-323-2535-2

Published by:
Orange Apple
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

Table of Contents

Chapter- 1

Management Information System

A **management information system** (**MIS**) is a system that provides information needed to manage organizations effectively. Management information systems are regarded to be a subset of the overall internal controls procedures in a business, which cover the application of people, documents, technologies, and procedures used by management accountants to solve business problems such as costing a product,service or a business-wide strategy. Management information systems are distinct from regular information systems in that they are used to analyze other information systems applied in operational activities in the organization. Academically, the term is commonly used to refer to the group of information management methods tied to the automation or support of human decision making, e.g. Decision Support Systems, Expert systems, and Executive information systems.

Overview

Initially in businesses and other organizations, internal reporting was made manually and only periodically, as a by-product of the accounting system and with some additional statistic(s), and gave limited and delayed information on management performance. Previously, data had to be separated individually by the people as per the requirement and necessity of the organization. Later, data was distinguished from information, and so instead of the collection of mass of data, important and to the point data that is needed by the organization was stored.

Earlier, business computers were mostly used for relatively simple operations such as tracking sales or payroll data, often without much detail. Over time, these applications became more complex and began to store increasing amount of information while also interlinking with previously separate information systems. As more and more data was stored and linked man began to analyze this information into further detail, creating entire management reports from the raw, stored data. The term "MIS" arose to describe these kinds of applications, which were developed to provide managers with information about sales, inventories, and other data that would help in managing the enterprise. Today, the term is used broadly in a number of contexts and includes (but is not limited to): decision support systems, resource and people management applications, Enterprise Resource Planning (ERP), Supply Chain Management (SCM), Customer Relationship Management (CRM), project management and database retrieval applications.

An 'MIS' is a planned system of the collection, processing, storage and dissemination of data in the form of information needed to carry out the management functions. In a way, it is a documented report of the activities that were planned and executed. According to Philip Kotler "A marketing information system consists of people, equipment, and procedures to gather, sort, analyze, evaluate, and distribute needed, timely, and accurate information to marketing decision makers."

The terms *MIS* and *information system* are often confused. Information systems include systems that are not intended for decision making. The area of study called MIS is sometimes referred to, in a restrictive sense, as information technology management. That area of study should not be confused with computer science. IT service management is a practitioner-focused discipline. MIS has also some differences with ERP which incorporates elements that are not necessarily focused on decision support.

Any successful MIS must support a business's Five Year Plan or its equivalent. It must provide for reports based upon performance analysis in areas critical to that plan, with feedback loops that allow for titivation of every aspect of the business, including recruitment and training regimens. In effect, MIS must not only indicate how things are going, but why they are not going as well as planned where that is the case. These reports would include performance relative to cost centers and projects that drive profit or loss, and do so in such a way that identifies individual accountability, and in virtual real-time.

Anytime a business is looking at implementing a new business system it is very important to use a system devlopment method such as System Development Life Cycle. The life cycle includes Analysis, Requirements, Design, Development, Testing and Implementation.

Professor Allen S. Lee states that *"...research in the information systems field examines more than the technological system, or just the social system, or even the two side by side; in addition, it investigates the phenomena that emerge when the two interact."*.

Internal control

In accounting and auditing, **internal control** is defined as a process effected by an organization's structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives. It is a means by which an organization's resources are directed, monitored, and measured. It plays an important role in preventing and detecting fraud and protecting the organization's resources, both physical (e.g., machinery and property) and intangible (e.g., reputation or intellectual property such as trademarks). At the organizational level, internal control objectives relate to the reliability of financial reporting, timely feedback on the achievement of operational or strategic goals, and compliance with laws and regulations. At the specific transaction level, internal control refers to the actions taken to

achieve a specific objective (e.g., how to ensure the organization's payments to third parties are for valid services rendered.) Internal control procedures reduce process variation, leading to more predictable outcomes. Internal control is a key element of the Foreign Corrupt Practices Act (FCPA) of 1977 and the Sarbanes–Oxley Act of 2002, which required improvements in internal control in United States public corporations. Internal controls within business entities are also referred to as **operational controls**.

Internal controls have existed from ancient times. In Hellenistic Egypt there was a dual administration, with one set of bureaucrats charged with collecting taxes and another with supervising them. In the Republic of China, the Control *Yuan* (監察院; pinyin: Jiānchá Yùan), one of the five branches of government, is an investigatory agency that monitors the other branches of government.

Definitions

There are many definitions of internal control, as it affects the various constituencies (stakeholders) of an organization in various ways and at different levels of aggregation.

Under the COSO Internal Control-Integrated Framework, a widely-used framework in the United States, internal control is broadly defined as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: a) Effectiveness and efficiency of operations; b) Reliability of financial reporting; and c) Compliance with laws and regulations.

COSO defines internal control as having five components:

1. Control Environment-sets the tone for the organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control.
2. Risk Assessment-the identification and analysis of relevant risks to the achievement of objectives, forming a basis for how the risks should be managed
3. Information and Communication-systems or processes that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities
4. Control Activities-the policies and procedures that help ensure management directives are carried out.
5. Monitoring-processes used to assess the quality of internal control performance over time.

The COSO definition relates to the aggregate control system of the organization, which is composed of many individual control procedures.

Discrete control procedures, or *controls* are defined by the SEC as: "...a specific set of policies, procedures, and activities designed to meet an objective. A control may exist within a designated function or activity in a process. A control's impact...may be entity-

wide or specific to an account balance, class of transactions or application. Controls have unique characteristics – for example, they can be: automated or manual; reconciliations; segregation of duties; review and approval authorizations; safeguarding and accountability of assets; preventing or detecting error or fraud. Controls within a process may consist of financial reporting controls and operational controls (that is, those designed to achieve operational objectives)."

Context

More generally, setting objectives, budgets, plans and other expectations establish criteria for control. Control itself exists to keep performance or a state of affairs within what is expected, allowed or accepted. Control built within a process is internal in nature. It takes place with a combination of interrelated components - such as social environment effecting behavior of employees, information necessary in control, and policies and procedures. Internal control structure is a plan determining how internal control consists of these elements.

The concepts of corporate governance also heavily rely on the necessity of internal controls. Internal controls help ensure that processes operate as designed and that risk responses (risk treatments) in risk management are carried out. In addition, there needs to be in place circumstances ensuring that the aforementioned procedures will be performed as intended: right attitudes, integrity and competence, and monitoring by managers.

Roles and responsibilities in internal control

According to the COSO Framework, everyone in an organization has responsibility for internal control to some extent. Virtually all employees produce information used in the internal control system or take other actions needed to effect control. Also, all personnel should be responsible for communicating upward problems in operations, noncompliance with the code of conduct, or other policy violations or illegal actions. Each major entity in corporate governance has a particular role to play:

Management: The Chief Executive Officer (the top manager) of the organization has overall responsibility for designing and implementing effective internal control. More than any other individual, the chief executive sets the "tone at the top" that affects integrity and ethics and other factors of a positive control environment. In a large company, the chief executive fulfills this duty by providing leadership and direction to senior managers and reviewing the way they're controlling the business. Senior managers, in turn, assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions. In a smaller entity, the influence of the chief executive, often an owner-manager, is usually more direct. In any event, in a cascading responsibility, a manager is effectively a chief executive of his or her sphere of responsibility. Of particular significance are financial officers and their staffs, whose control activities cut across, as well as up and down, the operating and other units of an enterprise.

Board of Directors: Management is accountable to the board of directors, which provides governance, guidance and oversight. Effective board members are objective, capable and inquisitive. They also have a knowledge of the entity's activities and environment, and commit the time necessary to fulfill their board responsibilities. Management may be in a position to override controls and ignore or stifle communications from subordinates, enabling a dishonest management which intentionally misrepresents results to cover its tracks. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal and internal audit functions, is often best able to identify and correct such a problem.

Auditors: The internal auditors and external auditors of the organization also measure the effectiveness of internal control through their efforts. They assess whether the controls are properly designed, implemented and working effectively, and make recommendations on how to improve internal control. They may also review Information technology controls, which relate to the IT systems of the organization. There are laws and regulations on internal control related to financial reporting in a number of jurisdictions. In the U.S. these regulations are specifically established by Sections 404 and 302 of the Sarbanes-Oxley Act. Guidance on auditing these controls is specified in PCAOB *Auditing Standard No. 5* and SEC guidance, further discussed in SOX 404 top-down risk assessment. To provide reasonable assurance that internal controls involved in the financial reporting process are effective, they are tested by the external auditor (the organization's public accountants), who are required to opine on the internal controls of the company and the reliability of its financial reporting.

Limitations

Internal control can provide reasonable, not absolute, assurance that the objectives of an organization will be met. The concept of reasonable assurance implies a high degree of assurance, constrained by the costs and benefits of establishing incremental control procedures.

Effective internal control implies the organization generates reliable financial reporting and substantially complies with the laws and regulations that apply to it. However, whether an organization achieves operational and strategic objectives may depend on factors outside the enterprise, such as competition or technological innovation. These factors are outside the scope of internal control; therefore, effective internal control provides only timely information or feedback on progress towards the achievement of operational and strategic objectives, but cannot guarantee their achievement.

Describing Internal Controls

Internal controls may be described in terms of: a) the objective they pertain to; and b) the nature of the control activity itself.

Objective categorization

Internal control activities are designed to provide reasonable assurance that particular objectives are achieved, or related progress understood. The specific target used to determine whether a control is operating effectively is called the *control objective*. Control objectives fall under several detailed categories; in financial auditing, they relate to particular *financial statement assertions,* but broader frameworks are helpful to also capture operational and compliance aspects:

1. Existence (Validity): Only valid or authorized transactions are processed (i.e., no invalid transactions)
2. Occurrence (Cutoff): Transactions occurred during the correct period or were processed timely.
3. Completeness: All transactions are processed that should be (i.e., no omissions)
4. Valuation: Transactions are calculated using an appropriate methodology or are computationally accurate.
5. Rights & Obligations: Assets represent the rights of the company, and liabilities its obligations, as of a given date.
6. Presentation & Disclosure (Classification): Components of financial statements (or other reporting) are properly classified (by type or account) and described.
7. Reasonableness-transactions or results appears reasonable relative to other data or trends.

For example, a control observices received." This is a validity objective. A typical control procedure designed to achieve this objective is: "The accounts payable system compares the purchase order, receiving record, and vendor invoice prior to authorizing payment."

Management is responsible for implementing appropriate controls that apply to transactions in their areas of responsibility. Internal auditors perform their audits to evaluate whether the controls are designed and implemented effectively to address the relevant objectives.

Activity categorization

Control activities may also be explained by the type or nature of activity. These include (but are not limited to):

- Segregation of duties - separating authorization, custody, and record keeping roles of fraud or error by one person.
- Authorization of transactions - review of particular transactions by an appropriate person.
- Retention of records - maintaining documentation to substantiate transactions.
- Supervision or monitoring of operations - observation or review of ongoing operational activity.
- Physical safeguards - usage of cameras, locks, physical barriers, etc. to protect property, such as merchandise inventory.

- Top-level reviews-analysis of actual results versus organizational goals or plans, periodic and regular operational reviews, metrics, and other key performance indicators (KPIs).
- IT Security - usage of passwords, access logs, etc. to ensure access restricted to authorized personnel.
- Top level reviews-Management review of reports comparing actual performance versus plans, goals, and established objectives.
- Controls over information processing-A variety of control activities are used in information processing. Examples include edit checks of data entered, accounting for transactions in numerical sequences, comparing file totals with control accounts, and controlling access to data, files and programs.

Control precision

Control precision describes the alignment or correlation between a particular control procedure and a given control objective or risk. A control with direct impact on the achievement of an objective (or mitigation of a risk) is said to be more precise than one with indirect impact on the objective or risk. Precision is distinct from sufficiency; that is, multiple controls with varying degrees of precision may be involved in achieving a control objective or mitigating a risk.

Precision is an important factor in performing a SOX 404 top-down risk assessment. After identifying specific financial reporting material misstatement risks, management and the external auditors are required to identify and test controls that mitigate the risks. This involves making judgments regarding both precision and sufficiency of controls required to mitigate the risks.

Risks and controls may be entity-level or assertion-level under the PCAOB guidance. Entity-level controls are identified to address entity-level risks. However, a combination of entity-level and assertion-level controls are typically identified to address assertion-level risks. The PCAOB set forth a three-level hierarchy for considering the precision of entity-level controls. Later guidance by the PCAOB regarding small public firms provided several factors to consider in assessing precision.

Fraud and internal control

Internal control plays an important role in the prevention and detection of fraud. Under the Sarbanes-Oxley Act, companies are required to perform a fraud risk assessment and assess related controls. This typically involves identifying scenarios in which theft or loss could occur and determining if existing control procedures effectively manage the risk to an acceptable level. The risk that senior management might override important financial controls to manipulate financial reporting is also a key area of focus in fraud risk assessment.

The AICPA, IIA, and ACFE also sponsored a guide published during 2008 that includes a framework for helping organizations manage their fraud risk.

Internal Controls and Improvement

If the internal control system is implemented only to prevent fraud and comply with laws and regulations, then an important opportunity is missed. The same internal controls can also be used to systematically improve businesses, particularly in regard to effectiveness and efficiency.

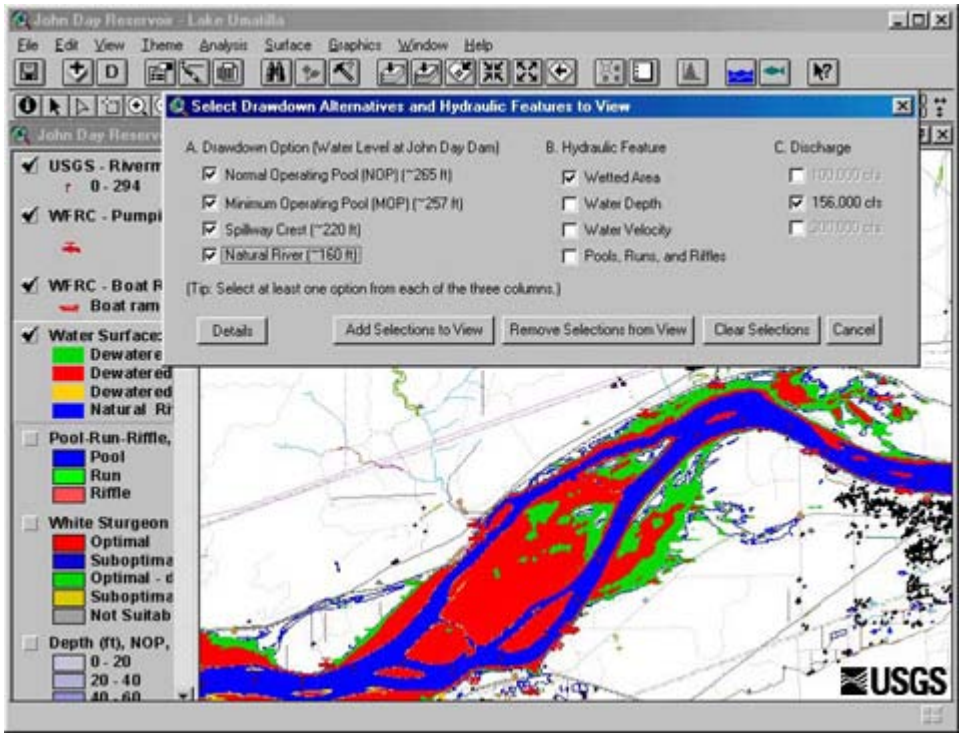
Continuous Controls Monitoring

Advances in technology and data analysis have led to the development of numerous tools which can automatically evaluate the effectiveness of internal controls. Used in conjunction with continuous auditing, continuous controls monitoring provides assurance on financial information flowing through the business processes.

Chapter- 2

Decision Support Systems and Executive Information Systems

Decision Support System



Example of a Decision Support System for John Day Reservoir

A **decision support systems** (**DSS**) is a computer-based information system that supports business or organizational decision-making activities. DSSs serve the management, operations, and planning levels of an organization and help to make decisions, which may be rapidly changing and not easily specified in advance.

DSSs include knowledge-based systems. A properly designed DSS is an interactive software-based system intended to help decision makers compile useful information from a combination of raw data, documents, personal knowledge, or business models to identify and solve problems and make decisions.

Typical information that a decision support application might gather and present are:

- inventories of information assets (including legacy and relational data sources, cubes, data warehouses, and data marts),
- comparative sales figures between one period and the next,
- projected revenue figures based on product sales assumptions.

History

According to Keen (1978), the concept of decision support has evolved from two main areas of research: The theoretical studies of organizational decision making done at the Carnegie Institute of Technology during the late 1950s and early 1960s, and the technical work on interactive computer systems, mainly carried out at the Massachusetts Institute of Technology in the 1960s. It is considered that the concept of DSS became an area of research of its own in the middle of the 1970s, before gaining in intensity during the 1980s. In the middle and late 1980s, executive information systems (EIS), group decision support systems (GDSS), and organizational decision support systems (ODSS) evolved from the single user and model-oriented DSS.

According to Sol (1987) the definition and scope of DSS has been migrating over the years. In the 1970s DSS was described as "a computer based system to aid decision making". Late 1970s the DSS movement started focusing on "interactive computer-based systems which help decision-makers utilize data bases and models to solve ill-structured problems". In the 1980s DSS should provide systems "using suitable and available technology to improve effectiveness of managerial and professional activities", and end 1980s DSS faced a new challenge towards the design of intelligent workstations.

In 1987 Texas Instruments completed development of the Gate Assignment Display System (GADS) for United Airlines. This decision support system is credited with significantly reducing travel delays by aiding the management of ground operations at various airports, beginning with O'Hare International Airport in Chicago and Stapleton Airport in Denver Colorado.

Beginning in about 1990, data warehousing and on-line analytical processing (OLAP) began broadening the realm of DSS. As the turn of the millennium approached, new Web-based analytical applications were introduced.

The advent of better and better reporting technologies has seen DSS start to emerge as a critical component of management design. Examples of this can be seen in the intense amount of discussion of DSS in the education environment.

DSS also have a weak connection to the user interface paradigm of hypertext. Both the University of Vermont PROMIS system (for medical decision making) and the Carnegie Mellon ZOG/KMS system (for military and business decision making) were decision support systems which also were major breakthroughs in user interface research. Furthermore, although hypertext researchers have generally been concerned with information overload, certain researchers, notably Douglas Engelbart, have been focused on decision makers in particular.

Taxonomies

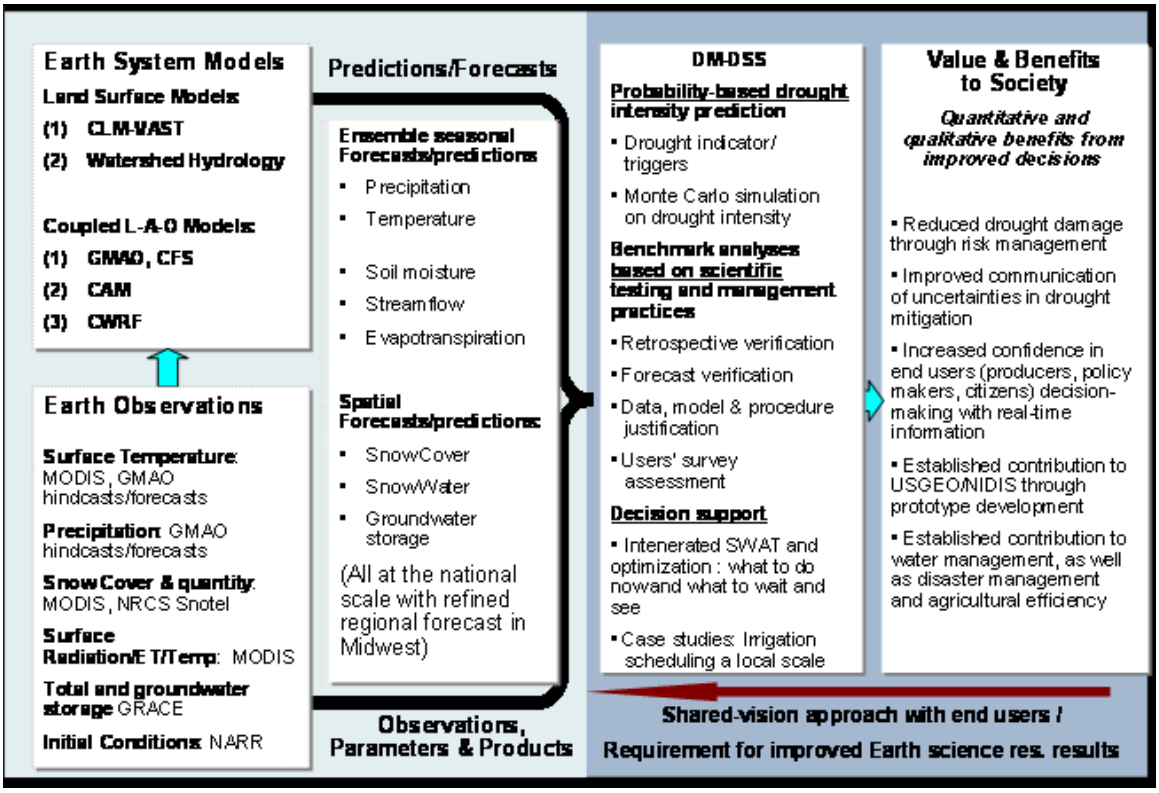
As with the definition, there is no universally-accepted taxonomy of DSS either. Different authors propose different classifications. Using the relationship with the user as the criterion, Haettenschwiler differentiates *passive*, *active*, and *cooperative DSS*. A *passive DSS* is a system that aids the process of decision making, but that cannot bring out explicit decision suggestions or solutions. An *active DSS* can bring out such decision suggestions or solutions. A *cooperative DSS* allows the decision maker (or its advisor) to modify, complete, or refine the decision suggestions provided by the system, before sending them back to the system for validation. The system again improves, completes, and refines the suggestions of the decision maker and sends them back to her for validation. The whole process then starts again, until a consolidated solution is generated.

