KARNATAKA STATE OPEN UNIVERSITY

MUKTHAGANGOTRI, MYSORE- 570 006

DEPARTMENT OF STUDIES IN INFORMATION TECHNOLOGY

M.Sc IN INFORMATION TECHNOLOGY

III SEMESTER

ELECTIVE 1

E-COMMERCE

MSIT- 116B

MSIT-116B:

E-Commerce

Course Design and Editorial Committee

Prof. M.G.Krishnan
Vice Chancellor
Karnataka State Open University
Mukthagangotri, Mysore – 570 006

Prof. Vikram Raj Urs
Dean (Academic) & Convener
Karnataka State Open University
Mukthagangotri, Mysore – 570 006

Head of the Department and Course Co-Ordinator

Rashmi B.S
Assistant Professor & Chairperson
DoS in Information Technology
Karnataka State Open University
Mukthagangotri, Mysore – 570 006

Course Editor

Ms. Nandini H.M
Assistant Professor of Information Technology
DoS in Information Technology
Karnataka State Open University
Mukthagangotri, Mysore – 570 006

Course Writers

Mr. Naresh
Assisstant Professor
B.Tech and MS (Chinese program)
Department of Computer Science
Manasagangothri, University of Mysore
Mysore

Mr. Narendra
Assistant Professor
Department of Computer Science
Manasagangothri, University of Mysore
Mysore

Publisher

Registrar
Karnataka State Open University
Mukthagangotri, Mysore – 570 006

Developed by Academic Section, KSOU, Mysore
Karnataka State Open University, 2014

Printed and Published on behalf of Karnataka State Open University, Mysore-6 by the **Registrar (Administration)**

Karnataka State Open University

Manasagangothri, Mysore – 570 006

MSc in Information Technology III Semester

MSIT – 116B E-Commerce

Preface

In recent few years, there has been enormous global change in business firms, markets and consumer behavior. In the next 5 years, e-commerce is projected to continue growing at high single-digit rates, becoming the fastest-growing form of commerce in the world. Recent technologies have created a better-informed consumer and a manager who is equipped with up-to-the-second information. Communities have sprung up and supply chains have been redesigned.

In the course material for this semester, we have four modules which cover many topics in E-commerce. Each module has four units. Many of the important issue have been included. Security issues of electronic payments systems is a key issues which has been elaborated in a detailed manner. This material addresses some case studies in E-commerce.

We take this opportunity to welcome you to your education on E-Commerce. Preparing this course material has been a lot of a good experience for us and we sincerely hope that you get a lot out of it. We have tried to be balanced in presenting both the advantages and disadvantages of some of the new ides. We encourage you to adopt a similar open and critical stance when reading this course material.

Wish you happy reading!!!

UNIT 1: INTRODUCTION TO E-COMMERCE

Structure

1.8 Summary

1.9 Review questions

1.0 OBJECTIVES

After studying this unit we will be able

- To understand the meaning of E-commerce and difference with E-Business
- To understand the levels of E-Commerce
- To understand the benefits and limitations of E-commerce

1.1 INTRODUCTION TO ELECTRONIC-COMMERCE

Today, some considerable time after the so called 'dot com/Internet revolution', electronic commerce (e-commerce) remains a relatively new, emerging and constantly changing area of business management and information technology. There has been and continues to be much publicity and discussion about e-commerce. Library catalogues and shelves are filled with books and articles on the subject. However, there remains a sense of confusion, suspicion and is understanding surrounding the area, which has been exacerbated by the different contexts in which electronic commerce is used, coupled with the myriad related buzzwords and acronyms. This book aims to consolidate the major themes that have arisen from the new area of electronic commerce and to provide an understanding of its application and importance to management. In order to understand electronic commerce it is important to identify the different terms that are used, and to assess their origin and usage.

With the advent of the Internet, the term e-commerce began to include:

- Electronic trading of physical goods and of intangibles such as information.
- All the steps involved in trade, such as on-line marketing, ordering payment and support for delivery.
- The electronic provision of services such as after sales support or on-line legal advice.
- Electronic support for collaboration between companies such as collaborative on-line design and engineering or virtual business consultancy teams.

Some of the definitions of e-commerce often heard and found in publications and the media are:

Electronic Commerce (EC) *is where business transactions take place via telecommunications networks, especially the Internet.*

Electronic commerce *describes the buying and selling of products, services, and information via computer networks including the Internet.*

Electronic commerce *is about doing business electronically.*

E-commerce, ecommerce, or electronic commerce *is defined as the conduct of a financial transaction by electronic means.*

The wide range of business activities related to e-commerce brought about a range of other new terms and phrases to describe the Internet phenomenon in other business sectors. Some of these focus on purchasing from on-line stores on the Internet. Since transactions go through the internet and the Web, the terms I-commerce (Internet commerce), *icommerce* and even Web-commerce have been suggested but are now very rarely used. Other terms that are used for on-line retail selling include e-tailing, virtual-stores or cyber stores. A collection of these virtual stores is sometimes gathered into a 'virtual mall' or 'cybermall'.

1.2 INTRODUCTION TO ELECTRONIC-BUISNESS

As with e-commerce, e-business (electronic business) also has a number of different definitions and is used in a number of different contexts. One of the first to use the term was IBM, in October 1997, when it launched a campaign built around e-business. Today, major corporations are rethinking their businesses in terms of the Internet and its new culture and capabilities and this is what some see as e-business.

E-business is the conduct of business on the Internet, not only buying and selling but also servicing customers and collaborating with business partners.

E-business includes customer service (e-service) and intra-business tasks.

E-business is the transformation of key business processes through the use of Internet technologies. An e-business is a company that can adapt to constant and continual change. The development of intranet and extranet is part of e-business.

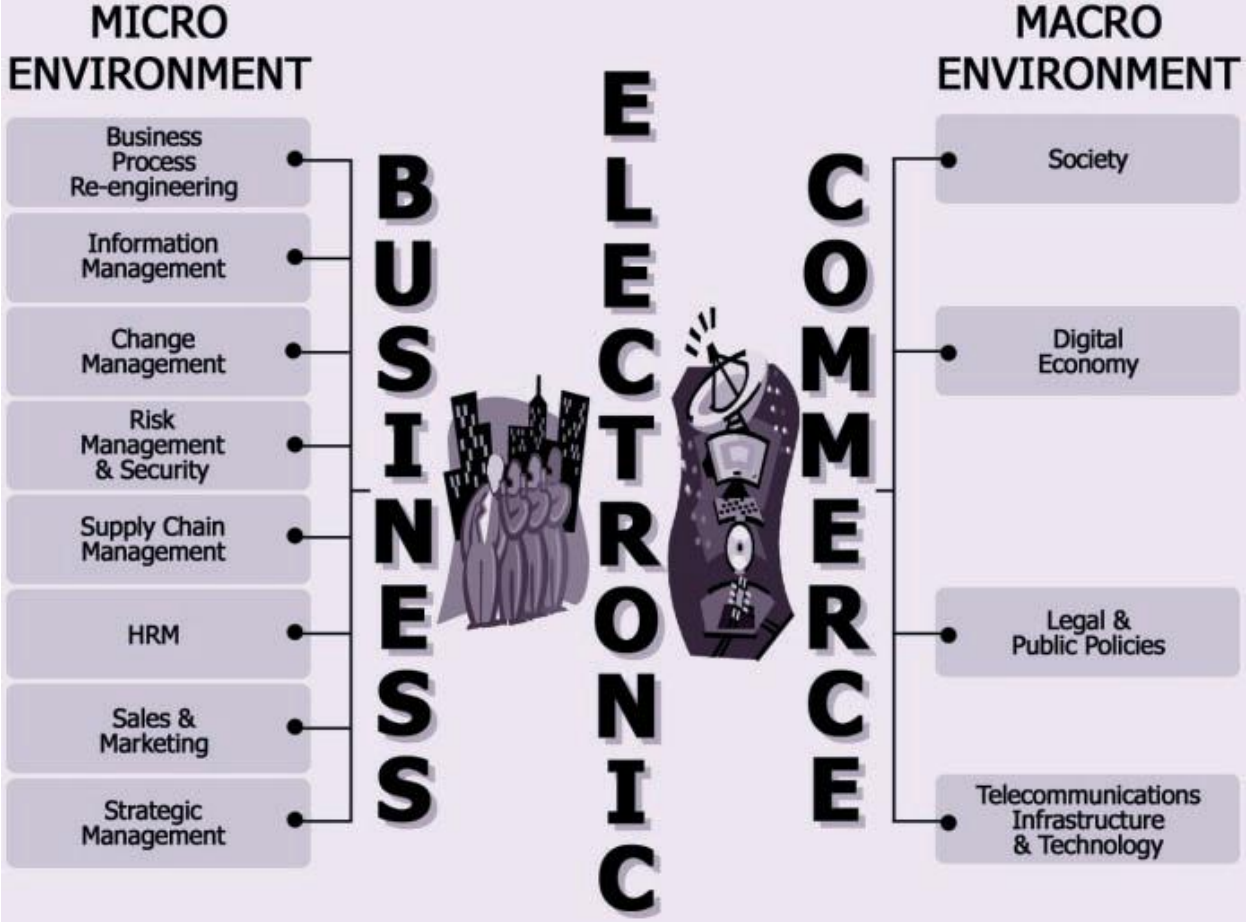
E-business is everything to do with back-end systems in an organisation.

In practice, e-commerce and e-business are often used interchangeably

1.3 DISTINCTION BETWEEN E-COMMERCE AND E-BUISNESS

Commerce is defined as embracing the concept of trade,'exchange of merchandise on a large scale between different countries'. By association, e-commerce can be seen to include the electronic medium for this exchange. Thus electronic commerce can be broadly defined as the exchange of merchandise (whether tangible or intangible) on a large scale between different countries using an electronic medium – namely the Internet. The implications of this are that e-commerce incorporates a whole socio-economic, telecommunications technology and commercial infrastructure at the macro-environmental level. All these elements interact together to provide the fundamentals of e-commerce. Business, on the other hand, is defined as 'a commercial enterprise as a going concern'. E-business can broadly be defined as the processes or areas involved in the running and operation of an organisation that are electronic or digital in nature. These include direct business activities such as marketing, sales and human resource management but also indirect activities such as business process re-engineering and change management, which impact on the improvement in efficiency and integration of business processes and activities.

Figure 1.1 illustrates the major differences in e-commerce and e-business, where e-commerce has a broader definition referring more to the macro-environment, e-business relates more to the micro-level of the firm.



THE KEY DRIVERS

It is important to identify the key drivers of e-commerce to allow a comparison between different countries. It is often claimed that e-commerce is more advanced in the USA than in Europe. These key drivers can be measured by a number of criteria that can highlight the stages of advancement of e-commerce in each of the respective countries. The criteria that can determine the level of advancement of e-commerce are summarized in Table 1.1 and can be categorised as:

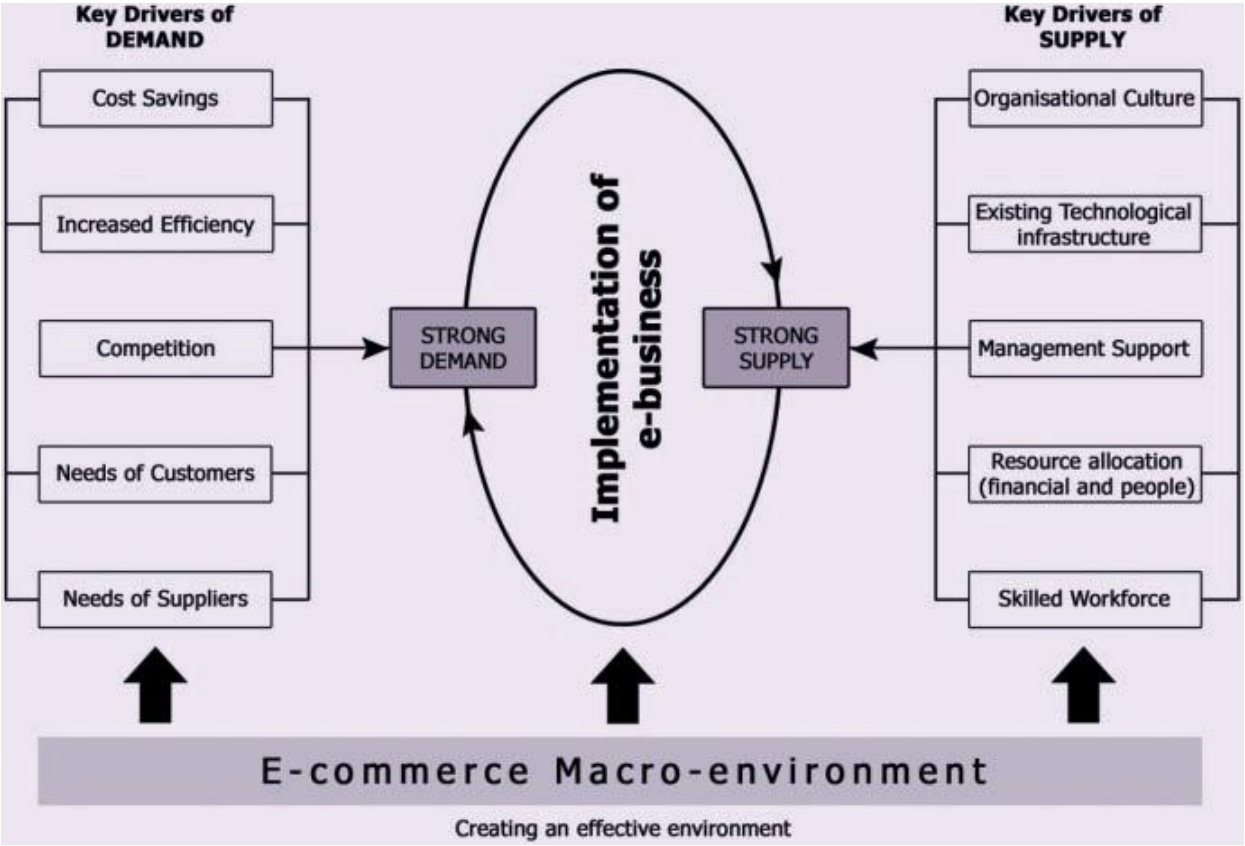
- *Technological factors* – The degree of advancement of the telecommunications infrastructure which provides access to the new technology for business and consumers.
- *Political factors* – including the role of government in creating government legislation, initiatives and funding to support the use and development of e-commerce and information technology.

- *Social factors* – incorporating the level and advancement in IT education and training which will enable both potential buyers and the workforce to understand and use the new technology.
- *Economic factors* – including the general wealth and commercial health of the nation and the elements that contribute to it. Since a distinction has been made in this book between e-commerce and e-business for consistency, the key drivers of e-business are also identified.

These are mainly at the level of the firm and are influenced by the macro-environment and e-commerce, which include:

- *Organisational culture* – attitudes to research and development (R&D); its willingness to innovate and use technology to achieve objectives.
- *Commercial benefits* – in terms of cost savings and improved efficiency that impact on the financial performance of the firm. *Skilled and committed workforce* – that understands, is willing and able to implement new technologies and processes.
- *Requirements of customers and suppliers* – in terms of product and service demand and supply.
- *Competition* – ensuring the organisation stays ahead of or at least keeps up with competitors and industry leaders.

These key drivers for the implementation of e-business can be put into the context of the classic economic equation of supply and demand illustrated in Figure 1.2.



1.4 THE IMPACT OF ELECTRONIC-COMMERCE

E-commerce and e-business are not solely the Internet, websites or dot com companies. It is about a new business concept that incorporates all previous business management and economic concepts. As such, e-business and e-commerce impact on many areas of business and disciplines of business management studies.

For example:

Marketing – issues of on-line advertising, marketing strategies and consumer behaviour and cultures. One of the areas in which it impacts particularly is direct marketing. In the past this was mainly door-todoor, home parties (like the Tupperware parties) and mail order using catalogues or leaflets. This moved to telemarketing and TV selling with the advances in telephone and television technology and finally developed into e-marketing spawning 'eCRM' (customer relationship management) data mining and the like by creating new channels for direct sales and promotion.

Computer sciences – development of different network and computing technologies and languages to support e-commerce and e-business, for example linking front and back office legacy systems with the 'webbased' technology.

Finance and accounting – on-line banking; issues of transaction costs; accounting and auditing implications where 'intangible' assets and human capital must be tangibly valued in an increasingly knowledge based economy.

Economics – the impact of e-commerce on local and global economies; understanding the concepts of a digital and knowledge-based economy and how this fits into economic theory.

Production and operations management – the impact of on-line processing has led to reduced cycle times. It takes seconds to deliver digitized products and services electronically; similarly the time for processing orders can be reduced by more than 90 per cent from days to minutes. Production systems are integrated with finance marketing and other functional systems as well as with business partners and customers.

Production and operations management (manufacturing) – moving from mass production to demand-driven, mass customisation customer pull rather than the manufacturer push of the past. Web-based Enterprise Resource Planning systems (ERP) can also be used to forward orders directly to designers and/or production floor within seconds, thus cutting production cycle times by up to 50 per cent, especially when manufacturing plants, engineers and designers are located in different countries. In sub-assembler companies, where a product is assembled from a number of different components sourced from a number of manufacturers, communication, collaboration and coordination are critical – so electronic bidding can yield cheaper components and having flexible and adaptable procurement systems allows fast changes at a minimum cost so inventories can be minimised and money saved.

Management information systems – analysis, design and implementation of e-business systems within an organisation; issues of integration of front-end and back-end systems.

Human resource management – issues of on-line recruiting, home working and 'intrapreneurs' working on a project by project basis replacing permanent employees.

Business law and ethics – the different legal and ethical issues that have arisen as a result of a global 'virtual' market. Issues such as copyright laws, privacy of customer information, legality of electronic contracts, etc.

1.5 LEVELS OF ELECTRONIC-COMMERCE

Electronic commerce is the process of conducting commercial transactions electronically over the Internet. This process is carried out primarily in five levels, and the main aspect of e-commerce is a merchant selling products or service to the consumers. There are five major segments under the broader category of e-business. However, the following are some popular e-commerce models used by companies engaged in e-commerce:-

- ***Business to business e-commerce (B2B)***
- ***Business to consumers e-commerce (B2C)***
- ***Consumers to consumers e-commerce (C2C)***
- ***Business to employees e-commerce (B2E) and***
- ***Consumer to business e-commerce (C2B)***

Business to Business E-commerce (B2B)

Business to Business e-commerce provides small and medium enterprises (SMES) with an excellent opportunity to access new markets, improve customer service and reduce costs. And while hurdles exist, they should be viewed more as speed breakers rather than road barriers. As a medium of information storage and dissemination, the internet has and is emerging a clear winner. Its rate of penetration has far outpaced the growth of other popular media such as newspaper, radio and television.

Business to Consumers E-commerce (B2C)

B2C is the most popular form of e-commerce, wherein the individuals are directly involved in B2C e-commerce, and businesses use the internet for offering their products or services 24 hours

a day through global access. The sites Amazon.com and Rediff are among these. These websites spell goods directly to consumers over the Internet. The two way accessibility feature of the internet enables operating companies to ascertain consumer preferences and buying trends directly.

Consumer to Consumer E-commerce (C2C)

This form of e-commerce is nothing but the cyber version of the good old auction houses. If anyone wants to sell anything, all one has to do is post a message on the site, giving details of the product and the expected price and wait for an interested customer to turn up and buy it. The buyer gets in touch with the seller through the Internet and the deal is crossed once the amount is finalised. Online message boards and barters are also examples of C2C e-commerce.

Consumer-to-Business E-commerce (C2B)

E-commerce, by empowering the customer, has been strategically redefining business. An example of C2B model of e-commerce is the site Price line.Com, which allows prospective airline travellers, tourists in need of hotel reservations etc. to visit its websites and indicate their preferred price for travel between any two cities. If an airline is willing to issue a ticket on the customers offered price, the consumer can then travel to the mentioned destination at his terms.

Business to Employees E-commerce (B2E)

This is concerned more with marketing a corporation's internal processes more efficiently. Customer care and support activities also hold ground. The requirement is that are all self-service with applications on the web that the employees can use themselves.

1.6 THE BENEFITS OF ELECTRONIC-COMMERCE

The previous sections have included discussions about what e-commerce is and its impact, but what are the benefits of e-commerce? What does it offer and why do it? The benefits of e-commerce can be seen to affect three major stakeholders: organizations, consumers and society.

Benefits of e-commerce to organizations

- ***International marketplace***. What used to be a single physical marketplace located in a geographical area has now become a borderless marketplace including national and international markets. By becoming e-commerce enabled, businesses now have access to people all around the world. In effect all e-commerce businesses have become virtual multinational corporations.
- ***Operational cost savings***. The cost of creating, processing, distributing, storing and retrieving paper-based information has decreased.
- ***Mass customisation***. E-commerce has revolutionised the way consumers buy good and services. The pull-type processing allows for products and services to be customised to the customer's requirements. In the past when Ford first started making motor cars, customers could have any colour so long as it was black. Now customers can configure a car according to their specifications within minutes on-line via the www.ford.com website.
- ***Enables reduced inventories*** and overheads by facilitating 'pull'-type supply chain management – this is based on collecting the customer order and then delivering through JIT (just-in-time) manufacturing. This is particularly beneficial for companies in the high technology sector, where stocks of components held could quickly become obsolete within months. For example, companies like Motorola (mobile phones), and Dell (computers) gather customer orders for a product, transmit them electronically to the manufacturing plant where they are manufactured according to the customer's specifications (like colour and features) and then sent to the customer within a few days.
- ***Lower telecommunications cost***. The Internet is much cheaper than value added networks (VANs) which were based on leasing telephone lines for the sole use of the organisation and its authorised partners. It is also cheaper to send a fax or e-mail via the Internet than direct dialling.
- ***Digitisation of products and processes***. Particularly in the case of software and music/video products, which can be downloaded or e-mailed directly to customers via the Internet in digital or electronic format.

- ***No more 24-hour-time constraints***. Businesses can be contacted by or contact customers or suppliers at any time.

Benefits of e-commerce to consumers

24/7 access. Enables customers to shop or conduct other transactions 24 hours a day, all year round from almost any location. For example, checking balances, making payments, obtaining travel and other information. In one case a pop star set up web cameras in every room in his house, so that he could check the status of his home by logging onto the Internet when he was away from home on tour.

More choices. Customers not only have a whole range of products that they can choose from and customise, but also an international selection of suppliers.

Price comparisons. Customers can 'shop' around the world and conduct comparisons either directly by visiting different sites, or by visiting a single site where prices are aggregated from a number of providers and compared (for example www.moneyextra.co.uk for financial products and services).

Improved delivery processes. This can range from the immediate delivery of digitised or electronic goods such as software or audio-visual files by downloading via the Internet, to the on-line tracking of the progress of packages being delivered by mail or courier.

An environment of competition where substantial discounts can be found or value added, as different retailers vie for customers. It also allows many individual customers to aggregate their orders together into a single order presented to wholesalers or manufacturers and obtain a more competitive price (aggregate buying), for example www.letsbuyit.com.

Benefits of e-commerce to society

Enables more flexible working practices, which enhances the quality of life for a whole host of people in society, enabling them to work from home. Not only is this more convenient and provides happier and less stressful working environments, it also potentially reduces environmental pollution as fewer people have to travel to work regularly. *Connects people*.

Enables people in developing countries and rural areas to enjoy and access products, services, information and other people which otherwise would not be so easily available to them.

Facilitates delivery of public services. For example, health services available over the Internet (on-line consultation with doctors or nurses), filing taxes over the Internet through the Inland Revenue website.

1.7 LIMITATIONS OF ELECTRONIC-COMMERCE

There was much hype surrounding the Internet and e-commerce over the last few years of the twentieth century. Much of it promoted the Internet and e-commerce as the panacea for all ills, which raises the question, are there any limitations of e-commerce and the Internet? Isaac Newton's 3rd Law of Motion, 'For every action there is an equal and opposite reaction' suggests that for all the benefits there are limitations to e-commerce. These again will be dealt with according to the three major stakeholders – organizations, consumers and society.

Limitations of e-commerce to organizations

Lack of sufficient system security, reliability, standards and communication protocols. There are numerous reports of websites and databases being hacked into, and security holes in software. For example, Microsoft has over the years issued many security notices and 'patches' for their software. Several banking and other business websites, including Barclays Bank, Powergen and even the Consumers' Association in the UK, have experienced breaches in security where 'a technical oversight' or 'a fault in its systems' led to confidential client information becoming available to all.

Rapidly evolving and changing technology, so there is always a feeling of trying to 'catch up' and not be left behind.

Under pressure to innovate and develop business models to exploit the new opportunities which sometimes leads to strategies detrimental to the organisation. The ease with which business models can be copied and emulated over the Internet increase that pressure and curtail longer-term competitive advantage.

Facing increased competition from both national and international competitors often leads to price wars and subsequent unsustainable losses for the organisation.

Problems with compatibility of older and 'newer' technology. There are problems where older business systems cannot communicate with webbased and Internet infrastructures, leading to some organisations running almost two independent systems where data cannot be shared. This often leads to having to invest in new systems or an infrastructure, which bridges the different systems. In both cases this is both financially costly as well as disruptive to the efficient running of organisations.

Limitations of e-commerce to consumers

Computing equipment is needed for individuals to participate in the new 'digital' economy, which means an initial capital cost to customers.

A basic technical knowledge is required of both computing equipment and navigation of the Internet and the World Wide Web.

Cost of access to the Internet, whether dial-up or broadband tariffs.

Cost of computing equipment. Not just the initial cost of buying equipment but making sure that the technology is updated regularly to be compatible with the changing requirement of the Internet, websites and applications.

Lack of security and privacy of personal data. There is no real control of data that is collected over the Web or Internet. Data protection laws are not universal and so websites hosted in different countries may or may not
have laws which protect privacy of personal data.

Physical contact and relationships are replaced by electronic processes. Customers are unable to touch and feel goods being sold on-line or gauge voices and reactions of human beings.

A lack of trust because they are interacting with faceless computers.

Limitations of e-commerce to society

Breakdown in human interaction. As people become more used to interacting electronically there could be an erosion of personal and social skills which might eventually be detrimental to the world we live in where people are more comfortable interacting with a screen than face to face.