Another taxonomy for DSS has been created by Daniel Power. Using the mode of assistance as the criterion, Power differentiates *communication-driven DSS*, *data-driven DSS*, *document-driven DSS*, *knowledge-driven DSS*, and *model-driven DSS*.

- A **communication-driven DSS** supports more than one person working on a shared task; examples include integrated tools like Microsoft's NetMeeting or Groove
- A **data-driven DSS** or data-oriented DSS emphasizes access to and manipulation of a time series of internal company data and, sometimes, external data.
- A **document-driven DSS** manages, retrieves, and manipulates unstructured information in a variety of electronic formats.
- A **knowledge-driven DSS** provides specialized problem-solving expertise stored as facts, rules, procedures, or in similar structures.
- A **model-driven DSS** emphasizes access to and manipulation of a statistical, financial, optimization, or simulation model. Model-driven DSS use data and parameters provided by users to assist decision makers in analyzing a situation; they are not necessarily data-intensive. Dicodess is an example of an open source model-driven DSS generator.

Using scope as the criterion, Power differentiates *enterprise-wide DSS* and *desktop DSS*. An *enterprise-wide DSS* is linked to large data warehouses and serves many managers in the company. A *desktop, single-user DSS* is a small system that runs on an individual manager's PC.

Components



Design of a Drought Mitigation Decision Support System

Three fundamental components of a DSS architecture are:

1. the database (or knowledge base),
2. the model (i.e., the decision context and user criteria), and
3. the user interface.

The users themselves are also important components of the architecture.

Development Frameworks

DSS systems are not entirely different from other systems and require a structured approach. Such a framework includes people, technology, and the development approach.

DSS technology levels (of hardware and software) may include:

1. The actual application that will be used by the user. This is the part of the application that allows the decision maker to make decisions in a particular problem area. The user can act upon that particular problem.
2. Generator contains Hardware/software environment that allows people to easily develop specific DSS applications. This level makes use of case tools or systems such as Crystal, AIMMS, and iThink.

3. Tools include lower level hardware/software. DSS generators including special languages, function libraries and linking modules

An iterative developmental approach allows for the DSS to be changed and redesigned at various intervals. Once the system is designed, it will need to be tested and revised for the desired outcome.

Classification

There are several ways to classify DSS applications. Not every DSS fits neatly into one category, but may be a mix of two or more architectures.

Holsapple and Whinston classify DSS into the following six frameworks: Text-oriented DSS, Database-oriented DSS, Spreadsheet-oriented DSS, Solver-oriented DSS, Rule-oriented DSS, and Compound DSS.

A compound DSS is the most popular classification for a DSS. It is a hybrid system that includes two or more of the five basic structures described by Holsapple and Whinston.

The support given by DSS can be separated into three distinct, interrelated categories: Personal Support, Group Support, and Organizational Support.

DSS components may be classified as:

1. **Inputs:** Factors, numbers, and characteristics to analyze
2. **User Knowledge and Expertise:** Inputs requiring manual analysis by the user
3. **Outputs:** Transformed data from which DSS "decisions" are generated
4. **Decisions:** Results generated by the DSS based on user criteria

DSSs which perform selected cognitive decision-making functions and are based on artificial intelligence or intelligent agents technologies are called Intelligent Decision Support Systems (IDSS).

The nascent field of Decision engineering treats the decision itself as an engineered object, and applies engineering principles such as Design and Quality assurance to an explicit representation of the elements that make up a decision.

Applications

As mentioned above, there are theoretical possibilities of building such systems in any knowledge domain.

One example is the clinical decision support system for medical diagnosis. Other examples include a bank loan officer verifying the credit of a loan applicant or an engineering firm that has bids on several projects and wants to know if they can be competitive with their costs.

DSS is extensively used in business and management. Executive dashboard and other business performance software allow faster decision making, identification of negative trends, and better allocation of business resources.

A growing area of DSS application, concepts, principles, and techniques is in agricultural production, marketing for sustainable development. For example, the DSSAT4 package, developed through financial support of USAID during the 80's and 90's, has allowed rapid assessment of several agricultural production systems around the world to facilitate decision-making at the farm and policy levels. There are, however, many constraints to the successful adoption on DSS in agriculture.

DSS are also prevalent in forest management where the long planning time frame demands specific requirements. All aspects of Forest management, from log transportation, harvest scheduling to sustainability and ecosystem protection have been addressed by modern DSSs. A comprehensive list and discussion of all available systems in forest management is being compiled under the COST action Forsys

A specific example concerns the Canadian National Railway system, which tests its equipment on a regular basis using a decision support system. A problem faced by any railroad is worn-out or defective rails, which can result in hundreds of derailments per year. Under a DSS, CN managed to decrease the incidence of derailments at the same time other companies were experiencing an increase.

Benefits

1. Improves personal efficiency
2. Speeds up problem solving in an organization
3. Facilitates interpersonal communication
4. Promotes learning or training
5. Increases organizational control
6. Generates new evidence in support of a decision
7. Creates a competitive advantage over competition
8. Encourages exploration and discovery on the part of the decision maker
9. Reveals new approaches to thinking about the problem space
10. Helps automate managerial processes

Executive Information System

An **Executive Information System** (EIS) is a type of management information system intended to facilitate and support the information and decision-making needs of senior executives by providing easy access to both internal and external information relevant to meeting the strategic goals of the organization. It is commonly considered as a specialized form of a Decision Support System (DSS)

The emphasis of EIS is on graphical displays and easy-to-use user interfaces. They offer strong reporting and drill-down capabilities. In general, EIS are enterprise-wide DSS that help top-level executives analyze, compare, and highlight trends in important variables so that they can monitor performance and identify opportunities and problems. EIS and data warehousing technologies are converging in the marketplace.

In recent years, the term EIS has lost popularity in favour of Business Intelligence (with the sub areas of reporting, analytics, and digital dashboards).

History

Traditionally, executive information systems were developed as mainframe computer-based programs. The purpose was to package a company's data and to provide sales performance or market research statistics for decision makers, such as financial officers, marketing directors, and chief executive officers, who were not necessarily well acquainted with computers. The objective was to develop computer applications that would highlight information to satisfy senior executives' needs. Typically, an EIS provides data that would only need to support executive level decisions instead of the data for all the company.

Today, the application of EIS is not only in typical corporate hierarchies, but also at personal computers on a local area network. EIS now cross computer hardware platforms and integrate information stored on mainframes, personal computer systems, and minicomputers. As some client service companies adopt the latest enterprise information systems, employees can use their personal computers to get access to the company's data and decide which data are relevant for their decision makings. This arrangement makes all users able to customize their access to the proper company's data and provide relevant information to both upper and lower levels in companies.

Components

The components of an EIS can typically be classified as:

Hardware

When talking about hardware for an EIS environment, we should focus on the hardware that meet the executive's needs. The executive must be put first and the executive's needs must be defined before the hardware can be selected. The basic computer hardware needed for a typical EIS includes four components:

1. Input data-entry devices. These devices allow the executive to enter, verify, and update data immediately;
2. The central processing unit (CPU), which is the kernel because it controls the other computer system components;

3. Data storage files. The executive can use this part to save useful business information, and this part also help the executive to search historical business information easily;
4. Output devices, which provide a visual or permanent record for the executive to save or read. This device refers to the visual output device or printer.

In addition, with the advent of local area networks (LAN), several EIS products for networked workstations became available. These systems require less support and less expensive computer hardware. They also increase access of the EIS information to many more users within a company.

Software

Choosing the appropriate software is vital to design an effective EIS. Therefore, the software components and how they integrate the data into one system are very important. The basic software needed for a typical EIS includes four components:

1. Text base software. The most common form of text are probably documents;
2. Database. Heterogeneous databases residing on a range of vendor-specific and open computer platforms help executives access both internal and external data;
3. Graphic base. Graphics can turn volumes of text and statistics into visual information for executives. Typical graphic types are: time series charts, scatter diagrams, maps, motion graphics, sequence charts, and comparison-oriented graphs (i.e., bar charts);
4. Model base. The EIS models contain routine and special statistical, financial, and other quantitative analysis.

Perhaps a more difficult problem for executives is choosing from a range of highly technical software packages. Ease of use, responsiveness to executives' requests, and price are all reasonable considerations. Further, it should be considered whether the package can run on existing hardware.

User Interface

An EIS needs to be efficient to retrieve relevant data for decision makers, so the user interface is very important. Several types of interfaces can be available to the EIS structure, such as scheduled reports, questions/answers, menu driven, command language, natural language, and input/output. It is crucial that the interface must fit the decision maker’s decision-making style. If the executive is not comfortable with the information questions/answers style, the EIS will not be fully utilized. The ideal interface for an EIS would be simple to use and highly flexible, providing consistent performance, reflecting the executive’s world, and containing help information.

Telecommunication

As decentralizing is becoming the current trend in companies, telecommunications will play a pivotal role in networked information systems. Transmitting data from one place to another has become crucial for establishing a reliable network. In addition, telecommunications within an EIS can accelerate the need for access to distributed data.

Applications

EIS enables executives to find those data according to user-defined criteria and promote information-based insight and understanding. Unlike a traditional management information system presentation, EIS can distinguish between vital and seldom-used data, and track different key critical activities for executives, both which are helpful in evaluating if the company is meeting its corporate objectives. After realizing its advantages, people have applied EIS in many areas, especially, in manufacturing, marketing, and finance areas.

Manufacturing

Basically, manufacturing is the transformation of raw materials into finished goods for sale, or intermediate processes involving the production or finishing of semi-manufactures. It is a large branch of industry and of secondary production. Manufacturing operational control focuses on day-to-day operations, and the central idea of this process is effectiveness and efficiency. To produce meaningful managerial and operational information for controlling manufacturing operations, the executive has to make changes in the decision processes. EIS provides the evaluation of vendors and buyers, the evaluation of purchased materials and parts, and analysis of critical purchasing areas. Therefore, the executive can oversee and review purchasing operations effectively with EIS. In addition, because production planning and control depends heavily on the plant's data base and its communications with all manufacturing work centers, EIS also provides an approach to improve production planning and control.

Marketing

In an organization, marketing executives' role is to create the future. Their main duty is managing available marketing resources to create a more effective future. For this, they need make judgments about risk and uncertainty of a project and its impact on the company in short term and long term. To assist marketing executives in making effective marketing decisions, an EIS can be applied. EIS provides an approach to sales forecasting, which can allow the market executive to compare sales forecast with past sales. EIS also offers an approach to product price, which is found in venture analysis. The market executive can evaluate pricing as related to competition along with the relationship of product quality with price charged. In summary, EIS software package enables marketing executives to manipulate the data by looking for trends, performing audits of the sales data, and calculating totals, averages, changes, variances, or ratios. All of these sales analysis functions help marketing executives to make final decisions.

Financial

A financial analysis is one of the most important steps to companies today. The executive needs to use financial ratios and cash flow analysis to estimate the trends and make capital investment decisions. An EIS is a responsibility-oriented approach that integrates planning or budgeting with control of performance reporting, and it can be extremely helpful to finance executives. Basically, EIS focuses on accountability of financial performance and it recognizes the importance of cost standards and flexible budgeting in developing the quality of information provided for all executive levels. EIS enables executives to focus more on the long-term basis of current year and beyond, which means that the executive not only can manage a sufficient flow to maintain current operations but also can figure out how to expand operations that are contemplated over the coming years. Also, the combination of EIS and EDI environment can help cash managers to review the company's financial structure so that the best method of financing for an accepted capital project can be concluded. In addition, the EIS is a good tool to help the executive to review financial ratios, highlight financial trends and analyze a company's performance and its competitors.

Advantages and Disadvantages EIS

Advantages of EIS

- Easy for upper-level executives to use, extensive computer experience is not required in operations
- Provides timely delivery of company summary information
- Information that is provided is better understood
- Filters data for management
- Improves to tracking information
- Offers efficiency to decision makers

Disadvantages of EIS

- System dependent
- Limited functionality, by design
- Information overload for some managers
- Benefits hard to quantify
- High implementation costs
- System may become slow, large, and hard to manage
- Need good internal processes for data management
- May lead to less reliable and less secure data

Future Trends

The future of executive info systems will not be bound by mainframe computer systems. This trend allows executives escaping from learning different computer operating systems and substantially decreases the implementation costs for companies. Because

utilizing existing software applications lies in this trend, executives will also eliminate the need to learn a new or special language for the EIS package. Future executive information systems will not only provide a system that supports senior executives, but also contain the information needs for middle managers. The future executive information systems will become diverse because of integrating potential new applications and technology into the systems, such as incorporating artificial intelligence (AI) and integrating multimedia characteristics and ISDN technology into an EIS. EIS - timely, efficient and effective in supporting the decision making process.

Chapter- 3

Collaborative Software

Collaborative software (also referred to as **groupware**, **workgroup support systems** or simply **group support systems**) is software designed to help people involved in a common task achieve their goals.

Overview

Collaborative software is a concept that greatly overlaps with computer-supported cooperative work (CSCW). Some authors argue they are equivalent. According to Carstensen and Schmidt (1999) groupware is part of CSCW, since CSCW addresses "how collaborative activities and their coordination can be supported by means of computer systems.

Software systems such as email, calendaring, text chat and bookmarking belong to this category. It has been suggested that Metcalfe's law — the more people who use something, the more valuable it becomes — applies to these types of software.

Whereas the more general term social software applies to systems used outside the workplace, for example, online dating services and social networks like Friendster, Twitter and Facebook, the use of **collaborative software** in the workspace creates a collaborative working environment (CWE). A collaborative working environment supports people in both their individual and cooperative work thus giving birth to a new class of professionals, e-professionals, who can work together irrespective of their geographical location.

Finally collaborative software relates to the notion of collaborative work systems which are conceived as any form of human organization that emerges any time that collaboration takes place, whether it is formal or informal, intentional or unintentional.

Whereas the groupware or collaborative software pertains to the technological elements of computer supported cooperative work, collaborative work systems become a useful analytical tool to understand the behavioral and organizational variables that are associated to the broader concept of CSCW.

Philosophical Underpinnings

Technology has long been used to bring together. However, as distance increases, rules and protocols need to be implemented. One seminal book on the process of working together from a distance is 'Virtual Teams' by Jessica Lipnack and Jeffrey Stamps.

Origins

Online collaborative software began with online gaming between early computer users. In 1975 by Will Crowther created Colossal Cave Adventure on a DEC PDP-10 computer. As internet connections grew, so did the numbers of users and multi-user games. In 1978 Roy Trubshaw, a student at Essex University in the UK, created the game MUD (Multi-User Dungeon). A number of other MUDs were created, but remained a computer science novelty until the late 1980s, when personal computers with dial-up modems began to be more common in homes, largeley through the use of multi-line Bulletin Board Systems and online service providers.

Parallel to development of MUDs were applications for online chat, video sharing and voice over IP. These would be essential for further development. Studies at MITRE showed the value of voice and text chat, and sharing pictures for shared understanding.

The US Government began using truly collaborative applications in the early 1990s. One of the first robust applications was the Navy's Common Operational Modeling, Planning and Simulation Strategy (COMPASS). The COMPASS system allowed up to 6 users created point-to-point connections with one another; the collaboraive session only remained while at least one user stayed active, and would have to be recreated if all six logged out. MITRE improved on that model by hosting the collaborative session on a server that each user logged into. Called the Collaborative Virtual Workstation (CVW), this allowed the session to be set up in a virtual file cabinet and virtual rooms, and left as a persistent session that could be joined later. In 1996, Pavel Curtis, who had built MUDs at PARC, created PlaceWare, a server that simulated a one-to-many auditorium, with side chat between "seat-mates", and the ability to invite a limited number of audence members to speak. In 1997, engineers at GTE used the PlaceWare engine in a commercial version of MITRE's CVW, calling it InfoWorkSpace (IWS). In 1998, IWS was chosen as the military standard for the standardized Air Operations Center. The IWS product was sold to General Dynamics and then later to Ezenia.

Groupware

The term *groupware* can be traced as far back as the late 1980s, when Richman and Slovak (1987) wrote:

"Like an electronic sinew that binds teams together, the new *groupware* aims to place the computer squarely in the middle of communications among managers, technicians, and anyone else who interacts in groups, revolutionizing the way they work."

In the early 1990s the first groupware commercial products began delivering up to their promises, and big companies such as Boeing or IBM started using electronic meeting systems to leverage key internal projects. Lotus Notes appeared as a major example of that product category, allowing remote group collaboration when the Internet was still in its infancy. Kirkpatrick and Losee (1992) wrote then:

"If GROUPWARE really makes a difference in productivity long term, the very definition of an office may change. You will be able to work efficiently as a member of a group wherever you have your computer. As computers become smaller and more powerful, that will mean anywhere."

As collaborative software evolves and migrates into the Internet itself, it contributes to the development of the so called Web 2.0 bringing a host of collaborative features that were originally conceived for within the corporate network. These include functionalities such as document sharing (including group editing), group calendar and instant messaging, web conferencing, among others. The study of computer-supported collaboration includes the study of collaborative software and social phenomena associated with it.

Design & Implementation Issues

- Persistence is needed in some sessions. Chat and voice communications are routinely non-persistent and evaporate at the end of the session. Virtual room and online file cabinets can persist for years. The designer of the collaborative space needs to consider the information suration needs and implement accordingly.
- Authentication has always been a problem with groupware. When connections are made point-to-point, of when log-in registration is enforced, it's clear who is engaged in the session. However, audio and unmoderated sessions carry the risk of unannounced 'lurkers' who observe but do not announce themselves or contribute.
- Until recently, bandwidth issues at fixed location limited full use of the tools. These are exacerbated with mobile devices.

Collaborative software and collaboration

The design intent of collaborative software (groupware) is to transform the way documents and rich media are shared in order to enable more effective team collaboration.

Collaboration, with respect to information technology, seems to have several definitions. Some are defensible but others are so broad they lose any meaningful application. Understanding the differences in human interactions is necessary to ensure the appropriate technologies are employed to meet interaction needs.

There are three primary ways in which humans interact: conversations, transactions, and collaborations.

Conversational interaction is an exchange of information between two or more participants where the primary purpose of the interaction is discovery or relationship building. There is no central entity around which the interaction revolves but is a free exchange of information with no defined constraints. Communication technology such as telephones, instant messaging, and e-mail are generally sufficient for conversational interactions.

Transactional interaction involves the exchange of transaction entities where a major function of the transaction entity is to alter the relationship between participants. The transaction entity is in a relatively stable form and constrains or defines the new relationship. One participant exchanges money for goods and becomes a customer. Transactional interactions are most effectively handled by transactional systems that manage state and commit records for persistent storage.

In *collaborative interactions* the main function of the participants' relationship is to alter a collaboration entity (i.e., the converse of transactional). The collaboration entity is in a relatively unstable form. Examples include the development of an idea, the creation of a design, the achievement of a shared goal. Therefore, real collaboration technologies deliver the functionality for many participants to augment a common deliverable. Record or document management, threaded discussions, audit history, and other mechanisms designed to capture the efforts of many into a managed content environment are typical of collaboration technologies.

Collaboration in Education- two or more co-equal individuals voluntarily bring their knowledge and experiences together by interacting toward a common goal in the best interest of students' needs for the betterment of their educational success.

Collaboration cannot take place in a vacuum, it requires individuals working together in a coordinated fashion, towards a common goal. Accomplishing the goal is the primary purpose for bringing the team together. Collaborative software helps facilitate the action-oriented team working together over geographic distances by providing tools that help communication, collaboration and the process of problem solving by providing the team with a common means for communicating ideas and brainstorming. Additionally, collaborative software should support project management functions, such as task assignments, time-management with deadlines and shared calendars. The artifacts, the tangible evidence of the problem solving process, including the final outcome of the collaborative effort, require documentation, archiving and promotion for potential reuse. This should also include the artifacts of the process itself, such as project plans and schedules noting deadlines and deliverables.

Collaborative software should support the individuals that make up the team and the interactions between them during the group decision making process. Today's teams are composed of members from around the globe with many using their second or third language in communicating with the group. This provides cultural as well as linguistic challenges for any software that supports the collaborative effort. The software should also support team membership, roles and responsibilities. Additionally, collaborative

support systems may offer the ability to support ancillary systems, such as budgets and physical resources.