Social division. There is a potential danger that there will be an increase in the social divide between technical haves and have-nots – so people who do not have technical skills become unable to secure better-paid jobs and
could form an underclass with potentially dangerous implications for social stability.

Reliance on telecommunications infrastructure, power and IT skills, which in developing countries nullifies the benefits when power, advanced telecommunications infrastructures and IT skills are unavailable or scarce or underdeveloped.

Wasted resources. As new technology dates quickly how do you dispose of all the old computers, keyboards, monitors, speakers and other hardware or software?

Facilitates Just-In-Time manufacturing. This could potentially cripple an economy in times of crisis as stocks are kept to a minimum and delivery patterns are based on pre-set levels of stock which last for days rather than weeks

1.8 SUMMARY

Thus, e-commerce is still commerce and still about human beings. Customers are still customers and merchants want people at their end. They send confidential, personal and financial information only by e-mail or can cash on the phone or might just prefer to visit in person. E-commerce is just only a new way of doing business or an additional method of doing business. It is a new generation technology, a new method of doing business with new generation

technology. Still, there are many drawbacks which fail to benefit the users of technology to a great extent. E-commerce is to be viewed as business but not as a technology issue. It must be business driven but not IT driven and initiatives must be integrated thoroughly into the existing commerce structure and strategy.

1.9 KEYWORDS

Electronic Commerce, E- Business, Levels of E-Commerce, Benefits of E-Commerce, Limitations of E- Commerce.

1.10 LIMITATIONS OF ELECTRONIC-COMMERCE

1. What is e-commerce? Discuss various characteristics of e-commerce.
2. Discuss various limitations of e-commerce.
3. "E-commerce is the new way to do business. Justify the statement.
4. What is scope of e-commerce in country like India?
5. Discuss various types of e-commerce models.
6. What is future of e-commerce in India?

1.11 REFERENCES/SUGGESTED READINGS

- Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc.
- Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.
- Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.
- Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.

UNIT 2: STRATEGIES IN E-COMMERCE

Structure

2.0 Objectives

After studying this unit we will be able

- To understand brand creation on the web and web auction strategies.
- To understand the legal environment in e-commerce

2.1 BRAND CREATION ON THE WEB

- Branding is about consumer's perception of the offering – how it performs, how it looks, how it makes one feel, and what messages it sends
- Market communications represent customers' interaction with the brand and, more generally, mass-marketing approaches
    - In the offline world, market communications tend to be one-way, from the firm to the customer
    - In the online world, market communications become much more interactive (two-way).

A Simple Conceptual Model of Brand Equity

- Brand equity is "a set of assets (and liabilities) linked to a brand's name and symbol that add to the value provided by a product or service to a firm and/or it's customers"
- A brand has three components:

i. Core product/service
ii. "Wrap-around"
iii. Marketing communications

- **Consumer responses** can take two broad forms:

i. Brand awareness (depth, breadth)
ii. Brand associations (strength, valence, uniqueness)

- **Consumer benefits** may include the increased confidence in the purchase decision, loyalty to the brand, and satisfaction with the experience
- **Firm benefits** translate into top-line revenue growth, increased margins, and lower marketing costs.

Types of Brands

i. Traditional Brands

- The product / service with which the brand is associated was established offline in the bricks-and-mortar world.

Examples: Gap,UPS, Dell,J.Crew,McDonald's,Office Depot,Ragu,Coca-Cola Disney.

ii. Online Brands

- The product / service with which the brand is associated established in the online world.

Examples: Amazon, Yahoo,ZDNet,AOL,Priceline,CDNow,Excite,E*Trade

Need of Brand Creation in the Web

- A known and respected brand name can present to potential customers a powerful stmt of quality value and other qualities.
- Branded products are easier to advertise and promote bcoz each product carries the reputation of the brand name.
- A firm's online branding choices depend upon its communications objectives
    - **Brand creation**. The objective may be to build a new-to-the-world brand name
    - **Sales leads**. The company may decide that the Internet will be used to facilitate the sales-lead process
    - **Store traffic**. The principal objective for some sites may be to increase store traffic
    - **Product trial**. A fourth objective may be trial usage of the product
    - **Product sales**. The company can also measure the success of a campaign based upon the actual increase in product or service sales
    - **Brand reinforcement**. Finally, it is possible that the communications effort is focused on reinforcing a brand image that is already widely accepted in the marketplace.

Elements of Branding

- The key elements of a brand are

1. **Differentiation**

- the company clearly distinguish its pdt from all others in the market.

2. **Relevance**

- degree to which the product offers utility to a potential customer.

3. **Perceived value.**

- It is a key element in creating a brand that has value.

Types of Branding

- **Emotional Branding**.

  - Companies use emotional appeals in their advertising and promotion efforts to establish and maintain brands

  - This approach work well on television, radio etc..

  - Emotional appeals are difficult to convey on the web.

- **Rational Branding**.

  - is used to maintain brands on the web.

  - does not rely on broad emotional appeal.

  - relies on the cognitive appeal of the specific help offered.

    eg: Web mail service like yahoo mail give users a valuable service- an email and a storage space for messages.

Brand Leveraging Strategies

- One method to build brands on the web for well established site is to extend their dominant positions to other parts and services .This strategy is called brand leveraging.
  eg **yahoo** ->here it is a search engine first, then it acquire other web business

  amazon-> from books to stronger CD, videos.

2.2 WEB AUCTION STRATEGIES

Auction Basics

- Online auctions provide a business opportunity that is perfect for the Web.
- An auction site can charge both buyers and sellers to participate, and it can sell advertising on its page.

- Web auctions can provide a general auction site that has sections devoted to specific interests.

Types of Auctions

- There are **6 auction types**
    - **i. English Auctions**
    - **ii. Dutch Auctions**
    - **iii. First-price sealed-bid**
    - **iv. Second-price sealed-bid**
    - **v. Double Auctions(Open outery)**
    - **vi. Double Auctions(sealed-bid)**

i. **English Auctions**

- Bidders publicly announce their successively higher bids until no higher bid is offered
- Minimum price can be used to set the price at which the auction will begin
- Reserve price is the minimum price the seller will accept
- Yankee auctions allow the bidder to choose the quantity of multiple items offered at the auction.

ii. **Dutch Auctions**

- Form of open auction in which bidding starts at a high price and drops until a bidder accepts the price.
- Usually the seller offers a number of similar items for sale.
- Good for moving large numbers of commodity items quickly.

iii. **Sealed-Bid Auctions**

- Bidders submit their bids independently and are usually prohibited from sharing information with each other
    - ☐ First-price sealed-bid

- Highest bidder wins

- Second-price sealed bid
  - Highest bidder wins, but at the second-highest bidder's price
  - Encourages all bidders to bid their private valuations, reducing collusion

iv. **Double Auctions**

- Buyers and sellers each submit combined price-quantity bids to an auctioneer
- The auctioneer matches the seller's offer (lowest price, then up) to the buyer's offers (highest price, then down)
- New York Stock Exchange conducts sealed-bid double auctions of stocks and bonds

Web Auction Strategies

- Web auctions are one of the fastest-growing segments of online business today.
- Three broad categories of auction Web sites are emerging:
  - **i. General consumer auctions.**
  - **ii. Specialty consumer auctions**
  - **iii. Business-to Business auctions**

i. General Consumer Auctions

- One of the most successful consumer auction Web sites is eBay.
- The eBay home page includes links to categories of items.
- Sellers pay eBay a listing fee and a sliding percentage of the final selling price.
- Buyers pay nothing to eBay.
- The most common format used on eBay is a computerized version of the English auction.
- Another auction type offered by eBay is an increasing-price format for multiple item auctions that eBay calls a Dutch auction.

- In either type of eBay auction, bidders must constantly monitor the bidding activity.

Example: **eBay**

- Search for specific items
- Browse by categories of items
- Seller options include bold-face type and featured listings
- Rating system to provide feedback to alleviate fears concerning seller reliability.

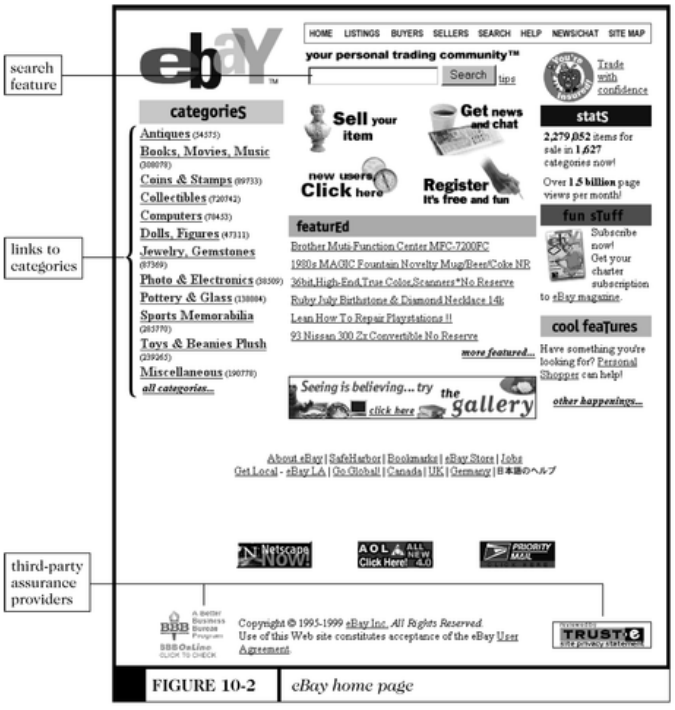


FIGURE 10-2 *eBay home page*

Additional General Consumer Auctions

- **Auction Universe**, owned by Classified Ventures, a partnership of eight major newspapers
  - Apartments.com
  - Cars.com
  - NewHomeNetwork.com

- **Yahoo! and Excite** have created auctions based on the eBay model.
- **Amazon.com**

  - Offers "Auctions Guarantee" to reimburse any buyer for merchandise purchased that was not delivered, or "materially different" than represented.

  -Provides escrow service for items over $250.

- **Klik-Klok Dutch Auction**

  - Short time-period auctions for quantity offerings.

ii. <u>Specialty Consumer Auctions</u>

- Here some Web auction sites exist to meet the needs of specialty market segments.

Examples:

CNET.com = computers.

Golf Club Exchange Web = golfers.

Coin collectors = Coin Universe.

iii. <u>Business-to-Business Web Auctions</u>

- Business-to-business auctions evolved to meet specific need, such as handling excess inventory.
- The large companies may create their own auction sites that sell excess inventory.
- A third-party Web auction site auctions excess inventory.
- Smaller companies often sell their excess inventory to liquidation brokers, who, in turn, create auction sites.

Auction-Related Services

- A common concern among people bidding in Web auctions is the reliability of the sellers.
- When purchasing high-value items, buyers can use an escrow service to protect their interests.
- Examples of Escrow services - I-Escrow, Secure Trades, and Trade Safe Online.
- Another service offered by some firms on the Web = directory of auctions, such as "Auction Guide" and "Auction Insider" sites.

Virtual Community and Portal Strategies

- Three key elements are required to make a virtual community:
    i. Cellular-satellite communications technology.
    ii. Electronic market places.
    iii. Software Agents.
- In 1999, eBay and cellular-satellite communications company SkyTel Communications announced a wireless person-to-person online trading service.
- Electronic marketplaces are growing out of virtual online communities, such as GeoCities and Tripod.
- Software agents are programs that traverse the Web and find items for sale that meet a buyer's specification.
- A virtual community is a gathering place for people and businesses that do not have a physical existence – exists in various forms, including Usenet newsgroups, chat rooms, and Web sites.
- Virtual communities help companies, customers, and suppliers to plan, collaborate, transact business, and interact in ways that benefit all of them.

Web Communities

- **WELL**
    - ***W***hole ***E***arth '***l***ectronic ***L***ink

- Predates the web, began as a series of dialogs among San Francisco authors and readers

- Purchased by Salon.com

- **GeoCities**
  - Free web space for members
  - Sells advertising to generate revenue
  - Owned by Yahoo!
- **Tripod**
  - Similar to GeoCities
  - Owned by Lycos
- **Theglobe.com**
  - Created by Cornell University students
  - News feeds, art gallery.

Web Portal Strategies

- By the late 1990s, virtual communities were selling advertising to generate revenue.
- Combinations of virtual communities, search engines, and Web directories
- Provide a high degree of "stickiness" that is extremely attractive to advertisers
- Examples include AOL, Excite, Infoseek, Lycos, MSN, Netscape Netcenter, Snap, and Yahoo!
- Search engine, entertainment, and Web directory sites were also selling advertising to generate revenue.
- Beginning in 1998, a wave of purchases and mergers occurred among these sites.
- The new sites that emerged still used an advertising-only revenue generation model and included all the features offered by virtual communities, search engines sites, Web directories, information and entertainment sites.
- Industry observers predicting success for Web portals may be correct.

- The companies that run Web portals certainly believe in the power of portals.
- They have been aggressively adding sticky features, such as chat rooms, e-mail, and calendar functions.

2.3 THE LEGAL ENVIRONMENT IN E-COMMERCE

- Legal Environment is an integral part of the world, and we should take it into account in developing a strategy for e-commerce.
- Legal issues regarding e-commerce have only begun to be addressed.
- Categories of issues:
    - **i. Borders and jurisdiction**
    - **ii. Jurisdiction on the Internet**
    - **iii. Contracting and contract enforcement**
    - **iv. Web site content**

i. Borders and jurisdiction

- Culture affects both laws and ethical standards.
- Territorial borders in the physical world serve as notice that culture and laws may be changing.
- The relationship between geographic boundaries and legal boundaries deals with four elements:
    i. Power
    ii. Effects
    iii. Legitimacy
    iv. Notice

Power

- Some of the defining characteristics of a sovereign government are control over:
    - A physical space
    - Objects that reside in that space
    - People who reside in that space

- The ability of a government to exert control over a person or corporation is called *jurisdiction.*
- Laws in the physical world do not apply to people who are not located in or own assets in the area that created those laws.

Effects

- Laws in the physical world are based on the relationship between physical proximity and the effects of a person's behavior.
- Actions have a stronger hold on things nearby.
- Example: Trademark enforcement
  Two restaurants with the same name, one in Chicago and one in France.

Legitimacy

- The right to create laws and enforce laws derives from the mandate of those who will be subject to those laws.
- Some cultures allow their governments a high degree of autonomy and authority.
  Example: China and Singapore
- Other cultures place severe restrictions on the authority of the government.
  Example: Scandinavian countries.

Notice

- Physical boundaries are an effective way to announce the ending of one legal or cultural system and the beginning of another.
- The perception that the laws and norms have changed is needed to allow people to adjust.
- Borders provide this notice.

ii. Jurisdiction on the Internet

- Determining who has jurisdiction can be difficult.
- Example: Mexican customer dealing with a firm from Sweden, hosted by a Canadian site, and maintained by a programmer from India.

- A ***contract*** is an agreement between two or more legal entities that provides for an exchange of value (goods, services, money).
- A ***tort*** is an action taken by a legal entity that causes harm to another legal entity.

Sufficient jurisdiction

- If a person or organization wants to enforce their rights under contracts or seek tort damages, they must find courts that have sufficient jurisdiction.
- A court has sufficient jurisdiction in a matter if it has both:
  - Subject matter jurisdiction
  - Personal jurisdiction.

Subject-matter jurisdiction

- Subject-matter jurisdiction is a court's authority to decide the type of dispute.
- In the United States:
  - Federal courts preside over federal law
    (Bankruptcy, copyright, patent, federal taxes)
  - State courts deal with issues governed by states
    (Professional licensing, state taxes)

The rules are easy to apply for subject-matter.

Personal jurisdiction

- Personal jurisdiction is, in general, determined by the residence of the parties in question.
- A court has jurisdiction if the defendant resides in the state in which the court is located.
- An out-of-state person can submit to a court's jurisdiction by signing a contract that includes a statement that the contract will be enforced according to the laws of a particular state.

Long-arm statutes

- States can enact statutes that create personal jurisdiction over nonresidents conducting business or committing tortious acts in the state.

- In many cases, these laws are not clear with respect to e-commerce.
- The more business conducted, the more likely a court will be to use a long-arm statute.
- Courts are also assert jurisdiction when a crime or intentional tort has occurred.

International issues

- The exercise of jurisdiction across national borders is governed by treaties between the countries.
- In general, personal jurisdiction for foreign firms and persons is determined by U.S. courts in the same way as long-arm statues.
- Jurisdictional issues are complex and changing.
- Businesses should consult an attorney for advice.

Taxation and e-commerce

- A government acquires the power to tax a business when the business establishes a connection with the area controlled by the government. This connection is called *nexus*.
- Nexus is similar to personal jurisdiction.
- Determining nexus can be difficult when a company conducts only a few activities in a state.
- Online companies may be subject to multiple tax laws from day one.

Types of taxes

A online business is potentially subject to several types of taxes:

- **Income taxes**: Levied by national, state, and local governments on the net income generated by business activities.
- **Transaction taxes**: Includes sales taxes, use taxes, and customs duties.
- **Property taxes**: Levied on the personal property and real estate used in the business.
- Income and transaction taxes are most important

iii. Contracting and Contract enforcement

- Any ***contract*** includes an offer and an acceptance.
- An ***offer*** is a declaration of willingness to buy or sell a product or service with enough details to be firm, precise, and unambiguous.
- An ***acceptance*** is the expression of willingness to take an offer, including all of its stated terms.
- When one party makes an offer that is accepted, a contract is created.

Contracting on the Web

- A seller advertising on the Web is not making an offer but inviting offers from potential buyers.
- When the buyer submits an order, the seller accepts and a contract is made.
- Some examples of legally binding acceptances in the physical world:
  - Mailing a check
  - Shipping goods
  - Shaking hands
  - Taking an item off a shelf
  - Opening a wrapped package

Written contracts

- In the U.S. written contracts must be used for goods worth more than $500 and contracts requiring actions that cannot be completed with a year.
- Things that constitute a signature:
  - Faxes
  - Typed names
  - Printed names
  - Digital signatures.

Warranties

- Any contract for sale includes implied warranties.
- Sellers can create explicit warranties.
- Statements in promotional material may create an implied warranty.
- Sellers can use a warranty disclaimer to avoid some implied warranties.
- It must be clearly displayed.
- Example: Lands' End in Germany.

2.4 WEBSITE CONTENT

- Legal issues can arise relating to the Web page content of an e-commerce site. These include:

  Trademark infringement
  Deceptive trade practices
  Regulation of advertising claims
  Defamation

Trademark infringement

- Web designers must be careful not to use any trade-marked name, logo, or other identifying mark without the written consent of the trademark owner.
- Example: A picture of a company (other than Pepsi) president holding a can of Pepsi.
- Manipulating trademarked images and placing them on a site can cause problems.

Deceptive trade practices

- Web sites that include links to other sites must be careful not to imply a relationship with the company if there is none.
- A firm cannot use a similar name, logo, or other identifying characteristic that causes confusion in the customer's mind.

- *Trademark dilution* is the reduction of the distinctive quality of a trademark by alternate uses.

Defamation

- A *defamatory statement* is one that is false and injures the reputation of another person or company.
- A statement injuring the reputation of a product or service is called *product disparagement*.
- The line between justifiable criticism and defamation can be hard to determine.

2.5 SUMMARY

This unit introduces to how to create a Web, gives knowledge on Conceptual model of brand equity, focuses on types of brands, elements of branding. Introduces to Web Auction Strategies, gives detail knowledge on its basics, types of Auctions. Legal Environment In E-Commerce.

2.6 KEYWORDS

Creation of Web, Types of Brands, Web Auction Strategies.

2.7 REVIEW QUESTIONS

1. Explain Simple Conceptual Model of Brand Equity?

2. Discuss different types of Brands in detail.

3. What is Auction Strategies? Explain its types in detail.

4. Explain the concept of legal environment in E-Commerce.

2.8 REFERENCES/ SUGGESTED READINGS

Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc.

• Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.

• Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.

• Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.

UNIT 3: INTEGRATION OF APPLICATIONS

Structure

3.0 OBJECTIVES

After studying this unit we will be able

- To understand e – Business Integration and middleware approaches.
- To understand enterprise application Integration

3.1 E-BUISNESS INTEGRATION (PATTERNS)

e-Business Integration occurs in as many forms as there are e-Businesses. At first glance, integration problems and the corresponding solutions are seldom identical. Yet, upon closer examination, you discover that integration solutions can actually be classified into common categories. Each of these categories describes both a "type" of integration problem as well as a solution method. These categories are called integration patterns. Integration patterns help you understand the different methods available to you for a given type of integration problem. They allow you to take a step back and understand the differences in the various scenarios and appreciate the different approaches to integration. Finally, they allow you to view "integration in

the big picture." You can learn to break down what may be a complex integration into conceptual categories and understand which technologies to apply.

What Are Integration Patterns?

A pattern is commonly defined as a reliable sample of traits, acts, tendencies, or other observable characteristics. In software development, you may be familiar with the idea of design patterns or process patterns. Design patterns systematically describe object designs that can be employed for a common set of problems. Similarly, process patterns describe proven methods and processes used in software development. In practice, patterns are simply a logical classification of commonly recurring actions, techniques, designs, or organizations. What are integration patterns? Integration patterns emerge from classification of standard solutions for integration scenarios. They are not patterns of design or code. Nor are they patterns of operational processes for an integration project. Instead, each integration pattern defines a type of integration problem, a solution technique, as well as parameters applied for e-Business Integration. Following are seven common e-Business Integration patterns. They are not meant to be comprehensive, but they cover most of the common integration scenarios implemented today. They encompass both EAI scenarios as well as B2Bi scenarios:

• **EAI (intra-enterprise) Patterns**

一. Database Replication

一. Single-Step Application Integration

一. Multi-Step Application Integration

一. Brokering Application

• **B2Bi (inter-enterprise) Patterns**

一. Application-to-Application B2Bi

一. Data Exchange B2Bi

一. B2B Process Integration

The EAI Patterns represent patterns commonly applied within a corporate enterprise, whereas the B2Bi Patterns represent the different methods in conducting integrated B2B transactions. The following sections provide a closer look at each of these patterns and discuss some of the details.

Database Replication

The Database Replication pattern may be the most prevalent pattern of EAI integration today. Database replication involves managing copies of data over two or more databases, resulting in redundant data. Companies engage in database replication for numerous reasons. One reason is that many organizations are becoming more distributed in their operations, requiring multiple copies of the same data over several physical locations. Replication is also a means of data recovery. In many organizations, an active secondary database is maintained for data recovery purposes. In the event that the production database needs to be recovered, the secondary replicated database can be used. This also applies for "high availability" systems. In these situations, a redundant copy of "live" data is maintained to ensure that if the first system is not available, the redundant database system is activated. The two general categories for database replication are synchronous and asynchronous replication.

Single Step Application Integration

The Single-Step Application Integration (SSAI) pattern extends the asynchronous database replication pattern. Instead of focusing on data consistency between two databases, the SSAI pattern integrates data between applications, moving data from one context to another. It does so by translating data syntax of the source message and reformatting data elements into a new target message. It is "single step" because it requires an intermediary broker to map source messages to target messages. Typically, it is an extension of the asynchronous replication technology, in that it utilizes Message Queuing Middleware such as MQ Series. It is just as likely to be implemented with the less sophisticated FTP in a batch mode. In either case, the point is that it does more than simply move data from point A to point B for consistency's sake. Whereas, in the replication pattern both the source and target data models are likely similar, if not identical at times, this is not necessarily the case for the SSAI pattern. The objective here is not data consistency, but application data integration.

Multi Step Application Integration

The Multi-Step Application Integration (MSAI) pattern is an extension of the SSAI pattern. MSAI enables the integration of n (source) to m (target) applications. It addresses many-to-many integration, which SSAI cannot, by providing what is known as sequential logical processing. In other words, steps in this pattern are processed sequentially, and rules applied are Boolean

logical in nature. Like the single-step pattern, MSAI requires an intermediary to broker the transaction of data between applications. It is often built around an asynchronous event-based system and typically is implemented through the use of Message Queuing Middleware as well. The asynchronous event based approach creates loose coupling. Although each system is physically independent, they are logically dependent. In other words, interdependencies exist between the application events that can be expressed in terms of transformations and data integration rules. Data elements from one application can drive the retrieval or processing of messages in another application. The simplest multi-step example in Figure 3.3 involves three applications in which a message from application A is combined with a message from application B that is reformatted for a target application C. It is common for a data element from application A to act as a key to drive the request for information from application B.

Brokering Application

At times integrating two applications is not principally a matter of integrating data, but integrating business logic. The Brokering Application pattern addresses the use of intermediary application logic to link together two or more applications. In plain terms, it means that custom application code is written containing logic to broker interactions between the disparate applications. This custom brokering application sits in the middle as an intermediary for processing requests from different applications

The use of this solution pattern is particularly applicable in the scenarios below:

Applications Need to Reuse Logic

Applications Linked by Complex Logic

Applications Unified Through User Interface

Application to Application B2Bi

Now you're ready to move beyond EAI to learn about Application-to-Application B2Bi, extending integration beyond the corporate enterprise. I will describe four additional patterns related specifically to B2B integration, beginning first with the Application-to-Application B2Bi pattern. The Application-to-Application pattern is the logical extension of what occurs in EAI. When EAI vendors tout their products as being B2Bi, this specific pattern is what they have in mind. However, as you will discover, this is not the only pattern and very likely not even the

primary pattern for B2Bi. Application-to-Application B2Bi, which is often referred to as inter-enterprise integration, involves corporate entities linking their applications directly to the applications of their partners or customers. In practice, this type of integration is often implemented as part of a supply chain of goods and services to the customer.

This extension for inter-enterprise integration means that a number of additional issues need to be accounted for:

Security

Federated Control

Systems Management

Data Exchange B2Bi

The limitation of the Application-to-Application B2Bi pattern is that it can be more demanding to implement. It necessitates that each participant handles and externalizes application native data directly. This makes it difficult to scale the B2B interaction model rapidly when such a demand is placed on the participants. The optimal solution is to provide a rapidly scalable B2Bi model in which participants can exchange data freely with minimal expectation on their infrastructure. The Data Exchange B2Bi pattern enables B2B transactions predicated on a common data exchange format. It is the most widely applied pattern for B2B commerce today. Data Exchange B2Bi is effective because it is simple in concept and has been in use since the days of Electronic Data Interchange (EDI), the forerunner to today's B2B over the Internet.