Brainstorming is considered to be a tenant of collaboration, with the rapid exchange of ideas facilitating the group decision making process. Collaborative software provides areas that support multi-user editing with virtual whiteboards and chat or other forms of communication. Better solutions record the process and provide revision history. An emerging category of computer software, a collaboration platform is a unified electronic platform that supports synchronous and asynchronous communication through a variety of devices and channels.

An extension of groupware is *collaborative media*, software that allows several concurrent users to create and manage information in a website. By method used we can divide them into:

- Web-based collaborative tools
- Software collaborative tools

Along with these, already traditional, methods recent expansion of corporate use of Second Life and other virtual worlds lead to development of a newer generation of software that takes advantage of a 3D data presentation. Some of this software (3D Topicscape) works independently from virtual worlds and simply uses 3D to support user *in concept creation, planning, organization, development and actualization*. Other () designed specifically to assist in collaboration when using virtual worlds as a business platform, while yet another type of software, Collaborative Knowledge Management (cKM), bridges the gap and can be used simultaneously in Second Life and on the web.

By area served we can divide collaborative software into:

- Knowledge management tools
- Knowledge creation tools
- Information sharing tools
- Collaborative project management tools

Collaborative project management tools

Collaborative project management tools (CPMT) are very similar to collaborative management tools (CMT) except that CMT may only facilitate and manage a certain group activities for a part of a bigger project or task, while CPMT covers all detailed aspects of collaboration activities and management of the overall project and its related knowledge areas.

Another major difference is that CMT may include social software while CPMT mostly considers business or corporate related goals with some kind of social boundaries most commonly used for project management.

Background

During the mid-1990s project management started to evolve into collaborative project management; this was when the process in which a project's inputs and outputs were carried out started to change with the evolution of the internet. Since the geographical boundaries broadened the development teams increasingly became more remote changing the dynamics of a project team thus changing the way a project was managed.

Former chairman of GE Jack Welch believed that you could not be successful if you went it alone in a global economy. Therefore Welch became a driving force behind not only collaboration between organizations, but also collaborative project management.

Difference between collaborative management tools and collaborative project management tools

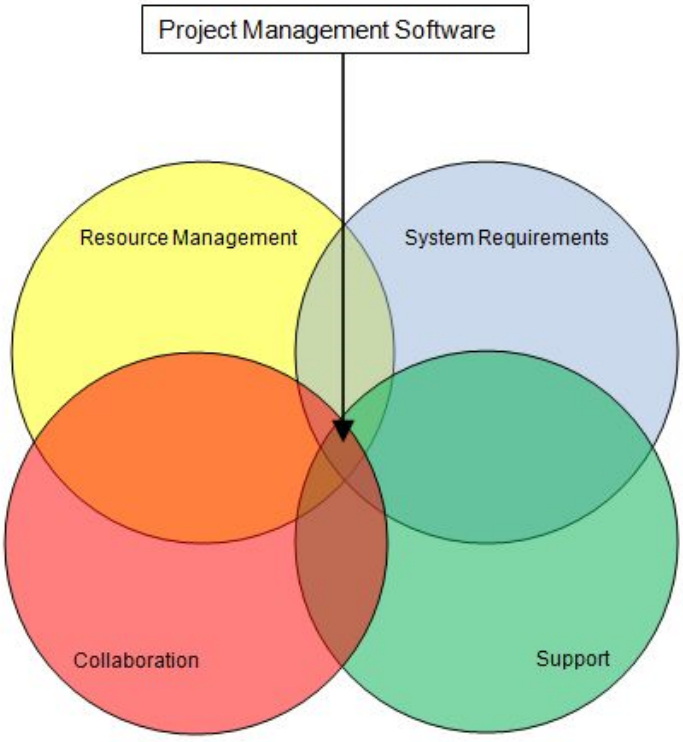
Collaborative project management tools	Collaborative management tools
In addition to most CMT examples, CPMT also includes: • HR and equipment management • Time and cost management • Online chat • Instant messaging • Telephony • Videoconferencing • Web conferencing • Data conferencing • Application sharing • Electronic meeting systems (EMS) • Synchronous conferencing • E-mail • Faxing • voice mail • Web publishing • Revision control • Charting • Document versioning • Document retention • Document sharing • Document repository • Evaluation and survey	CMT facilitate and manage social or group activities. Examples include: • Electronic calendars • Project management systems • Workflow systems • Knowledge management • Prediction markets • Extranet systems • Social software • Online spreadsheets • Online artwork proofing, feedback, review and approval tool

Dimensions

Different frameworks could be established based on a project needs and requirements in order to find the best software. But the best framework is the one in which the characteristics are so well defined that they cover all the aspects of collaboration activities and management of the overall project.

The challenge in determining which CPM software to use is having a good understanding of the requirements and tools needed for project development. There are many dynamics that make project management challenging (coordination, collaboration, sharing of knowledge and effectiveness of pm's to facilitate the process). Choosing the right CPM software is essential to complementing these issues. According to a survey conducted in 2008 to find out what project managers' expectations and uses of project management software are, the features most important to project managers with project management software were:

- Ability to plan using and sequence activities using CPM/PDM/PERT or Gantt Chart method,
- Produce project master schedules based on project/task breakdown structures, with subordinate details,
- Critical path calculation.



Dimensions Diagram

Dimensions	Descriptions / Examples
Resources Requirements	• Human • Equipment • Time • Cost
System Requirements	• Platform: The operating system that the system can perform on (example Windows, Mac, Linux). Platform type single and multiple. • Hardware: physical requirements such as hard drive space and amount of memory. • Installation/access: How and where the software is installed. • Types of installations stand alone, server based, web portal.
Support Requirements	• Email • 24/7 or restricted schedules • Online or web help • Built-in Help i.e. MS Office • On location assistance • Training on-site/off-site
Collaboration Requirements	• Group Size: The number of users that software supports • Email list • Revision Control • Charting • Document versioning • Document retention • Document sharing • Document repository

The Three levels of collaboration

Groupware can be divided into three categories depending on the level of collaboration: (1) communication tools, (2) conferencing tools and (3) collaborative management (Co-ordination) tools.

1. **Communication** can be thought of as unstructured interchange of information. A phone call or an IM Chat discussion are examples of this.
2. **Conferencing** (or collaboration level, as it is called in the academic papers that discuss these levels) refers to interactive work toward a shared goal. Brainstorming or voting are examples of this.
3. **Co-ordination** refers to complex interdependent work toward a shared goal. A good metaphor for understanding this is to think about a sports team; everyone

has to contribute the right play at the right time as well as adjust their play to the unfolding situation - but everyone is doing something different - in order for the team to win. That is complex interdependent work toward a shared goal: collaborative management.

Electronic communication tools

Electronic communication tools send messages, files, data, or documents between people and hence facilitate the sharing of information. Examples include:

- synchronous conferencing
- asynchronous conferencing
- e-mail
- faxing
- voice mail
- Web publishing
- revision control

Electronic conferencing tools

Electronic conferencing tools facilitate the sharing of information, but in a more interactive way. Examples include:

- Internet forums (also known as message boards or discussion boards) — a virtual discussion platform to facilitate and manage online text messages
- Online chat — a virtual discussion platform to facilitate and manage real-time text messages
- Instant Messaging
- Telephony — telephones allow users to interact
- Videoconferencing — networked PCs share video and audio signals
- Data conferencing — networked PCs share a common whiteboard that each user can modify
- Application sharing — users can access a shared document or application from their respective computers simultaneously in real time
- Electronic meeting systems (EMS) — originally these were described as "electronic meeting systems," and they were built into meeting rooms. These special purpose rooms usually contained video projectors interlinked with numerous PCs; however, electronic meeting systems have evolved into web-based, any time, any place systems that will accommodate "distributed" meeting participants who may be dispersed in several locations.

Collaborative management (coordination) tools

Collaborative management tools facilitate and manage group activities. Examples include:

- electronic calendars (also called time management software) — schedule events and automatically notify and remind group members
- project management systems — schedule, track, and chart the steps in a project as it is being completed
- workflow systems — collaborative management of tasks and documents within a knowledge-based business process
- knowledge management systems — collect, organize, manage, and share various forms of information
- enterprise bookmarking — collaborative bookmarking engine to tag, organize, share, and search enterprise data
- prediction markets — let a group of people predict together the outcome of future events
- extranet systems (sometimes also known as 'project extranets') — collect, organize, manage and share information associated with the delivery of a project (e.g.: the construction of a building)
- social software systems — organize social relations of groups
- online spreadsheets — collaborate and share structured data and information

Gathering applications

This functionality may be included in some blogs, e.g. *Wetpaint*. Primarily includes:

- surveys
- project management
- feedback
- time tracking.

Implementation

One of the biggest hurdles in implementing groupware applications within an organization is to achieve a high level of adoption from its members. Without clear commitment from top management any groupware implementation risks failure. Employees can be involved in the design of groupware and given incentives to contribute: the rewards could be either financial or psychological. Training is required to make people comfortable using it, otherwise they may not use it.

In many cases collaboration is at odds with the company's corporate culture so implementation will be disruptive. Shifting a corporate culture from being competitive to being cooperative is no small undertaking. It will require changes at all levels of the organization, including top management and CEO.

One of the biggest hurdles in the typical large enterprise is the desire to standardize knowledge practices across that enterprise and to implement tools and processes which support that aim. Much greater value and quicker implementation can be achieved by avoidance of the "one size fits all" meme. Driving people to adopt the same active role (for example: contribution measured by number of uploads) only produces the behavior

driven by the metric - "the game exists of the rules by which it is played". Cultivate the practice of collaboration where it flourishes of its own volition to gain the quickest return. Carefully designed collaborative work systems will achieve this goal.

Voting methods

Some collaboration software allows users to vote, rate, and rank choices, often for the purpose of extracting the collective intelligence of the participants. The votes, ratings, and rankings can be used in various ways such as:

- Producing an average rating, such as 4 out of 5 stars.
- Calculating a popularity ranking, such as a "top 10" list.
- Guiding the creation and organization of documents.
- Making a recommendation that may assist in making a decision.

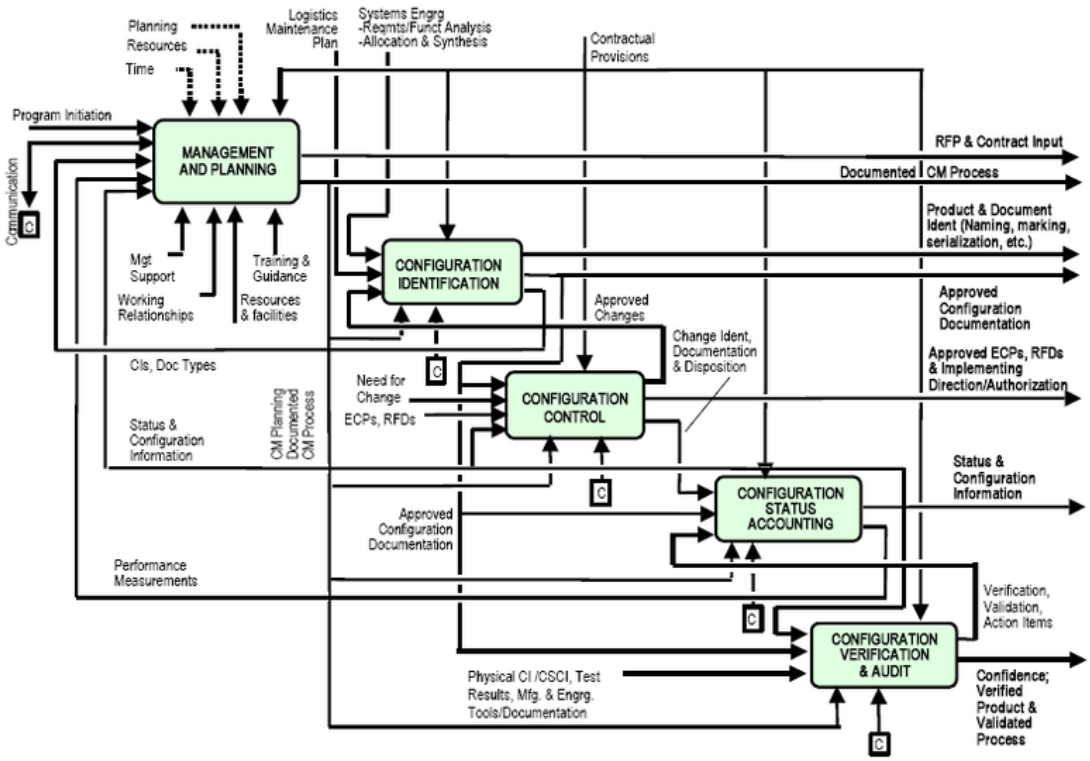
In the case of decision making, Condorcet voting can combine multiple perspectives in a way that reduces intransitivity. It's worth noting that no matter what voting method is implemented, Arrow's Impossibility Theorem guarantees that an ideal voting system can never be attained if there are three or more alternatives that are voted upon.

In addition to allowing participants to rank pre-existing choices, some collaboration software allows participants to add new choices to the list of choices being ranked.

Voting in collaboration software is related to recommendation systems that generate appreciated recommendations based on ratings or rankings collected from many people.

Chapter- 4

Configuration Management



Top level Configuration Management Activity model

Configuration management (CM) is a field of management that focuses on establishing and maintaining consistency of a system or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life.

For information assurance, CM can be defined as the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an

information system. CM for information assurance, sometimes referred to as **S**ecure **C**onfiguration **M**anagement, relies upon performance, functional, and physical attributes of IT platforms and products and their environments to determine the appropriate security features and assurances that are used to measure a system configuration state.

For example, configuration requirements may be different for a network firewall that functions as part of an organization's Internet boundary versus one that functions as an internal local network firewall.

History

Configuration management was first developed by the United States Air Force for the Department of Defense in the 1950s as a technical management discipline of hardware. The concepts of this discipline have been widely adopted by numerous technical management functions, including systems engineering (SE), integrated logistics support (ILS), Capability Maturity Model Integration (CMMI), ISO 9000, Prince2 project management methodology, COBIT, Information Technology Infrastructure Library (ITIL), product lifecycle management, and application lifecycle management. Many of these functions and models have redefined configuration management from its traditional holistic approach to technical management. Some treat configuration management as being similar to a librarian activity, and break out change control or change management as a separate or stand alone discipline. However the bottomline is and always shall be Traceability.

Software configuration management

The traditional software configuration management (SCM) process is looked upon by practitioners as the best solution to handling changes in software projects. It identifies the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle.

The SCM process further defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented. They are:

1. Configuration identification
2. Configuration control
3. Configuration status accounting
4. Configuration audits

These terms and definitions change from standard to standard, but are essentially the same.

- Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

- Configuration change control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them.

- Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time.

- Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

Configuration management is widely used by many military organizations to manage the technical aspects of any complex systems, such as weapon systems, vehicles, and information systems. The discipline combines the capability aspects that these systems provide an organization with the issues of management of change to these systems over time.

Outside of the military, CM is appropriate to a wide range of fields and industry and commercial sectors.

Computer hardware configuration management

Computer hardware configuration management is the process of creating and maintaining an up-to-date record of all the components of the infrastructure, including related documentation. Its purpose is to show what makes up the infrastructure and illustrate the physical locations and links between each item, which are known as configuration items.

Computer hardware configuration goes beyond the recording of computer hardware for the purpose of asset management, although it can be used to maintain asset information. The extra value provided is the rich source of support information that it provides to all interested parties. This information is typically stored together in a configuration management database (CMDB). This concept was introduced by ITIL.

The scope of configuration management is assumed to include, at a minimum, all configuration items used in the provision of live, operational services.

Computer hardware configuration management provides direct control over information technology (IT) assets and improves the ability of the service provider to deliver quality IT services in an economical and effective manner. Configuration management should work closely with change management.

All components of the IT infrastructure should be registered in the CMDB. The responsibilities of configuration management with regard to the CMDB are:

- identification
- control
- status accounting
- verification

The scope of configuration management is assumed to include:

- physical client and server hardware products and versions
- operating system software products and versions
- application development software products and versions
- technical architecture product sets and versions as they are defined and introduced
- live documentation
- networking products and versions
- live application products and versions
- definitions of packages of software releases
- definitions of hardware base configurations
- configuration item standards and definitions

The benefits of computer hardware configuration management are:

- helps to minimize the impact of changes
- provides accurate information on CIs
- improves security by controlling the versions of CIs in use
- facilitates adherence to legal obligations
- helps in financial and expenditure planning

Maintenance systems

Configuration management is used to maintain an understanding of the status of complex assets with a view to maintaining the highest level of serviceability for the lowest cost. Specifically, it aims to ensure that operations are not disrupted due to the asset (or parts of the asset) overrunning limits of planned lifespan or below quality levels.

In the military, this type of activity is often classed as "mission readiness", and seeks to define which assets are available and for which type of mission; a classic example is whether aircraft on-board an aircraft carrier are equipped with bombs for ground support or missiles for defense.

A theory of configuration maintenance was worked out by Mark Burgess, with a practical implementation on present day computer systems in the software Cfengine able to perform real time repair as well as preventive maintenance.

Preventive maintenance

Understanding the "as is" state of an asset and its major components is an essential element in preventive maintenance as used in maintenance, repair, and overhaul and enterprise asset management systems.

Complex assets such as aircraft, ships, industrial machinery etc. depend on many different components being serviceable. This serviceability is often defined in terms of the amount of usage the component has had since it was new, since fitted, since repaired, the amount of use it has had over its life and several other limiting factors. Understanding how near the end of their life each of these components is has been a major undertaking involving labor intensive record keeping until recent developments in software.

Predictive maintenance

Many types of component use electronic sensors to capture data which provides live condition monitoring. This data is analyzed on board or at a remote location by computer to evaluate its current serviceability and increasingly its likely future state using algorithms which predict potential future failures based on previous examples of failure through field experience and modeling. This is the basis for "predictive maintenance".

Availability of accurate and timely data is essential in order for CM to provide operational value and a lack of this can often be a limiting factor. Capturing and disseminating the operating data to the various support organizations is becoming an industry in itself.

The consumers of this data have grown more numerous and complex with the growth of programs offered by original equipment manufacturers (OEMs). These are designed to offer operators guaranteed availability and make the picture more complex with the operator managing the asset but the OEM taking on the liability to ensure its serviceability. In such a situation, individual components within an asset may communicate directly to an analysis center provided by the OEM or an independent analyst.

Standards

- ANSI/EIA-649-1998 National Consensus Standard for Configuration Management
- EIA-649-A 2004 National Consensus Standard for Configuration Management
- ISO 10007:2003 Quality management systems - Guidelines for configuration management
- Federal Standard 1037C

- GEIA Standard 836-2002 Configuration Management Data Exchange and Interoperability
- IEEE Std. 828-1998 IEEE Standard for Software Configuration Management Plans
- MIL-STD-973 Configuration Management (cancelled on September 20, 2000)
- STANAG 4159 NATO Materiel Configuration Management Policy and Procedures for Multinational Joint Projects
- STANAG 4427 Introduction of Allied Configuration Management Publications (ACMPs)
- CMMI CMMI for Development, Version 1.2 CONFIGURATION MANAGEMENT
- CMII - The Path to Integrated Process Excellence

Chapter- 5

Enterprise Resource Planning

An **Enterprise Resource Planning** (**ERP**) system is an integrated computer-based application used to manage internal and external resources, including tangible assets, financial resources, materials, and human resources. Its purpose is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders. Built on a centralized database and normally utilizing a common computing platform, ERP systems consolidate all business operations into a uniform and enterprise-wide system environment.

An ERP system can either reside on a centralized server or be distributed across modular hardware and software units that provide "services" and communicate on a local area network. The distributed design allows a business to assemble modules from different vendors without the need for the placement of multiple copies of complex and expensive computer systems in areas which will not use their full capacity.

Origin of the term

The initialism ERP was first employed by research and analysis firm Gartner Group in 1990 as an extension of MRP (Material Requirements Planning; later manufacturing resource planning) and CIM (Computer Integrated Manufacturing), and whilst not supplanting these terms, it has come to represent a larger whole. It came into use, as the creators of MRP software started to develop software applications beyond the manufacturing arena. However, this does not mean that ERP packages have typically been developed from a manufacturing core. Many of the major players started their development of an integrated package from other directions, such as accounting, maintenance and human resources management. ERP systems now attempt to cover all core functions of an enterprise, regardless of the organization's business or charter. These systems can now be found in non-manufacturing businesses, non-profit organizations and governments.

To be considered as an ERP system, a software package should have the following traits:

- An integrated system that operates in (next to) real time, without relying on periodic batch updates.
- A common database, that is accessed by all applications, preventing redundant data and multiple data definitions.
- A consistent look and feel throughout each module (sales, manufacturing, accounting etc.).
- The ability to access the system without specialist integration by the Information System (or IT) department.

Components / Modules

- Transactional Backbone
  - Financials
  - Distribution
  - Human Resources
  - Product lifecycle management

- Advanced Applications
  - Customer Relationship Management (CRM)
  - Supply chain management software
    - Purchasing
    - Manufacturing
    - Distribution
  - Warehouse Management System.