Although there is a significant incumbency of legacy EDI transactions, the XML-based B2B will ultimately displace EDI as the primary mechanism for e-Business transactions. XML-based data packets are transmitted between two business entities through the use of a data exchange gateway service on both ends. One of the primary responsibilities of the gateway service is to prepare the data packets by placing them within a security envelope. The B2B gateway service supports security standards such as MIME, X.509, and S/Key. It is also responsible for routing data through a standard transport. Most B2B gateway services provide numerous transport options including HTTPS, FTP, and TCP/IP Sockets. However, upon examination, you will find that most B2Bi transactions still deliver XML documents over an HTTPS pipe.

B2B Process Integration

Even with industry wide initiatives such as Rosetta Net, a point-to-point data exchange that manages static interactions has some limitations. If Corporation A wants to purchase office supplies from Depot X, it must agree ahead of time on the content of the documents exchanged and buying process. This is, of course, to be expected. However, what if the situation involves managing multiple suppliers or if the interactions become more complex? For instance, a scenario in which suppliers openly bid to compete on pricing will increase the dimensions of process interactions. In that case, managing the B2B transaction is no longer an activity of managing a single point-to-point interaction. Instead, it becomes a challenge of managing business processes that are dynamic rather than static.

The B2B Process Integration pattern takes the limitations raised by the Data Exchange pattern and addresses them by providing Business Process Integration (BPI) services. Just as the Data Exchange pattern allows participants to manage data exchanges dynamically through XML-based documents, the B2B Process Integration pattern allows the participants to manage processes in the same way.

Therefore, richer, more complex relationships can occur between trading partners. B2B Process Integration pattern can be implemented as one of two variations: Closed Process B2Bi or Open Process B2Bi. You might argue that each of these variations constitutes an individual pattern, but because they share the common attribute of being process focused, I have decided to treat them as variations to the B2B Process Integration pattern.

3.2 APPROACHES TO MIDDLEWARE

Middleware is computer software that connects software components or some people and their applications. The software consists of a set of services that allows multiple processes running on one or more machines to interact. This technology evolved to provide for interoperability in support of the move to coherent distributed architectures, which are most often used to support and simplify complex distributed applications. It includes web servers, application servers, and similar tools that support application development and delivery. Middleware is especially integral to modern information technology based on XML, SOAP, Web services, and service-oriented architecture.

Middleware sits "in the middle" between application software that may be working on different operating systems. It is similar to the middle layer of a three-tier single system architecture, except that it is stretched across multiple systems or applications. Examples include EAI software, telecommunications software, transaction monitors, and messaging-and-queueing software.

The distinction between operating system and middleware functionality is, to some extent, arbitrary. While core kernel functionality can only be provided by the operating system itself, some functionality previously provided by separately sold middleware is now integrated in operating systems. A typical example is the TCP/IP stack for telecommunications, nowadays included in virtually every operating system.

In simulation technology, middleware is generally used in the context of the high level architecture (HLA) that applies to many distributed simulations. It is a layer of software that lies between the application code and the run-time infrastructure. Middleware generally consists of a library of functions, and enables a number of applications—simulations or federates in HLA terminology—to page these functions from the common library rather than re-create them for each application

Definition of Middleware

Software that provides a link between separate software applications. Middleware is sometimes called plumbing because it connects two applications and passes data between them. Middleware allows data contained in one database to be accessed through another. This definition would fit enterprise application integration and data integration software.

Object Web defines middleware as: "The software layer that lies between the operating system and applications on each side of a distributed computing system in a network."

Middleware is computer software that connects software components or applications. The software consists of a set of services that allows multiple processes running on one or more machines to interact. This technology evolved to provide for interoperability in support of the move to coherent distributed architectures, which are most often used to support and simplify complex, distributed applications.

It includes web servers, application servers, and similar tools that support application development and delivery. Middleware is especially integral to modern information technology based on XML, SOAP, Web services, and service-oriented architecture.

In simulation technology, middleware is generally used in the context of the high level architecture (HLA) that applies to many distributed simulations. It is a layer of software that lies between the application code and the run-time infrastructure. Middleware generally consists of a library of functions, and enables a number of applications—simulations or federates in HLA terminology—to page these functions from the common library rather than re-create them for each application.

Origin of Middleware

Middleware is a relatively new addition to the computing landscape. It gained popularity in the 1980s as a solution to the problem of how to link newer applications to older legacy systems, although the term had been in use since 1968. It also facilitated distributed processing, the connection of multiple applications to create a larger application, usually over a network.

Use of middleware

Middleware services provide a more functional set of application programming interfaces to allow an application to (when compared to the operating system and network services.):

Locate transparently across the network, thus providing interaction with another service or application

Filter data to make them friendly usable or public via anonymization process for privacy protection (for example)

Be independent from network services

Be reliable and always available

Add complementary attributes like semantics

Middleware offers some unique technological advantages for business and industry. For example, traditional database systems are usually deployed in closed environments where users access the system only via a restricted network or intranet (e.g., an enterprise's internal network). With the phenomenal growth of the World Wide Web, users can access virtually any database for which they have proper access rights from anywhere in the world. Middleware addresses the

problem of varying levels of interoperability among different database structures. Middleware facilitates transparent access to legacy database management systems (DBMSs) or applications via a web server without regard to database-specific characteristics .

Businesses frequently use middleware applications to link information from departmental databases, such as payroll, sales, and accounting, or databases housed in multiple geographic locations. In the highly competitive healthcare community, laboratories make extensive use of middleware applications for data mining, laboratory information system (LIS) backup, and to combine systems during hospital mergers. Middleware helps bridge the gap between separate LISs in a newly formed healthcare network following a hospital buyout.

Wireless networking developers can use middleware to meet the challenges associated with wireless sensor network (WSN), or WSN technologies. Implementing a middleware application allows WSN developers to integrate operating systems and hardware with the wide variety of various applications that are currently available.

Middleware can help software developers avoid having to write application programming interfaces (API) for every control program, by serving as an independent programming interface for their applications. For Future Internet network operation through traffic monitoring in multi-domain scenarios, using mediator tools (middleware) is a powerful help since they allow operators, searchers and service providers to supervise Quality of service and analyse eventual failures in telecommunication services.

Finally, e-commerce uses middleware to assist in handling rapid and secure transactions over many different types of computer environments. In short, middleware has become a critical element across a broad range of industries, thanks to its ability to bring together resources across dissimilar networks or computing platforms.

Types of middleware

Hurwitz's classification system organizes the many types of middleware that are currently available. These classifications are based on scalability and recoverability:

Remote Procedure Call — Client makes calls to procedures running on remote systems. Can be asynchronous or synchronous.

Message Oriented Middleware — Messages sent to the client are collected and stored until they are acted upon, while the client continues with other processing.

Object Request Broker — This type of middleware makes it possible for applications to send objects and request services in an object-oriented system.

SQL-oriented Data Access — middleware between applications and database servers.

Embedded Middleware — communication services and integration interface software/firmware that operates between embedded applications and the real time operating system.

• Other sources include these additional classifications:

• Transaction processing monitors — Provides tools and an environment to develop and deploy distributed applications.

• Application servers — software installed on a computer to facilitate the serving (running) of other applications.

• Enterprise Service Bus — An abstraction layer on top of an Enterprise Messaging System.

RPC

In computer science, a remote procedure call (RPC) is an inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction. That is, the programmer writes essentially the same code whether the subroutine is local to the executing program, or remote. When the software in question uses object-oriented principles, RPC is called remote invocation or remote method invocation. Note that there are many different (often incompatible) technologies commonly used to accomplish this.

History and origins

The idea of RPC (Remote Procedure Call) goes back at least as far as 1976, when it was described in RFC 707. One of the first business uses of RPC was by Xerox under the name "Courier" in 1981. The first popular implementation of RPC on Unix was Sun's RPC (now called ONC RPC), used as the basis for NFS (Sun). Another early Unix implementation was Apollo Computer's Network Computing System (NCS). NCS later was used as the foundation of

DCE/RPC in the OSF's Distributed Computing Environment (DCE). A decade later Microsoft adopted DCE/RPC as the basis of the Microsoft RPC (MSRPC) mechanism, and implemented DCOM on top of it. Around the same time (mid-90's), Xerox PARC's ILU, and the Object Management Group's CORBA, offered another RPC paradigm based on distributed objects with an inheritance mechanism.

Message passing

An RPC is initiated by the client, which sends a request message to a known remote server to execute a specified procedure with supplied parameters. The remote server sends a response to the client, and the application continues its process. There are many variations and subtleties in various implementations, resulting in a variety of different (incompatible) RPC protocols. While the server is processing the call, the client is blocked (it waits until the server has finished processing before resuming execution). An important difference between remote procedure calls and local calls is that remote calls can fail because of unpredictable network problems. Also, callers generally must deal with such failures without knowing whether the remote procedure was actually invoked. Idempotent procedures (those that have no additional effects if called more than once) are easily handled, but enough difficulties remain that code to call remote procedures is often confined to carefully written low-level subsystems.

The steps in making a RPC

1. The client calling the Client stub. The call is a local procedure call, with parameters pushed on to the stack in the normal way.
2. The client stub packing the parameters into a message and making a system call to send the message. Packing the parameters is called marshaling.
3. The kernel sending the message from the client machine to the server machine.
4. The kernel passing the incoming packets to the server stub.
5. Finally, the server stub calling the server procedure. The reply traces the same in other direction.

Standard contact mechanisms

To let different clients access servers, a number of standardized RPC systems have been created. Most of these use an interface description language (IDL) to let various platforms call the RPC.

The IDL files can then be used to generate code to interface between the client and server. The most common tool used for this is RPCGEN.

Other RPC analogues

RPC analogues found elsewhere:

Java's Java Remote Method Invocation (Java RMI) API provides similar functionality to standard UNIX RPC

methods.

Modula-3's Network Objects, which were the basis for Java's RMI

XML-RPC is an RPC protocol that uses XML to encode its calls and HTTP as a transport mechanism.

Microsoft .NET Remoting offers RPC facilities for distributed systems implemented on the Windows platform.

RPyC implements RPC mechanisms in Python, with support for asynchronous calls.

Pyro Object Oriented form of RPC for Python.

Etch (protocol) framework for building network services.

Facebook's Thrift protocol and framework.

CORBA provides remote procedure invocation through an intermediate layer called the "Object Request Broker"

DRb allows Ruby programs to communicate with each other on the same machine or over a network. DRb uses

remote method invocation (RMI) to pass commands and data between processes.

AMF allows Flex applications to communicate with back-ends or other applications that support AMF.

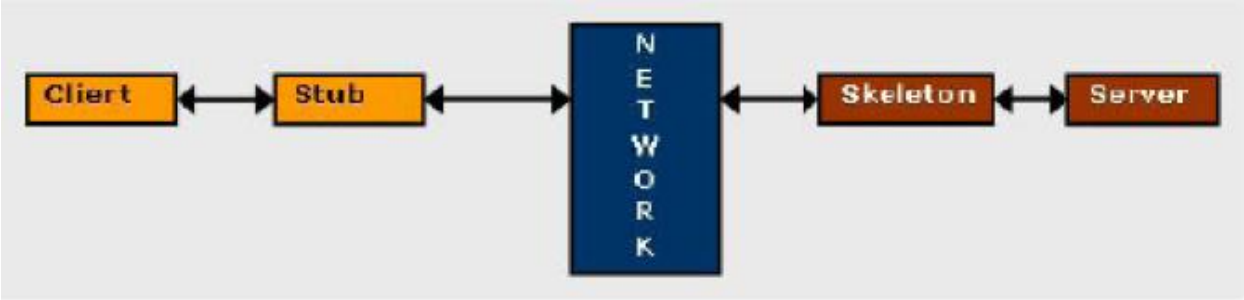
Libevent provides a framework for creating RPC servers and clients.

Windows Communication Foundation is an application

RMI

The Java Remote Method Invocation Application Programming Interface (API), or Java RMI, is a Java application programming interface that performs the object-oriented equivalent of remote procedure calls (RPC).

1. The original implementation depends on Java Virtual Machine (JVM) class representation mechanisms and it thus only supports making calls from one JVM to another. The protocol underlying this Java-only implementation is known as Java Remote Method Protocol (JRMP).



A typical implementation model of Java-RMI using stub and skeleton objects. Java 2 SDK, Standard Edition, v1.2 removed the need for a skeleton.

Usage of the term RMI may denote solely the programming interface or may signify both the API and JRMP, whereas the term RMI-IIOP (read: RMI over IIOP) denotes the RMI interface delegating most of the functionality to the supporting CORBA implementation.

The programmers of the original RMI API generalized the code somewhat to support different implementations, such as a HTTP transport. Additionally, the ability to pass arguments "by value" was added to CORBA in order to support the RMI interface. Still, the RMI-IIOP and JRMP implementations do not have fully identical interfaces.

RMI functionality comes in the package java.rmi, while most of Sun's implementation is located in the sun.rmi package. Note that with Java versions before Java 5.0 developers had to compile RMI stubs in a separate compilation step using rmic. Version 5.0 of Java and beyond no longer require this step.

3.3 ENTERPRISE APPLICATION INTEGRATION

Enterprise Application Integration (EAI) is defined as the use of software and computer systems architectural principles to integrate a set of enterprise computer applications. Enterprise Application Integration (EAI) is an integration framework composed of a collection of technologies and services which form a middleware to enable integration of systems and applications across the enterprise. Supply chain management applications (for managing inventory and shipping), customer relationship management applications (for managing current

and potential customers), business intelligence applications (for finding patterns from existing data from operations), and other types of applications (for managing data such as human resources data, health care, internal communications, etc) typically cannot communicate with one another in order to share data or business rules.

For this reason, such applications are sometimes referred to as islands of automation or information silos. This lack of communication leads to inefficiencies, wherein identical data are stored in multiple locations, or straightforward processes are unable to be automated. Enterprise application integration (EAI) is the process of linking such applications within a single organization together in order to simplify and automate business processes to the greatest extent possible, while at the same time avoiding having to make sweeping changes to the existing applications or data structures. In the words of the Gartner Group, EAI is the "unrestricted sharing of data and business processes among any connected application or data sources in the enterprise."

One large challenge of EAI is that the various systems that need to be linked together often reside on different operating systems, use different database solutions and different computer languages, and in some cases are legacy systems that are no longer supported by the vendor who originally created them. In some cases, such systems are dubbed "stovepipe systems" because they consist of components that have been jammed together in a way that makes it very hard to modify them in any way.

Purposes of EAI

EAI can be used for different purposes:

Data (information) Integration: Ensuring that information in multiple systems is kept consistent. This is also known as EII (Enterprise Information Integration).

Vendor independence: Extracting business policies or rules from applications and implementing them in the EAI system, so that even if one of the business applications is replaced with a different vendor's application, the business rules do not have to be re-implemented.

Common Facade: An EAI system could front-end a cluster of applications, providing a single consistent access interface to these applications and shielding users from having to learn to interact with different software packages.

EAI patterns

Integration patterns

There are two patterns that EAI systems implement:

Mediation: Here, the EAI system acts as the go-between or broker between (interface or communicating) multiple applications. Whenever an interesting event occurs in an application (e. g., new information created, new transaction completed, etc.) an integration module in the EAI system is notified. The module then propagates the changes to other relevant applications.

Federation: In this case, the EAI system acts as the overarching facade across multiple applications. All event calls from the 'outside world' to any of the applications are front-ended by the EAI system. The EAI system is configured to expose only the relevant information and interfaces of the underlying applications to the outside world, and performs all interactions with the underlying applications on behalf of the requester.

Both patterns are often used concurrently. The same EAI system could be keeping multiple applications in sync (mediation), while servicing requests from external users against these applications (federation).

Access patterns

EAI supports both asynchronous and synchronous access patterns, the former being typical in the mediation case and the latter in the federation case.

Lifetime patterns

An integration operation could be short-lived (e. g., keeping data in sync across two applications could be completed within a second) or long-lived (e. g., one of the steps could involve the EAI system interacting with a human work flow application for approval of a loan that takes hours or days to complete).

EAI topologies

There are two major topologies: hub-and-spoke, and bus. Each has its own advantages and disadvantages. In the hub-and-spoke model, the EAI system is at the center (the hub), and interacts with the applications via the spokes. In the bus model, the EAI system is the bus (or is implemented as a resident module in an already existing message bus or message-oriented middleware).

3.4 SUMMARY

This unit introduces various concepts on Integration patterns, different approaches to middleware and its different types. A detailed information about the enterprise application integration has also been discussed.

3.5 KEYWORDS

Middleware, Integration patterns, Remote method invocation

3.6 REVIEW QUESTIONS

1. Explain different Integration patterns in detail
2. What are the different approaches to middleware? Explain them in brief.
3. Explain different types of middleware
4. Explain enterprise application integration briefly.

3.7 REFERENCES / SUGGESTED READINGS

- Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc.
- Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.
- Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.
- Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.

UNIT 4: LAUNCHING A E-BUISNESS ON THE INTERNET

Structure

4.0 OBJECTIVES

After studying this unit we will be able

- To understand the framework for enterprise architecture.
- To understand the disaster plan and disaster recovery process

4.1 INTRODUCTION

For starters, you need a domain name, a web page, and a way to take your orders. It can be quite a daunting experience to take these first steps into eCommerce. Here are some tips to help you get started on your way.

Your domain name will identify your particular business on the internet. When registering and deciding on a domain name for your business there are a number of things you need to consider.

ourproductsarethebestontheweb.com - Avoid using excessively long and tedious domain names. Choose something simple and easy to remember. Also try to use popular keywords that people would use to search for products or services such as yours. This can help you get ranked higher in search engines as well as help consumers remember your site.

.com vs .biz - Always use .com instead of .biz or .info. Your company will be taken more seriously. If necessary you can use .net, but more people are familiar with .com and will remember it more easily.

Shop Around - There are a number of sites that offer domain registration. Prices vary, but expect to pay a yearly registration fee. Some popular domain registration web sites include GoDaddy.com, Web.com, and Register.com. Many domain registrars also offer web design, web hosting and email.

A web site is like having a store front in every corner of the world. What do you want people to see when they look in your window? Consumers today are more intelligent and wary than when the web was in its infancy. You need your web page to project a professional image, draw your customers in, and keep them interested long enough to see the value of doing business with you instead of your competitors. Easier said than done right? Successful web design is crucial to converting your web visitors into web sales. Here are a few avenues you can take to achieve a successful web site.

Hire Someone Who Knows - There are countless companies out there that you can pay to develop a professional web site for your business. Ask around. With so many to choose from, referrals are usually the best way to find a reliable and affordable company, or even person, with the expertise to create a professional web site for your needs.

The Fruits of Others Labors - Web page templates are a less expensive alternative to having a site custom made. On average templates range in price from $13 to $300 dollars depending on how original you want your site to be as well as how large. Some come with only an index, or front page, while still others include the index as well as supporting content pages. Some

templates will require you to have some basic knowledge of html editing and working with a graphics program such as Adobe Photoshop to tweak the site to fit your business. Other templates allow you to simply enter in your text in the pre-designated boxes and youre ready to go. A good place to start looking is TemplateMonster.com.

Head Long and Feet First - For the ambitious or those on an extremely tight budget, there is a third solution. Do it yourself. There are many web page editing programs available and you may even have one on your computer already and dont even know it. A few of the most popular are Macromedia Dreamweaver, Microsoft Front page, and Adobe GoLive. All come with tutorials and if the help you need is not found there, it is not far away. Type your question into your favorite search engine and you are sure to find the information you need. Surf the web and look at other web pages. See what you like about them and what you dont. Does it look professional? Why? Does it inspire confidence and reliability? How? Most importantly, be patient with yourself. This is a big project you are undertaking and a lot of the learning will happen by trial and error.

No store, online or offline, can be successful without a way to make sales and take orders. With an online store you have a couple of options. Some businesses will want to encourage their customers to place their orders online, others will want them to call to place their orders, and some will want to offer both options.

Virtual Shopping Carts - If you are selling a number of different products online, a shopping cart will be necessary. This will allow your customers to add things to their cart as they shop your online store. Unless you are a programmer or having your site professional designed, you will need to find a shopping cart that you can add onto your site. You can choose to buy your software or take advantage of a free one such as that found at osCommerce.com. There are advantages to both paid software and free. Your exact needs will determine the best course for you.

Phone Orders - Because of the high rate of fraud on the Internet, many consumers feel more comfortable placing their orders over the phone with a live person. They like knowing there is a person behind the page. You will want a professional sounding phone system. Something more than your cell phone with voicemail. One of the best solutions for web based businesses is a virtual phone system, or virtual PBX. They allow you to forward your calls to any location - home phone, cell phone, VOIP phone - give you a professional sounding main greeting, multiple extensions and voicemail. Many will also allow you to have automated order taking over the phone, send and receive faxes, and receive messages to your email. You want to make sure that the professional business image you are presenting with your web page is continued when your customers call you. Freedom800.com is a good place to start looking at what virtual PBX systems have to offer.

Starting an online business is an exciting time. It can also be a confusing time if you are unfamiliar with what it takes to establish yourself on the web. Getting your domain name, a professional website and setting up an order taking process are some of the first things that you will need to do to get started.

4.2 MARKETING AN E-BUISNESS

Marketing your online store involves more than just registering your Web site with a couple of search engines and waiting for the world to beat a path to your door.

As the number of shoppers on the Internet has grown, so too has the number of Web sites and land-based businesses clamoring for a piece of the multi-trillion-dollar e-commerce pie. As many Internet companies have discovered, even with a multi-million dollar marketing campaign, its difficult to get the attention of Internet users even for just a split second. After all, Internet users are bombarded with so many advertisements every day and see so many Web sites, its hard for any one firm to stand out.

One of the most difficult jobs youll have as an e-commerce merchant is figuring out what blend of offline and online marketing techniques to use to promote your Web site. If youre a small business, that challenge is even greater on a tight budget. The right marketing mix depends on

many factors, including the types of products you are selling, the types of people you are trying to target, and, of course, your marketing budget.

Attracting shoppers to your Web site. Marketing your Web site is not an easy task, nor is it ashort one youll need to work hard and work continuously to make sure that your online store doesnt get lost among the billions of pages of information on the Web.

(1) Know Your Audience!

The key to successful marketing is very simple: know your audience. Before you spend any time or money on marketing, you need to know who your target market is. What types of customers are most likely to buy the types of products you are selling? For example, males or females? What age bracket? What income bracket? Are you trying to reach people with certain interests or skills? Once you know the profile of your typical customer, you need to find ways of reaching customers with that demographic profile. This may involve online advertising, offline advertising, or a combination of the two. But dont even begin to think about spending money on marketing until youve spent time thinking about who you are trying to reach. You may even need to do some market research to uncover this information. We cant emphasize this step enough. Your marketing efforts wont be successful unless you are spending your marketing dollars in the right places.

(2) Your Brand Name

One of the most important marketing assets that you have is the name of your online store. Give it careful consideration. You should pick a name thats easy to remember yet distinct from other similar names on the Internet. Closely related to the issue of picking a name is choosing a suitable domain name. The domain name is the part of your Web site address that appears after www. For example, the domain name for the Office Depot is officedepot.com and the domain name for Eddie Bauer is eddiebauer.com. Office Depots Web site is at www.officedepot.com and Eddie Bauers Web site can be found at www.eddiebauer.com.

To avoid confusing your customers, you will want to have a domain name that is as close as possible to your organizations name. This will also make it easier for customers to find your Web site. For example, customers looking for Eddie Bauers Web site would probably start by

typing www.eddiebauer.com into their Web browsers. In addition to being close to your business name, your chosen domain name should be short, easy for your customers to remember, and intuitive.

Finally, keep in mind that you don't have to have www in your Web address. Some organizations have chosen to drop it entirely, e.g. CBS promotes itself simply as CBS.com.

In addition, you can, with the help of the technical folks who support your site, sometimes use words or characters in front of your actual domain name, and get an extra identity hook that might be unique enough to draw attention to your site. One such example of this is the Web site Beer.com, which gained some attention during the 2000 Olympics. It ran an ad that used the address mmm.beer.com indeed, during the commercial, the graphic showed the www flipping over to become mmm, as the announcer mimicked the mmmm or tastes good sound. There was a huge increase in traffic to the site.

Issues to Consider When Choosing a Name for Your Online Store

- Can you get a Web site address (i.e., domain name) for that name?
- Is the name too long?
- Is the name easy to pronounce?
- Are there other Web sites or online stores with similar-sounding or similar-looking brand names or domain names?
- Is your name unique or distinctive enough?
- Is your name memorable and does it make an impression?
- Is the name consistent with the image you want to project?

How to Get a Domain Name

To get a domain name, you can go to any one of the accredited domain name registers on the Internet, including Register.com (**www.register.com**). You can get a complete list of accredited domain name registrars on the InterNIC Web site at **www.internic.com**. The list can be viewed alphabetically or by geographical location.

You dont need to have a Web site in order to register a domain name and most registrars will hold your domain name for you until you are ready to activate it on your online store. Many browser based storefront solutions allow you to set up a domain name for your online store when you are setting up your account. This removes the need for you to go directly to a domain name registrar.

(3) Offline Marketing

Perhaps the most important piece of advice we can give you in this guide is this: Dont restrict your advertising and promotional efforts to the Web. Online stores often rely too heavily on online advertising at the expense of more traditional advertising vehicles that may actually produce better results.

Think about the types of customers you are trying to attract and what the best methods would be to reach those customers. Rather than spending your money advertising on the Web, you may find that a more effective strategy would be to place advertisements in a couple of well-targeted magazines.

For example, Noggintops (www.noggintops.com), an online hat retailer, has spent very little on Internet advertising. Instead, the company did some marketing research and identified a number of magazines that appealed to the companys target market: outdoorsmen.

It is important to use your imagination when looking for ways to raise awareness of your Web site.

Dont limit yourself to radio, television, and print media. Why not advertise your Web address in buses or subways, or on the transfers handed out by your local transit authority? How about on newspaper polybags (the plastic bags that newspapers are wrapped in when they are delivered to your front door)? Or in movie theatres? Some organizations have even gone so far as to include their Internet addresses on bananas! The possibilities are endless.

(4) Your Retail Store

If your business has a brick-and-mortar retail presence, use it to promote your online store aggressively. Include your Web site on your receipts, invoices, and shopping bags, and print it on

your catalogs and sales literature. Make sure that your Web address is advertised prominently both within your store and outside if you can. Many retailers, unfortunately, dont leverage their retail presence in this way.

(5) Gift Certificates

Brick-and-mortar stores give out gift certificates, so why not online stores too? Consider offering an online gift certificate that your customers can give to a family member or a friend. Gift certificates purchased online make great last-minute gifts because they can be sent by e-mail to arrive almost instantly. The recipient can then visit the stores Web site and apply the gift certificate toward the purchase of any products offered by the store. How does it work? Online stores that offer this service let you pay with your credit card and the gift certificate is delivered to the recipient by e-mail as soon as the payment is authorized. The gift certificate is essentially an e-mail message with a number attached to it. The recipient can redeem the certificate on their next purchase at that online store. When the recipient proceeds to check out of the store, they will be asked to provide their certificate number. The value of the gift certificate will then be deducted from the total amount of the purchase. Electronic gift certificates not only make great gifts theyre a great way to drive new customers into your online store!

(6) Cross-Selling

You should get in the habit of cross-selling products in your online store to increase sales. This means that where possible, product pages on your online store should feature accessories or complementary products that your customers may be interested in. For example, consider what Smith & Hawken has done in their online store (**www.smithandhawken.com**). Whenever a customer views a product, complementary products are displayed on the right-hand side of the page.

For example, a customer may select a bench. Smith & Hawken realizes that customers who are interested in purchasing a bench may also be interested in purchasing a matching chair or table.

That’s why there is a section called Also Look At: where complementary products are displayed, including an armchair and table. As you might expect, if you look at the Web page advertising for the armchair, the bench is recommended as a complementary product.

(7) Product Referral Services

Many people find out about Web sites through word of mouth. So make it easy for your customers to tell other shoppers about your online store.

For example, as customers are browsing through your Web site, they may come across products that their friends, co-workers, or family members may be interested in. Or they may want to tell a friend or family member about a product they would like to receive as a gift. That is why you should make it easy for customers to refer friends and relatives directly to specific product pages on your site. For an excellent example of how this can be done, visit RadioShacks online store (**www.radioshack.com**). At the bottom of every product page on the site is a graphic that says, e-mail this page to a friend. Customers who click on that icon will be taken to another Web page where they are asked to provide the name and e-mail address of a friend. The recipient will receive an e-mail message that invites them to visit RadioShacks online store. A referral mechanism like this is an effective way to bring more people into your Web site.

(8) Affiliate Programs

Many online merchants have built successful affiliate programs for their online stores.An affiliate program involves paying owners of other Web sites a commission for referring customers to your online store. In other words, you reward other Web sites for sending new customers to you. The idea is to find Web sites with visitors who are likely to be interested in your products. To this end, Web site owners usually try to find merchants who sell products or services related to their own Web sites. A Web site with movie reviews may try to affiliate with a merchant who sells movies, and a Web site devoted to golf may align itself with a Web site that sells sporting goods or athletic apparel. Its in a Web site owners best interests to identify merchants with compatible products because it will increase the likelihood of making lots of sales. For example, suppose you sell travel guidebooks. You could sign up travel agencies to your affiliate program and invite them to create links from their Web sites to yours. You would then pay the travel agencies a commission on any book sales and/or leads you get from their customers.

Online retailers with affiliate programs compensate customers in different ways. Some merchants pay affiliates strictly for sales (pay-for-sale), while other merchants compensate

affiliates simply for sending a potential customer their way (pay-per-lead). Other programs may compensate affiliates if a person clicks on an advertisement, regardless of whether that person turns into a lead or ends up purchasing a product. This is called a pay-per-click program.

Affiliate programs can be extremely powerful because they allow you to increase your revenues by having your brand name displayed on dozens if not hundreds of complementary Web sites. There are literally thousands of affiliate programs on the Web. For an example, visit the online store for Staples (**www.staples.com**) and read about their affiliate program. Web sites that sign up can earn a percentage of every sale for referring customers to Staples.com.

(9) Permission Marketing

You may have heard the term permission marketing before. It refers to a method of online marketing where the merchant asks permission from online shoppers to market to them directly by e-mail. Permission marketing is also known as opt-in e-mail.

Permission marketing follows two main principles. First, you only market to those customers who have specifically told you that they are interested in receiving e-mail messages from you. Second, you must give away something in order to get a customers e-mail address. In other words, shoppers are more likely to give you their e-mail address if you give them an incentive or reward for doing so. This incentive could be a discount on a future purchase, entry in a sweepstakes or contest, or just the promise of relevant advice by e-mail. The easiest way to undertake permission marketing is by establishing a mailing list that customers can join. You can then use the mailing list to send out promotional messages to your customers. The trick is to give your customers an incentive to join your mailing list. For an example of how a permission-based e-mail marketing program can be implemented, consider what Payless ShoeSource (**www.payless.com**) did on their online store. They ran a contest on their home page for a dream trip to Tahiti. Customers were invited to enter their e-mail address into a box on the screen. Once a customer entered his/her e-mail address, a new page appeared inviting the customer to join Payless ShoeSource's mailing list. The contest was the hook to get customers to spend a few minutes filling out the form that is required to join the mailing list. Once customers joined the Payless mailing list, they were automatically entered into the vacation contest. Keep in mind that

if you are going to set up a mailing list for your customers, you should clearly tell your potential customers how they can leave the list, and about any other conditions that might apply to the list.

(10) Search Engines and Web Directories

Many online shoppers use a search engine or a Web directory when they are trying to find something on the Internet. A search engine is a Web site that indexes the contents of millions of Web pages. A Web directory, on the other hand, organizes Web sites by category so that they can be easily browsed by Internet users. Unlike search engines, directories are usually compiled by human beings. In the following table, we have listed the names and addresses of the most popular search engines and Web directories. Making sure that your Web site is registered with all of these sites is one of the most important things you can do to draw traffic to your store. Why all of them? Your customers (and potential customers) wont all be using the same search engine or Web directory. Some people use Excite, some use AltaVista, some use Lycos, etc. By registering with all the major search engines and Web directories, you have the best chance of being found by online shoppers regardless of what search engine or Web directory they are using.

Search Engine and Directory Databases

Before you submit your site to any search engine or Web directory, you need to understand how their databases are developed. A search engine database is significantly different from a directory database. Automated computer programs called spiders develop search engine databases. These programs scour the Internet indexing the full contents (i.e., all of the words on a page) of the millions of Web pages they find. This is also true of Web directory sites, most of which have a search engine database in addition to the directory database. As an Internet merchant, the ideal situation is to have your Web site included in both databases of any search engine or directory Web site.

Submitting Your Web Site to a Search Engine Database

When you launch a Web site, you want to make sure that it is included in the search engine databases of both search engine Web sites and directory Web sites. There is a good possibility that the spider programs that these Web sites use will find your Web site, index it, and add it to the search engines database. However, it could take months for these spiders to discover your

site, if they ever do. For these reasons, its generally a good idea to visit each search engine and directory Web site and manually submit your Web site for inclusion in their search engine databases.

(11) Search Engine Optimization

As we noted at the beginning of this guide, there are billions of Web pages on the Internet and thousands upon thousands of online stores, all clamoring for attention. When you submit your Web site to a search engine, you typically dont have any control over where your Web site will show up in the sites results list when someone searches for your company name or a keyword related to your business. For example, suppose you open an online store selling pasta products. If someone goes to a search engine, and types in the word pasta, you are not going to be very happy if your Web site shows up on the seventh page of results. Most people won't bother looking past the second or third page of results when they are doing a search on the Internet. In fact, many people won't even bother looking beyond the first page of results. This means that if your Web site doesn't show up in the top ten or so results for a specific search such as pasta, the chances of your Web site being seen by Internet users diminishes considerably. Hence, an important part of online marketing involves a process known as search engine optimization ensuring that your Web site receives prominent placement on all the major search engines. Ideally, you want your Web site to show up on the first page of results when a potential customer searches for a keyword related to your business.

Before we go any further, you need to understand three things. First, there is no simple method or magical formula for achieving good rankings on search engines. Second, every search engine uses different ranking criteria. This is why the same search performed on different search engines will yield different results. It is also why your Web site may be ranked number one on one search engine but appear in the twentieth position on another. Third, search engines are constantly changing the algorithms they use to index Web sites, so your sites ranking on any given search engine may be in a continual state of flux. Most search engines provide some information on their Web sites to help you understand how they rank Web pages. Visit each search engine, read the help files, and try to accommodate as many of the suggestions as possible. For example, the Lycos search engine (**www.lycos.com**) has a page of information on

its Web site with several tips and pointers to help you optimize your Web sites ranking in their index.

Using a Search Engine Optimization (SEO) Company

Many Web site owners, sometimes in sheer desperation or frustration, have enlisted professional help to try and improve their rankings on search engines. The reason that search engine optimization (SEO) firms are in such demand is explained well by one of many companies that specializes in search optimization: ...Over the years the search engines and directories have gotten smarter and keep changing to the point where we have to work very hard to keep up to date on what techniques work best (or at all). Search engine optimization has become a very complex, sophisticated practice that requires constant research, practice, and reevaluation to be effective. In other words, understanding how search engines work is a complex business and most Web site owners dont have the time, inclination, or skill to try and manage their own Web site rankings. Search engine optimization has become a popular business in recent years. There are also many small organizations that offer search engine optimization services. Many Web design and online advertising firms have also entered this market.

(12) Online Shopping Directories

Most of the major search engines and Web directories have shopping areas on their Web sites that showcase selected merchants and that list hundreds of merchants by product category. Many Internet users use one of these shopping directories when looking for online merchants to buy from, so its a good way to get exposure for your online store. However, to get included in a search engine or Web directorys shopping directory, or to become one of its featured stores or premier merchants, you usually need to be an advertising partner or be using the sites online storefront software. To become an advertiser, you will need to get in contact with the search engine or directorys advertising department for details about pricing. America Online, for example, has advertising agreements with a number of large retailers that give these retailers prominent positioning on AOLs shopping directory. It is important to point out that these types of advertising opportunities are often targeted are larger, established retailers as opposed to small businesses, so depending on your advertising budget and the size/profile of your business, you may find that this type of advertising opportunity is not practical or affordable.

(13) Online Advertising and Sponsorships

One of the most popular online marketing strategies is to advertise on or sponsor other Web sites that attract the types of people who may be interested in buying your products and services. Suppose, for example, you sell luggage products. Why not advertise your online store on Web sites that attract travelers? For example, you might want to approach a travel Web site, such as one of the popular travel-booking services like Travelocity.com, about sponsoring a section of their site. In addition, many of the popular travel magazines like Cond Nast Traveler have their own Web sites, and accept advertising. Most Web sites that accept advertising have a section somewhere on the site that provides contact information for advertising inquiries as well as a general overview of advertising and sponsorship opportunities.

Before choosing to advertise on or sponsor any Web site, make sure that the site is reputable. You dont want to advertise on any Web site with a doubtful reputation or poor credibility. You should also obtain audited statistics that tell you how many visitors the site receives on a daily, weekly, and monthly basis. Also try to obtain as much demographic information as you can data that will tell you what types of people the site attracts, including average age, income, and spending habits.

Banner Advertisements

Online advertisements come in all different sizes and shapes, just like newspaper ads. However, online advertising often appears in the form of a banner ad. A banner ad is a small rectangular graphic that can either be animated or static. You can design it yourself, or have someone design it on your behalf its basically a small Web page or graphic. People can click on a banner ad to be immediately connected to the advertisers Web site.

Banner advertisements are usually sold on the basis of page views (every time a person accesses the Web page, that is considered a page view), and page views are usually purchased on a cost per thousand (CPM) basis. For example, if you are told by a Web site that the cost of banner advertising is $60 per CPM, this means that you pay $60 for every thousand page views. This might represent a thousand people looking at that page or it might mean five hundred people looking at that page two times each. There are hundreds of thousands of Web sites on the Internet that accept banner advertising. The key is to find Web sites that attract the types of

customers you are interested in reaching. There is no sense buying banner advertising on a Web site if its visitors arent in your target market.

Creating Your Own Banner Ad Campaign

Larger Web sites may require a minimum advertising buy of several thousand dollars. For a small business, this can be prohibitive. An alternative to purchasing banner ads through one of the big search engines and directories is to use a service like Microsofts Small Business Center (**www.microsoft.com/smallbusiness/products/online/bannerads**) where small businesses can create their own banner advertising campaigns and place them on select Web sites for a smaller up-front investment.

(14) Keyword-Based Advertising

Many Web sites, including many of the major search engines and Web directories, offer keyword based advertising. Here's how it works. You purchase one or more words and/or phrases related to your business. When a customer searches for any of those words, an advertisement for your Web site will appear. The advertisement may be a banner ad or another type of online advertisement that you create. For example, suppose your own a business that sells pools and spas. You could purchase the word pools on Yahoo! so that whenever someone searches for that word, a banner ad for your company will appear on the search results screen. Keyword-based advertising doesn't necessarily involve banner ads. For example, Google (**www.google.com**), one of the Internet most popular search engines, allows you to create text ads for your company that will be displayed whenever an Internet user searches for a keyword that you've selected. Googles program, called AdWords (**adwords.google.com**), is affordable for small businesses because there is no monthly minimum spending limit and it costs just $5 to set up your account.

Keyword Research

Part of the challenge in using keyword-based marketing on the Internet is to pick the keywords that your customers are most likely to be using when they are doing searches on search engines and Web directories. This will likely require a bit of brainstorming on the part of yourself and your staff.Thats your job. To help you brainstorm, you might want to check out a few of the search engines that reveal what Internet users are searching for. For example, Lycos has a service

called The Lycos 50 Daily Report (**50.lycos.com**) that shows you what people are searching for on the Lycos search engine. Every week, Lycos publishes the 50 most popular searches from the past week.

(15) Links from Other Web Sites

One of the least expensive online marketing techniques, but perhaps one of the most effective, is getting links from other Web sites. Contact suppliers and manufacturers you work with to see if they will link from their Web sites to yours. Why is this important? Customers often visit the Web sites of manufacturers or suppliers when they are researching a purchase. If the manufacturer provides a link from their Web site to yours, the customer may end up making the purchase online from you. This manufacturer benefits from the sale as well, given that you are selling more product, so its in the manufacturers best interest to link to you. You should also contact any industry associations you belong to and ask if they will link to you. The idea is to try and get as many Web sites to link to you as possible. As noted earlier, this can even help you with your placement on search engines since many search engines take a sites links into account when they decide where to rank it.

(16) Monitor Activity on Your Web Site

Once you invest in an online store, you owe it to yourself to monitor how well your investment is paying off. The number of sales you receive is only part of the picture.

You also want to be able to track the number of people who visit your online store, where they come from, and which search engines and directories they use to find you. This information is vital to your business because it will help you assess whether your marketing activities both online and offline are succeeding or failing. If you dont already receive daily traffic statistics from your Internet service provider, Web hosting service, or online store service, or if the reports you receive dont provide enough detail, consider signing up for one of many the third-party Web site analysis services. In the box below, we have listed some of the more popular programs that will allow you to monitor how your customers are using your Web site.

Two thirds of all online shoppers abandon their shopping carts before making a purchase. A software program like the ones listed above can help you analyze what path customers are taking through your site and what the most popular exit pages are so that you can minimize customer abandonment (the exit page is the last page visited by the customer before the customer leaves your site). One powerful Web site tracking program is WebTrends (**www.webtrends.com**). Webtrends has a number of different versions of its program that will allow you to track sales activity on your Web site. WebTrends is capable of generating very detailed sales reports for your Web site. For example,

4.3 A FRAMEWORK FOR ENTERPRISE ARCHITECTURE

The Enterprise Architecture model provides an extension on the basic communication based business paradigm as proposed by Medina-Mora and Dietz. The model is composed of four interrelated aspect layers and a background providing layer. The top layer describes the reason for existence of the organisation. This layer is added because the business process structure of an organisation cannot be understood without understanding the context and the goal of the organisation The layer contains a behavioural description of the definition of the organisation as described by the mission and the strategy to reach this mission. This top layer provides a point of reference for the activities in the underlying level. The business architecture layer contains a description of business processes in the organisation. The business architecture provides an operationalisation of the mission and strategy layer. On the basis of the expected behaviour, as described in the mission and strategy layer, the construction of the business processes is laid out. On its turn, the business architecture provides the behavioural constraints for the information architecture. Founded in the business architecture, the information architecture extends the business processes with a necessary information infrastructure. In other words, it provides a detailed description of the information that is needed to execute the business processes. At the lowest level, the ICT infrastructure, which also includes software architectures, and the organisational structure are described. This level provides the tools with which the levels above are realised. This description may contain machines, applications and application structures, workflow procedures, but also people in organisational functions.

The four layers are embedded in a layer that describes the culture of the organisation. The culture can be considered to be the glue between the other layers of the Enterprise Architecture model. Whereas the other layers are founded in formal action oriented communication in the organisation, culture is created by informal precondition creating communication between the elements in the organisation.

In line with the guidelines for postulating information architectures (Land et al, 1999), an architectural description of an organisation addresses three different aspects: models, constraints and decisions. Models describe the current state of affairs of the organisation. In other words, what is done when and how? The models describe the structure of the organisation at each level of the Enterprise model. A precondition for the models is that they facilitate manipulations to create an optimised situation. This presumes that the models have some kind of formalised basis. The architecture models also need to be as stable as possible, so that they can serve as a basis for multiple decisions. Constraints describe internal or external elements that restrict changes to the organisation. These constraints can be uncontrollable for the organisation like for example laws, economic principles, technical standards, or ethical and cultural norms, but the constraints may also be within the change potential of the organisation. The last constraints mostly originate from inside the organisation. The proposed architecture has to obey these internal and external constraints. The last aspect of an architectural description is formed by the decisions that organisations take about the direction of the organisation and therewith the architecture they chose.

In an architectural description of Enterprise Architecture, the three aspects are combined with the different layers of the Enterprise model. This means that each of the layers is described according to these guidelines. Table 1 below describes the result of the cross-correlation of the enterprise layers and the architectural aspects. The cells contain examples, and the list is not exhaustive.

	Models	Constraints	Decisions
Mission/strategy	Strategic business models, e.g. Balanced Scorecard, SWOT, Value Chain	Trading laws, macro economy, core competencies, supply chain characteristics	Improved competitive position, changed needs and increased resources
Business architecture	Business process models, e.g., Soft Systems Methodology, Petri-Nets, DEMO	Resources, business procedures, business rules, business objects	Increased efficiency and effectiveness of commitments and action in processes
Information architecture	Information models, e.g. ER, ORM, Yourdon, Information Engineering, IDEF	Availability and integrity of internal and external information sources, workflow procedures	Increased availability of information, improved management information
ICT/organisation architecture	Technological/organisational models, e.g. UML, Organisation Charts, Task diagrams	Technical standards and technical possibilities. Organisational function requirements	Increased speed, reliability, security and availability of ICT, changed organisational configuration
Culture	Cultural models, e.g. Socio-technique, socio-mapping	Qualifications and personality	Changed organisational

	Models	Constraints	Decisions
		of the employees	norms and values

Table 1: Possible elements in an architectural description

In the architectural description, the Constraints and the Decisions at each level can be formulated as principles or standards. Principles are textual statements that describe the constraints the organisation is currently facing, or decisions based on the beliefs about the future direction of the organisation. Standards are a more formalised description of the principles and therefore more suitable to guide, qualify, and often quantify the architectural direction. Standards restrict an architecture by providing measurable and testable performance criteria, metrics for business and IT practices, and specifications for IT products, protocols, and methods. In analogy to the division of standards and principles, one can use more or less formalised models in combination with texts to complete the architectural description of the current situation of the organisation. However, in order to restructure the elements in the organisation, formalised models are preferred.

The architectural description forms the basis for the process of architecturing. In an architectural process the existing structures of an organisation are transformed into a desired architecture. The process of creating a new architecture for an organisation is guided by the decisions, and limited by the constraints that were described in the architectural description.

The result of the process of architecturing is a new architecture description of the organisation. This new enterprise architecture forms the foundation for the realisation of possible new strategic elements, business processes, information/ICT or organisational infrastructure, but also for the culture that binds the organisation together. The new architecture can be expressed in new models, but it can also be expressed in textual description formulated as principles and standards.

Electronic Services

The idea of electronic services is as old the telegraph, but over the years we have observed important changes of the magnitude of the possibilities.

When we analyse E-service initiatives, we can identify three different objectives: E-advertising, E-commerce and E-business. The most low-key application of E-services can be labelled as electronic advertising. A web-site is used to position the organisation with electronic means. The web-site is used as a replacement for the traditional corporate brochures of an organisation. Web-sites of this type are mainly passive and they provide very little added value over the traditional paper brochures. In the second stage, we observe that E-services are used to support the current business processes of an organisation. Mostly it is observed that web-sites are used to support the sales process. When engaged in E-commerce, the traditional channel is replaced by electronic means. When visiting the organisations web-site, the customer does not only get information about the organisation as with E-advertising, but the customers can also communicate with the organisation and engage in business transactions via the web-site. In the case of E-business, the web-site is used to create business that was not existed in the organisation before the web-site was instantiated. In other words, electronic means are used to alter the business objectives of the organisation and can create a new position in the value chain. The three applications of E-services are displayed in figure 2 below. In this figure we also observe that the applications are overlapping. This means that an organisation cannot engage in E-business when they have not included E-commerce and E-advertising. The figure also shows that the potential business benefits are expected to increase with the choice of the different E-services.

The Enterprise Architecture model provides a good framework to further position the three types of E-services. In E-advertising, the service is located in the lower layer of the Enterprise Architecture model because the information architecture, the business architecture and the mission/strategy are not affected. E-commerce relates to the information infrastructure and the business process structure, but the business is not altered. This is only done when the organisation engages into E-business. Figure 3 illustrates the three types of E-services within the Enterprise model. It is important to realise that also in this model the three types of E-services overlap.

4.4 DISASTER RECOVERY PLAN

The terrorist attacks of September 11, 2001 have taught many businesses one thing: prepare for the unexpected. Companies must take steps to make their businesses less dependent on a single office or data infrastructure. Consider implementing technologies that can quickly duplicate company data at a remote location. Gartner Research predicts that two out of five enterprises that experience a disaster the magnitude of the World Trade Center attack will go out of business within five years. Therefore, it is more important than ever to either build a redundant IT facility, or select an IT outsourcing service provider for disaster recovery.

Traditional implementation of Disaster Recovery and Business Continuity Planning are rather complex and extremely expensive. That is why many small to medium size companies do not have a Disaster Recovery and Business Continuity Plan in place. Fortunately, new Internet technologies are reducing the cost and complexity of implementing the Disaster Recovery and Business Continuity Plans. For a few hundred dollars a month, your mission critical data can be replicated to a secure, remote data center in real time. None of your data will be lost when a disaster hits your primary IT facility. For a few thousand dollars a month, you can mirror your mission-critical IT systems at a remote data center (a hot-site). When your primary IT facility goes down, you can switch your IT systems to the mirrored site in a few minutes or less. With Internet DNS technology, you can even make the fail over to the mirror site transparent to end-users. End users will not need to make any changes or feel any impact on their productivity when a disaster hits. Internet VPN technology makes data transfer to a remote site secure and is HIPPA compliant.

Virtual Servers: Vitual server images based on VMWare, XEN and Microsoft Hyper-V virtualization technology can be hosted at Cybercon data center. These virtual servers can be uploaded, activated, updated 24 hours a day 7 days a week. There are firms to handle virtual server farms from a few virtual servers to thousands of virtual servers.

Hot-Site: A mirror's system of customer production eBusiness or IT system will be located at Cybercon's data center. System hardware is provided by either the customer or Cybercon and data is frequently synchronized via a network using a choice of industry leading data

synchronization and replication software. When customer's production system goes down, services will be switch to the mirrored site in a few minutes or less. This service is designed for businesses that cannot tolerate any downtime in their mission-critical environments. Additional benefits to have a Hot-Site are: Testing upgrades, patches, new setups at the backup Hot-Site before you apply them to your live production eBusiness or IT system.

Cold-Site: Customer will provide a list of hardware needed to run its mission critical eBusiness or IT system. Cybercon will have such hardware ready immediately upon customer's declaration of a disaster. We keep customer specified servers and network equipment in our data center. Customer redundant systems can be powered up and activated within minutes of notices. It works 24x7x365!

Online Data Storage: Critical data (databases, server images, ... etc) is replicated or backed up to Cybercon backup storage systems. Customer systems are restored from such backup data to hardware that will be purchased by customer and delivered to Cybercon's data center upon declaration of a disaster.

Relationship to the Business Continuity Plan

The Business Continuity Plan may be written for a specific business process or may address all mission-critical business processes. The BCP is an umbrella plan whose major sub-components include the Disaster Recovery Plan. Information systems are considered in the BCP only in terms of their support of those business processes. A Business Continuity Plan (BCP) consists of the following component plans:

Business Resumption Plan

Occupant Emergency Plan

Incident Management Plan

Continuity of Operations Plan

Disaster Recovery Plan

The Business Resumption Plan, Occupant Emergency Plan, and Continuity of Operations Plan do not deal with the Information Technology (IT) Infrastructure. The Incident Management Plan (IMP), which does deal with the IT infrastructure, establishes structure and procedures to address cyber attacks against an organization IT systems and generally does not involve activation of the Disaster Recovery Plan.

4.5 DISASTER RECOVERY PROCESS

A disaster is defined as a sudden, unplanned catastrophic event that renders the organizations ability to perform mission-critical and critical processes, including the ability to do normal production processing of systems that support critical business processes. A disaster could be the result of significant damage to a portion of the operations, a total loss of a facility, or the inability of the employees to access that facility.