- Management Portal/Dashboard
  - Decision Support System

These modules can exist in a system or can be utilized in an ad-hoc fashion.

Commercial applications

Manufacturing
: Engineering, bills of material, work orders, scheduling, capacity, workflow management, quality control, cost management, manufacturing process, manufacturing projects, manufacturing flow

Supply chain management
: Order to cash, inventory, order entry, purchasing, product configurator, supply chain planning, supplier scheduling, inspection of goods, claim processing, commission calculation

Financials
: General ledger, cash management, accounts payable, accounts receivable, fixed assets

Project management
: Costing, billing, time and expense, performance units, activity management

Human resources
: Human resources, payroll, training, time and attendance, rostering, benefits

Customer relationship management
: Sales and marketing, commissions, service, customer contact, call-center support

Data services
: Various "self-service" interfaces for customers, suppliers and/or employees

Access control
: Management of user privileges for various processes

History

The term "Enterprise resource planning" originally derived from manufacturing resource planning (MRP II) that followed material requirements planning (MRP). MRP evolved into ERP when "routings" became a major part of the software architecture and a company's capacity planning activity also became a part of the standard software activity. ERP systems typically handle the manufacturing, logistics, distribution, inventory, shipping, invoicing, and accounting for a company. ERP software can aid in the control of many business activities, including sales, marketing, delivery, billing, production, inventory management, quality management, and human resource management.

ERP systems saw a large boost in sales in the 1990s as companies faced the Y2K problem in their legacy systems. Many companies took this opportunity to replace such information systems with ERP systems. This rapid growth in sales was followed by a slump in 1999, at which time most companies had already implemented their Y2K solution.

ERP systems are often incorrectly called *back office systems*, indicating that customers and the general public are not directly involved. This is contrasted with *front office systems* like customer relationship management (CRM) systems that deal directly with the customers, or the eBusiness systems such as eCommerce, eGovernment, eTelecom, and eFinance, or supplier relationship management (SRM) systems.

ERP systems are cross-functional and enterprise-wide. All functional departments that are involved in operations or production are integrated in one system. In addition to areas such as manufacturing, warehousing, logistics, and information technology, this typically includes accounting, human resources, marketing and strategic management.

ERP II, a term coined in the early 2000s, is often used to describe what would be the next generation of ERP software. This new generation of software is web-based and allows both employees and external resources (such as suppliers and customers) real-time access to the system's data.

EAS — Enterprise Application Suite is a new name for formerly developed ERP systems which include (almost) all segments of business using ordinary Internet browsers as thin clients.

Though traditionally ERP packages have been on-premise installations, ERP systems are now also available as Software as a Service.

Best practices are incorporated into most ERP vendor's software packages. When implementing an ERP system, organizations can choose between customizing the software or modifying their business processes to the "best practice" function delivered in the "out-of-the-box" version of the software.

Prior to ERP, software was developed to fit individual processes of an individual business. Due to the complexities of most ERP systems and the negative consequences of a failed ERP implementation, most vendors have included "Best Practices" into their software. These "Best Practices" are what the Vendor deems as the most efficient way to carry out a particular business process in an Integrated Enterprise-Wide system. A study conducted by Ludwigshafen University of Applied Science surveyed 192 companies and concluded that companies which implemented industry best practices decreased mission-critical project tasks such as configuration, documentation, testing and training. In addition, the use of best practices reduced over risk by 71% when compared to other software implementations.

The use of best practices can make complying with requirements such as IFRS, Sarbanes-Oxley, or Basel II easier. They can also help where the process is a commodity such as electronic funds transfer. This is because the procedure of capturing and reporting legislative or commodity content can be readily codified within the ERP software, and then replicated with confidence across multiple businesses who have the same business requirement.

Implementation

Businesses have a wide scope of applications and processes throughout their functional units, producing ERP software systems that are typically complex and usually impose significant changes on staff work practices. Implementing ERP software is typically too complex for in-house developers, lacking the required skills, so it is desirable and advisable to hire outside consultants who are professionally trained to implement these systems. This is typically the most cost-effective way. There are three types of services that may be employed - Consulting, Customization, and Support. The length of time to implement an ERP system depends on the size of the business, the number of modules, the extent of customization, the scope of the change, and the willingness of the customer to take ownership for the project. ERP systems are modular, so they don't all need be implemented at once. Implementation can be divided into various stages, or phase-ins. The typical project is about 14 months and requires around 150 consultants. A small project (e.g. a company of less than 100 staff) can be planned and delivered within 3–9 months; however, a large, multi-site or multi-country implementation can take years. The length of the implementations is closely tied to the amount of customization desired.

To implement ERP systems, companies often seek the help of an ERP vendor or a third-party consulting company. Consulting firms typically provide three areas of professional services: consulting, customization, and support. The client organization can also employ independent program management, business analysis, change management, and UAT specialists to ensure their business requirements remain a priority during implementation.

Data Migration

Data migration is one of the most important activities in determining the success of an ERP implementation. Since many decisions must be made before migration, a significant amount of planning must occur. Unfortunately, data migration is the last activity before the production phase of an ERP implementation, and therefore receives minimal attention due to time constraints. The following are steps of a data migration strategy that can help with the success of an ERP implementation:

1. Identify the data to be migrated
2. Determine the timing of data migration
3. Generate the data templates
4. Freeze the tools for data migration
5. Decide on migration-related setups
6. Decide on data archiving

Process preparation

ERP vendors have designed their systems around standard business processes, based upon best business practices. Different vendor(s) have different types of processes but they are all of a standard, modular nature. Firms that want to implement ERP systems are consequently forced to adapt their organizations to standardized processes as opposed to adapting the ERP package to the existing processes. Neglecting to map current business processes prior to starting ERP implementation is a main reason for failure of ERP projects. It is therefore crucial that organizations perform a thorough business process analysis before selecting an ERP vendor and setting off on the implementation track. This analysis should map out all present operational processes, enabling selection of an ERP vendor whose standard modules are most closely aligned with the established organization. Redesign can then be implemented to achieve further process congruence. Research indicates that the risk of business process mismatch is decreased by:

- linking each current organizational process to the organization's strategy;
- analyzing the effectiveness of each process in light of its current related business capability;
- understanding the automated solutions currently implemented.

ERP implementation is considerably more difficult (and politically charged) in organizations structured into nearly independent business units, each responsible for their own profit and loss, because they will each have different processes, business rules, data semantics, authorization hierarchies and decision centers. Solutions include requirements coordination negotiated by local change management professionals or, if this is not possible, federated implementation using loosely integrated instances (e.g. linked via Master data management) specifically configured and/or customized to meet local needs.

A disadvantage usually attributed to ERP is that business process redesign to fit the standardized ERP modules can lead to a loss of competitive advantage. While

documented cases exist where this has indeed materialized, other cases show that, following thorough process preparation, ERP systems can actually increase sustainable competitive advantage.

Configuration

Configuring an ERP system is largely a matter of balancing the way you want the system to work with the way the system lets you work. Begin by deciding which modules to install, then adjust the system using configuration tables to achieve the best possible fit in working with your company's processes.

Modules — Most systems are modular simply for the flexibility of implementing some functions but not others. Some common modules, such as finance and accounting are adopted by nearly all companies implementing enterprise systems; others however such as human resource management are not needed by some companies and therefore not adopted. A service company for example will not likely need a module for manufacturing. Other times companies will not adopt a module because they already have their own proprietary system they believe to be superior. Generally speaking, the greater the number of modules selected, the greater the integration benefits, but also the increase in costs, risks and changes involved.

Configuration Tables – A configuration table enables a company to tailor a particular aspect of the system to the way it chooses to do business. For example, an organization can select the type of inventory accounting – FIFO or LIFO – it will employ, or whether it wants to recognize revenue by geographical unit, product line, or distribution channel.

So what happens when the options the system allows just aren't good enough? At this point a company has two choices, both of which are not ideal. It can re-write some of the enterprise system's code, or it can continue to use an existing system and build interfaces between it and the new enterprise system. Both options will add time and cost to the implementation process. Additionally they can dilute the system's integration benefits. The more customized the system becomes the less possible seamless communication between suppliers and customers.

Connectivity to Plant Floor Information

ERP systems connect to real-time data and transaction data (data accumulated into collections to deliver sets of information) in a variety of ways. These systems are typically configured by System Integrators, able to bring their unique knowledge on process, equipment and vendor solutions.

Direct Integration – ERP systems connectivity (communications to plant floor equipment) as part of their product offering. This requires the ERP system developers to offer specific support for the variety of plant floor equipment that they want to interface with. ERP Vendors must be expert in their own products, and connectivity to other vendor products, often those offered by competitors.

Relational Database (RDB) Integration – ERP systems connect to plant floor data sources through a Relational Database Staging Table. Plant floor systems will deposit the necessary information into a Relational Data Base. The ERP system will remove and use the information from the RDB Table. The benefit of RDB Staging is that ERP vendors do not need to get involved in the complexities of plant floor equipment integration. Connectivity becomes the responsibility of the System Integrator.

EATM (Enterprise Transaction Modules) – These devices have the ability to communicate directly with plant floor equipment and will transact data with the ERP system in methods best supported by the ERP system. Again, this can be through a staging table, Web Services, or through system specific business system APIs. The benefit of an EATM is that it offers a complete, off the shelf solution, minimizing long term costs and customization.

Custom Integrated Solutions – Many system integrators designs offer custom crafted solutions, created on a per instance basis to meet site and system requirements. There are a wide variety of communications drivers available for plant floor equipment and there are separate products that have the ability to log data to relational database tables. Standards exist within the industry to support interoperability between software products, the most widely known being OPC, managed by the OPC Foundation. Custom Integrated Solutions typically run on workstation or server class computers. These systems tend to have the highest level of initial integration cost, and can have a higher long term cost in terms on maintenance and reliability. Long term costs can be minimized through careful system testing and thorough documentation.

Consulting services

Many organizations do not have sufficient internal skills to implement an ERP project. This results in many organizations offering consulting services for ERP implementation. Typically, a consulting team is responsible for the entire ERP implementation including:

1. selecting
2. planning
3. training
4. testing
5. implementation
6. delivery

of any customized modules. Examples of customization includes creating processes and reports for compliance; additional product training; creation of process triggers and workflow; specialist advice to improve how the ERP is used in the business; system optimization; and assistance writing reports, complex data extracts or implementing Business Intelligence.

For most mid-sized companies, the cost of the implementation will range from around the list price of the ERP user licenses to up to twice this amount (depending on the level of

customization required). Large companies, and especially those with multiple sites or countries, will often spend considerably more on the implementation than the cost of the user licenses—three to five times more is not uncommon for a multi-site implementation.

Unlike most single-purpose applications, ERP packages have historically included full source code and shipped with vendor-supported team IDEs for customizing and extending the delivered code. During the early years of ERP the guarantee of mature tools and support for extensive customization was an important sales argument when a potential customer was considering developing their own unique solution in-house, or assembling a cross-functional solution by integrating multiple "best of breed" applications.

"Core system" customization vs configuration

Increasingly, ERP vendors have tried to reduce the need for customization by providing built-in "configuration" tools to address most customers' needs for changing how the out-of-the-box core system works. Key differences between customization and configuration include:

- Customization is always optional, whereas some degree of configuration (e.g., setting up cost/profit centre structures, organisational trees, purchase approval rules, etc.) may be needed before the software will work at all.
- Configuration is available to all customers, whereas customization allows an individual customer to implement proprietary "market-beating" processes.
- Configuration changes tend to be recorded as entries in vendor-supplied data tables, whereas customization usually requires some element of programming and/or changes to table structures or views.
- The effect of configuration changes on the performance of the system is relatively predictable and is largely the responsibility of the ERP vendor. The effect of customization is unpredictable and may require time-consuming stress testing by the implementation team.
- Configuration changes are almost always guaranteed to survive upgrades to new software versions. Some customizations (e.g. code that uses pre-defined "hooks" that are called before/after displaying data screens) will survive upgrades, though they will still need to be retested. More extensive customizations (e.g. those involving changes to fundamental data structures) will be overwritten during upgrades and must be reimplemented manually.

By this analysis, customizing an ERP package can be unexpectedly expensive and complicated, and tends to delay delivery of the obvious benefits of an integrated system. Nevertheless, customizing an ERP suite gives the scope to implement secret recipes for excellence in specific areas while ensuring that industry best practices are achieved in less sensitive areas.

Extensions

In this context, "Extensions" refers to ways that an ERP environment can be "extended" (supplemented) with third-party programs. It is technically easy to expose most ERP transactions to outside programs that do other things, e.g.:

- archiving, reporting and republishing (these are easiest to achieve, because they mainly address static data);
- performing transactional data captures, e.g. using scanners, tills or RFIDs (also relatively easy because they touch existing data).

However, because ERP applications typically contain sophisticated rules that control how data can be created or changed, such functions can be very difficult to implement.

Advantages

In the absence of an ERP system, a large manufacturer may find itself with many software applications that cannot communicate or interface effectively with one another. Tasks that need to interface with one another may involve:

- ERP systems connect the necessary software in order for accurate forecasting to be done. This allows inventory levels to be kept at maximum efficiency and the company to be more profitable.
- Integration among different functional areas to ensure proper communication, productivity and efficiency
- Design engineering (how to best make the product)
- Order tracking, from acceptance through fulfillment
- The revenue cycle, from invoice through cash receipt
- Managing inter-dependencies of complex processes bill of materials
- Tracking the three-way match between purchase orders (what was ordered), inventory receipts (what arrived), and costing (what the vendor invoiced)
- The accounting for all of these tasks: tracking the revenue, cost and profit at a granular level.

ERP systems centralize the data in one place. Benefits of this include:

- Eliminates the problem of synchronizing changes between multiple systems - consolidation of finance, marketing and sales, human resource, and manufacturing applications
- Permits control of business processes that cross functional boundaries
- Provides top-down view of the enterprise (no "islands of information"), real time information is available to management anywhere, anytime to make proper decisions.
- Reduces the risk of loss of sensitive data by consolidating multiple permissions and security models into a single structure.
- Shorten production lead time and delivery time

- Facilitating business learning, empowering, and building common visions

Some security features are included within an ERP system to protect against both outsider crime, such as industrial espionage, and insider crime, such as embezzlement. A data-tampering scenario, for example, might involve a disgruntled employee intentionally modifying prices to below-the-break-even point in order to attempt to interfere with the company's profit or other sabotage. ERP systems typically provide functionality for implementing internal controls to prevent actions of this kind. ERP vendors are also moving toward better integration with other kinds of information security tools.

Disadvantages

Problems with ERP systems are mainly due to inadequate investment in ongoing training for the involved IT personnel - including those implementing and testing changes - as well as a lack of corporate policy protecting the integrity of the data in the ERP systems and the ways in which it is used.

Disadvantages

- Customization of the ERP software is limited.
- Re-engineering of business processes to fit the "industry standard" prescribed by the ERP system may lead to a loss of competitive advantage.
- ERP systems can be very expensive. (This has led to a new category of "ERP light" solutions.)
- ERPs are often seen as too rigid and too difficult to adapt to the specific workflow and business process of some companies—this is cited as one of the main causes of their failure.
- Many of the integrated links need high accuracy in other applications to work effectively. A company can achieve minimum standards, then over time "dirty data" will reduce the reliability of some applications.
- Once a system is established, switching costs are very high for any partner (reducing flexibility and strategic control at the corporate level).
- The blurring of company boundaries can cause problems in accountability, lines of responsibility, and employee morale.
- Resistance in sharing sensitive internal information between departments can reduce the effectiveness of the software.
- Some large organizations may have multiple departments with separate, independent resources, missions, chains-of-command, etc., and consolidation into a single enterprise may yield limited benefits.

Chapter- 6

Electronic Business

Electronic business, commonly referred to as "**eBusiness**" or "**e-business**", may be defined as the application of information and communication technologies (ICT) in support of all the activities of business. Commerce constitutes the exchange of products and services between businesses, groups and individuals and can be seen as one of the essential activities of any business. Electronic commerce focuses on the use of ICT to enable the external activities and relationships of the business with individuals, groups and other businesses.

Louis Gerstner, the former CEO of IBM, in his book, *Who Says Elephants Can't Dance?* attributes the term "e-Business" to IBM's marketing and Internet teams in 1996.

Electronic business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers.

In practice, e-business is more than just e-commerce. While e-business refers to more strategic focus with an emphasis on the functions that occur using electronic capabilities, e-commerce is a subset of an overall e-business strategy. E-commerce seeks to add revenue streams using the World Wide Web or the Internet to build and enhance relationships with clients and partners and to improve efficiency using the Empty Vessel strategy. Often, e-commerce involves the application of knowledge management systems.

E-business involves business processes spanning the entire value chain: electronic purchasing and supply chain management, processing orders electronically, handling customer service, and cooperating with business partners. Special technical standards for e-business facilitate the exchange of data between companies. E-business software solutions allow the integration of intra and inter firm business processes. E-business can be conducted using the Web, the Internet, intranets, extranets, or some combination of these.

Basically, electronic commerce (EC) is the process of buying, transferring, or exchanging products, services, and/or information via computer networks, including the internet. EC

can also be benifited from many perspective including business process, service, learning, collaborative, community. EC is often confused with e-business.

Subsets

Applications can be divided into three categories:

1. Internal business systems:
    - customer relationship management
    - enterprise resource planning
    - document management systems
    - human resources management
2. Enterprise communication and collaboration:
    - VoIP
    - content management system
    - e-mail
    - voice mail
    - Web conferencing
    - Digital work flows (or business process management)
3. electronic commerce - business-to-business electronic commerce (B2B) or business-to-consumer electronic commerce (B2C):
    - internet shop
    - supply chain management
    - online marketing
    - offline marketing

Models

When organizations go online, they have to decide which e-business models best suit their goals. A business model is defined as the organization of product, service and information flows, and the source of revenues and benefits for suppliers and customers. The concept of e-business model is the same but used in the online presence. The following is a list of the currently most adopted e-business models such as:

- E-shops
- E-commerce
- E-procurement
- E-malls
- E-auctions
- Virtual Communities
- Collaboration Platforms
- Third-party Marketplaces
- Value-chain Integrators
- Value-chain Service Providers
- Information Brokerage
- Telecommunication

- Customer relationship

Classification by provider and consumer

Roughly dividing the world into providers/producers and consumers/clients one can classify e-businesses into the following categories:

- business-to-business (B2B)
- business-to-consumer (B2C)
- business-to-employee (B2E)
- business-to-government (B2G)
- government-to-business (G2B)
- government-to-government (G2G)
- government-to-citizen (G2C)
- consumer-to-consumer (C2C)
- consumer-to-business (C2B)

It is notable that there are comparably less connections pointing "upwards" than "downwards" (few employee/consumer/citizen-to-X models).

Electronic Business Security

E-Business systems naturally have greater security risks than traditional business systems, therefore it is important for e-business systems to be fully protected against these risks. A far greater number of people have access to e-businesses through the internet than would have access to a traditional business. Customers, suppliers, employees, and numerous other people use any particular e-business system daily and expect their confidential information to stay secure. Hackers are one of the great threats to the security of e-businesses. Some common security concerns for e-Businesses include keeping business and customer information private and confidential, authenticity of data, and data integrity. Some of the methods of protecting e-business security and keeping information secure include physical security measures as well as data storage, data transmission, anti-virus software, firewalls, and encryption to list a few.

Key Security Concerns within E-Business

Privacy and confidentiality

Confidentiality is the extent to which businesses makes personal information available to other businesses and individuals. With any business, confidential information must remain secure and only be accessible to the intended recipient. However, this becomes even more difficult when dealing with e-businesses specifically. To keep such information secure means protecting any electronic records and files from unauthorized access, as well as ensuring safe transmission and data storage of such information. Tools such as encryption and firewalls manage this specific concern within e-business.

Authenticity

E-business transactions pose greater challenges for establishing authenticity due to the ease with which electronic information may be altered and copies. Both parties in an e-business transaction want to have the assurance that the other party is who they claim to be, especially when a customer places an order and then submits a payment electronically. One common way to ensure this is to limit access to a network or trusted parties by using a virtual private network (VPN) technology. The establishment of authenticity is even greater when a combination of techniques are used, and such techniques involve checking "something you know" (i.e. password or PIN), "something you have" (i.e. credit card), or "something you are" (i.e. digital signatures or voice recognition methods). Many times in e-business, however, "something you are" is pretty strongly verified by checking the purchaser's "something you have" (i.e. credit card) and "something you know" (i.e. card number).

Data integrity

Data integrity answers the question "Can the information be changed or corrupted in any way?" This leads to the assurance that the message received is identical to the message sent. A business needs to be confident that data is not changed in transit, whether deliberately or by accident. To help with data integrity, firewalls protect stored data against unauthorized access, while simply backing up data allows recovery should the data or equipment be damaged.

Non-repudiation

This concern deals with the existence of proof in a transaction. A business must have assurance that the receiving party or purchaser cannot deny that a transaction has occurred, and this means having sufficient evidence to prove the transaction. One way to address non-repudiation is using digital signatures. A digital signature not only ensures that a message or document has been electronically signed by the person, but since a digital signature can only be created by one person, it also ensures that this person cannot later deny that they provided their signature.

Access control

When certain electronic resources and information is limited to only a few authorized individuals, a business and its customers must have the assurance that no one else can access the systems or information. Fortunately, there are a variety of techniques to address this concern including firewalls, access privileges, user identification and authentication techniques (such as passwords and digital certificates), Virtual Private Networks (VPN), and much more.

Availability

This concern is specifically pertinent to a business' customers as certain information must be available when customers need it. Messages must be delivered in a reliable and timely fashion, and information must be stored and retrieved as required. Because availability of service is important for all e-business websites, steps must be taken to prevent disruption of service by events such as power outages and damage to physical infrastructure. Examples to address this include data backup, fire-suppression systems, Uninterrupted Power Supply (UPS) systems, virus protection, as well as making sure that there is sufficient capacity to handle the demands posed by heavy network traffic.

Common Security Measures for E-Business Systems

Many different forms of security exist for e-businesses. Some general security guidelines include areas in physical security, data storage, data transmission, application development, and system administration.

Physical security

Despite e-business being business done online, there are still physical security measures that can be taken to protect the business as a whole. Even though business is done online, the building that houses the servers and computers must be protected and have limited access to employees and other persons. For example, this room should only allow authorized users to enter, and should ensure that "windows, dropped ceilings, large air ducts, and raised floors" do not allow easy access to unauthorized persons. Preferably these important items would be kept in an air-conditioned room without any windows.

Protecting against the environment is equally important in physical security as protecting against unauthorized users. The room may protect the equipment against flooding by keeping all equipment raised off of the floor. In addition, the room should contain a fire extinguisher in case of fire. The organization should have a fire plan in case this situation arises.

In addition to keeping the servers and computers safe, physical security of confidential information is important. This includes client information such as credit card numbers, checks, phone numbers, etc. It also includes any of the organization's private information. Locking physical and electronic copies of this data in a drawer or cabinet is one additional measure of security. Doors and windows leading into this area should also be securely locked. Only employees that need to use this information as part of their job should be given keys.

Important information can also be kept secure by keeping backups of files and updating them on a regular basis. It is best to keep these backups in a separate secure location in case there is a natural disaster or breach of security at the main location.

“Failover sites” can be built in case there is a problem with the main location. This site should be just like the main location in terms of hardware, software, and security features. This site can be used in case of fire or natural disaster at the original site. It is also important to test the “failover site” to ensure it will actually work if the need arises.

State of the art security systems, such as the one used at Tidepoint's headquarters, might include access control, alarm systems, and closed-circuit television. One form of access control is face (or another feature) recognition systems. This allows only authorized personnel to enter, and also serves the purpose of convenience for employees who don't have to carry keys or cards. Cameras can also be placed throughout the building and at all points of entry. Alarm systems also serve as an added measure of protection against theft.

Data storage

Storing data in a secure manner is very important to all businesses, but especially to e-businesses where most of the data is stored in an electronic manner. Data that is confidential should not be stored on the e-business' server, but instead moved to another physical machine to be stored. If possible this machine should not be directly connected to the internet, and should also be stored in a safe location. The information should be stored in an encrypted format.

Any highly sensitive information should not be stored if it is possible. If it does need to be stored, it should be kept on only a few reliable machines to prevent easy access. Extra security measures should be taken to protect this information (such as private keys) if possible. Additionally, information should only be kept for a short period of time, and once it is no longer necessary it should be deleted to prevent it from falling into the wrong hands. Similarly, backups and copies of information should be kept secure with the same security measures as the original information. Once a backup is no longer needed, it should be carefully but thoroughly destroyed.

Data transmission and application development

All sensitive information being transmitted should be encrypted. Businesses can opt to refuse clients who can't accept this level of encryption. Confidential and sensitive information should also never be sent through e-mail. If it must be, then it should also be encrypted.

Transferring and displaying secure information should be kept to a minimum. This can be done by never displaying a full credit card number for example. Only a few of the numbers may be shown, and changes to this information can be done without displaying the full number. It should also be impossible to retrieve this information online.

Source code should also be kept in a secure location. It should not be visible to the public.

Applications and changes should be tested before they are placed online for reliability and compatibility.

System administration

Security on default operating systems should be increased immediately. Patches and software updates should be applied in a timely manner. All system configuration changes should be kept in a log and promptly updated.

System administrators should keep watch for suspicious activity within the business by inspecting log files and researching repeated logon failures. They can also audit their e-business system and look for any holes in the security measures. It is important to make sure plans for security are in place but also to test the security measures to make sure they actually work. With the use of social engineering, the wrong people can get a hold of confidential information. To protect against this, staff can be made aware of social engineering and trained to properly deal with sensitive information.

E-businesses may use passwords for employee logons, accessing secure information, or by customers. Passwords should be made impossible to guess. They should consist of both letters and numbers, and be at least seven to eight digits long. They should not contain any names, birth dates, etc. Passwords should be changed frequently and should be unique each time. Only the password's user should know the password and it should never be written down or stored anywhere. Users should also be locked out of the system after a certain number of failed logon attempts to prevent guessing of passwords.

Security Solutions

When it comes to security solutions, there are some main goals that are to be met. These goals are data integrity, strong authentication, and privacy.

Access and data integrity

There are several different ways to prevent access to the data that is kept online. One way is to use anti-virus software. This is something that most people use to protect their networks regardless of the data they have. E-businesses should use this because they can then be sure that the information sent and received to their system is clean. A second way to protect the data is to use firewalls and network protection. A firewall is used to restrict access to private networks, as well as public networks that a company may use. The firewall also has the ability to log attempts into the network and provide warnings as it is happening. They are very beneficial to keep third-parties out of the network. Businesses that use Wi-Fi need to consider different forms of protection because these networks are easier for someone to access. They should look into protected access, virtual private networks, or internet protocol security. Another option they have is an intrusion detection system. This system alerts when there are possible intrusions. Some companies set up traps or “hot spots” to attract people and are then able to know when someone is trying to hack into that area.

Encryption

Encryption, which is actually a part of cryptography, involves transforming texts or messages into a code which is unreadable. These messages have to be decrypted in order to be understandable or usable for someone. There is a key that identifies the data to a certain person or company. With public key encryption, there are actually two keys used. One is public and one is private. The public one is used for encryption, and the private for decryption. The level of the actual encryption can be adjusted and should be based on the information. The key can be just a simple slide of letters or a completely random mix-up of letters. This is relatively easy to implement because there is software that a company can purchase. A company needs to be sure that their keys are registered with a certificate authority.

Digital certificates

The point of a digital certificate is to identify the owner of a document. This way the receiver knows that it is an authentic document. Companies can use these certificates in several different ways. They can be used as a replacement for user names and passwords. Each employee can be given these to access the documents that they need from wherever they are. These certificates also use encryption. They are a little more complicated than normal encryption however. They actually used important information within the code. They do this in order to assure authenticity of the documents as well as confidentiality and data integrity which always accompany encryption. Digital certificates are not commonly used because they are confusing for people to implement. There can be complications when using different browsers, which means they need to use multiple certificates. The process is being adjusted so that it is easier to use.

Digital signatures

A final way to secure information online would be to use a digital signature. If a document has a digital signature on it, no one else is able to edit the information without being detected. That way if it is edited, it may be adjusted for reliability after the fact. In order to use a digital signature, one must use a combination of cryptography and a message digest. A message digest is used to give the document a unique value. That value is then encrypted with the sender's private key.

E-Services

The concept of **E-service** (short for electronic service),represents one prominent application of utilizing the use of Information and communication technologies (ICTs) in different areas. However, providing an exact definition of e-service is hard to come by as researchers have been using different definitions to describe e-service. Despite these different definitions, it can be argued that they all agree about the role of technology in facilitating the delivery of services which make them more of electronic services.

It seems compelling to adopt Rowley (2006) approach who defines e-services as: "…deeds, efforts or performances whose delivery is mediated by information technology. Such e-service includes the service element of e-tailing, customer support, and service delivery". This definition reflect three main components- service provider, service receiver and the channels of service delivery (i.e., technology). For example, as concerned to public e-service, public agencies are the service provider and citizens as well as businesses are the service receiver. The channel of service delivery is the third requirement of e-service. Internet is the main channel of e-service delivery while other classic channels (e.g. telephone, call center, public kiosk, mobile phone, television) are also considered.

Origin of the term E-service

Since its conceptual inception in the late 1980s in Europe and formal introduction in 1993 by the US Government, the term 'E-Government' has now become one of the recognized research domains especially in the context of public policy and now has been rapidly gaining strategic importance in public sector modernization. E-service is one of the branches of this domain and its attention has also been creeping up among the practitioners and researchers.

E-service benefits

Lu (2001) identifies a number of benefits for e-services, some of these are:

- Accessing a greater customer base
- Broadening market reach
- Lowering of entry barrier to new markets and cost of acquiring new customers
- Alternative communication channel to customers
- Increasing services to customers
- Enhancing perceived company image
- Gaining competitive advantages
- Potential for increasing customer knowledge

E-service domain

The term 'E-service' has many applications and can be found in many disciplines. The two dominant application areas of e-services are:

E-Business (or E-Commerce): e-services mostly provided by businesses or Non-government Organizations (NGOs) (private sector).

E-government: e-services provided by government to citizens or business (public sector is the supply side). The use and description of the e-service in this page will be limited to the context of e-government only where of the e-service is usually associated with prefix "public": Public e-services. In some cases, we will have to describe aspects that are

related to both fields like some conferences or journals which cover the concept of "e-Service" in both domains of e-government and e-business.

Architecture

Depending on the types of services, there are certain functionalities required in the certain layers of e-service architectural framework, these are but not limited to – Data layer (data sources), processing layers (customer service systems, management systems, data warehouse systems, integrated customer content systems), exchange layer (Enterprise Application Integration– EAI), Interaction layer (integrating e-services), and presentation layer (customer interface through which the web pages and e-services are linked).

E-service Quality

Measuring quality service and service excellence are important in a competitive organizational environment. The SERVQUAL- service quality model is one of the widely used tools for measuring quality of the service on various aspects. The five attributes of this model are: reliability, responsiveness, assurance, tangibles, and empathy. The following table summarizes some major of these:

SERVQUAL	Kaynama & Black (2000)	Zeithaml (2002)	Janda et al. (2002)	Alawattegama & Wattegama (2008)
Reliability	Content	Access	Access	Factual information
Responsiveness	Access	Ease of navigation	Security	Business information
Assurance	Navigation	Efficiency	Sensation	General information
Tangibles	Design	Flexibility	Information/content	Consumer - related information
Empathy	Response	Reliability		
	Background	Personalization		
	Personalization	Security/privacy		
		Responsiveness		
		Assurance/trust		
		Site aesthetics		
		Price knowledge		

The LIRNEasia study on benchmarking national telecom regulator websites focuses on content than on accessibility and ease of use, unlike the other studies mentioned here.

Websites are increasingly important portals to government agencies, especially in the context of information society reforms. Stakeholders, including businesses, investors and even the general public, are interested in information produced by these agencies, and websites can help to increase their transparency and accountability. The quality of its website also demonstrates how advanced a regulatory agency is.

E-service cost factor

Some major cost factors are (Lu, 2001):

- Expense of setting up applications
- Maintaining applications
- Internet connection
- Hardware/software
- Security concerns
- legal issues
- Training; and
- Rapid technology changes

Practical Examples of E-Services in the Developing World

Information Technology is a powerful tool for accelerating economic development. Developing countries have focused on the development of ICT during the last two decades and as a result, it has been recognized that ICT is critical to economy and is as a catalyst of economic development. So, in recent years there seems to have been efforts for providing various e-services in many developing countries since ICT is believed to offer considerable potential for the sustainable development of e-Government and as a result, e-Services.

Many government agencies in developed countries have taken progressive steps toward the web and ICT use, adding coherence to all local activities on the Internet, widening local access and skills, opening up interactive services for local debates, and increasing the participation of citizens on promotion and management of the territory(Graham and Aurigi, 1997).

But the potential for eGovernment in developing countries remains largely unexploited, even though. ICT is believed to offer considerable potential for the sustainable development of eGovernment. Different human, organizational and technological factors, issues and problems pertain in these countries, requiring focused studies and appropriate approaches. ICT, in general, is referred to as an “enabler”, but on the other hand it should also be regarded as a challenge and a peril in itself. The organizations, public or private,which ignore the potential value and use of ICT may suffer pivotal competitive disadvantages. Nevertheless, some eGovernment initiatives have flourished in developing countries too, e.g. Brazil, India, Chile, etc. What the experience in these countries shows, is that governments in the developing world can effectively exploit and appropriate the benefits of ICT, but eGovernment success entails the accommodation of certain unique

conditions,needs and obstacles. The adaptive challenges of eGovernment go far beyond technology, they call for organizational structures and skills, new forms of leadership, transformation of public-private partnerships (Allen et al., 2001).

Following are a few examples regarding e-services in some developing countries:

E-services in Rwanda

Only a decade after emerging from the fastest genocide of the 20th Century, Rwanda, a small country in Eastern Central Africa, has become one of the continent's leaders in, and model on, bridging the digital divide through e-government. Rwanda has undergone a rapid turnaround from one of the most technologically deficient countries only a decade ago to a country where legislative business is conducted online and wireless access to the Internet is available anywhere in the country. This is puzzling when viewed against the limited progress made in other comparable developing countries, especially those located in the same region, sub-Saharan Africa, where the structural and institutional constraints to e-government diffusion are similar.

E-services in South Africa

In the South African post-apartheid era, there continues to be high expectations of government in respect of improved delivery of service and of closer consultation with citizens. Such expectations are not unique to this country, and in this regard there is a need for governments to recognise that the implementation of e-government systems and e-services affords them the opportunity to enhance service delivery and good governance. The implementation of e-Government has been widely acclaimed in that it provides new impetus to deliver services quickly and efficiently (Evans & Yen, 2006:208). In recognition of these benefits, various arms of the South African government have embarked on a number of e-government programmes for example the Batho Pele portal,SARS e-filing, the e-Natis system, electronic processing of grant applications from remote sites, and a large number of departmental information websites. Also a number of well publicised e-government ventures such as the latter, analysts and researchers consider the state of e-government in South Africa to be at rudimentary stages. There are various factors which collectively contribute to such an assessment. Amongst these, key factors relate to a lack of a clear strategy to facilitate uptake and adoption of e-government services as well as evaluation frameworks to assess expectations of citizens who are one of the primary user groups of these services.

E-services in Malaysia

E-Services is one of the pilot projects under the Electronic Government Flagship within the Multimedia Super Corridor (MSC) initiative. With E-Services, one can now conduct transactions with Government agencies, such as the Road Transport Department (RTD) and private utility companies such as Tenaga Nasional Berhad (TNB) and Telekom Malaysia Berhad (TM) through various convenient channels such as the eServices kiosks and internet. No more queuing, traffic jams or bureaucratic hassles and one can now

conduct transaction at one's own convenience. Also, Electronic Labour Exchange (ELX)is one stop-centre for labor market information, as supervised by the Ministry of Human Resource (MOHR), to enable employers and job seekers to communicate on the same platform.

e-Syariah is the seventh project under the Electronic Government flagship application of the Multimedia Super Corridor (MSC). A case management system that integrates the processes related to management of cases for the Syariah Courts.

Challenges to E-services in the Developing World

The future of e-service is bright but some challenges remain. There are some challenges in e-service, as Sheth & Sharma (2007) identify, are:

- Low penetration of ICT especially in the developing countries;
- Fraud on the internet space which is estimated around 2.8billion USD
- Privacy due the emergence of various types of spyware and security holes, and
- intrusive characteristics of the service (e.g. mobile phones based) as customers may not like to be contacted with the service providers at any time and at any place.

The first challenge and primary obstacle to the e-service platform will be penetration of the internet. In some developing countries, the access to the internet is limited and speeds are also limited. In these cases firms and customers will continue to use traditional platforms. The second issue of concern is fraud on the internet. It is anticipated that the fraud on the e-commerce internet space costs $2.8 billion. Possibility of fraud will continue to reduce the utilization of the internet. The third issue is of privacy. Due to both spyware and security holes in operating systems, there is concern that the transactions that consumers undertake have privacy limitations. For example, by stealthily following online activities, firms can develop fairly accurate descriptions of customer profiles. Possibility of privacy violations will reduce the utilizations of the internet. The final issue is that e-service can also become intrusive as they reduce time and location barriers of other forms of contract. For example, firms can contact people through mobile devices at any time and at any place. Customers do not take like the intrusive behavior and may not use the e-service platform. (Heiner and lyer, 2007)

Major E-service Keywords

A considerable amount of research efforts already exists on the subject matter exploring different aspects of e-service and e-service delivery ; one worth noting effort is Rowley's study (2006) who did a review study on the e-service literature. The key finding of his study is that there is need to explore dimensions of e-service delivery not focusing only on service quality "In order to understand e-service experiences it is necessary to go beyond studies of e-service quality dimensions and to also take into account the inherent characteristics of e-service delivery and the factors that differentiate one service experience from another."

Some of the major keywords of e-service as found in the e-government research are as follows:

Acceptance

User acceptance of technology is defined according to Morris (1996, referred by Wu 2005, p. 1) as "the demonstrable willingness within a user group to employ information technology for the tasks it is designed to support". This definition can be brought into the context of e-service where acceptance can be defined as the users' willingness to use e-service or the willingness to decide when and how to use the e-service.

Accessibility

Users' ability to access to the e-service is important theme in the previous literature. For example, Huang (2003) finds that most of the websites in general fail to serve users with disabilities. Recommendation to improve accessibility is evident in previous literature including Jaeger (2006) who suggests the following to improve e-services' accessibility like: design for accessibility from the outset of website development, Involve users with disabilities in the testing of the site …Focus on the benefits of an accessible Web site to all users.

Administrative literacy

According to Grönlund et al. (2007), for a simple e-service, the needs for knowledge and skills, content and procedures are considerably less. However, in complicated services there are needed to change some prevailed skills, such as replacing verbal skills with skill in searching for information online.

Benchmarking

This theme is concerned with establishing standards for measuring e-services or the best practices within the field. This theme also includes the international benchmarking of e-government services (UN reports, EU reports); much critic has been targeting these reports being incomprehensive and useless. According Bannister (2007) "… benchmarks are not a reliable tool for measuring real e-government progress. Furthermore, if they are poorly designed, they risk distorting government policies as countries may chase the benchmark rather than looking at real local and national needs"

Digital divide

Digital divide is considered one of the main barriers to implementing e-services; some people do not have means to access the e-services and some others do not know how to use the technology (or the e-service). According to Helbig et al. (2009), "we suggest E-Government and the digital divide should be seen as complementary social phenomena (i.e., demand and supply). Moreover, a serious e-government digital divide is that services mostly used by social elites."

E-readiness

Most of the reports and the established criteria focus on assessing the services in terms of infrastructure and public policies ignoring the citizen participation or e-readiness. According to by Shalini (2009), “the results of the research project reveal that a high index may be only indicating that a country is e-ready in terms of ICT infrastructure and info-structure, institutions, policies, and political commitment, but it is a very poor measure of the e-readiness of citizens. To summarize the findings, it can be said that Mauritius is ready but the Mauritians are not”

``E-readiness, as the Economist Intelligence Unit defines, is the measure of a country’s ability to leverage digital channels for communication, commerce and government in order to further economic and social development. Implied in this measure is the extent to which the usage of communications devices and Internet services creates efficiencies for business and citizens, and the extent to which this usage is leveraged in the development of information and communications technology (ICT) industries. In general terms, the definition of e-readiness is relative,for instance depending on a country in question's priorities and perspective.

Efficiency

As opposed to effectiveness, efficiency is focused on the internal competence within the government departments when delivering e-services. There is a complaint that researchers focus more on effectiveness “There is an emerging trend seemingly moving away from the efficiency target and focusing on users and governance outcome. While the latter is worthwhile, efficiency must still remain a key priority for eGovernment given the budget constraints compounded in the future by the costs of an ageing population. Moreover, efficiency gains are those that can be most likely proven empirically through robust methodologies”

Security

Security is the most important challenge that faces the implementation of e-services because without a guarantee of privacy and security citizens will not be willing to take up e-government services. These security concerns, such as hacker attacks and the theft of credit card information, make governments hesitant to provide public online services. According to the GAO report of 2002 “security concerns present one of the toughest challenges to extending the reach of e-government.The rash of hacker attacks, Web page defacing, and credit card information being posted on electronic bulletin boards can make many federal agency officials—as well as the general public—reluctant to conduct sensitive government transactions involving personal or financial data over the Internet.” By and Large, Security is one of the major challenges that faces the implementation and development of electronic services. people want to be assured that they are safe when they are conducting online services and that their information will remain secure and confidential

Stakeholders

Axelsson et al. (2009) argue that the stakeholder concept-which was originally used in private firms-, can be used in public setting and in the context of e-government. According to them, several scholars have discussed the use of the stakeholder theory in public settings. The stakeholder theory suggests that need to focus on all the involved stakeholder s when designing the e-service; not only on the government and citizens.