The disaster recovery process consists of defining rules, processes, and disciplines to ensure that the critical business processes will continue to function if there is a failure of one or more of the information processing or telecommunications resources upon which their operations depends. The following are key elements to a disaster recovery plan:

- Establish a planning group
- Perform risk assessment and audits
- Establish priorities for applications and networks
- Develop recovery strategies
- Prepare inventory and documentation of the plan
- Develop verification criteria and procedures
- Implement the plan

IT Disaster Recovery Planning Process

Developing a technical disaster recovery strategy is just one step in the overall IT Disaster Recovery Planning process. This process is common to all IT systems and utilizes the following six steps:

1. Develop the Business Contingency Planning Policy and Business Process

   Priorities

2. Conduct a Risk Assessment

3. Conduct the Business Impact Analysis (BIA)

4. Develop Business Continuity and Recovery Strategies

5. Develop Business Continuity Plans

6. Conduct awareness, testing, and training of the DRP

7. Conduct Disaster Recovery Plan maintenance and exercise

Fundamentals of a Disaster Recovery Planning Process

The fundamental basis of Disaster Recovery Planning is to develop a methodology beginning with project planning and loss avoidance and following through to ongoing testing and maintenance.

Fundamental 1 - Preparing for the Planning Process

A. Executive Management Meets to define Objectives and Goals of a Disaster Recovery Plan

B. Senior Management appoints Disaster Recovery Specialist

C. Prepare Business/Process Effort Chart & Project Plan

D. Executive Management communicates to all Directors and Managers of upcoming Disaster Recovery

Planning Program

E. Receive Department Head Commitment to Goals of Disaster Recovery Planning

Fundamental 2 - Preparing Departments for Planning

A. Department Directors and Managers appointment Subject Matter Experts

B. Disaster Recovery Specialist meets with Department Directors and Managers to Discuss Objectives

Fundamental 3 - Risk Assessment

A. Disaster Mitigation (Risk Avoidance)

B. Insurance Evaluation (Risk Transfer)

C. Security Assessment (Risk Reduction)

Fundamental 4 - Business Impact Analysis

A. Subject Matter Experts, the Disaster Recovery Specialist and Department Directors and Managers Identify Critical Business Processes with the use of Business Impact Analysis tools

B. Subject Matter Experts, the Disaster Recovery Specialist and Department Directors and Managers define Interdependencies (Inputs and Outputs)

C. Executives Prioritize Recovery Objectives Recovery Time Objectives

Fundamental 5 - Prioritize Critical Business Process

A. Create Score Card of Critical Business Processes

B. Department Manager prioritizes all Critical Business Processes in their view of what is necessary to recover basic services or processes

C. The Disaster Recovery Technical Committee evaluates the strategy applied by the Department Directors and Managers

D. Department Manager makes presentation on Critical Business Processes and their priority to Executive Management along with resource requirements and interdependences with other departments

E. The Disaster Recovery Technical Committee identifies minimum workstation requirements

Fundamental 6 - Develop Recovery Strategy

A. Critical Business Processes are submitted for review to their Executives and their priority are reviewed Each Critical Business Process is either approved, rejected, modified or reprioritized

B. Executives meet and prioritize companywide Critical Business Processes

C. Upon approval of companywide recovery strategy, Department Directors and Managers are informed of the priorities

D. Disaster Recovery Specialist identifies Critical Business Partners, Vendors, and develops a budget.

E. The Disaster Recovery Specialist and the Department Directors and Managers review Critical Business Partners, Vendors, and the budget.

F. Executives, Department Directors and Managers reviews the information supplied, including the budget.

G. Executives meet to determine minimal recovery requirements that can be met or priorities change. Can the company afford to recover each Critical Business Process identified? Does the sequence of recovery change the cost of recovery? The Disaster Recovery Specialist and the Department Directors and Managers should be available for their input.

H. The Disaster Recovery Specialist and the Department Directors and Managers may need to refine their Disaster Recovery Plan Strategy.

Fundamental 7 - Plan Development

A. Develop Disaster Recovery Plan Format

B. Identify Teams and Team Members

C. Identify vendors and other contacts

D. Collect data for Disaster Recovery Plan

E. Prepare draft of Disaster Recovery Plan

F. Submit draft for approval to Department Directors and Managers

G. Prepare final copy of Disaster Recovery Plans & obtain Sign-Off from Senior and Executive Management

H. Obtain Involvement and assistance for implementation from Vendors and Suppliers as needed

Fundamental 8 - Test and Maintain Plan

A. The Disaster Recovery Specialist develops and communicates Disaster Recovery Plan maintenance schedule for business units testing

B. The Disaster Recovery Specialist develops and communicates Testing Formats

C. Test and maintenance schedules are posted and followed

D. The Disaster Recovery Specialist executes and update testing formats

E. The Disaster Recovery Specialist, Subject Matter Experts and Department Heads update Disaster Recovery Plans as required.

4.6 SUMMARY

This unit introduces the essential steps required to start an e-Business and the framework of Enterprise Architecture. The disaster recovery planning process has been covered extensively. Some concepts based on Search Engine Optimization are also covered in this unit.

4.7 KEYWORDS

e- Business, Enterprise architecture, disaster planning

4.8 REVIEW QUESTIONS

1. What are the essential steps required to start an e-Business?
2. Explain the framework of Enterprise Architecture.
3. What are the fundamental steps for Disaster recovery planning process?
4. Write a short note on keyword based advertising?

5. What do you mean by Search Engine Optimization?

4.9 REFERENCES / SUGGESTED READINGS

• Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc.

• Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.

• Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.

• Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.

UNIT 5: DESIGNING WEBSITES

Structure

5.0 OBJECTIVES

After studying this unit we will be able

- To understand the web design strategies.
- To understand the life cycle of life building with different stages.

5.1 WEBSITE DESIGN STRATEGY

Web design has evolved from static hypertext publishing in the early days to dynamic multimedia, Web database application servers. More importantly, new business models that bring savings, revenues, and customer relationships are being incorporated into commercial Web site design. There are two generic Web site design strategies:

- informational/communicational strategy
- on-line/transactional strategy

5.1.1 Informational/communicational design:

Definition

This approach is for companies to use the Web as a supplement to traditional marketing, delivering additional benefits to customers and building relationships with them.

Promotion measures and ways

1. Putting companies' catalog on-line

2. Building broad awareness and image

3. Using the Web as a cost-effective way to augment their core products with related information and service function.

4. Obtaining cost savings from automating routine customer services.

Advantages:

1. Providing large quantities of information to customers

2. Giving a company an instant global presence and attracting people toone's ad, some of them are not the company's target market, but potentially will be.

3. Opening a new communication channel allowing a company to develop further relationships with customers.

4. All at a reasonable cost.

5.1.2 On-line/transactional design

Definition

This approach is for companies to use the Web to construct ``virtual business'' ± independent, profitable ventures that exist only on the Internet.

Promotion measures and ways

1. Creating a retail presence larger than any physical store could

2. Creating a virtual business providing extra information in a form competitors cannot imitate

3. Creating a virtual business that takes a specialty product or collectible and sell sit worldwide

4. Creating a virtual business that uses the Internet to produce superior economic benefits to customers that competitors cannot imitate

5. Creating a virtual business providing convenience to customers that competitors cannot match.

Advantages:

1.Providing a larger or more specialized selection of products than competitors can offer

2. Providing higher quality and higher quantity information, more economic benefits, and more convenience than competitors can offer.

3. Providing a sense of community for customers.

5.2 THE LIFE CYCLE OF SITE BUILDING FROM PAGE TO STAGE

A system development process can follow a number of standard or company specific frameworks, methodologies, modeling tools and languages. Software development life cycle normally comes with some standards which can fulfill the needs of any development team. Like software, web sites can also be developed with certain methods with some changes and additions with the existing software development process. Let us see the steps involve in any web site development.

1. Analysis

Once a customer is started discussing his requirements, the team gets into it, towards the preliminary requirement analysis. As the web site is going to be a part of a system, It needs a complete analysis as, how the web site or the web based application is going to help the present system and how the site is going to help the business. Moreover the analysis should cover all the aspects especially on how the web site is going to join the existing system. The first important thing is finding the targeted audience. Then, All the present hardware, software, people and data should be considered during the time of analysis. For example, if a company XYZ corp is in need of a web site to have its human resource details online, the analysis team may try to utilize the existing data about the employees from the present database. The analysis should be done in the way, that it may not be too time consuming or with very less informative. The team should be able to come up with the complete cost- benefit analysis and as the plan for the project will be an output of analysis, it should be realistic. To achieve this analyst should consult the designers, developers and testers to come up with a realistic plan.

Input: Interviews with the clients, Mails and supporting docs by the client, Discussions Notes, Online chat, recorded telephone conversations, Model sites/applications etc.,
Output: 1. Work plan, 2. Cost involved, 3. Team requirements, 4. Hardware-software requirements, 5. Supporting documents and 6. the approval.

2. Specification Building:

Preliminary specifications are drawn up by covering up each and every element of the requirement. For example if the product is a web site then the modules of the site including

general layout, site navigation and dynamic parts of the site should be included in the spec. Larger projects will require further levels of consultation to assess additional business and technical requirements. After reviewing and approving the preliminary document, a written proposal is prepared, outlining the scope of the project including responsibilities, timelines and costs.

Input: Reports from the analysis team.
Output: Complete requirement specifications to the individuals and the customer/customer's representative.

3. Design and development:

After building the specification, work on the web site is scheduled upon receipt of the signed proposal, a deposit, and any written content materials and graphics you wish to include. Here normally the layouts and navigation will be designed as a prototype.

Some customers may be interested only in a full functional prototype. In this case we may need to show them the interactivity of the application or site. But in most of the cases customer may be interested in viewing two or three design with all images and navigation.

There can be a lot of suggestions and changes from the customer side, and all the changes should be freezed before moving into the next phase. The revisions could be redisplayed via the web for the customer to view.

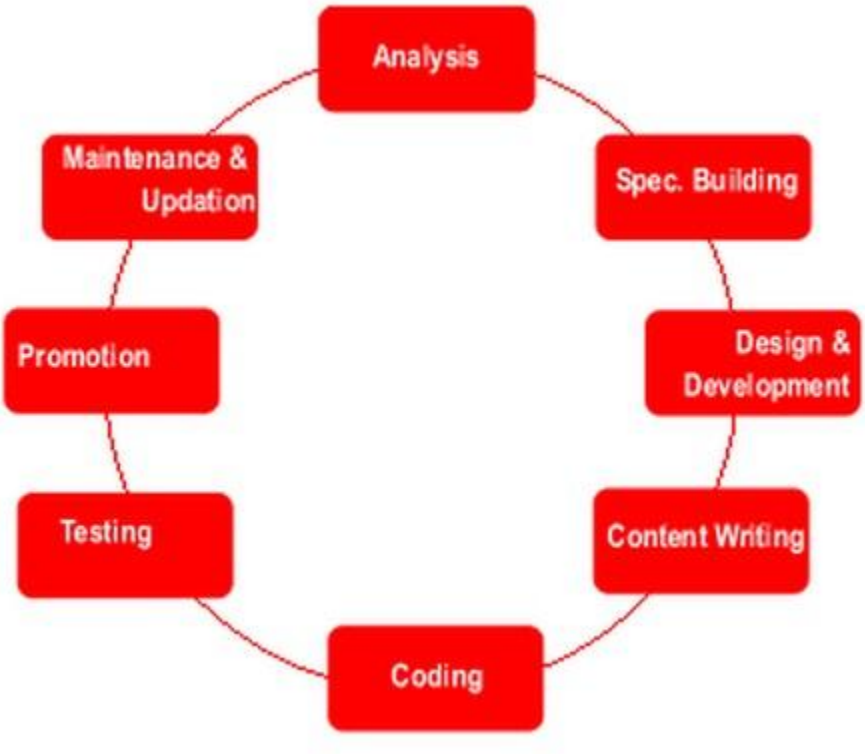
As needed, customer comments, feedback and approvals can be communicated by e-mail, fax and telephone.

Throughout the design phase the team should develop test plans and procedures for quality assurance. It is necessary to obtain client approval on design and project plans.

In parallel the Database team will sit and understand the requirements and develop the database with all the data structures and sample data will also be prepared.

Input: Requirement specification.

Output: Site design with templates, Images and prototype.



4. Content writing:

This phase is necessary mainly for the web sites. There are professional content developers who can write industry specific and relevant content for the site. Content writers to add their text can utilize the design templates. The grammatical and spelling check should be over in this phase.

Input: Designed template.

Output: Site with formatted content.

5. Coding:

Now its programmers turn to add his code without disturbing the design. Unlike traditional design the developer must know the interface and the code should not disturb the look and feel of the site or application. So the developer should understand the design and navigation. If the site is dynamic then the code should utilize the template. The developer may need to interact with the designer, in order to understand the design. The designer may need to develop some graphic

buttons when ever the developer is in need, especially while using some form buttons. If a team of developers is working they should use a CVSto control their sources. Coding team should generate necessary testing plans as well as technical documentation. For example Java users can use JavaDoc to develop their documents to understand their code flow. The end-user documentation can also be prepared by the coding team, which can be used by a technical writer who can understand them, writes helps and manuals later.

Input: The site with forms and the requirement specification.
Output : Database driven functions with the site, Coding documents.

6. Testing:

Unlike software, web based applications need intensive testing, as the applications will always function as a multi-user system with bandwidth limitations. Some of the testing which should be done are, Integration testing, Stress testing, Scalability testing, load testing, resolution testing and cross-browser compatibility testing. Both automated testing and manual testing should be done without fail. For example its needed to test fast loading graphics and to calculate their loading time, as they are very important for any web site. There are certain testing tools as well as some online testing tools which can help the testers to test their applications. For example ASP developers can use Microsoft's Web Application Test Tool to test the ASP applications, which is a free tool available from the Microsoft site to download.

After doing all the testing a live testing is necessary for web sites and web based applications. After uploading the site there should be a complete testing(E.g.. Links test)

Input: The site, Requirement specifications, supporting documents, technical specifications and technical documents.
Output: Completed application/site, testing reports, error logs, frequent interaction with the developers and designers.

7. Promotion:

This phase is applicable only for web sites. Promotion needs preparation of meta tags, constant analysis and submitting the URL to the search engines and directories. There is a details article in this site on site promotion. The site promotion is normally an ongoing process as the strategies

of search engine may change quite often. Submitting a site URLs once in 2 months can be an ideal submission policy. If the customer is willing, then paid click and paid submissions can also be done with additional cost.

Input: Site with content, Client mails mentioning the competitors.
Output: Site submission with necessary meta tag preparation.

8. Maintenance and Updating:

Web sites will need quite frequent updations to keep them very fresh. In that case we need to do analysis again, and all the other life cycle steps will repeat. Bug fixes can be done during the time of maintenance. Once your web site is operational, ongoing promotion, technical maintenance, content management & updating, site visit activity reports, staff training and mentoring is needed on a regular basis depend on the complexity of your web site and the needs within your organization.

Input: Site/Application, content/functions to be updated, re-Analysis reports.
Output: Updated application, supporting documents to other life cycle steps and teams.

5.3 SUMMARY

This unit introduces various design strategies namely**,** on-line/transactional design and Informational/communicational. A detailed explanation of lifecycle of site building has been given in this unit.

5.4 KEYWORDS

Life Cycle, Web Design, Design Strategies

5.5 REVIEW QUESTIONS

1. Explain the life cycle of Site building from Page to Stage with neat diagram.

2. Elaborate on-line/transactional design with its advantages.

3. Explain in Informational/communicational design.

5.6 REFERENCES / SUGGESTED READINGS

- Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc.
- Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.
- Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.
- Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.

UNIT 6: BUILDING A CARPORATE WEBSITE

Structure

6.0 OBJECTIVES

After studying this unit we will be able

- To understand the how to build the corporate websites.
- To understand the legal issues which are related to e commerce.
- To understand about digital signatures.

6.1 CORPORATE WEBSITE

A **corporate website** or **corporate site** is an informational website operated by a business or other private enterprise such as a charity or nonprofit foundation.

Corporate sites differ from electronic commerce, portal, or sites in that they provide information to the public about the company rather than transacting business or providing other services. The phrase is a term of art referring to the purpose of the site rather than its design or specific features, or the nature, market sector, or business structure of the site operator.

Nearly every company that interacts with the public has a corporate site or else integrates the same features into its other websites. Large companies typically maintain a single umbrella corporate site for all of their various brands and subsidiaries.

Corporate websites usually include the following:

- A homepage
- A navigation bar or other means for accessing various site sections
- A unified look and feel incorporating the company logos, style sheets, and graphic images.

An "about us" section with some or all of these:

- A summary of company operations, history, and mission statement
- A list of the company's products and services
- A "people" section with biographical information on founders, board members, and/or key executives. Sometimes provides an overview of the company's overall workforce.
- A "news" section containing press releases, press kits, and/or links to news articles about the company
- An "investor" section describing key owners / investors of the company

A list of key clients, suppliers, achievements, projects, partners, or others

- Pages of special interest to specific groups. These may include:
- An employment section where the company lists open positions and/or tells job seekers how to apply
- Investor pages with the annual report, business plan, current stock price, financial statements, overview of the company structure, SEC filing or other regulatory filings
- Pages for employees, suppliers, customers, strategic partners, affiliates, etc.
- Contact information. Sometimes includes a feedback form by which visitors may submit messages
- A terms of use document and statement of intellectual property ownership and policies as they apply to site content
- A privacy policy

Effective Corporate Websites

From mythology to motorcycles, from cabinet-making to cross-stitching, every specialized or topical Website knows its readership. It's a safe bet that any reader who hits the site and stays is interested (however slightly) in the topic at hand.

A corporate Website, on the other hand, does not have the luxury of knowing its readership in advance. The sheer diversity of its audience makes it impossible to predict what a given reader (or readers) will want to know. A prospective client is going to want different information than a prospective employee, who in turn will want to know something different from a prospective investor. Understanding and exploiting that diversity is one of the secrets to creating an effective corporate Website.

Know & Target Your Audiences

An astute reader will have already partially formed the conclusion that a corporate site really doesn't have a single, definable audience. Readership of a corporate site actually comprises a collection of smaller special interest groups. So while a topical site can rely on the homogeneity of its audience and "ramble" a bit from time to time, a good corporate site must be precise and narrow in its focus.

A well-crafted corporate site fully exploits the capabilities of hypertext documents to target each of its various audiences individually and directly. Optimize the structure of your site around a collection of small, tightly-focused "bite-sized" pages, liberally linked to other, directly related bites. Let each document and each section speak to a portion of your potential readership.

The Same Old Stuff

Certain basic things just make for decent Web pages. Virtually all of the rules for building a good topical Web page apply equally well to corporate pages. The only real difference is that the attributes that might be "recommended" for a topical site become absolutely critical in a corporate site. Just a few reminders:

- **Keep it small**

A corporate site does not have the luxury of long pages. A good corporate site is strongly encapsulated and liberally linked.

- **Keep it fast**

The bulk of the bytes pumped out by most sites are graphical. Keep your site lightning quick. Discard all superfluous graphics, and thoroughly optimize the images you truly must keep. Remember, you have seconds, not minutes, before you start losing readership.

- **Make maneuvering easy**

It's a mathematical inevitability: small pages + lots of content = lots of pages. But lots of pages is no excuse for a cumbersome, complicated site structure. Don't let your reader become lost in a labarynthine maze. Keep your basic navigational structure supremely simple, and make navigation mechanically quick and absolutely painless.

- **Keep it accessible**

Browser-specific formatting on a corporate site is a guaranteed loser.

- **Water & weed often**

Update your site at least once a month. With each update, add new content, to keep the site fresh and lure repeat visitors, and prune all your dead links.

Checklist for websites

- Quality and presentation of the information.
    - Can you tell quickly, if not immediately, what this company does?
    - Is there information about products and services?
    - Is there complete corporate and contact information?
    - Is there a product specification or evaluation tool that differentiates the site?
- Ease of navigation
    - Is the site well organized, especially if the company is targeting numerous audiences?
    - Is there a search engine?
    - Is it easy to move from one section of the site to another without backtracking?
- Design

- Is the site aesthetically pleasing?
- Are the graphics used appropriately?
- Does the site creatively exploit the medium with its use of audio and video?

▪ E-commerce

- Can you place an order?

▪ Extras

- Does the site have a community or forum section?
- Are there calculators or extra tools that enhance the user's experience?
- Can visitors sign up for online newsletters or email alerts?
- Can users access real-time customer support (such as click-to-talk or chat function)?
- Does the site have links to other sites with relevant supplemental information?

6.2 LEGAL ISSUES RELATED TO E-COMMERCE

Approximately 100 countries now enjoy Internet access, and a recent survey reported that there are approximately 20 million Internet hosts worldwide. The number of Internet users is currently estimated to be in the region of 100 million people.

The exponential growth of the Internet and online activity raise a number of new regulatory issues and legal questions. How does copyright apply to digital content? How can national laws apply to activities in cyberspace? Can privacy and data protection exist on the Web? Can electronic commerce really be secure? Should governments tax cyber trade? Can cyberspace be regulated by one, or by many authorities? In seeking to apply the law to the Internet, problems arise owing to the fact that most laws largely apply to the pre-cyberspace world.

In the modern era of electronic technology, many people want to get their work done quickly with little effort. At times, people forget or do not consider the legal and ethical values of their procedures. In traditional commerce, it's not easy to start a business. You must implement strategies that follow rules and regulations enforced by government. Electronic commerce makes

it possible to do almost any kind of business in a very simple way. What makes it simple? The reason is that existing legal frameworks and enforcement mechanisms are not strong.

E-commerce presents a world of opportunity for doing businesses, reaching global markets and purchasing without leaving the home or office. E-commerce can provide opportunities to improve business processes, just as phones, faxes and mobile communications have in the past. However, just as any new business tool has associated issues and risks so does e-commerce. It's important to understand the legal issues and potential risks to ensure a safe, secure environment for trading with customers and other businesses.
Some of the legal issues related to website and e-commerce transactions are discussed here :

Incorporation

Why Incorporate? Incorporation means that your company is a separate legal and financial entity from yourself. It even has its own social security number for tax purposes, called a Federal Tax ID. Most people incorporate to limit their personal liability so that their personal assets are not at risk for debts of the corporation. For example, if your incorporated company was sued and lost the suit, the winner could not take your personal car or home.

Plus, of course, incorporating makes you look more professional, and often helps with your taxes. Also, if you plan to receive investment in your company, have employees, and grow to be more than a one-person show, incorporation is an important step that helps promote these future goals. While incorporation protects you in many regards, it does not protect you from any criminal charges by you or the corporation, which can come into play if, for instance, you run an adult or gambling business on the Internet.

Trademark

The trademark act etc. is meant to ensure that consumers can correctly identify the sources of goods or services. A trademark is a word, phrase, symbol or design, or combination of words, phrases, symbols or designs, which identifies and distinguishes the source of particular goods. A service mark is the same as a trademark, except that it identifies and distinguishes the source of a service rather than a product.

Normally, a mark for goods appears on the product or its packaging, while a service mark appears in advertising for the services. A "tm" on a product indicates unregistered (common law) trademark rights, and an "" indicates a registered mark. It is illegal to place an "" on a mark that does not have national registration.

As your domain name and your branding is valuable, you should think in terms of trademark registration. This can be done later in the business process once you have more revenue available, but it is important to consider it upfront in choosing your domain name, company name, product and/or service name.

When trying to determine whether you've picked a good name in relation to others' marks, remember that the point of trademark law is to prevent consumer confusion about the source of goods or services. Ask yourself whether a consumer would confuse your name with that of another product, service or company.

Copyright

Copyright can be important when you obtain content for your site, and in the protection of your site's content.

The owner of a copyright has the exclusive right:

to copy the work

to modify the work (create "derivative works")

to distribute the work

to perform the work publicly

to display the work publicly

Copyright arises upon the creation of a copyrightable works (typically substantial text, images, music, etc.). Facts, titles, recipes, form designs, alphabetical lists and other items do not have the required "originality" to merit copyright protection. Your are not required to register works to have copyright protection, however if you do register your materials, you preserve the fact that

they are yours as of the date of registration, and you gain more rights under Copyright law, such as being able to win attorneys' fees and, sometimes, higher damages.

The term "Public Domain" does not mean that everything in public or on the Internet is freely usable. It refers to items that either do not qualify for copyright protection under the law, or for which the protection has expired.

When you buy content for your Website or business, the best approach is to obtain a warranty from the seller or licensor stating that the seller owns all the rights in it and agrees to indemnify you (i.e. pay you for the costs) if someone else sues you for using the content. Large content providers should be willing to do this, and many small ones will be also. If not, you'll have to hope for the best and take the risk.

Clickwrap Agreement for Users: An agreement with your users as part of the purchase process gives you a legal remedy (for breach of contract) to ensure:

that you will be paid,

that you waive legal warranties that are implied by law into sales of products of goods,

that you may disclose users' identities to government authorities upon request (there have been law suits to prevent this, or as a result of this),

that the user is over 18 and a US citizen,

that the site may only be used as permitted,

that venue and jurisdiction for disputes are in whatever state you prefer,

that there are limits to your civil (anything other than criminal) liability,

Historically, if the steps outlined in case law have been followed, these agreements have been upheld as binding. This can be very important as your merchant bank will issue credits for any disputed Internet transactions unless you have hand signed documents from your purchaser.

Federal Trade Commission (FTC):the FTC regulates trade and commerce with regard to consumers. The FTC monitors businesses to ensure:

truthful advertising, that mail-order, catalog and Web product purchase guidelines are followed, that sweepstakes and contest are conduct in compliance with the law, and that collection of consumer data and privacy policy guidelines are followed.

Indian IT Laws :

MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department)

New Delhi, the 9th June, 2000 /Jyaistha* 19, 1922 *(Saka)

The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:

THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 of 2000) [9th June, 2000]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental there to.

where as the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law; and whereas the said resolution recommends *inter alia* that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information; and whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

be it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:

THE THIRD SCHEDULE - AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT ' 891
THE FOURTH SCHEDULE - AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934

Information Technology Act

New communication systems and digital technology have made dramatic changes in way of transacting business. Use of computers to create, transmit and store information is increasing. Computer has many advantages in e-commerce. It is difficult to shift business from paper to electronic form due to two legal hurdles - (a) Requirements as to writing and (b) Signature for legal recognition. Many legal provisions assume paper based records and documents and signature on paper.

The General Assembly of the United Nations by resolution dated the 30th January, 1997 adopted the Model Law on Electronic Commerce and recommended that all States should give favourable consideration to the Model Law when they enact or revise their laws.
The Information Technology Act has been passed to give effect to the UN resolution and to promote efficient delivery of Government services by means of reliable electronic records.

As per preamble to the Act, the purpose of Act is (a) to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and (b) to facilitate electronic filing of documents with the Government agencies. - - The Act came into effect on 17.10.2000.

The Act does not apply to (a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, except cheque (b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act (c) a trust as defined in section 3 of the Indian Trusts Act(d) a will as defined in section 2(h) of the Indian Succession Act, including any other testamentary disposition by

whatever name called (e) any contract for the sale or conveyance of immovable property or any interest in such property (f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette. - - Broadly, documents which are required to be stamped are kept out of the provisions of the Act.

Overview of the Act- The Act provides for - * Electronic contracts will be legally valid * Legal recognition of digital signatures * Digital signature to be effected by use of asymmetric crypto system and hash function * Security procedure for electronic records and digital signature * Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities * Controller to act as repository of all digital signature certificates * Certifying authorities to get License to issue digital signature certificates * Various types of computer crimes defined and stringent penalties provided under the Act * Appointment of Adjudicating Officer for holding inquiries under the Act * Establishment of Cyber Appellate Tribunal under the Act * Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court * Appeal from order of Cyber Appellate Tribunal to High Court * Act to apply for offences or contraventions committed outside India * Network service providers not to be liable in certain cases * Power of police officers and other officers to enter into any public place and search and arrest without warrant * Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller.

What does IT Act enable? - The Information Technology Act enables:* Legal recognition to Electronic Transaction / Record * Facilitate Electronic Communication by means of reliable electronic record * Acceptance of contract expressed by electronic means * Facilitate Electronic Commerce and Electronic Data interchange * Electronic Governance * Facilitate electronic filing of documents * Retention of documents in electronic form * Where the law requires the signature, digital signature satisfy the requirement * Uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records or documents * Publication of official gazette in the electronic form * Interception of any message transmitted in the electronic or encrypted form * Prevent Computer Crime, forged electronic records, international alteration of electronic records fraud, forgery or falsification in Electronic Commerce and electronic transaction.

DIGITAL SIGNATURE - Any subscriber may authenticate an electronic record by affixing his digital signature. [section 3(1)]. ?Subscriber" means a person in whose name the Digital Signature Certificate is issued. [section 2(1)(zg)]. "Digital Signature Certificate" means a Digital Signature Certificate issued under section 35(4) [section 2(1)(q)].

"Digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3. [section 2(1)(p)].

"Affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature. [section 2(1)(d)].

Authentication of records- The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. [section 3(2)].

Verification of digital signature- Any person by the use of a public key of the subscriber can verify the electronic record. [section 3(3)]. The private key and the public key are unique to the subscriber and constitute a functioning key pair. [section 3(4)].

The idea is similar to locker key in a bank. You have your =private key while bank manager has =public key. The locker does not open unless both the keys come together match.

Electronic records acceptable unless specific provision to contrary - Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is - (a) rendered or made available in an electronic form; and *(b)* accessible so as to be usable for a subsequent reference. [section 4]. - - Unless there is specific provision in law to contrary, electric record or electronic return is acceptable. - - Soon, it will be possible to submit applications, income tax returns and other returns through internet.

DEPARTMENT OR MINISTRY CANNOT BE COMPELLED TO ACCEPT ELECTRONIC RECORD - Section 8 makes it clear that no department or ministry can be compelled to accept application, return or any communication in electronic form.

Legal recognition of digital signatures **-**Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government. - - "Signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly. [section 5].

Secure digital signature -If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was - (a) unique to the subscriber affixing it *(b)* capable of identifying such subscriber (c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, - - then such digital signature shall be deemed to be a secure digital signature. [section 15].

Certifying digital signature-The digital signature will be certified by =Certifying Authority. The =certified authority will be licensed, supervised and controlled by =Controller of Certifying Authorities.

6.3 SUMMARY

This Unit covers the basic steps involved in launching an effective corporate website. Some issues regarding the cyber-crimes are also addressed and the required preparedness for curbing the cyber- crimes has been covered in this unit.

6.4 KEYWORDS

Corporate website, information technology Act

6.5 REVIEW QUESTIONS

1. What are the basic steps to launch an effective corporate website?

2. Prepare a survey on cyber-crimes related to e-commerce in India and the preparedness of agencies to deal with it.

3. What are the major legal issues for an online firm?

4. Write a short note on Information Technology Act.

6.6 REFERENCES / SUGGESTED READINGS

- Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc.
- Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.
- Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.
- Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.

UNIT 7: BUISNESS TO BUISNESS E-COMMERCE (B2B)

Structure

7.0 OBJECTIVES

After studying this unit we will be able

- To understand the different types of B2B models
- To understand the electronic payment systems and their risks to customers.

7.1 BUSINESS TO BUSINESS E-COMMERCE (B2B)

E-business is the process of conducting business on the Internet. Its scope includes not only buying and selling but also services, fulfilling the needs of customers and collaborating with business partners.

Business to business e-commerce is smart business. The opportunity for business to business e-commerce is even greater.

A wholesaler may sell products to the retailer. There are advanced e-commerce software which support multi-tier pricing. This helps to set up online stores to offer preferred pricing to some vendors and shared price to others.

This includes internet-enabled initiatives of an enterprise to form commercial linkages with another enterprise, dealer, warehouse or manufacturer. In this form of e-commerce, e paperwork and time-to-market get vastly reduced. Throughout the world, this e-commerce mode is the biggest.

In a B2B transaction, the interaction is between businesses. For example, a website that is catching for the steel industry might have facility for buyers and sellers to list their requirements and post their products. It helps them in quickly closing the transactions and the buyer can get quality, material and can choose from different suppliers.

B2B commerce is a growing business in the e-commerce arena- with the increasing use of the internet, more and more business are realizing the commercial advantage of giving business clients a streamlined and easy manner to order products or service online. It facilitates access to the ordering process to only those with whom a concern has a commercial relationship.

Business to Business e-commerce provides small and medium enterprises (SMES) with an excellent opportunity to access new markets, improve customer service and reduce costs. And while hurdles exist, they should be viewed more as speed breakers rather than road barriers. As a medium of information storage and dissemination, the internet has and is emerging a clear winner. Its rate of penetration has far outpaced the growth of other popular media such as newspaper, radio and television.

B2B transactions are however relatively high value in nature and organisations are slow to change their traditional systems for the supply chain management. The reasons for the growth in B2B e-commerce are many. In an increasing competitive scenario, e-commerce offers highly attractive cost saving options. The shift to this process is often driven by the needs of buyers.

Innovative methods of enhancing B2B and B2C levels of e-commerce include:

- CD-ROM catalogues that are linked to the user's online catalogue, enabling him to browse offline and order online.
- Kiosks placed at physical store locations or in shopping malls to introduce users to the easy online ordering options.
- Extranets to link businesses together that conduct regular business to .business transactions
- Affiliate programmes to drive business to your commerce site from other content related sites

B2B MODELS

There are four different types of B2B models available which are as follows:

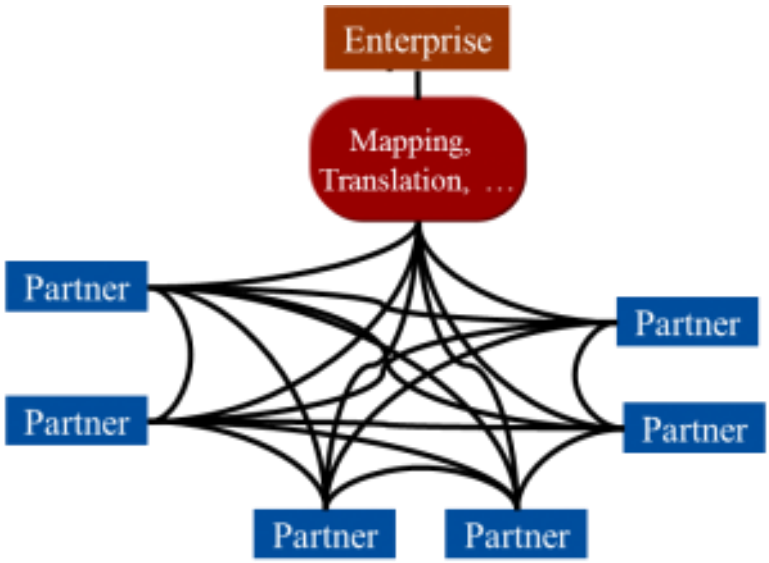
1. **Direct Connection Model**

In the direct model your business connects directly to each of your trading partners for sending and receiving electronic documents. Your IT organization is responsible for all mapping, translation, technical support and tracking documents. As long as everyone agrees on a single connectivity protocol, e.g. FTP over VPN, Rosetta Net, OFTP, AS2, and the community size remains relatively small (generally less than 100) this approach works well. This is how B2B was handled in the in the early days of EDI.

But, as the size of your community grows, you need more resources to implement and support each new trading partner. You need to continually monitor communications, manage trading partner calls and resolve issues quickly. Quick issue resolution is critical since the documents being exchanged (e.g. orders, invoices, ship notices) are frequently the lifeblood of your business.

Adding to the complexity, trading partners frequently insist on using different protocols, particularly if they are also trading with other enterprises. Now you must support multiple protocols, requiring more resources.

The graphic below illustrates the direct B2B scenario. Your business is represented as the "Enterprise" connecting with six trading partners who are trading other partners as well.

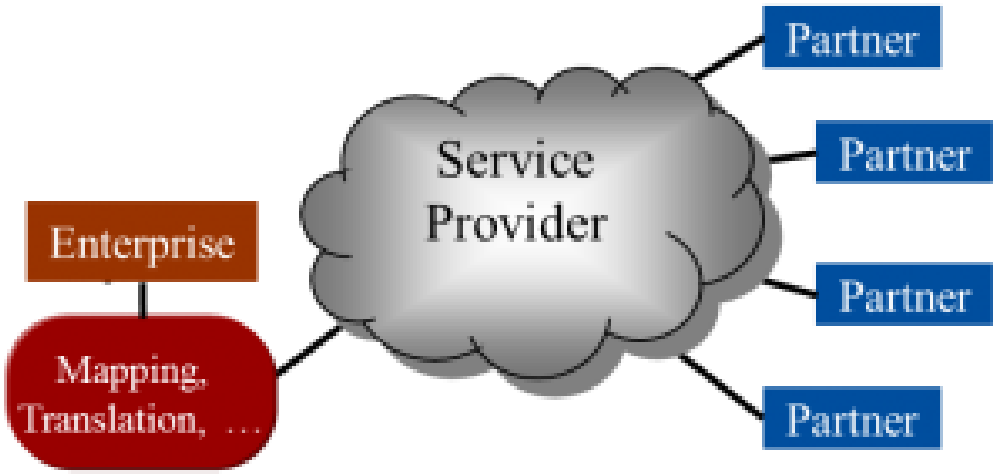


This model is sometimes called the "spaghetti model," or the "spider model" because of its complexity. Very few businesses today connect directly with all their trading partners because of the support issues.

2. Network Model

To avoid the complexity of the direct model, many companies decide to work exclusively through a B2B Service Provider, which, in the days prior to the internet, was referred to as a Value-Added Network (VAN). In this model, you have a single connection to the Service Provider using whatever protocol you prefer – e.g. AS2, SFTP, FTPS, FTP over VPN, RosettaNet . Likewise, your trading partners connect to the Service Provider, each selecting the connectivity protocol that best meets its company's requirements. In this way, each trading partner makes an independent decision regarding its preferred connectivity protocol and relies on the Service Provider to mediate the differences between the protocols as needed. The Service Provider facilitates the exchange of electronic documents via its network. The Service Provider also relieves all community members of the resource-intensive responsibilities for supporting all communications issues; ensures data security and non-repudiation; and provides audit information, reporting, backup and recovery. The Service Provider charges transactions fees for these services. Your business is still responsible for all mapping and translation as well as some reporting and translation-related technical support.

The graphic below illustrates the network model of B2B. Your business is represented as the "Enterprise" connecting with the Service using a single communications protocol. Likewise, each trading partner is connected to the Service Provider as well using their varying preferred protocols.

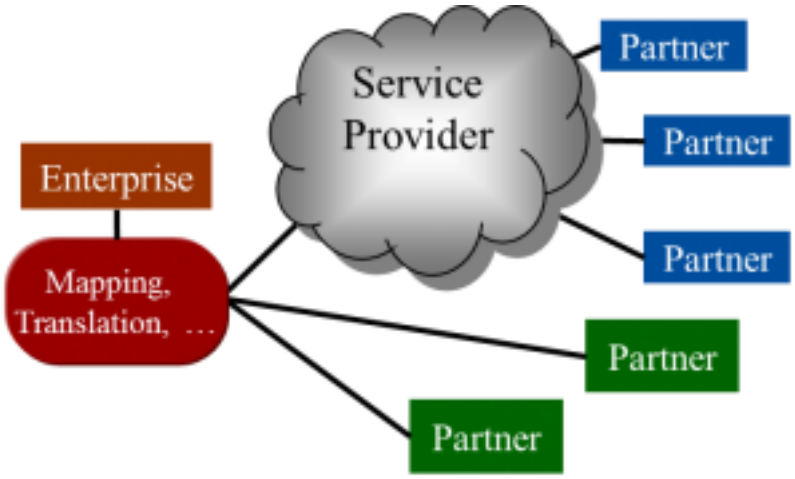


Use of the network model for 100% of a B2B trading community was extremely popular before the rise of the commercial use of the internet and large trading networks. Today, while it's still used by many companies, it's much less common to have 100% of the community on the network.

3. Hybrid Model

The hybrid approach to B2B is a combination of the direct and network models. Typically, businesses will connect directly via the internet to their trading partners with whom they do the highest volume of transactions, using one or two preferred protocols, in order to save on Service Provider transaction fees. The business continues to leverage the Service Provider for trading with the large number of lower-volume trading partners as well as for those that require a protocol other than the one or two that are used to connect directly.

The graphic below illustrates the *hybrid* model of B2B. Your business is represented as the "Enterprise" connecting directly with the two partners in green. You also have a connection to the Service Provider for trading with your partners in blue.



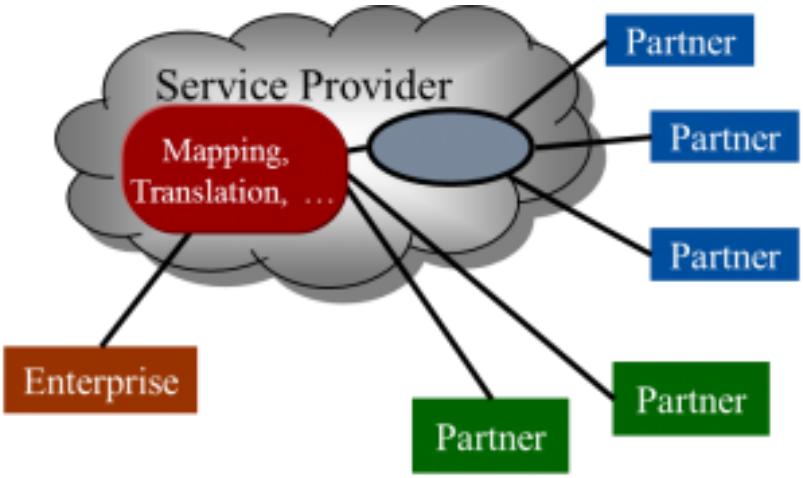
For large communities, the hybrid model is much more commonly used today.

4. Managed Model

In the managed model, the business outsources the entire B2B process to an external Service Provider. This greatly reduces resource requirements, expenses and complexity.

The Service Provider receives your business documents directly from your ERP system (SAP, Oracle, etc.) and then assumes responsibility for all the mapping, translation, technical support, data center operations and document tracking. Once documents are ready for delivery to your trading partners, the service provider delivers them either directly to the partners or via the network, depending on the individual trading partner requirements.

The graphic below illustrates the *managed* model. Your business is represented as the "Enterprise" that connects to the Service Provider. The Service Provider connects you directly with the two partners in green. It also connects you with the rest of your partners.



Companies are increasingly outsourcing their entire B2B process to avoid purchasing and managing complex, expensive B2B mapping, translation, and communications software.

7.2 ELECTRONIC PAYMENT SYSTEMS

Offline versus Online Offline payments involve no contact with a third party during payment: The transaction involves only the payer and payee. The obvious problem with offline payments is that it is difficult to prevent payers from spending more money than they actually possess. In a purely digital world, a dishonest payer can easily reset the local state of his system to a prior state after each payment. Online payments involve an authorization server (usually as part of the issuer or acquirer) in each payment. Online systems obviously require more communication. In general, they are considered more secure than offline systems. Most proposed Internet payment systems are online. All proposed payment systems based on electronic hardware, including Mondex and CAFE (Conditional Access for Europe), are offline systems. Mondex is the only system that enables offline transferability: The payee can use the amount received to make a new payment himself/herself, without having to go to the bank in between. However, this seems to be a politically unpopular feature. CAFE is the only system that provides strong payer anonymity and un-traceability. Both systems offer payers an electronic wallet, preventing fake-terminal attacks on the payer's PIN. CAFE also provides loss tolerance, which allows the payer to recover from coin losses (but at the expense of some anonymity in case of loss). Mondex and CAFE are

multicurrency purses capable of handling different currencies simultaneously. All these systems can be used for Internet payments, and there are several plans for so doing, but none is actually being used at the time of this writing. The main technical obstacle is that they require a smart card reader attached to the payer's computer. Inexpensive PCMCIA smart card readers and standardized infrared interfaces on notebook computers will solve this connectivity problem. Another system being developed along these lines is the FSTC (Financial Services Technology Consortium) Electronic Check Project, which uses a tamper-resistant PCMCIA card and implements a check-like payment model. Instead of tamper-resistant hardware, offline authorization could be given via preauthorization: The payee is known to the payer in advance, and the payment is already authorized during withdrawal, in a way similar to a certified bank check.

- **Electronic payment systems** are non-credit-card online payment systems.
- Used to transfer money over the Internet
- The goal of their development is to create analogs of checks and cash on the Internet, i.e. to implement all or some of the following features:
    - Protecting customers from merchant's fraud by keeping credit card numbers unknown to merchants.
    - Allowing people without credit cards to engage in online transactions.
    - Protecting confidentiality of customers.
    - In some cases providing anonymity of customers("electronic cash").
- The problems in implementing electronic payment systems, especially anonymous electronic money, are:
    - Preventing double-spending: copying the "money" and spending it several times. This is especially hard to do with anonymous money.

- Making sure that neither the customer nor the merchant can make an unauthorized transaction.

- Preserving customer's confidentiality without allowing customer's fraud.

- While electronic payment systems have not gained a very wide popularity, except for PayPal system used on online auctions, such as eBay, they may become more popular in the future if more businesses start using them.

- Electronic payment systems may be more convenient for international online business due to differences in credit card customer protection laws in different countries.

- The availability of appropriate e-payment method is a crucial element of e-business.

An electronic payment system must provide:

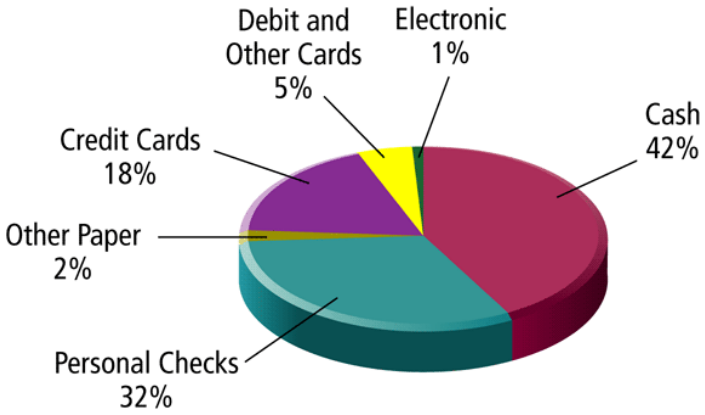
- **Privacy** – details about any transaction must be kept securely away from unauthorized parties. An intercepted transaction can expose a sender to fraud or theft. Privacy is usually ensured by using encryption techniques.

- **Integrity** – users must be confident that a transaction will be received and processed without loss, being altered or tampered with while in transit. Integrity can be ensured using digital signatures and certificates.

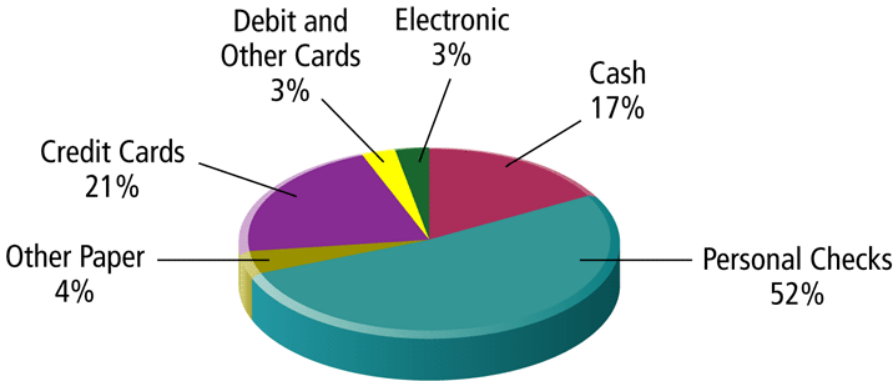
- **Authentication** – the sender must be confident that the recipient(s) are who they say they are, and vice versa. Authentication is vital to prevent fraud. It is usually the responsibility of the merchant to enforce appropriate authentication procedures.

- **Non-Repudiation** – the ability to prove that a transaction has been made. An important aspect of trust is the ability for senders to prove they have made the payment. This can be done using receipts.

Most Common Payment Systems, Based on Number or Transactions



Most Common Payment Systems, Based on Dollar Amount



Requirements for e-payments

- **Atomicity**
  - Money is not lost or created during a transfer.
- **Good atomicity**
  - Money and good are exchanged atomically.
- **Non-repudiation**
  - No party can deny its role in the transaction.
  - Digital signatures.

Digital Payment Systems

- Allows transfer of value without transfer of physical objects.
- Payment by bits rather than atoms.

Desirable Properties of Digital Money

- Universally accepted.
- Transferable electronically.
- Divisible.
- Non-forgeable, non-stealable.
- Private (no one except parties know the amount).
- Anonymous (no one can identify the payer).
- Work off-line (no on-line verification needed).

Types of E-payments

- E-cash
- Electronic wallets
- Smart card
- Credit card

ELECTRONIC CASH(E-cash)

- Term that describes any value storage and exchange system created by a private entity that does not use paper documents or coins.
- Can serve as a substitute for government-issued physical currency.
- Attractive in two arenas.

- Sale of goods and services of less than $10
- Sale of higher-priced goods and services to those without credit cards

- DigiCash (also known as E-cash) is an electronic payment system developed by Dr. David Chaum, who is widely regarded as an inventor of digital cash.
- The system was based on digital tokens called digital coins. DigiCash operated as follows:

Operation of Electronic cash

- A customer establishes an account with the bank or other organization that could mint and receive digital coins. The customer's account was backed by real money in some form, for instance it could be linked to the customer's checking account.
- The customer also needs to download and install a software called electronic wallet.
- To obtain DigiCash, the customer uses the electronic wallet to create digital coins. The coins are sent to the bank to sign.
- When the coins are signed, the equivalent amount of money is withdrawn from the customer's account.
- When the customer wants to make a purchase, he/she sends signed digital coins to the merchant. The merchant verifies the bank's signature and deposits the coins to the bank, where they are credited to the merchant's account.

E-cash Concept

1. Consumer buys e-cash from Bank

2. Bank sends e-cash bits to consumer (after charging that amount plus fee).

3. Consumer sends e-cash to merchant.

4. Merchant checks with Bank that e-cash is valid (check for forgery or fraud)

5. Bank verifies that e-cash is valid.

6. Parties complete transaction: e.g., merchant present e-cash to issuing back for deposit once goods or services are delivered.

7.3 E-PAYMENT RISKS TO CUSTOMER

- Merchant could misuse information provided for transactions by customer.
- Merchant could penetrate customer's site, glean information about the customer, and misuse that.
- E.g., Merchant offers higher prices based on customer's past behavior

. **E-Payment Risks to Customer**

- Customer could really be a competitor attempting to learn prices or strategy.
- Customer could be an imposter, and bill will not be paid.
- Customer could be a hacker:
  - changes what will get ordered by bona fide customers
  - changes what prices are charged.
  - changes what is available.
  - steals customer contact information.

- E-cash focuses on replacing cash as the principal, payment vehicle in consumer-oriented electronic payments.
- Although it may be surprising to some, cash is still the most prevalent consumer payment instrument even after thirty years of continuous developments in electronic payment systems.
- Cash remains the dominant form of payment for three reasons:

    (1) lack of trust in the banking system,

    (2) inefficient clearing and settlement of non-cash transactions.

    (3) negative real interest rates paid on bank deposits.
- The predominance of cash indicates an opportunity for innovative business practice that revamps the purchasing process where consumers are heavy users of cash.
- To really displace cash, the electronic payment systems need to have some qualities of cash that current credit and debit cards lack.
- For example, cash is negotiable, meaning it can be given or traded to some-one else.
- Cash is legal tender, meaning the payee is obligated to take it.
- Also, cash can be held and used by anyone even those who don't have a bank account, and cash places no risk on the part of the acceptor that the medium of exchange may not be good.
- Now compare cash to credit and debit cards.
- First, they can't be given away because, technically, they are identification cards owned by the issuer and restricted to one user.
- Credit and debit cards are not legal tender, given that merchants have the right to refuse to accept them.

- Nor are credit and debit cards bearer instruments; their usage requires an account relationship and authorization system.