Usability

Compared to Accessibility, There is sufficient literature that addresses the issue of usability; researchers have developed different models and methods to measure the usability and effectiveness of eGovernment websites. However, But still there is call to improve these measures and make it more compressive

``The word usability has cropped up a few times already in this unit. In the context of biometric identification, usability referred to the smoothness of enrollment and other tasks associated with setting up an identification system. A system that produced few false matches during enrollment of applicants was described as usable. Another meaning of usability is related to the ease of use of an interface. Although this meaning of the term is often used in the context of computer interfaces, there is no reason to confine it to computers.´´

Social, Cultural and Ethical Implications of E-services

The perceived effectiveness of e-Service can be influenced by public's view of the social and cultural implications of e-Technologies and e-Service.

Impacts on Individuals' Rights and Privacy – as more and more companies and government agencies use technology to collect, store, and make accessible data on individuals, privacy concerns have grown. Some companies monitor their employees' computer usage patterns in order to assess individual or workgroup performance. Technological advancements are also making it much easier for businesses, government and other individuals to obtain a great deal of information about an individual without their knowledge. There is a growing concern that access to a wide range of information can be dangerous within politically corrupt government agencies.

Impact on Jobs and Workplaces - in the early days of computers, management scientists anticipated that computers would replace human decision-makers. However, despite significant technological advances, this prediction is no longer a mainstream concern. At the current time, one of the concerns associated with computer usage in any organization (including governments) is the health risk – such as injuries related to working continuously on a computer keyboard. Government agencies are expected to work with regulatory groups in order to avoid these problems.

Potential Impacts on Society – despite some economic benefits of ICT to individuals, there is evidence that the computer literacy and access gap between the haves and have-nots may be increasing. Education and information access are more than ever the keys to economic prosperity, yet access by individuals in different countries is not equal - this social inequity has become known as the digital divide.

Impact on Social Interaction – advancements in ICT and e-Technology solutions have enabled many government functions to become automated and information to be made available online. This is a concern to those who place a high value on social interaction.

Information Security - technological advancements allow government agencies to collect, store and make data available online to individuals and organizations. Citizens and businesses expect to be allowed to access data in a flexible manner (at any time and from any location). Meeting these expectations comes at a price to government agencies where it concerns managing information – more specifically, ease of access; data integrity and accuracy; capacity planning to ensure the timely delivery of data to remote (possibly mobile) sites; and managing the security of corporate and public information.

Chapter- 7

E-Marketing

Internet marketing, also referred to as **i-marketing**, **web-marketing**, **online-marketing** or **e-Marketing**, is the marketing of products or services over the Internet.

The Internet has brought media to a global audience. The interactive nature of Internet marketing in terms of providing instant responses and eliciting responses are the unique qualities of the medium. Internet marketing is sometimes considered to be broad in scope because it not only refers to marketing on the Internet, but also includes marketing done via e-mail and wireless media. Management of digital customer data and electronic customer relationship management (ECRM) systems are also often grouped together under internet marketing.

Internet marketing ties together creative and technical aspects of the Internet, including: design, development, advertising, and sales.

Internet marketing also refers to the placement of media along many different stages of the customer engagement cycle through search engine marketing (SEM), search engine optimization (SEO), banner ads on specific websites, e-mail marketing, and Web 2.0 strategies. In 2008, *The New York Times* - working with comScore - published an initial estimate to quantify the user data collected by large Internet-based companies. Counting four types of interactions with company websites in addition to the hits from advertisements served from advertising networks, the authors found the potential for collecting data upward of 2,500 times on average per user per month.

Business models

Internet marketing is associated with several business models:

- E-commerce – In this model, goods are sold directly to consumers (B2C) or businesses (B2B) or consumer to consumer(c2c)
- Lead-based Websites – Strategy where an organization generates value by acquiring sales leads from its website

- Affiliate Marketing – The process in which a product or service developed by one entity (e-commerce business, single person, or a combination) is sold by other active sellers for a share of profits. The entity of the product may provide some marketing material (sales letter, affiliate link, tracking facility), however, the vast majority of affiliate marketing relationships come from e-commerce businesses that offer affiliate programs.
- Local Internet Marketing – Strategy through which a small company utilizes the Internet to find and nurture relationships that are to be used for real-world advantage. Local Internet marketing uses tools such as social media marketing, local directory listing, and targeted online sales promotions.
- Blackhat Marketing – This is a form of Internet marketing that employs deceptive, abusive, or less than truthful methods to drive web traffic to a website or affiliate marketing offer. This method sometimes includes spam, cloaking within search engine result pages, or routing users to pages they didn't initially request.

One-to-one approach

The targeted user is typically browsing the Internet alone therefore the marketing messages can reach them personally. This approach is used in search marketing, where the advertisements are based on search engine keywords entered by the users.

And now with the advent of Web 2.0 tools, many users can interconnect as "peers."

Appeal to specific interests

Internet marketing and geo marketing places an emphasis on marketing that appeals to a specific behavior or interest, rather than reaching out to a broadly defined demographic. "On- and Offline" marketers typically segment their markets according to age group, gender, geography, and other general factors. Marketers have the luxury of targeting by activity and geolocation. For example, a kayak company can post advertisements on kayaking and canoeing websites with the full knowledge that the audience has a related interest.

Internet marketing differs from magazine advertisements, where the goal is to appeal to the projected demographic of the periodical, but rather the advertiser has knowledge of the target audience — people who engage in certain activities (e.g., uploading pictures, contributing to blogs)— so the company does not rely on the expectation that a certain group of people will be interested in its new product or service.

Geo-targeting

Geo targeting (in Internet marketing) and geo marketing are the methods of determining the geolocation (the physical location) of a website visitor with geolocation software, and delivering different content to that visitor based on his or her location, such as country,

region/state, city, metro code/zip code, organization, Internet Protocol (IP) address, ISP or other criteria.

Advantages

Internet marketing is relatively inexpensive when compared to the ratio of cost against the reach of the target audience. Companies can reach a wide audience for a small fraction of traditional advertising budgets. The nature of the medium allows consumers to research and purchase products and services at their own convenience. Therefore, businesses have the advantage of appealing to consumers in a medium that can bring results quickly. The strategy and overall effectiveness of marketing campaigns depend on business goals and cost-volume-profit (CVP) analysis.

Internet marketers also have the advantage of measuring statistics easily and inexpensively. Nearly all aspects of an Internet marketing campaign can be traced, measured, and tested. The advertisers can use a variety of methods: pay per impression, pay per click, pay per play, or pay per action. Therefore, marketers can determine which messages or offerings are more appealing to the audience. The results of campaigns can be measured and tracked immediately because online marketing initiatives usually require users to click on an advertisement, visit a website, and perform a targeted action. Such measurement cannot be achieved through billboard advertising, where an individual will at best be interested, then decide to obtain more information at a later time.

Because exposure, response, and overall efficiency of Internet media are easier to track than traditional off-line media—through the use of web analytics for instance—Internet marketing can offer a greater sense of accountability for advertisers. Marketers and their clients are becoming aware of the need to measure the collaborative effects of marketing (i.e., how the Internet affects in-store sales) rather than siloing each advertising medium. The effects of multichannel marketing can be difficult to determine, but are an important part of ascertaining the value of media campaigns. So finally Internet Marketing refers the online marketing which are related to email and wireless marketing method.

Limitations

From the buyer's perspective, the inability of shoppers to touch, smell, taste or "try on" tangible goods before making an online purchase can be limiting. However, there is an industry standard for e-commerce vendors to reassure customers by having liberal return policies as well as providing in-store pick-up services.

Security concerns

Information security is important both to companies and consumers that participate in online business. Many consumers are hesitant to purchase items over the Internet because they do not trust that their personal information will remain private.

Some companies that purchase customer information offer the option for individuals to have their information removed from the database, also known as opting out. However, many customers are unaware if and when their information is being shared, and are unable to stop the transfer of their information between companies if such activity occurs.

Another major security concern that consumers have with e-commerce merchants is whether or not they will receive exactly what they purchase. Online merchants have attempted to address this concern by investing in and building strong consumer brands (e.g., Amazon.com, eBay, Overstock.com), and by leveraging merchant/feedback rating systems and e-commerce bonding solutions. All of these solutions attempt to assure consumers that their transactions will be free of problems because the merchants can be trusted to provide reliable products and services. Additionally, the major online payment mechanisms (credit cards, PayPal, Google Checkout, etc.) have also provided back-end buyer protection systems to address problems if they actually do occur.

Usage trends

Online advertising techniques have dramatically been affected by technological advancements in the telecommunications industry. Many firms are embracing a paradigm that is shifting the focus of advertising methodology from traditional text and image advertisement creatives to rich multimedia experiences such as those containing more updated technology like HTML, JavaScript, and Adobe Flash. As a result, advertisers can more effectively engage and connect their audience with their campaigns which seek to shape consumer attitudes and feelings towards specific products and services. The paradigm shift from dialup to high speed internet has fueled these changes.

In a national survey between November 30, 2009 and December 27, 2009, the Pew Research Center found that 74% of American adults (ages 18 and older) use the Internet. The same study found that 60% of American adults use broadband connections at home. 55% of American adults connect to the Internet through a wireless network like a public/private access point, a WiMax network, or a cellular 3G/4G network through a mobile cellular device.

Effects on industries

The number of banks offering the ability to perform banking tasks over the internet has also increased. Online banking appeals to customers because it is often faster and considered more convenient than visiting bank branches. Currently over 150 million U.S. adults now bank online, with increasing Internet connection speed being the primary reason for fast growth in the online banking industry. Of those individuals who use the Internet, 44 percent now perform banking activities over the Internet.

Internet auctions have become a multi-billion dollar business. Unique items that could only previously be found at flea markets are now being sold on Internet auction websites such as eBay. Specialized e-stores sell an almost endless amount of items ranging from antiques, movie props, clothing, gadgets and much more. As the premier online reselling

platform, eBay is often used as a price-basis for specialized items. Buyers and sellers often look at prices on the website before going to flea markets; the price shown on eBay often becomes the item's selling price. It is increasingly common for flea market vendors to place a targeted advertisement on the Internet for each item they are selling online, all while running their business out of their homes.

In addition to the major effect internet marketing has had on the technology industry, the effect on the advertising industry itself has been profound. In just a few years, online advertising has grown to be worth tens of billions of dollars annually. PricewaterhouseCoopers reported that US$16.9 billion was spent on Online marketing in the U.S. in 2006.

This has had a growing impact on the electoral process. In 2008 candidates for President heavily utilized Internet marketing strategies to reach constituents. During the 2007 primaries candidates added, on average, over 500 social network supporters per day to help spread their message. President Barack Obama raised over US$1 million in a single day during his extensive Democratic candidacy campaign, largely due to online donors.

There are several industries that have heavily invested in and benefited from internet marketing and online advertising. While some of these were originally brick and mortar businesses such as publishing, music, automotive or gambling, others have sprung up as purely online businesses, such as digital design and media, blogging or internet service hosting.

Search Engine marketing

Search engine marketing, or **SEM**, is a form of Internet marketing that seeks to promote websites by increasing their visibility in search engine result pages (SERPs) through the use of search engine optimization, paid placement, contextual advertising, and paid inclusion.

Market structure

In 2008, North American advertisers spent US$13.5 billion on search engine marketing. The largest SEM vendors are Google AdWords, Yahoo! Search Marketing and Microsoft adCenter. As of 2006, SEM was growing much faster than traditional advertising and even other channels of online marketing. Because of the complex technology, a secondary "search marketing agency" market has evolved. Some marketers have difficulty understanding the intricacies of search engine marketing and choose to rely on third party agencies to manage their search marketing.

History

As the number of sites on the Web increased in the mid-to-late 90s, search engines started appearing to help people find information quickly. Search engines developed business models to finance their services, such as pay per click programs offered by Open Text in 1996 and then Goto.com in 1998. Goto.com later changed its name to Overture in 2001, and was purchased by Yahoo! in 2003, and now offers paid search opportunities for advertisers through Yahoo! Search Marketing. Google also began to offer advertisements on search results pages in 2000 through the Google AdWords program. By 2007, pay-per-click programs proved to be primary money-makers for search engines. In a market dominated by Google, in 2009 Yahoo! and Microsoft announced the intention to forge an alliance. The Yahoo! & Microsoft Search Alliance eventually received approval from regulators in the US and Europe in February 2010.

Search engine optimization consultants expanded their offerings to help businesses learn about and use the advertising opportunities offered by search engines, and new agencies focusing primarily upon marketing and advertising through search engines emerged. The term "Search Engine Marketing" was proposed by Danny Sullivan in 2001 to cover the spectrum of activities involved in performing SEO, managing paid listings at the search engines, submitting sites to directories, and developing online marketing strategies for businesses, organizations, and individuals.

Some of the latest theoretical advances include Search Engine Marketing Management (SEMM). SEMM relates to activities including SEO but focuses on return on investment (ROI) management instead of relevant traffic building (as is the case of mainstream SEO). SEMM also integrates organic SEO, trying to achieve top ranking without using paid means of achieving top in search engines, and PayPerClick SEO. For example some of the attention is placed on the web page layout design and how content and information is displayed to the website visitor.

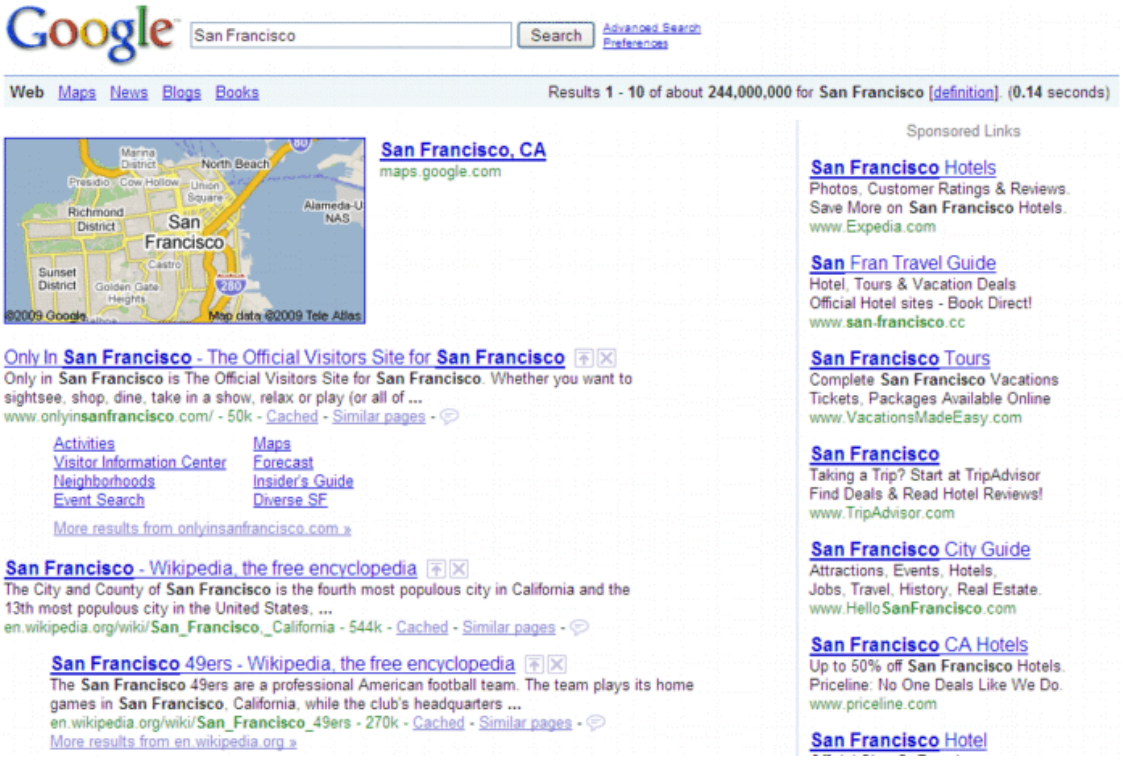
Ethical questions

Paid search advertising has not been without controversy, and the issue of how search engines present advertising on their search result pages has been the target of a series of studies and reports by Consumer Reports WebWatch. The Federal Trade Commission (FTC) also issued a letter in 2002 about the importance of disclosure of paid advertising on search engines, in response to a complaint from Commercial Alert, a consumer advocacy group with ties to Ralph Nader.

Vested interests appear to use the expression *SEM* to mean exclusively *Pay per click advertising* to the extent that the wider advertising and marketing community have accepted this narrow definition. Such usage excludes the wider search marketing community that is engaged in other forms of SEM such as Search Engine Optimization and Search Retargeting.

Another ethical controversy associated with search marketing has been the issue of trademark infringement. The debate as to whether third parties should have the right to bid on their competitors' brand names has been underway for years. In 2009 Google changed their policy, which formerly prohibited these tactics, allowing 3rd parties to bid on branded terms as long as their landing page in fact provides information on the trademarked term. Though the policy has been changed this continues to be a source of heated debate.

Search engine optimization



A typical search engine results page

Search engine optimization (**SEO**) is the process of improving the visibility of a website or a web page in search engines via the "natural" or un-paid ("organic" or "algorithmic") search results. Other forms of search engine marketing (SEM) target paid listings. In general, the earlier (or higher on the page), and more frequently a site appears in the search results list, the more visitors it will receive from the search engine. SEO may target different kinds of search, including image search, local search, video search and industry-specific vertical search engines. This gives a website web presence.

As an Internet marketing strategy, SEO considers how search engines work and what people search for. Optimizing a website may involve editing its content and HTML and associated coding to both increase its relevance to specific keywords and to remove barriers to the indexing activities of search engines. Promoting a site to increase the number of backlinks, or inbound links, is another SEO tactic.

The acronym "SEO" can refer to "search engine optimizers," a term adopted by an industry of consultants who carry out optimization projects on behalf of clients, and by employees who perform SEO services in-house. Search engine optimizers may offer SEO as a stand-alone service or as a part of a broader marketing campaign. Because effective SEO may require changes to the HTML source code of a site and site content, SEO tactics may be incorporated into website development and design. The term "search engine friendly" may be used to describe website designs, menus, content management systems, images, videos, shopping carts, and other elements that have been optimized for the purpose of search engine exposure.

Another class of techniques, known as black hat SEO or spamdexing, uses methods such as link farms, keyword stuffing and article spinning that degrade both the relevance of search results and the user-experience of search engines. Search engines look for sites that employ these techniques in order to remove them from their indices.

History

Webmasters and content providers began optimizing sites for search engines in the mid-1990s, as the first search engines were cataloging the early Web. Initially, all webmasters needed to do was submit the address of a page, or URL, to the various engines which would send a "spider" to "crawl" that page, extract links to other pages from it, and return information found on the page to be indexed. The process involves a search engine spider downloading a page and storing it on the search engine's own server, where a second program, known as an indexer, extracts various information about the page, such as the words it contains and where these are located, as well as any weight for specific words, and all links the page contains, which are then placed into a scheduler for crawling at a later date.

Site owners started to recognize the value of having their sites highly ranked and visible in search engine results, creating an opportunity for both white hat and black hat SEO practitioners. According to industry analyst Danny Sullivan, the phrase "search engine optimization" probably came into use in 1997. The first documented use of the term Search Engine Optimization was John Audette and his company Multimedia Marketing Group as documented by a web page from the MMG site from February, 1997 on the Internet Way Back machine.

Early versions of search algorithms relied on webmaster-provided information such as the keyword meta tag, or index files in engines like ALIWEB. Meta tags provide a guide to each page's content. Using meta data to index pages was found to be less than reliable, however, because the webmaster's choice of keywords in the meta tag could potentially

be an inaccurate representation of the site's actual content. Inaccurate, incomplete, and inconsistent data in meta tags could and did cause pages to rank for irrelevant searches. Web content providers also manipulated a number of attributes within the HTML source of a page in an attempt to rank well in search engines.

By relying so much on factors such as keyword density which were exclusively within a webmaster's control, early search engines suffered from abuse and ranking manipulation. To provide better results to their users, search engines had to adapt to ensure their results pages showed the most relevant search results, rather than unrelated pages stuffed with numerous keywords by unscrupulous webmasters. Since the success and popularity of a search engine is determined by its ability to produce the most relevant results to any given search, allowing those results to be false would turn users to find other search sources. Search engines responded by developing more complex ranking algorithms, taking into account additional factors that were more difficult for webmasters to manipulate.

Graduate students at Stanford University, Larry Page and Sergey Brin, developed "backrub," a search engine that relied on a mathematical algorithm to rate the prominence of web pages. The number calculated by the algorithm, PageRank, is a function of the quantity and strength of inbound links. PageRank estimates the likelihood that a given page will be reached by a web user who randomly surfs the web, and follows links from one page to another. In effect, this means that some links are stronger than others, as a higher PageRank page is more likely to be reached by the random surfer.