- Similarly, checks require either personal knowledge of the payer or a check guarantee system. Hence, to really create a novel electronic payment method, we need to do more than recreate the convenience that is offered by credit and

debit cards.

- We need to develop e-cash that has some of the properties of cash.

7.4 SUMMARY

Although there is a plethora of disparate payment systems offered for electronic commerce, many firms are reluctant to expand into online commerce because of the perceived lack of suitable payment mechanisms. Widely different technical specifications make it difficult to choose an appropriate payment method. In this chapter, instead of focusing on the technical specifications of proposed electronic payment systems, we have distinguished electronic payment methods based on what is being transmitted over the network. Since consumers are familiar with credit card payment methods, they may accept its electronic versions as the standard for electronic commerce. Nevertheless, Web-based information trading cannot be adequately supported by existing payment methods that have been developed for relatively high-value transactions. A cost effective micropayment system is essential for transactions of extremely small value just as cash is still the preferred payment method for these transactions. Anonymity is only one aspect of cash transaction but it has received a disproportionate, often sensational, attention in the press and by regulatory agencies while the economic need for a cash-like payment system in electronic commerce is largely ignored. Factors such as micropayments and peer-to-peer transfers in electronic commerce-especially for the information market-seem to indicate a healthy market for digital currency or small-value digital checks or credit cards. In terms of the regulatory and monetary impact, private digital monies clearly present both problems and opportunities. But, as with any digital product, the future of digital currency will be determined by the market demand and supply. Consequently, it is more than likely that each of the payment methods we reviewed will find a niche market and consumers will selectively use

an appropriate payment method depending on whether one prefers convenience, costs, privacy, or the advantage of credit extension. The usefulness of digital currency, however, has to be emphasized in terms of what the Web-based information economy would mean for the future of electronic commerce and the Internet. With a suitable payment method, the age of information will manifest itself on the Internet, albeit in a commercial form.

This unit introduces the different models of business to business e-commerce. Later the E-Payment Risks to Customer are covered extensively. Some of the interesting topics on electronic cash have been covered.

7.5 KEYWORDS

Business to business, E-payment risks

7.6 REVIEW QUESTIONS

1. Dicuss B2b in detail.
2. Explain E-Payment Risks to Customer.
3. Explain Electronic cash (E-cash)

7.7 REFERENCES / SUGGESTED READINGS

- Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc.
- Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.
- Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.
- Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.

UNIT 8: REQUIREMENT FOR INTERNET BASED SYSTEMS

Structure

8.0 Objectives

After studying this unit we will be able

- To understand the properties and prospects of Electronic payment systems
- To understand the working of Electronic cash and wallets.

8.1 REQUIREMENT FOR INTERNET BASED SYSTEMS

8.1.1 DESIRABLE PROPERTIES OF DIGITAL CURRENCY

Developers of digital currency have a wide range of options to implement strong safety requirements of transmitting values over the network. For example, a secure digital currency can be implemented by using strong encryption algorithms, by employing tamper-resistant hardware, or by securing the network communication. Although physical specifications of digital coins and tokens may vary, the following properties are fundamental to any digital currency payment system.

• Monetary Value To be used as a monetary unit, digital currency must have value that can be exchanged for other goods and services, be used to pay fiduciary obligations, or be transferred to another person. Since digital currency is essentially a file, it does not have

an intrinsic value, but must be linked to other system of value. The most common implementation is to base the value of digital currency on bank deposits, credits, or prepayments using outside money. Once a digital currency is convertible to dollars, the next step is for it to be accepted in the market as a monetary token. Once accepted and trusted, a digital currency can establish related properties such as exchangeability and transferability.

- Convenience has been the biggest factor in the growth of notational currencies such as checks, which are scalable and easy to transport. Similarly, digital currencies must be convenient to use, store, access, and transport. As a digital file, it may allow remote access to money via telephone, modem, or Internet connection. Electronic storage and transfer devices or network capabilities will be needed. To gain wide acceptance, digital cash also must be convenient in terms of scalability and interoperability so that users need not carry multiple denominations or multiple versions for each operating system.

• Security To secure physical money and coins, one needs to store them in wallets, safes or other private places. If digital currencies are stored in hard drives connected to an open network, theoretically anybody can snoop and tamper with the money. Encryption is used to protect digital currency against tampering. Some proposals using smart cards, e.g. Mondex, store digital currency in tamper-resistant hardware that can be maintained offline. Ecash relies on the security of Ecash client software residing on users' computers. At the same time, digital currencies must be resistant to accidents by owners. Rupee bills are printed on strong paper that withstands many adverse treatments, such as washing. To achieve similar security, adequate protection standards are needed both in physical specifications of digital coins and in policy matters for legal and commercial liabilities.

• Authentication of money is done by visually inspecting bills and coins. Although further tests could weighing, chemical analysis, and contacting the authorities, authentication is usually a simple matter for physical currency. Digital currency, however, cannot be visually inspected, and it is difficult to distinguish the original and a counterfeit. Because of this, inspection of digital currency depends on authenticating secondary information that accompanies the bills or coins such as the digital signatures of banks or payers

attached to the currency (serial number). A more rigid system will require contacting a third party each time a transaction is made. Although this system is more secure, the transaction costs may be too high for small-value purchases. A hardware based system like Mondex relies on software and hardware and does not require authentication for each transfer of values. Other systems will have to strengthen their client software or introduce hardware protection to allow peer-to-peer transactions.

- Non-refutability Acknowledging payment and receipt is a basic property required of a payment system. In cash transactions, simple receipt is enough to establish non-refutability. A similar exchange of digital receipts can be used for digital transactions. An alternative is to append all transaction records into the digital currency itself. In this system, digital coins accumulate information about all parties involved in past transactions. These are called identified tokens compared to anonymous tokens, which do not reveal information about users.

- Accessibility and Reliability One advantage of digital currency over cash is its capability to be transported over the network. Therefore, users can store digital money at home but access it remotely via telephone or modem, the same network used to clear payments. Because of this crucial role, digital payment systems must provide continuous, fast, and reliable connections.

- Anonymity Unlike checks and cards, cash transactions are anonymous. An anonymous payment system is needed to protect against revealing purchase patterns and other consumer information, although untraceable transactions are opposed by the government in view of possible criminal uses. Nevertheless, the need will persist, and anonymity is perhaps the single most important property of cash transactions. Digital currency can be equipped with varying degree of anonymity masking the user identity to the bank, the payee, or both. Strong anonymity guarantees un-traceability while a weaker version allows the user's identity to be traced when the need arises. While the issue of anonymity invokes debates about tax evasion, money laundering and other criminal uses of digital currency, the economic rationale for simple, anonymous digital coins is that they reduce

transaction costs by eliminating third parties and protect consumer information that could be used to price-discriminate among consumers.

8.2 PROSPECTS OF ELECTRONIC PAYMENT SYSTEMS

As the volume of Electronic Commerce becomes larger, the role of secure and economical online payments on the Internet will, accordingly, become more important. At the moment, the credit card payment for B2C trades with SSL protocol is the most widely adopted. However, SET protocol tailored to credit card payment may become one of the next generation standards. For micro payment, smart-card-based e-cash will become popular and will be recharged through the Internet from the cyber-banks, which will revitalize the benefit of cyber-banks.

As B2B occupies the major portion of Electronic Commerce, more economical payment methods like Internet-based funds transfer equipped with the benefit of check systems will become the major medium for large-amount payments. The credit card fee seems too high to transfer large amounts among credible corporations. This prospective trend should envision opportunities to payment businesses and corporate finance managers. electronic payment systems to e-stores and banks. The SET solution of having the certificate on the smart card is an emerging issue to be resolved.

- Electronic stores should select an appropriate set of electronic payment systems. Until electronic payment methods become popular among customers, it is necessary to offer traditional payment methods as well.

- Banks need to develop cyber-banks compatible with the various electronic payment systems (credit card, debit card, stored-value card, and e-check) that will be used by customers at e-stores. Watch for the development of consistent standards in certificates and stored-value-card protocols.

- Credit card brand companies need to develop standards like SET and watch 'the acceptance by customers. It is necessary to balance security with efficiency. Careful attention is needed to determine when the SSL-based solution will be replaced by the SET -based

solution and whether to combine the credit card with the open or closed stored-value card.

- Smart card brands should develop a business model in cooperation with application sectors (like transportation and pay phones) and banks. Having standards is the key to expand interoperable applications. In designing business models, it is important to consider the adequate number of smart cards from the customer's point of view.

- Certificate authorities need to identify all types of certificates to be provided. Banks and credit card companies need to consider whether they should become a clearing agent.

8.2.1 SECURITY REQUIREMENTS IN ELECTRONIC PAYMENT SYSTEMS

The concrete security requirements of electronic payment systems vary, depending both on their features and the trust assumptions placed on their operation. In general, however, electronic payment systems must exhibit integrity, authorization, confidentiality, availability, and reliability.

Integrity and authorization

A payment system with integrity allows no money to be taken from a user without explicit authorization by that user. It may also disallow the receipt of payment without explicit consent, to prevent occurrences of things like unsolicited bribery. Authorization constitutes the most important relationship in a payment system. Payment can be authorized in three ways: via out-band authorization, passwords, and signature.

Out-band authorization

In this approach, the verifying party (typically a bank) notifies the authorizing party (the payer) of a transaction. The authorizing party is required to approve or deny the payment using a secure, out-band channel (such as via surface mail or the phone). This is the current approach for credit cards involving mail orders and telephone orders: Anyone who knows a user's credit card data can initiate transactions, and the legitimate user must check the statement and actively complain

about unauthorized transactions. If the user does not complain within a certain time (usually 90 days), the transaction is considered “approved” by default.

Password authorization

A transaction protected by a password requires that every message from the authorizing party include a cryptographic check value. The check value is computed using a secret known only to the authorizing and verifying parties. This secret can be a personal identification number, a password, or any form of shared secret. In addition, shared secrets that are short - like a six-digit PIN - are inherently susceptible to various kinds of attacks. They cannot by themselves provide a high degree of security. They should only be used to control access to a physical token like a smart card (or a wallet) that performs the actual authorization using secure cryptographic mechanisms, such as digital signatures.

Signature authorization

In this type of transaction, the verifying party requires a digital signature of the authorizing party. Digital signatures provide nonrepudiation of origin: Only the owner of the secret signing key can “sign” messages (whereas everybody who knows the corresponding public verification key can verify the authenticity of signatures.)

Confidentiality

Some parties involved may wish confidentiality of transactions. Confidentiality in this context means the restriction of the knowledge about various pieces of information related to a transaction: the identity of payer/payee, purchase content, amount, and so on. Typically, the confidentiality requirement dictates that this information be restricted only to the participants involved. Where anonymity or un-traceability are desired, the requirement may be to limit this knowledge to certain subsets of the participants only, as described later.

Availability and reliability

All parties require the ability to make or receive payments whenever necessary. Payment transactions must be atomic: They occur entirely or not at all, but they never hang in an unknown or inconsistent state. No payer would accept a loss of money (not a significant amount, in any

case) due to a network or system crash. Availability and reliability presume that the underlying networking services and all software and hardware components are sufficiently dependable. Recovery from crash failures requires some sort of stable storage at all parties and specific resynchronization protocols. These fault tolerance issues are not discussed here, because most payment systems do not address them explicitly.

8.2.2 Properties of Electronic Cash

- Specifically, e-cash must have the following four properties**: monetary value,**

interoperability, irretrievability, and security.

- E-cash must have a **monetary value**; bank authorized credit, or a bank-certified cashier's check.
- When e-cash created by one bank is accepted by others, reconciliation must occur without any problems.
- Stated, another way, e-cash without proper bank certification carries the risk that when deposited, it might be returned for insufficient funds.
- E-cash must be **interoperable-**that is, exchangeable as payment for other e-cash, paper cash, goods or services, lines of credit, deposits in banking accounts, bank notes or obligations and for electronic benefits transfers .
- Most e-cash proposals use a single bank.
- In practice, multiple banks are required with an international clearinghouse that handles the exchange-ability issues because all customers are not going to be using the same bank or even be in the same country.
- E-cash must be storable and **retrievable.**
- Remote storage and retrieval (e.g., from a telephone or personal communications

  device) would allow users to exchange e-cash (e.g., withdraw from and deposit into banking accounts) from home or office or while traveling.

- The cash could be stored on a remote computer's memory, in smart cards, or in other easily transported standard or special purpose devices. Because it might be easy to create counterfeit cash that is stored in a computer, it might be preferable to store cash on a dedicated device that cannot be altered.

- This device should have a suitable interface to facilitate personal authentication using passwords or other means and a display so that the user can viewthe card's contents.

- One example of a device that can store e-cash is the Mondex card-a pocket-sized electronic wallet.

- E-cash should not be easy to copy or tamper with while being exchanged; this includes preventing or detecting duplication and double-spending.

- Counterfeiting poses a particular problem, since a counterfeiter may, in the Internet environment, be anywhere in the world and consequently be difficult to catch without appropriate international agreements.

- Detection is essential in order to audit whether prevention is working. Then there is the tricky issue of double spending. For instance, you could use your e-cash simultaneously to buy something in Japan, India, and England.

- Preventing double spending from occurring is extremely difficult if multiple banks are involved in the transaction.

- For this reason, most systems rely on post-fact detection and punishment. Now we will see the concept of Electronic Cash actually works.

8.3 WORKING OF ELECTRONIC CASH

- Electronic cash is based on cryptographic systems called "digital signatures".

- This method involves a pair of numeric keys (very large integers or numbers) that work in tandem: one for locking (or encoding) and the other for unlocking (or decoding).

- Messages encoded with one numeric key can only be decoded with the other numeric key and n one other.

- The encoding key is kept private and the decoding key is made public.
- By supplying all customers (buyers and sellers) with its public key, a bank enables customers to decode any message (or currency) encoded with the bank's private key.
- If decoding by a customer yields a recognizable message;" the customer can be fairly confident that only the bank could have encoded it.
- These digital signatures are as secure as the mathematics involved and have proved over .the past two decades to be more resistant to forgery than handwritten signatures.
- Before e-cash can be used to buy products or services, it must be procured from a currency server.

8.3.1PURCHASING E-CASH FROM CURRENCY SERVERS

- The purchase of e cash from an on-line currency server (or bank) involves two steps:

  (1) Establishment of an account and

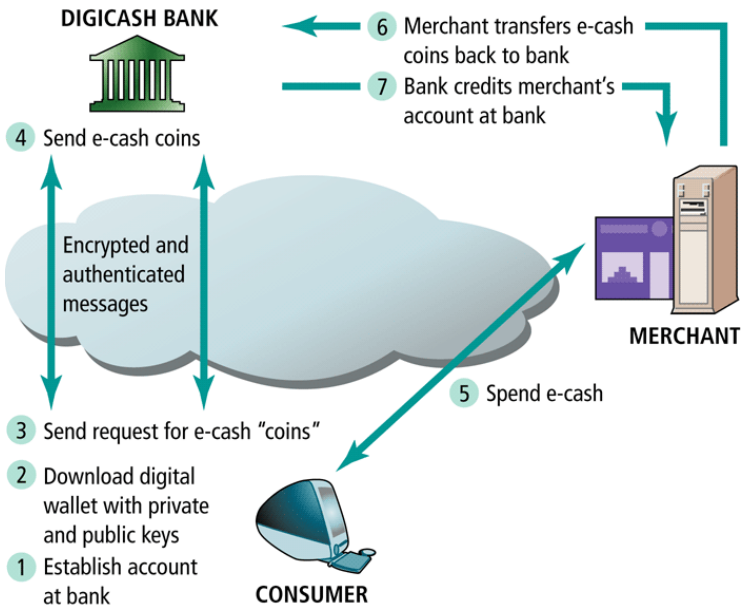
  (2) Maintaining enough money in the account to back the purchase.
- Some customers might prefer to purchase e-cash with paper currency, either to maintain anonymity or because they don't have a bank account.
- Currently, in most e-cash trials all customers must have an account with a central on-line bank.
- This is overly restrictive for international use and multi-currency transactions, for customers should be able to access and pay for foreign services as well as local services.
- To support this access, e-cash must be available in multiple currencies backed by several banks.
- A service provider in one country could then accept tokens of various currencies from users in many different countries, redeem them with their issuers, and have the funds transferred back to banks in the local country.
- A possible solution is to use an association of digital banks similar to organizations like VISA to serve as a clearinghouse for many credit card issuing banks.

- And finally, consumers use the e-cash software on the computer to generate a random number, which serves as the "note."
- In exchange for money debited from the customer's account, the bank uses its private key to digitally sign the note for the amount requested and transmits the note back to the customer.
- The network currency server, in effect, is issuing a "bank note," with a serial number and a dollar amount.
- By digitally signing it, the bank is committing itself to back that note with its face value in real dollars.
- This method of note generation is very secure, as neither the customer (payer) nor the merchant (payee) can counterfeit the bank's digital signature (analogous to the watermark in paper currency).
- Payer and payee can verify that the payment is valid, since each knows the bank's public key.
- The bank is protected against forgery, the payee against the bank's refusal to honor a legitimate note, and the user against false accusations and invasion of privacy.

8.3.2 DIGICASH

- Also called e-cash
- Digital forms of value storage or value exchange that have limited convertibility into other forms of value and require intermediaries to convert
- In the case of DigiCash, every person using e-cash has an e-cash account at a digital bank (First Digital Bank) on the Internet.
- Using that account, people can withdraw and deposit e-cash.
- When an e-cash withdrawal is made, the PC of the e-cash user calculates how many digital coins of what denominations are needed to withdraw the requested amount.
- Next, random serial numbers for those coins will be generated and the blinding (random number) factor will be included.

- The ‘ “ result of these calculations will be sent to the digital bank.
- The bank will encode the blinded numbers with its secret key (digital signature) and at the same time debit the account of the client for the same amount.
- The authenticated coins are sent back to the user and finally the user will take out the blinding factor that he or she introduced earlier.
- The serial numbers-plus their signatures are now digital coins; their value is guaranteed by the bank.
- Electronic cash can be completely anonymous. Anonymity allows freedom of usage to buy illegal products such as drugs or pornographic material or to buy legal product and services.
- This is accomplished in the following manner. When the e-cash software generates a note, it masks the original number or “blinds” the note using a random number and transmits it to a bank.
- The “blinding” carried out by the customer’s software makes it impossible for anyone to link payment to payer.
- Even the bank can’t connect the signing with the payment, since the customer’s original note number was blinded when it was signed.
- In other words, it is a way of creating anonymous, untraceable currency. What makes it even more interesting is that users can prove unequivocally that they did or did not make a particular payment.
- This allows the bank to sign the “note” without ever actually knowing how the issued currency will be used.
- For those readers who are mathematically inclined, the protocol behind blind signatures is presented.



8.3.3ELECTRONIC CASH STORAGE METHODS

- **On-line**
    - Individual does not have possession personally of electronic cash
    - Trusted third party, e.g. online bank, holds customers' cash accounts
- **Off-line**
    - Customer holds cash on smart card or software wallet
    - Fraud and double spending require tamper-proof encryption

Advantages and Disadvantages of Electronic Cash

- **Advantages**
    - More efficient, eventually meaning lower prices
    - Lower transaction costs

- Anybody can use it, unlike credit cards, and does not require special authorization
- Transactions are more efficient
- Transfer on the Internet costs less than processing credit card transactions

- **Disadvantages**
  - Tax trail non-existent, like regular cash
  - Money laundering
  - Susceptible to forgery

8.4 ELECTRONIC WALLETS

- These "wallets" store credit card numbers on personal computers in encrypted forms.
- Consumers can make purchases using their credit cards at web sites that support one of these wallets.
- A secure transaction is created by the electronic wallet company's server.
- Stores credit card, electronic cash, owner identification and address
- Makes shopping easier and more efficient.
- Eliminates need to repeatedly enter identifying information into forms to purchase.
- Works in many different stores to speed checkout
- Amazon.com one of the first online merchants to eliminate repeat form-filling for purchases.
- Give consumers the benefit of entering their information just once.
- Provide convenience to online shoppers.
- Eliminate the need to reenter payment card and shipping information at a site’s electronic checkout counter.

8.4.1 Types of Electronic Wallets

- **Server-side electronic wallet**

- Stores a customer's information on a remote server belonging to a particular merchant or wallet publisher

- **Client-side electronic wallet**

- Stores a consumer's information on his or her own computer.

8.4.2 Digital Wallets

- Client-based digital wallets are software applications that consumers install on their computer, and that offer consumer convenience by automatically filling out forms at online stores

- Server-based digital wallets are software-based authentication and payment services and products sold to financial institutions that market the systems to merchants either directly or as a part of their financial service package

- Electronic Commerce Modeling Language is a standard of digital wallets.

8.4.3 Examples of Electronic Wallets

1. **Microsoft .NET Passport**

   - An electronic wallet operated by Microsoft

   - Passport consists of four integrated services

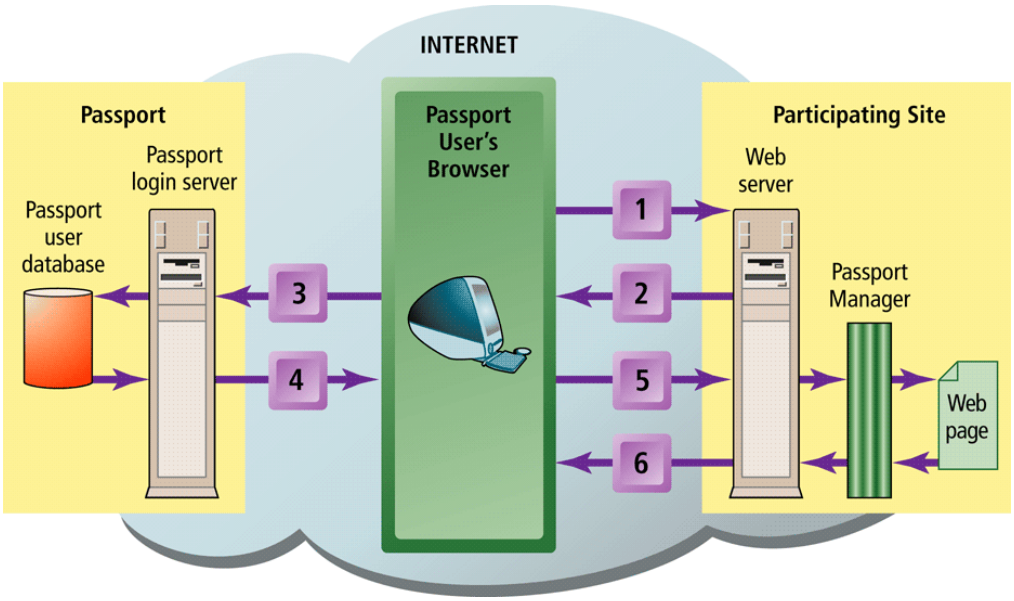
     - Passport single sign-in service (SSI)

     - Passport Wallet service

     - Kids Passport service

     - Public profiles

How Microsoft's Passport Wallet Works



2. **Agile Wallet**

- Developed by Cyber Cash
- Allows customers to enter credit card and identifying information once, stored on a central server
- Information pops up in supported merchants' payment pages, allowing one-click payment.
- Does not support smart cards or Cyber Cash, but company expects to soon

4. **eWallet**

- Developed by Launchpad Technologies
- Free wallet software that stores credit card and personal information on users' computer, not on a central server; info is dragged into payment form from eWallet.
- Information is encrypted and password protected.
- Works with Netscape and Internet Explorer.

5. **Microsoft Wallet**

   - Comes pre-installed in Internet Explorer 4.0, but not in Netscape
   - All information is encrypted and password protected
   - Microsoft Wallet Merchant directory shows merchants setup to accept Microsoft Wallet.

6. **Yahoo! Wallet**

   - Server side electronic wallet offered by Yahoo!
   - Lets users store information about several major credit and charge cards
   - Many industry observers and privacy rights activist groups are concerned about electronic wallets

8.4.4W3C Proposed Standard for Electronic Wallets

- World Wide Web Consortium (W3C) is attempting to create an extensible and interoperable method of embedding micropayment information on a web page
- Extensible systems allow improvement of the system without eliminating previous work
- Merchants must accept several payment options to insure the widest possible Internet audience
- Merchants must embed in their Web page payment information specific to each payment system

8.4.5The ECML Standard

- Electronic Commerce Modeling Language (ECML) proposed standards for electronic wallets
- Companies forming the consortium are America Online, IBM, Microsoft, Visa, and MasterCard
- Ultimate goal is for all commerce sites to accept ECML
- Unclear how this standard will incorporate privacy standards W3C set forth

- Electronic Commerce Modeling Language (ECML) Wallet/Merchant Standards Initiative, July 1999.

8.5 SUMMARY

This unit covers the requirement for internet based payment systems and their prospects. The working of electronic cash has been covered extensively.

8.6 KEYWORDS

Electronic Cash , digital currency, Electronic Wallets

8.7 REVIEW QUESTIONS

1. Explain the types of Electronic Wallets.

2. Describe the Properties of digital currency.

3. Explain Working of Electronic Cash.

4. Comment on advantages and disadvantages of Electronic Cash.

8.8 REFERENCES / SUGGESTED READINGS

- • Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc.
- • Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.
- • Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.
- • Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.

UNIT-09: ELECTRONIC PAYMENT MEDIA, CREDIT CARDS, DEBIT CARDS, SMART CARDS AND DIGITAL SIGNATURE

Structure:

9.0 Objectives:

After studying this unit we will be able

- To know about different Electronic Payment Method
- How to uses of Credit Card and Debit Card
- Different Types of Debit cards
- Different Types of Smart Card
- To know about the concept of Digital Signature.

9.1 Electronic Payment Media:

9.1.0 Electronic media:

Electronic media are media that use electronics or electromechanical energy for the end-user (audience) to access the content. This is in contrast to static media (mainly print media), which today are most often created electronically, but don't require electronics to be accessed by the end-user in the printed form. The primary electronic media sources familiar to the general

public are better known as video recordings, audio recordings, multimedia presentations, slide presentations, CD-ROM and online content. Most new media are in the form of digital media. However, electronic media may be in either analog electronic data or digital electronic data format.