Page and Brin founded Google in 1998. Google attracted a loyal following among the growing number of Internet users, who liked its simple design. Off-page factors (such as PageRank and hyperlink analysis) were considered as well as on-page factors (such as keyword frequency, meta tags, headings, links and site structure) to enable Google to avoid the kind of manipulation seen in search engines that only considered on-page factors for their rankings. Although PageRank was more difficult to game, webmasters had already developed link building tools and schemes to influence the Inktomi search engine, and these methods proved similarly applicable to gaming PageRank. Many sites focused on exchanging, buying, and selling links, often on a massive scale. Some of these schemes, or link farms, involved the creation of thousands of sites for the sole purpose of link spamming.

By 2004, search engines had incorporated a wide range of undisclosed factors in their ranking algorithms to reduce the impact of link manipulation. Google says it ranks sites using more than 200 different signals. The leading search engines, Google and Yahoo, do not disclose the algorithms they use to rank pages. Notable SEO service providers, such as Rand Fishkin, Barry Schwartz, Aaron Wall and Jill Whalen, have studied different approaches to search engine optimization, and have published their opinions in online forums and blogs. SEO practitioners may also study patents held by various search engines to gain insight into the algorithms.

In 2005 Google began personalizing search results for each user. Depending on their history of previous searches, Google crafted results for logged in users. In 2008, Bruce Clay said that "ranking is dead" because of personalized search. It would become meaningless to discuss how a website ranked, because its rank would potentially be different for each user and each search.

In 2007 Google announced a campaign against paid links that transfer PageRank. On June 15, 2009, Google disclosed that they had taken measures to mitigate the effects of PageRank sculpting by use of the nofollow attribute on links. Matt Cutts, a well-known software engineer at Google, announced that Google Bot would no longer treat nofollowed links in the same way, in order to prevent SEO service providers from using nofollow for PageRank sculpting. As a result of this change the usage of nofollow leads to evaporation of pagerank. In order to avoid the above, SEO engineers developed alternative techniques that replace nofollowed tags with obfuscated Javascript and thus permit PageRank sculpting. Additionally several solutions have been suggested that include the usage of iframes, Flash and Javascript.

In December 2009 Google announced it would be using the web search history of all its users in order to populate search results.

Real-time-search was introduced in late 2009 in an attempt to make search results more timely and relevant. Historically site administrators have spent months or even years optimizing a website to increase search rankings. With the growth in popularity of social media sites and blogs the leading engines made changes to their algorithms to allow fresh content to rank quickly within the search results. This new approach to search places importance on current, fresh and unique content.

Relationship with search engines

By 1997 search engines recognized that webmasters were making efforts to rank well in their search engines, and that some webmasters were even manipulating their rankings in search results by stuffing pages with excessive or irrelevant keywords. Early search engines, such as Infoseek, adjusted their algorithms in an effort to prevent webmasters from manipulating rankings.

Due to the high marketing value of targeted search results, there is potential for an adversarial relationship between search engines and SEO service providers. In 2005, an annual conference, AIRWeb, Adversarial Information Retrieval on the Web, was created to discuss and minimize the damaging effects of aggressive web content providers.

Companies that employ overly aggressive techniques can get their client websites banned from the search results. In 2005, the Wall Street Journal reported on a company, Traffic Power, which allegedly used high-risk techniques and failed to disclose those risks to its clients. Wired magazine reported that the same company sued blogger and SEO Aaron Wall for writing about the ban. Google's Matt Cutts later confirmed that Google did in fact ban Traffic Power and some of its clients.

Some search engines have also reached out to the SEO industry, and are frequent sponsors and guests at SEO conferences, chats, and seminars. In fact, with the advent of paid inclusion, some search engines now have a vested interest in the health of the optimization community. Major search engines provide information and guidelines to help with site optimization. Google has a Sitemaps program to help webmasters learn if Google is having any problems indexing their website and also provides data on Google traffic to the website. Google guidelines are a list of suggested practices Google has provided as guidance to webmasters. Yahoo! Site Explorer provides a way for webmasters to submit URLs, determine how many pages are in the Yahoo! index and view link information. Bing Toolbox provides a way from webmasters to submit a sitemap and web feeds, allowing users to determine the crawl rate, and how many pages have been indexed by their search engine.

Methods

Getting indexed

The leading search engines, such as Google and Yahoo!, use crawlers to find pages for their algorithmic search results. Pages that are linked from other search engine indexed pages do not need to be submitted because they are found automatically. Some search engines, notably Yahoo!, operate a paid submission service that guarantee crawling for either a set fee or cost per click. Such programs usually guarantee inclusion in the database, but do not guarantee specific ranking within the search results. Two major directories, the Yahoo Directory and the Open Directory Project both require manual submission and human editorial review. Google offers Google Webmaster Tools, for which an XML Sitemap feed can be created and submitted for free to ensure that all pages are found, especially pages that aren't discoverable by automatically following links.

Search engine crawlers may look at a number of different factors when crawling a site. Not every page is indexed by the search engines. Distance of pages from the root directory of a site may also be a factor in whether or not pages get crawled.

Preventing crawling

To avoid undesirable content in the search indexes, webmasters can instruct spiders not to crawl certain files or directories through the standard robots.txt file in the root directory of the domain. Additionally, a page can be explicitly excluded from a search engine's database by using a meta tag specific to robots. When a search engine visits a site, the robots.txt located in the root directory is the first file crawled. The robots.txt file is then parsed, and will instruct the robot as to which pages are not to be crawled. As a search engine crawler may keep a cached copy of this file, it may on occasion crawl pages a webmaster does not wish crawled. Pages typically prevented from being crawled include login specific pages such as shopping carts and user-specific content such as search results from internal searches. In March 2007, Google warned webmasters that they

should prevent indexing of internal search results because those pages are considered search spam.

Increasing prominence

A variety of methods can increase the prominence of a webpage within the search results. Cross linking between pages of the same website to provide more links to most important pages may improve its visibility. Writing content that includes frequently searched keyword phrase, so as to be relevant to a wide variety of search queries will tend to increase traffic. Updating content so as to keep search engines crawling back frequently and give additional weight to your site. Adding relevant keywords to a web page's meta data, including the title tag and meta description, will tend to improve the relevancy of a site's search listings, thus increasing traffic. URL normalization of web pages accessible via multiple urls, using the "canonical" meta tag or via 301 redirects can help make sure links to different versions of the url all count towards the page's link popularity score.

File names

Search engines' algorithms prefer descriptive, relevant file names on web pages. For a search engine to interpret a page properly, keywords are more helpful than random characters and numbers. Each page should be optimized for a certain keyword or keyword phrases which should also appear in H1 tag but also in the page file name. Since no spaces are accepted in the file name, hyphens and underscores are preferred.

Google SEO

Google holds over 60% of the total search market. Its algorithm is naturally also unique, so ranking on Google carries its own unique considerations. Although there are over 200 criteria Google uses to rank sites, they can be categorized into two main sections: *on-site* and *off-site* factors:

Google values sites that deliver quality content, relevance, easy navigation and load and an overall user-friendliness to the site's visitors (on-site). However, a site's popularity is heavily weighted when Google ranks sites (off-site). Thus Google was originally designed to rank sites mostly based on the number of inbound links they were receiving from other sites. In other words, the more site A was used as a "reference" the higher it would rank. Anchored text links used to link to site A are also very important as well as the popularity and the relevance of the site that is referencing site A.

White hat versus black hat

SEO techniques are classified by some into two broad categories: techniques that search engines recommend as part of good design, and those techniques that search engines do not approve of and attempt to minimize the effect of, referred to as spamdexing. Some industry commentators classify these methods, and the practitioners who employ them, as either white hat SEO, or black hat SEO. White hats tend to produce results that last a long

time, whereas black hats anticipate that their sites will eventually be banned once the search engines discover what they are doing.

A SEO tactic, technique or method is considered white hat if it conforms to the search engines' guidelines and involves no deception. As the search engine guidelines are not written as a series of rules or commandments, this is an important distinction to note. White hat SEO is not just about following guidelines, but is about ensuring that the content a search engine indexes and subsequently ranks is the same content a user will see.

White hat advice is generally summed up as creating content for users, not for search engines, and then making that content easily accessible to the spiders, rather than attempting to game the algorithm. White hat SEO is in many ways similar to web development that promotes accessibility, although the two are not identical.

White Hat SEO is merely effective marketing, making efforts to deliver quality content to an audience that has requested the quality content. Traditional marketing means have allowed this through transparency and exposure. A search engine's algorithm takes this into account, such as Google's PageRank.

Black hat SEO attempts to improve rankings in ways that are disapproved of by the search engines, or involve deception. One black hat technique uses text that is hidden, either as text colored similar to the background, in an invisible div, or positioned off screen. Another method gives a different page depending on whether the page is being requested by a human visitor or a search engine, a technique known as cloaking.

Search engines may penalize sites they discover using black hat methods, either by reducing their rankings or eliminating their listings from their databases altogether. Such penalties can be applied either automatically by the search engines' algorithms, or by a manual site review. One infamous example was the February 2006 Google removal of both BMW Germany and Ricoh Germany for use of deceptive practices. Both companies, however, quickly apologized, fixed the offending pages, and were restored to Google's list.

As a marketing strategy

SEO is not necessarily an appropriate strategy for every website, and other Internet marketing strategies can be much more effective, depending on the site operator's goals. A successful Internet marketing campaign may drive organic traffic, achieved through optimization techniques and not paid advertising, to web pages, but it also may involve the use of paid advertising on search engines and other pages, building high quality web pages to engage and persuade, addressing technical issues that may keep search engines from crawling and indexing those sites, setting up analytics programs to enable site owners to measure their successes, and improving a site's conversion rate.

SEO may generate a return on investment. However, search engines are not paid for organic search traffic, their algorithms change, and there are no guarantees of continued referrals. (Some trading sites such as eBay can be a special case for this; it will announce how and when the ranking algorithm will change a few months before changing the algorithm). Due to this lack of guarantees and certainty, a business that relies heavily on search engine traffic can suffer major losses if the search engines stop sending visitors. It is considered wise business practice for website operators to liberate themselves from dependence on search engine traffic. A top-ranked SEO blog Seomoz.org has suggested, "Search marketers, in a twist of irony, receive a very small share of their traffic from search engines." Instead, their main sources of traffic are links from other websites.

International markets

Optimization techniques are highly tuned to the dominant search engines in the target market. The search engines' market shares vary from market to market, as does competition. In 2003, Danny Sullivan stated that Google represented about 75% of all searches. In markets outside the United States, Google's share is often larger, and Google remains the dominant search engine worldwide as of 2007. As of 2006, Google had an 85-90% market share in Germany. While there were hundreds of SEO firms in the US at that time, there were only about five in Germany. As of June 2008, the marketshare of Google in the UK was close to 90% according to Hitwise. That market share is achieved in a number of countries.

As of 2009, there are only a few large markets where Google is not the leading search engine. In most cases, when Google is not leading in a given market, it is lagging behind a local player. The most notable markets where this is the case are China, Japan, South Korea, Russia and the Czech Republic where respectively Baidu, Yahoo! Japan, Naver, Yandex and Seznam are market leaders.

Successful search optimization for international markets may require professional translation of web pages, registration of a domain name with a top level domain in the target market, and web hosting that provides a local IP address. Otherwise, the fundamental elements of search optimization are essentially the same, regardless of language.

Legal precedents

On October 17, 2002, SearchKing filed suit in the United States District Court, Western District of Oklahoma, against the search engine Google. SearchKing's claim was that Google's tactics to prevent spamdexing constituted a tortious interference with contractual relations. On May 27, 2003, the court granted Google's motion to dismiss the complaint because SearchKing "failed to state a claim upon which relief may be granted."

In March 2006, KinderStart filed a lawsuit against Google over search engine rankings. Kinderstart's website was removed from Google's index prior to the lawsuit and the amount of traffic to the site dropped by 70%. On March 16, 2007 the United States

District Court for the Northern District of California (San Jose Division) dismissed KinderStart's complaint without leave to amend, and partially granted Google's motion for Rule 11 sanctions against KinderStart's attorney, requiring him to pay part of Google's legal expenses.

Chapter- 8

Electronic Commerce

Electronic commerce, commonly known as **e-commerce** or **eCommerce**, consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. The amount of trade conducted electronically has grown extraordinarily with widespread Internet usage. The use of commerce is conducted in this way, spurring and drawing on innovations in electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web at least at some point in the transaction's lifecycle, although it can encompass a wider range of technologies such as e-mail as well.

A large percentage of electronic commerce is conducted entirely electronically for virtual items such as access to premium content on a website, but most electronic commerce involves the transportation of physical items in some way. Online retailers are sometimes known as e-tailers and online retail is sometimes known as **e-tail**. Almost all big retailers have electronic commerce presence on the World Wide Web.

Electronic commerce that is conducted between businesses is referred to as business-to-business or B2B. B2B can be open to all interested parties (e.g. commodity exchange) or limited to specific, pre-qualified participants (private electronic market). Electronic commerce that is conducted between businesses and consumers, on the other hand, is referred to as business-to-consumer or B2C. This is the type of electronic commerce conducted by companies such as Amazon.com. Online shopping is a form of electronic commerce where the buyer is directly online to the seller's computer usually via the internet. There is no intermediary service. The sale and purchase transaction is completed electronically and interactively in real-time such as Amazon.com for new books. If an intermediary is present, then the sale and purchase transaction is called electronic commerce such as eBay.com.

Electronic commerce is generally considered to be the sales aspect of e-business. It also consists of the exchange of data to facilitate the financing and payment aspects of the business transactions.

History

Early development

Originally, electronic commerce meant the facilitation of commercial transactions electronically, using technology such as Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT). These were both introduced in the late 1970s, allowing businesses to send commercial documents like purchase orders or invoices electronically. The growth and acceptance of credit cards, automated teller machines (ATM) and telephone banking in the 1980s were also forms of electronic commerce. Another form of e-commerce was the airline reservation system typified by Sabre in the USA and Travicom in the UK.

From the 1990s onwards, electronic commerce would additionally include enterprise resource planning systems (ERP), data mining and data warehousing.

In 1990, Tim Berners-Lee invented the WorldWideWeb web browser and transformed an academic telecommunication network into a worldwide everyman everyday communication system called internet/www. Commercial enterprise on the Internet was strictly prohibited until 1991. Although the Internet became popular worldwide around 1994 when the first internet online shopping started, it took about five years to introduce security protocols and DSL allowing continual connection to the Internet. By the end of 2000, many European and American business companies offered their services through the World Wide Web. Since then people began to associate a word "ecommerce" with the ability of purchasing various goods through the Internet using secure protocols and electronic payment services.

Timeline

- 1979: Michael Aldrich invented online shopping
- 1981: Thomson Holidays, UK is first B2B online shopping
- 1982: Minitel was introduced nationwide in France by France Telecom and used for online ordering.
- 1984: Gateshead SIS/Tesco is first B2C online shopping and Mrs Snowball, 72, is the first online home shopper
- 1985: Nissan UK sells cars and finance with credit checking to customers online from dealers' lots.
- 1987: Swreg begins to provide software and shareware authors means to sell their products online through an electronic Merchant account.
- 1990: Tim Berners-Lee writes the first web browser, WorldWideWeb, using a NeXT computer.
- 1994: Netscape releases the Navigator browser in October under the code name Mozilla. Pizza Hut offers online ordering on its Web page. The first online bank opens. Attempts to offer flower delivery and magazine subscriptions online. Adult materials also become commercially available, as do cars and bikes. Netscape 1.0 is introduced in late 1994 SSL encryption that made transactions secure.

- 1995: Jeff Bezos launches Amazon.com and the first commercial-free 24 hour, internet-only radio stations, Radio HK and NetRadio start broadcasting. Dell and Cisco begin to aggressively use Internet for commercial transactions. eBay is founded by computer programmer Pierre Omidyar as AuctionWeb.
- 1998: Electronic postal stamps can be purchased and downloaded for printing from the Web.
- 1999: Business.com sold for US $7.5 million to eCompanies, which was purchased in 1997 for US $149,000. The peer-to-peer filesharing software Napster launches. ATG Stores launches to sell decorative items for the home online.
- 2000: The dot-com bust.
- 2002: eBay acquires PayPal for $1.5 billion. Niche retail companies CSN Stores and NetShops are founded with the concept of selling products through several targeted domains, rather than a central portal.
- 2003: Amazon.com posts first yearly profit.
- 2007: Business.com acquired by R.H. Donnelley for $345 million.
- 2009: Zappos.com acquired by Amazon.com for $928 million. Retail Convergence, operator of private sale website RueLaLa.com, acquired by GSI Commerce for $180 million, plus up to $170 million in earn-out payments based on performance through 2012.
- 2010: US eCommerce and Online Retail sales projected to reach $173 billion, an increase of 7 percent over 2009.

Business applications

Some common applications related to electronic commerce are the following:

- Email
- Enterprise content management
- Instant messaging
- Newsgroups
- Online shopping and order tracking
- Online banking
- Online office suites
- Domestic and international payment systems
- Shopping cart software
- Teleconferencing
- Electronic tickets

Government regulations

In the United States, some electronic commerce activities are regulated by the Federal Trade Commission (FTC). These activities include the use of commercial e-mails, online advertising and consumer privacy. The CAN-SPAM Act of 2003 establishes national standards for direct marketing over e-mail. The Federal Trade Commission Act regulates all forms of advertising, including online advertising, and states that advertising must be

truthful and non-deceptive. Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the FTC has brought a number of cases to enforce the promises in corporate privacy statements, including promises about the security of consumers' personal information. As result, any corporate privacy policy related to e-commerce activity may be subject to enforcement by the FTC.

The Ryan Haight Online Pharmacy Consumer Protection Act of 2008, which came into law in 2008, amends the Controlled Substances Act to address online pharmacies.

Forms

Contemporary electronic commerce involves everything from ordering "digital" content for immediate online consumption, to ordering conventional goods and services, to "meta" services to facilitate other types of electronic commerce.

On the consumer level, electronic commerce is mostly conducted on the World Wide Web. An individual can go online to purchase anything from books or groceries, to expensive items like real estate. Another example would be online banking, i.e. online bill payments, buying stocks, transferring funds from one account to another, and initiating wire payment to another country. All of these activities can be done with a few strokes of the keyboard.

On the institutional level, big corporations and financial institutions use the internet to exchange financial data to facilitate domestic and international business. Data integrity and security are very hot and pressing issues for electronic commerce today.

Impact on markets and retailers

Economists have theorised that e-commerce ought to lead to intensified price competition, as it increases consumers' ability to gather information about products and prices. Research by four economists at the University of Chicago has found that the growth of online shopping has also affected industry structure in two areas that have seen significant growth in e-commerce, bookshops and travel agencies. Generally, larger firms have grown at the expense of smaller ones, as they are able to use economies of scale and offer lower prices. The lone exception to this pattern has been the very smallest category of bookseller, shops with between one and four employees, which appear to have withstood the trend.

Electronic Funds Transfer

Electronic funds transfer or **EFT** is the electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions, through computer-based systems.

The term is used for a number of different concepts:

- Cardholder-initiated transactions, where a cardholder makes use of a payment card
- Direct deposit payroll payments for a business to its employees, possibly via a payroll service bureau
- Direct debit payments, sometimes called ***electronic checks***, for which a business debits the consumer's bank accounts for payment for goods or services
- Electronic bill payment in online banking, which may be delivered by EFT or paper check
- Transactions involving stored value of electronic money, possibly in a private currency
- Wire transfer via an international banking network (generally carries a higher fee)
- Electronic Benefit Transfer

In 1978 U.S. Congress passed the Electronic Funds Transfer Act to establish the rights and liabilities of consumers as well as the responsibilities of all participants in EFT activities in the United States.

PayPal

PayPal is an e-commerce business allowing payments and money transfers to be made through the Internet. Online money transfers serve as electronic alternatives to traditional paper methods such as checks and money orders.

A PayPal account can be funded with an electronic debit from a bank account or by a credit card. The recipient of a PayPal transfer can either request a check from PayPal, establish their own PayPal deposit account or request a transfer to their bank account.

PayPal performs payment processing for online vendors, auction sites, and other commercial users, for which it charges a fee. It may also charge a fee for receiving money, proportional to the amount received. The fees depend on the currency used, the payment option used, the country of the sender, the country of the recipient, the amount sent and the recipient's account type. In addition, eBay purchases made by credit card through PayPal may incur extra fees if the buyer and seller use different currencies.

On October 3, 2002, PayPal became a wholly-owned subsidiary of eBay. Its corporate headquarters are in San Jose, California, United States at eBay's North First Street satellite office campus. The company also has significant operations in Omaha, Nebraska; Scottsdale, Arizona; and Austin, Texas in the U.S., Chennai, Dublin, Berlin and Tel-Aviv. As of July 2007, across Europe, PayPal also operates as a Luxembourg-based bank.

On March 17, 2010, PayPal entered into an agreement with China UnionPay (CUP), China's bankcard association, to allow Chinese consumers to use PayPal to shop online. PayPal is planning to expand its workforce in Asia to 2,000 by the end of the year 2010.

History

Beginnings

The current incarnation of PayPal is the result of a March 2000 merger between Confinity and X.com. Confinity was founded in December 1998 by Max Levchin, Peter Thiel, Luke Nosek, and Ken Howery, initially as a Palm Pilot payments and cryptography company. X.com was founded by Elon Musk in March 1999, initially as an Internet financial services company. Both Confinity and X.com launched their websites in late 1999. Both companies were located on University Avenue in Palo Alto. Confinity's website was initially focused on reconciling beamed payments from Palm Pilots with email payments as a feature and X.com's website initially featured financial services with email payments as a feature.

At Confinity, many of the initial recruits were alumni of *The Stanford Review*, also founded by Peter Thiel, and most early engineers hailed from the University of Illinois at Urbana-Champaign, recruited by Max Levchin. On the X.com side, Elon Musk recruited a wide range of technical and business personnel, including many that were critical to the combined company's success, such as Amy Klement, Sal Giambanco, Roelof Botha of Sequoia Capital, Sanjay Bhargava and Jeremy Stoppelman.

To block potentially fraudulent access by automated systems, PayPal used a system of making the user enter numbers from a blurry picture, which they coined the Gausebeck-Levchin test.

eBay watched the rise in volume of its online payments and realized the fit of an online payment system with online auctions. eBay purchased Billpoint in May 1999, prior to the existence of PayPal. eBay made Billpoint its official payment system, dubbing it "eBay Payments," but cut the functionality of Billpoint by narrowing it to only payments made for eBay auctions. For this reason, PayPal was listed in many more auctions than Billpoint. In February 2000, the PayPal service had an average of approximately 200,000 daily auctions while Billpoint (in beta) had only 4,000 auctions. By April 2000, more than 1,000,000 auctions promoted the PayPal service. PayPal was able to turn the corner and become the first dot-com to IPO after the September 11 attacks.

Acquisition by eBay

In October 2002, PayPal was acquired by eBay for $1.5 billion. PayPal had previously been the payment method of choice by more than fifty percent of eBay users, and the service competed with eBay's subsidiary Billpoint, Citibank's c2it, whose service was closed in late 2003, and Yahoo!'s PayDirect, whose service was closed in late 2004. Western Union announced the December 2005 shut down of their BidPay service but

subsequently sold it in 2006 to CyberSource Corporation. BidPay subsequently ceased operations on December 31, 2007. Some competitors which offer some of PayPal's services, such as Google Checkout, Wirecard, Moneybookers, The InstantPay (launching Jan 2011), 2Checkout.com, CCNow and Kagi, remain in business, despite the fact that eBay now requires everyone on its Australian and United Kingdom sites to offer PayPal. Eventually eBay moderated its position, and mandated that sellers on eBay Australia offer PayPal as one of the (but not necessarily the only) payment methods. These accepted payment methods include bank deposit, cheques and money orders, escrow, and credit cards (processed by other than PayPal).

In January 2008, PayPal agreed to acquire Fraud Sciences, a privately-held Israeli start-up company with expertise in online risk tools, for $169 million, in order to enhance eBay and PayPal's proprietary fraud management systems and accelerate the development of improved fraud detection tools. In November 2008, the company acquired Bill Me Later, an online payments company offering transactional credit at over 1000 online merchants in the US.

PayPal's total payment volume, the total value of transactions, was US$ 60 billion in 2008, an increase of 27 percent over the previous year, and US$ 71 billion in 2009, an increase of 19 percent over the previous year. The company continues to focus on international growth and growth of its Merchant Services division, providing e-payments for retailers off eBay.

Business today

Currently, PayPal operates in 190 markets, and it manages more than 228 million accounts, more than 73 million of them active. PayPal allows customers to send, receive, and hold funds in 19 currencies worldwide. These currencies are the Australian dollar, Brazilian real, Canadian dollar, Chinese renminbi yuan (only available for some Chinese accounts, see below), Euro, pound sterling, Japanese yen, Czech koruna, Danish krone, Hong Kong dollar, Hungarian forint, Indian rupee, Israeli new sheqel, Mexican peso, New Zealand dollar, Norwegian krone, Polish zloty, Singapore dollar, Swedish krona, Swiss franc and U.S. dollar. PayPal operates locally in 13 countries.

Residents in 194 markets can use PayPal in their local markets to send money online.

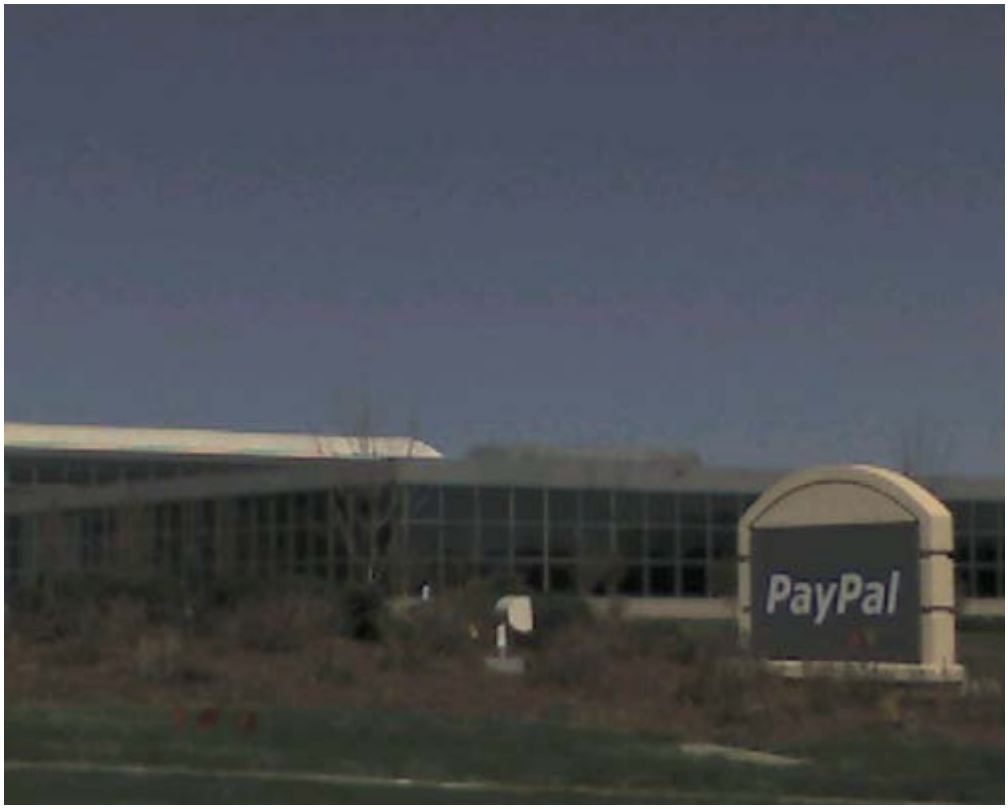
PayPal revenues for Q1 2009 were $643 million, up 11 percent year over year. 42 percent of revenues in q1 2009 were from international markets. PayPal's Total Payment Volume (TPV), the total value of transactions in Q1 2009 was nearly $16 billion, up 10 percent year over year.

In 2008, PayPal's TPV off eBay exceeded volume on eBay for the first time. PayPal's Total Payment Volume in 2008 was $60 billion representing nearly 9 percent of global e-commerce and 15 percent of US e-commerce.

At an analyst day on March 11, 2009, eBay CEO, John Donahoe announced that PayPal could be a larger driver of revenue than the eBay marketplaces business. RIM announced that PayPal will be the only payment mechanism for its Blackberry App World, which launched on April 1, 2009.

PayPal launched Student Accounts for teens in August 2009 allowing parents to set up a student account, transfer money into it, and obtain a debit card for student use. The program provides tools to teach teens how to spend money wisely and take responsibility for their actions.

In November 2009 PayPal opened its platform, allowing other services to get access to its code and to use its infrastructure in order to enable peer-to-peer online transactions.



PayPal Operations Center and main office outside Omaha, NE

Although PayPal's corporate headquarters are located in San Jose, PayPal's operations center is located near Omaha, Nebraska, where the company employs more than 2,000 people as of 2007. PayPal's European headquarters are in Luxembourg and international headquarters in Singapore. The company also recently opened a technology center in Scottsdale, Arizona, and Chennai, India.

PayPal business model evolution

PayPal's success in terms of users and volumes was the product of a three-phase strategy described by eBay CEO Meg Whitman: "*First, PayPal focused on expanding its service among eBay users in the U.S. Second, we began expanding PayPal to eBay's international sites. And third, we started to build PayPal's business off eBay*".

Phase-1

In the first phase, payments volumes were coming mostly from eBay auction web-site. The system was very attractive to auction sellers, most of which were individuals or small businesses that were unable to accept credit card, and for consumers as well. In fact, many sellers could not qualify for a credit card "merchant account" because they lacked a commercial credit history. By the way, fixed fees associated with a merchant account were and are still onerous, given small scale of monthly volumes. The service also appealed to auction buyers because they could fund PayPal accounts using credit cards or bank account balances, without divulging credit card numbers to unknown sellers. PayPal employed an aggressive marketing campaign to accelerate its growth, depositing $10 in new users' PayPal accounts (+$10 for each new user they referred).

Phase-2

The biggest challenge in 2000 remained PayPal's unsustainable business model. Initially, PayPal offered its service free of charge, planning to earn interest on funds in users' PayPal accounts (i.e., the "float"). However, most recipients withdrew their funds immediately. Furthermore, a large majority of senders funded their payments using credit cards, which cost PayPal roughly 2% of payment value, rather than relying on electronic transfers from bank accounts, which were much less costly.

In order to boost its user base over eBay, both in US and internationally, PayPal decided to lever some of the ever existing concerns of sellers and buyers dealing with the virtual world, simplifying and easing the procedures regarding litigations, frauds and liabilities (transaction losses borne by PayPal also included the cost of buyer and seller protection programs. In fact, when merchants went bankrupt—not rare events in online retailing—PayPal was liable for any outstanding chargebacks related to credit card-funded PayPal payments. As with credit cards, buyers were protected against unauthorized use of their PayPal accounts. In addition, eBay buyers using PayPal received up to $1,000 in fraud protection (with a limit of three refunds per year) for items never delivered or materially misrepresented, but only if the seller had high eBay feedback ratings. Finally, subject to a $5,000 annual cap, merchants with business accounts qualified for seller protection against losses due to chargebacks, provided that they complied with reimbursement policies (e.g., retaining traceable proof of shipping to a confirmed address or requiring a signature receipt for items valued over $250).

Phase-3

After fine-tuning PayPal's business model and increasing its domestic and international penetration on eBay, PayPal started its off-eBay strategy. Strong growth in active users growth by adding users across multiple platforms, despite the slowdown in on-eBay growth and low-single-digit user growth on the eBay site. A late 2003 reorganization created a new business unit within PayPal—Merchant Services—to provide payment solutions to small and large e-commerce merchants outside the eBay auction community. Starting in the second half of 2004, PayPal Merchant Services unveiled several initiatives to enroll online merchants outside the eBay auction community, including:

- Lowering its transaction fee for high-volume merchants from 2.2% to 1.9% (while increasing the monthly transaction volume required to qualify for the lowest fee to $100,000)
- Encouraging its users to recruit non-eBay merchants by increasing its referral bonus to a maximum of $1,000 (versus the previous $100 cap)
- Persuading credit card gateway providers, including CyberSource and Retail Decisions USA, to include PayPal among their offerings to online merchants.
- Hiring a new sales force to acquire large merchants such as Dell, Apple's iTunes, and Yahoo! Stores, which hosted thousands of online merchants
- Reducing fees for online music purchases and other "micropayments"
- Launching PayPal Mobile, which allowed users to make payments using text messaging on their cell phones

Local restrictions

China

In China PayPal offers two kinds of accounts:

- PayPal.com accounts, for sending and receiving money to/from other PayPal.com accounts. All non-Chinese accounts are PayPal.com accounts, so these accounts may be used to send money internationally.
- PayPal.cn accounts, for sending and receiving money to and from other PayPal.cn accounts.

It is impossible to send money between PayPal.cn accounts and PayPal.com accounts, so PayPal.cn accounts are effectively unable to make international payments. For PayPal.cn, the only supported currency is the renminbi.

Japan

In late March 2010, new Japanese regulations forced PayPal to suspend the ability of Japanese individuals to pay money to other individuals.

Taiwan

As of mid July 2010, users in Taiwan have noticed that the "Personal" tab for sending money has been omitted without notice. There is no longer an option to send personal payments, thus forcing all recipients to pay a fee.

Brazil

As of mid-November 2010, users in Brazil also have noticed that the "Personal" tab for sending money has been omitted without notice. There is no longer an option to send personal payments, thus forcing all recipients to pay a fee. Balance transfers between PayPal accounts of the same account holder incur an additional 6.4% fee.

PayPalLabs

PayPal's innovation environment, Paypal-Labs.com, hosts several outreach and experimental projects such as the storefront application, the MySpace and Facebook donation widgets, and the PayPal blog.

Bank status

In the United States, PayPal is licensed as a money transmitter on a state-by-state basis. PayPal is not classified as a bank in the United States, though the company is subject to some of the rules and regulations governing the financial industry including Regulation E consumer protections and the USA PATRIOT Act.

Commencing 2 July 2007, as PayPal (Europe) S.à r.l. & Cie, S.C.A., PayPal moved its European operations from the UK to Luxembourg. As a Luxembourg entity, it is since regulated as a bank by the Commission de Surveillance du Secteur Financier (CSSF) and provides PayPal service throughout the European Union.

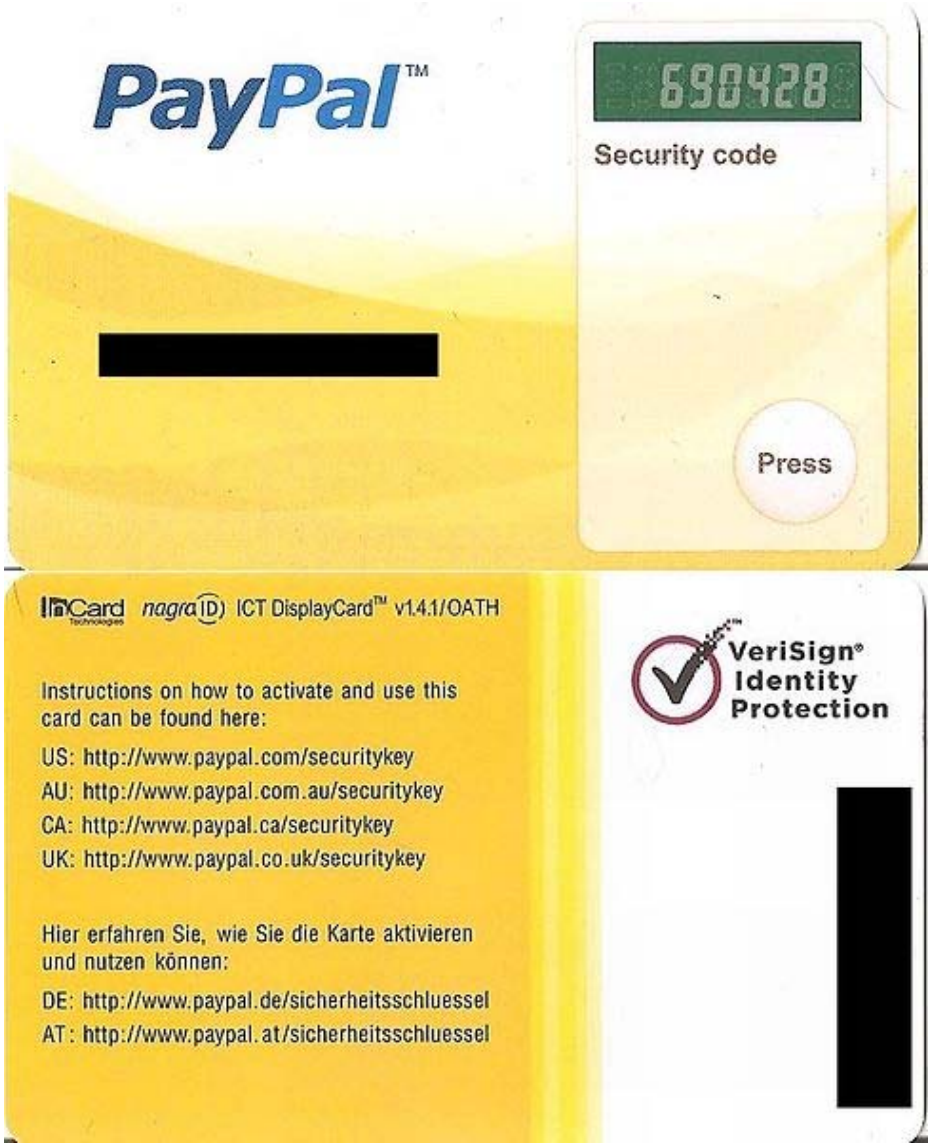
Safety and protection policies

The PayPal Buyer Protection Policy states that the customer may file a buyer complaint within 45 days if they did not receive an item or if the item they purchased was significantly not as described. If the buyer used a credit card, they might get a refund via chargeback from their credit-card company.

According to PayPal, it protects sellers in a limited fashion via the Seller Protection Policy. In general the Seller Protection Policy is intended to protect the seller from certain kinds of chargebacks or complaints if seller meets certain conditions including proof of delivery to the buyer. PayPal states the Seller Protection Policy is "designed to protect sellers against claims by buyers of unauthorized payments and against claims of non-receipt of any merchandise". The policy includes a list of "Exclusions" which itself includes "Intangible goods", "Claims for receipt of goods 'not as described'" and "Total reversals over the annual limit". There are also other restrictions in terms of the sale

itself, the payment method and the destination country the item is shipped to (simply having a tracking mechanism is not sufficient to guarantee the Seller Protection Policy is in effect).

Security



A credit-card sized alternative to the keychain security token, the PayPal Keycard generates a temporary login code to authenticate the user.

Security key

In early 2006, PayPal introduced an optional security key as an additional precaution against fraud. A user account tied to a security key has a modified login process: the account holder enters their login ID and password, as normal, but is then prompted to press the button on the security key and enter the six-digit number generated by it. This

two-factor authentication is intended to make account compromise by a malicious third party without access to the physical security key difficult, although it does not prevent so-called Man in the Browser (MITB) attacks. However, the user (or malicious third party) can alternatively authenticate by providing the credit card or bank account number listed on their account. Thus, the PayPal's implementation does not offer the security of true two-factor authentication.

The key currently costs US$5.00 for all users with no ongoing fees. The option of using a security key with one's account is currently available only to users registered in Australia, Germany, Canada, the United Kingdom and the United States.

MTAN

It is also possible to use a mobile phone to receive an MTAN (Mobile Transaction Authentication Number) via SMS,. Like all security measures, there have been reports of vulnerabilities to older mobile handsets.

Regulation

In Europe, PayPal is registered as a bank in Luxembourg under the legal name PayPal (Europe) Sàrl et Cie SCA, a company regulated centrally by the Luxembourg bank authority, the Commission de Surveillance du Secteur Financier (CSSF) (note that all of the company's European accounts were transferred to the PayPal's bank in Luxembourg on July 2, 2007.) Prior to this move, PayPal had been registered in the UK as PayPal (Europe) Ltd, an entity which was licensed as an Electronic Money Issuer with the UK's Financial Services Authority (FSA) from 2004. This ceased in 2007, when the company moved to Luxembourg.

In the US, although PayPal has an extensive User Agreement, PayPal is not directly regulated by the U.S. federal government, because it serves as a payment intermediary. The law is unclear as to whether PayPal is a bank, narrow bank, money services business or money transmitter. PayPal could also be subject to state regulation, but state laws vary, as do their definitions of banks, narrow banks, money services businesses and money transmitters. The most analogous regulatory source of law for PayPal transactions comes from P2P payments using credit and debit cards. Ordinarily, a credit card transaction, specifically the relationship between the issuing bank and the cardholder, is governed by the Truth in Lending Act (TILA) 15 U.S.C. §§ 1601-1667f as implemented by Regulation Z, 12 C.F.R. pt. 226, (TILA/Z). TILA/Z requires specific procedures for billing errors, dispute resolution and limits cardholder liability for unauthorized charges. Similarly, the legal relationship between a debit cardholder and the issuing bank is regulated by the Electronic Funds Transfer Act (EFTA) 15 U.S.C. §§ 1693-1693r, as implemented by Regulation E, 12 C.F.R. pr. 205, (EFTA/E). EFTA/E is directed at consumer protection and provides strict error resolution procedures. However, because PayPal is a *payment intermediary* and not otherwise regulated directly, TILA/Z and EFTA/E do not operate exactly as written once the credit/debit card transaction occurs via PayPal. Basically,

unless a PayPal transaction is funded with a credit card, the consumer has no recourse in the event of fraud by the seller.

In India, as of January 27, 2010, PayPal has no cross-border money transfer authorization. In The New York Times article "India's Central Bank Stops Some PayPal Services", Reserve Bank of India spokesman Alpana Killawalla stated: "Providers of cross-border money transfer service need prior authorization from the Reserve Bank under the Payment and Settlement Systems Act, PayPal does not have our authorization." PayPal is not listed in the "Certificates of Authorisation issued by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for Setting up and Operating Payment System in India".