Although the term is usually associated with content recorded on a storage medium, recordings are not required for live broadcasting and online networking. Any equipment used in the electronic communication process (e.g. television, radio, telephone, desktop computer, game console, handheld device) may also be considered electronic media.

9.1.1 What are the Types of Electronic Payment Systems?

Electronic payment systems have become more popular thanks to increased use of Internet shopping. These systems do not just involve Internet transactions, as there are more and more ways being developed to facilitate electronic money transfers. With increasing technology, the range of devices and processes used to transact electronically continues to increase while the use of cash and cheque transactions is decreasing. This is mainly because it is much easier to carry cards or use cell phones to pay for purchases compared to cash.

9.1.2 Cards:

These are the most common form of electronic payments. There are three types of cards: credit, debit and prepaid cards. They typically are made of plastic and have a magnetic stripe on the back of the card. This process typically takes only a few seconds to complete. Credit cards are an extremely popular form of electronic payment because you can use them almost anywhere for almost any kind of purchase, and you do not have to have cash on hand to pay for things.

9.1.3 Internet Payments:

Internet payments involve a person transferring money or making a purchase online. Consumers have a choice of either transferring the money directly from their bank account, which can easily be accessed online or they can use a credit, debit or prepaid card. Most people prefer to use the second option, especially when making online purchases. This form of payment continues to increase in popularity with the ever-growing e-commerce industry.

9.1.4 Mobile Payments:

Although the number of transactions that can be carried out via a cell phone are limited, they still can be used to facilitate some electronic transactions. Mobile phone manufacturers have enabled their phones' software to allow users to access electronic commerce. In some countries, mobile service providers allow their customers to have a bank account on their cell phone numbers and can use the funds in their accounts to carry out transactions.

9.1.5 Person-to-Person Payments:

These payments enable a person to pay another using an online account, a prepaid card or another mechanism that stores value. Various companies facilitating such payments are PayPal, Alert pay and Money bookers. These services can easily be accessed over the Internet via computers, phones and other devices. They provide an easy and secure means of making transactions online.

9.2 CREDIT Card:

9.2.0 Introduction:

A **credit card** is a payment card issued to users as a system of payment. It allows the cardholder to pay for goods and services based on the holder's promise to pay for them. The issuer of the card creates a revolving account and grants a line of credit to the consumer (or the user) from which the user can borrow money for payment to a merchant or as a cash advance to the user.

A credit card is different from a charge card: a charge card requires the balance to be paid in full each month. In contrast, credit cards allow the consumers a continuing balance of debt, subject to interest being charged. A credit card also differs from a cash card, which can be used like currency by the owner of the card. A credit card differs from a charge card also in that a credit card typically involves a third-party entity that pays the seller and is reimbursed by the buyer, whereas a charge card simply defers payment by the buyer until a later date. The size of most credit cards is 3 ⅜ × 2 ⅛ in (85.60 × 53.98 mm).

9.2.1 Parties involved in Credit Card:

Cardholder: The holder of the card used to make a purchase.

Card-issuing bank: The financial institution or other organization that issued the credit card to the cardholder. This bank bills the consumer for repayment and bears the risk that the card is used fraudulently.

Merchant: The individual or business accepting credit card payments for products or services sold to the cardholder.

9.2.2 How credit cards work?

Credit cards are issued by a credit card issuer, such as a bank or credit union, after an account has been approved by the credit provider, after which cardholders can use it to make purchases at Merchants accepting that card. Merchants often advertise which cards they accept by displaying acceptance marks – generally derived from logos – or may communicate this orally, as in "We take (brands X, Y, and Z)" or "We don't take credit cards".

When a purchase is made, the credit card user agrees to pay the card issuer. The cardholder indicates consent to pay by signing a receipt with a record of the card details and indicating the amount to be paid or by entering a personal identification number (PIN). Also, many merchants now accept verbal authorizations via telephone and electronic authorization using the Internet, known as a card not present transaction (CNP).

Many banks now also offer the option of electronic statements, either in lieu of or in addition to physical statements, which can be viewed at any time by the cardholder via the issuer's online banking website. Notification of the availability of a new statement is generally sent to the cardholder's email address. If the card issuer has chosen to allow it, the cardholder may have other options for payment besides a physical check, such as an electronic transfer of funds from a checking account. Depending on the issuer, the cardholder may also be able to make multiple payments during a single statement period, possibly enabling him or her to utilize the credit limit on the card several times over.

9.2.3 Benefits and Demerits of the Credit Card:

Benefits to customers:

The main benefit to each customer is convenience. Compared to debit cards and checks, a credit card allows small short-term loans to be quickly made to a customer who need not calculate a balance remaining before every transaction, provided the total charges do not exceed the maximum credit line for the card.

Different countries offer different levels of protection. In the UK, for example, the bank is jointly liable with the merchant for purchases of defective products over £100.

Many credit cards offer rewards and benefits packages, such as enhanced product warranties at no cost, free loss/damage coverage on new purchases, various insurance protections, for example, rental car insurance, common carrier accident protection, and travel medical insurance. Credit cards can also offer reward points which may be redeemed for cash, products, or airline tickets.

Demerits to customers:

Following are the major demerits to the customers:

- **High interest and bankruptcy:**

Low introductory credit card rates are limited to a fixed term, usually between 6 and 12 months, after which a higher rate is charged. As all credit cards charge fees and interest, some customers become so indebted to their credit card provider that they are driven to bankruptcy. Some credit cards often levy a rate of 20 to 30 percent after a payment is missed. In other cases a fixed charge is levied without change to the interest rate. In some cases universal default may apply: the high default rate is applied to a card in good standing by missing a payment on an unrelated account from the same provider. Complex fee structures in the credit card industry limit customers' ability to comparison shop, help ensure that the industry is not price-competitive and help maximize industry profits.

- **Inflated pricing for all consumers:**

Merchants that accept credit cards must pay interchange fees and discount fees on all credit-card transactions. In some cases merchants are barred by their credit agreements from passing these fees directly to credit card customers, or from setting a minimum transaction amount.

- **Weakens self regulation:**

Several studies have shown that consumers are likely to spend more money when they pay by credit card. Researchers suggest that when people pay using credit cards, they do not experience the abstract pain of payment.

- **Grace period:**

A credit card's grace period is the time the customer has to pay the balance before interest is assessed on the outstanding balance. Grace periods may vary, but usually range from 20 to 55 days depending on the type of credit card and the issuing bank. Some policies allow for reinstatement after certain conditions are met. Usually, if a customer is late paying the balance, finance charges will be calculated and the grace period does not apply. Finance charges incurred depend on the grace period and balance.

9.2.4 Benefits and Demerits to merchants:

Benefits to merchants:

For merchants, a credit card transaction is often more secure than other forms of payment, such as cheques, because the issuing bank commits to pay the merchant the moment the transaction is authorized, regardless of whether the consumer defaults on the credit card payment. In most cases, cards are even more secure than cash, because they discourage theft by the merchant's employees and reduce the amount of cash on the premises. Finally, credit cards reduce the back office expense of processing cheques/cash and transporting them to the bank.

Prior to credit cards, each merchant had to evaluate each customer's credit history before extending credit. That task is now performed by the banks which assume the credit risk. Credit cards can also aid in securing a sale, especially if the customer does not have enough cash on his or her person or checking account. Extra turnover is generated by the fact that the customer can purchase goods and/or services immediately and is less inhibited by the amount of cash in his or her pocket and the immediate state of his or her bank balance. Much of merchants' marketing is based on this immediacy.

For each purchase, the bank charges the merchant a commission (discount fee) for this service and there may be a certain delay before the agreed payment is received by the merchant. The commission is often a percentage of the transaction amount, plus a fixed fee (interchange rate).

Demerits to merchants:

Merchants are charged several fees for accepting credit cards. The merchant is usually charged a commission of around 1 to 4 percent of the value of each transaction paid for by credit card. The merchant may also pay a variable charge, called an Interchange rate, for each transaction. In some instances of very low-value transactions, use of credit cards will significantly reduce the profit margin or cause the merchant to lose money on the transaction.

Merchants with very low average transaction prices or very high average transaction prices are more averse to accepting credit cards. In some cases merchants may charge users a "credit card supplement", either a fixed amount or a percentage, for payment by credit card.

Merchants are also required to lease processing terminals, meaning merchants with low sales volumes may have to commit to long lease terms. For some terminals, merchants may also need to subscribe to a separate telephone line. Merchants must also satisfy data security compliance standards which are highly technical and complicated. In many cases, there is a delay of several days before funds are deposited into a merchant's bank account. Because credit card fee structures are very complicated, smaller merchants are at a disadvantage to analyze and predict fees. Finally, merchants assume the risk of charge backs by consumers.

9.2.5 Reasons to use Credit Card:

Personal finance experts spend a lot of energy trying to prevent us from using credit cards and with good reason.

1. Signup Bonuses: The standard debit card offers zero rewards or very small rewards. Many credit cards, however, offer significant rewards when used responsibly.

2. Cash Back: If we sign up for the right credit card, we can earn anywhere from 1-5% back on our purchases.

3. Investment Rewards: Some cards, like the Fidelity Investment Rewards card, offer a higher rate of cash back; in exchange we must deposit our cash back directly into an investment account.

4. Frequent-Flyer Miles: It seems like every airline these days has at least one credit card

available. Cardholders rack up miles at a rate of one mile per dollar spent, or sometimes one mile per two dollars spent.

5. Points: Many card rewards work on a point system where you earn up to five points per dollar spent. When we reach a certain point threshold, we can redeem our points for gift cards at some stores.

6. Safety: Paying with a credit card makes it easier to avoid losses from fraud. When our debit card is used fraudulently, the money is missing from our account instantly

By contrast, when our credit card is used fraudulently, we aren't out any money - we just notify our credit card company of the fraud and don't pay for the transactions we didn't make while the credit card company resolves the matter.

7. Grace Period: When we make a debit card purchase, our money is gone instantly. When we make a credit card purchase, our money remains in our checking account until a couple of weeks later when we pay our credit card bill. Hanging on to our money for this extra time can be helpful in two ways. First, if we pay our credit card from a high-interest checking account and earn interest on our money during the grace period, the extra interest will eventually add up to a meaningful amount. Second, when we always pay with a credit card, we don't have to watch our bank account balance like crazy to make sure we stay in the black.

8. Universal Acceptance: Certain purchases are difficult to make with a debit card. When we want to rent a car or stay in a hotel room, we'll almost certainly have an easier time if we have a credit card.

9. Building Credit: If we have no credit or are trying to improve our credit score, using a credit card responsibly will help our credit score because credit card companies will report our payment activity to the credit bureaus. Debit card use doesn't appear anywhere on our credit report, however, so it can't help we build or improve our credit.

9.3 DEBIT CARDS:

9.3.0 Introduction:

A **debit card** (also known as a **bank card** or **check card**) is a plastic payment card that provides the cardholder electronic access to his or her bank account(s) at a financial institution. Some cards have a stored value with which a payment is made, while most relay a message to the cardholder's bank to withdraw funds from a payer's designated bank account. The card, where accepted, can be used instead of cash when making purchases. In some cases, the primary account number is assigned exclusively for use on the Internet and there is no physical card. Debit cards usually also allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash.

In many countries, the use of debit cards has become so widespread that their volume has overtaken or entirely replaced cheques and, in some instances, cash transactions. The development of debit cards, unlike credit cards and charge cards, has generally been country specific resulting in a number of different systems around the world, which were often incompatible.

9.3.1 Types of Debit Card Systems:

- **Online debit system:**

Online debit cards require electronic authorization of every transaction and the debits are reflected in the user's account immediately. The transaction may be additionally secured with the personal identification number (PIN) authentication system; some online cards require such authentication for every transaction, essentially becoming enhanced automatic teller machine (ATM) cards.One difficulty with using online debit cards is the necessity of an electronic authorization device at the point of sale (POS) and sometimes also a separate PINpad to enter the PIN, although this is becoming commonplace for all card transactions in many countries.

- **Offline debit system:**

Offline debit cards have the logos of major credit cards (for example, Visa or MasterCard) or major debit cards and are used at the point of sale like a credit card. This type of debit card may be subject to a daily limit, and/or a maximum limit equal to the current/checking account balance from which it draws funds. Transactions conducted with offline debit cards require 2–3 days to be reflected on users' account balances.

- **Electronic purse card system:**

Smart-card-based electronic purse systems in which value is stored on the card chip, not in an externally recorded account, so that machines accepting the card need no network connectivity.

9.3.2 How to use a Debit Card?

Now, more and more people are using debit cards as a mode of payment. A reason for this is the convenience and speed of payment that it offers. Similar in look to a credit card, a debit card differs in that it is linked directly to a fund source such as a savings or a checking account. When the debit card is used, the payment is automatically deducted from the fund.

I. Activate the debit card with the bank where we obtained it from: Upon receipt of the debit card from our bank, make sure to activate it to make it ready for use. This can normally be done by contacting the number of the bank's assistance center listed on the back of the debit card.

II. Make sure that we have enough cash in the account linked to the debit card to fund for our purchases: Whereas we can use a credit card to make purchases even if we do not have enough funds in our account at the moment, For a debit card, we can typically only make as much purchases as the amount of funds we have in our account. In some cases, we can make purchases higher than the amount left in our account, but these would result in overdraw fees. Check that the fund in our account is not below the amount that we intend to spend, in order to maximize the use of the debit card.

III. Know the PIN number of our debit card: A debit card would usually come with a four-digit PIN (personal identification number), which you can change to another number that you can easily remember. Make sure that you have memorized our PIN, and that we do not disclose it to anyone.

IV. Hand our debit card to the cashier of the store where we are making a purchase: The cashier will swipe the debit card through the card reading machine. The card reader will then present an option whether to pay through debit or credit. Even if we are using a debit card, we can still opt to pay through a credit method.

- ✓ **Debit:** Verify that the amount of purchase entered in the card reader is correct. The card reader will then prompt you to enter your PIN. If you choose the debit option, we can normally opt for cash back as well. Instead of having to go to the ATM to get extra cash, cash back allows we to obtain the cash along with our purchase. The cash will be deducted from our account as well.
- ✓ **Credit:** Verify that the amount of purchase entered in the card reader is correct. Instead of having to input a PIN, we will be asked to sign the receipt, but the purchase amount will still be automatically deducted from our account.

V. Check that our transaction has been approved: A notice will be sent in the card reader indicating if our transaction has been approved. If it has not been approved, it is likely that we do not have sufficient funds in our account to make the purchase.

VI. Keep track of the purchases that we make with our debit card: It is always a good idea to log the expenses we pay with our debit card, to keep our spending patterns in check. Even if we would not incur debts as we might have with a credit card, forgetting to keep track of our debit card purchases might lead we to spend more than what we intended to, and leave we with less funds than we expected in our account.

9.3.3 Advantage and Disadvantage of Debit Card:

Advantages:

I. No need to carry cash. Just about every merchant accepts the debit card. including the dollar store and some thrift shops. We do not need to worry about losing cash or misplacing it in a pair of jeans only to find it two months later. If our purse or wallet is stolen our money is safe since the perpetrator would need our PIN number to access our funds.

II. We don't need to make a trip to the bank every time we need to withdrawal money. We can use our card just about any where we go, and if we need the cash we can access our money at an ATM machine any time of day or night.

III. Merchants may also offer cash back facilities to customers, where a customer can withdraw cash along with their purchase.

Disadvantages:

I. With a debit card we must keep accurate records. We must record each transaction so we will know what our account balance is at all times. If we do not keep records we run the risk of overdrawing our account which will result in bank fees. Not to mention the embarrassment we will suffer at the checkout line when our card is denied.

II. Some ATM machines charge a fee for their use and then our bank adds another foreign ATM charges (if the machine is not from our bank). Know ahead of time what the fees are and where we can access our money for free if possible.

9.4 SMART CARD:

9.4.0 Introduction:

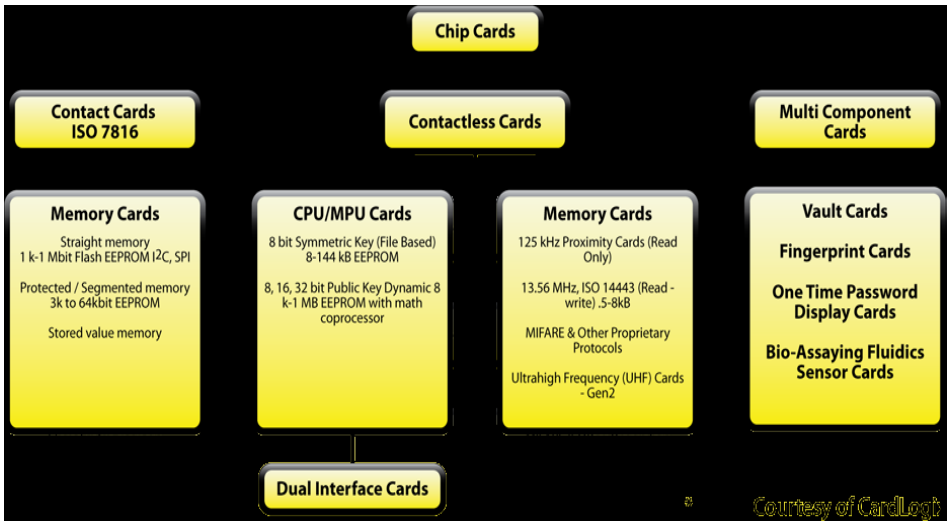
A **smart card**, **chip card**, or **integrated circuit card** (**ICC**) is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate. Since April 2009, a Japanese company has manufactured reusable financial smart cards made from paper. Smart cards can provide identification, authentication, data storage and

application processing. Smart cards greatly the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart card systems have proven to be more reliable than other machine-readable cards, such as magnetic-stripe and bar-code, with many studies showing card read life and reader life improvements demonstrating much lower cost of system maintenance. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Multifunction cards can also serve as network system access and store value and other data. Worldwide, people are now using smart cards for a wide variety of daily tasks.

9.4.1 Features of Smart Cards:

A smart card may have the following generic characteristics:

- Dimensions similar to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimetres (3.370 × 2.125 in).
- Contains a tamper-resistant security system and provides security services
- Managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.
- Communicates with external services via card-reading devices, such as ticket readers, ATMs, DIP reader, etc.



Contact Cards:

These are the most common type of smart card. Electrical contacts located on the outside of the card connect to a card reader when the card is inserted. This connector is bonded to the encapsulated chip in the card .Increased levels of processing power, flexibility and memory will add cost. Single function cards are usually the most cost-effective solution.

Contactless Cards:

These are smart cards that employ a radio frequency (RFID) between card and reader without physical insertion of the card. Instead, the card is passed along the exterior of the reader and read. Types include proximity cards which are implemented as a read-only technology for building access. These cards function with a very limited memory and communicate at 125 MHz. Another type of limited card is the Gen 2 UHF Card that operates at 860 MHz to 960 MHz True read and write contactless cards were first used in transportation for quick decrementing and reloading of fare values where their lower security was not an issue.

Hybrid Cards:

Hybrid cards have multiple chips in the same card. These are typically attached to each interface separately, such as a MIFARE chip and antenna with a contact 7816 chip in the same card.

Dual Interface Cards:

These cards have one chip controlling the communication interfaces. The chip may be attached to the embedded antenna through a hard connection, inductive method or with a flexible bump mechanism.

Multi-component Cards:

These types of cards are for a specific market solution. For example, there are cards where the fingerprint sensor is built on the card. Or one company has built a card that generates a one-time password and displays the data for use with an online banking application.

9.4.2 Applications:

- **Financial:**

Smart cards may also be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters, vending machines or merchants. Cryptographic protocols protect the exchange of money between the smart card and the machine. No connection to a bank is needed. The holder of the card may use it even if not the owner.

- **Public transit:**

Smart cards and integrated ticketing are used by many public transit operators. Card users may also make small purchases using the cards. Some operators offer points for usage, exchanged at retailers or for other benefits.

- **Schools:**

Smart cards are being provided to students at schools and colleges. Uses include:

- ✓ Tracking student attendance
- ✓ As an electronic purse, to pay for items at canteens, vending machines, laundry facilities, etc...
- ✓ Tracking and monitoring food choices at the canteen, to help the student maintain a healthy diet
- ✓ Tracking loans from the school library
- ✓ Access control for admittance to restricted buildings, dormitories, and other facilities.
- ✓ Access to transportation services

- **Healthcare:**

Smart health cards can improve the security and privacy of patient information, provide a secure carrier for portable medical records, reduce health care fraud, support new processes for portable medical records, provide secure access to emergency medical information, enable compliance with government initiatives (e.g., organ donation) and mandates, and provide the platform to implement other applications as needed by the health care organization.

9.4.3 Benefits:

The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card. Governments and regional authorities save money because of improved security, better data and reduced processing costs. These savings help reduce public budgets or enhance public services.

Individuals have better security and more convenience with using smart cards that perform multiple services. For example, they only need to replace one card if their wallet is lost or stolen. The data storage on a card can reduce duplication, and even provide emergency medical information.

Smart cards are widely used to protect digital television streams. Video Guard is a specific example of how smart card security worked.

9.4.4 Problems:

The plastic card in which the chip is embedded is fairly flexible. The larger the chip, the higher the probability that normal use could damage it. Cards are often carried in wallets or pockets, a harsh environment for a chip. However, for large banking systems, failure-management costs can be more than offset by fraud reduction.

Smart cards have also been the targets of security attacks. These attacks range from physical invasion of the card's electronics, to non-invasive attacks that exploit weaknesses in the card's software or hardware. The usual goal is to expose private encryption keys and then read and manipulate secure data such as funds. Once an attacker develops a non-invasive attack for a particular smart card model, he is typically able to perform the attack on other cards of that model in seconds, often using equipment that can be disguised as a normal smart card reader. While manufacturers may develop new card models with additional security, it may be costly or inconvenient for users to upgrade vulnerable systems.

Another problem is the lack of standards for functionality and security. To address this problem, The Berlin Group launched the ERIDANE Project to propose "a new functional and security framework for smart-card based Point of Interaction (POI) equipment".

9.5 DIGITAL SIGNATURE:

9.5.0. Introduction:

A digital signature is practically impossible to forge and cannot be sent by itself but only as a part of an electronic document or message. Signatures are commonly used to authenticate documents. When you sign a physical document, you are authenticating its contents. Similarly, digital signatures are used to authenticate the contents of electronic documents. They can be used with PDF, e-mail messages, and word processing documents.

To digitally sign a document, you must have a digital ID. This unique identifier can obtained from various certification authorities on the Web, such as VeriSign and EchoSign. Once we have a digital ID, we can add register it with programs that support digital signatures, such as Adobe Acrobat and Microsoft Outlook. Then you can use the program's "Sign" feature to add our digital signature to documents.

The digital signature is simply a small block of data that is attached to documents we sign. It is generated from our digital ID, which includes both a private and public key. The private key is used to apply the signature to the document, while the public key is sent with the file. The public key contains encrypted code, also called a "hash," that verifies your identity.

A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgeable. There are a number of different encryption techniques to guarantee this level of security.

9.5.1 Uses of Digital Signature:

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. Below are some common reasons for applying a digital signature to communications:

- **Authentication:**

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context.

- **Integrity:**

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. However, if a message is digitally signed, any change in the message after signature invalidates the signature.

- **Non-repudiation:**

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

9.5.2 Other Uses for Digital Signature:

Sometimes we need proof that the document came from we and no one has tampered with it since we sent it. Digital Signature with our SSL Certificate fills the bill.

On the other hand, sometimes we need to prove that a document came from someone else and has not been altered along the way. In legal matters, for example, we may need to prove that a contract has not been altered since someone sent it as an email.

9.6 SUMMARY:

This unit introduces the

- **Electronic Payment Media:** are media that use electronics or electromechanical energy for the end-user (audience) to access the content.
- **Credit Card:** is a payment card issued to users as a system of payment. It allows the cardholder to pay for goods and services based on the holder's promise to pay for them
- **Debit Card:** is a plastic payment card that provides the cardholder electronic access to his or her bank account at a financial institution.
- **Smart Card :** is any pocket-sized card with embedded integrated circuits
- **A digital signature :** is practically impossible to forge and cannot be sent by itself but only as a part of an electronic document or message

9.7 KEYWORDS:

Electronic Payment Media, Debit Card, Credit Card, Smart Card, Digital Signature

9.8 EXERCISES:

1) What is Electronic Payment Media? Explain different Methods of Payment Media.
2) Explain advantage and disadvantages of Credit Card?
3) Explain the parties involved in Credit Card.
4) Give the reasons to using Credit Cards.
5) Difference between Credit Card and Debit Card?
6) What is Debit Card and How to use it?
7) Describe types of Debit Cards?
8) What is Smart Card and its uses?
9) Explain the applications of the Smart Card?
10) Explain the uses of Digital Signature.

9.9 REFERENCES:

1. Electronic Commerce – Elias Malady
2. Frontiers of Electronic Commerce – Kalakos Whinstone
3. E-Commerce – Mamta Bhusry
4. Electronic Commerce – Gary P.Schneider

Unit 10: Security in cyberspace and designing for security

Structure:

10.0 Objectives:

After studying this unit we will be able to understand

- What is Cyberspace
- Methods of securities in Cyberspace
- Purpose of designing Securities
- How to design for Securities

10.1 Introduction of Cyberspace:

Cyberspace is a word that began in science fiction literature in the 1980s, was quickly and widely adopted by computer professionals as well as hobbyists, and became a household term in the 1990s. During this period, the uses of the internet, networking, and digital communication were all growing dramatically and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging. The parent term of cyberspace is "cybernetics", derived from the Ancient Greek a word introduced by Norbert Wiener for his pioneering work in electronic communication and control science.

The term cyberspace has become a conventional means to describe anything associated with the Internet and the diverse Internet culture. The United States government recognizes the

interconnected information technology and the interdependent network of information technology infrastructures operating across this medium as part of the US national critical infrastructure. Amongst individuals on cyberspace, there is believed to be a code of shared rules and ethics mutually beneficial for all to follow, referred to as cyber ethics.

In simple words **Cyberspace** means, the notional environment in which communication over computer networks occurs. In other words, **Cyberspace** is a worldwide network of computers and the equipment that connects them, which by its very design is free and open to the public (the Internet).

We've become increasingly reliant on the net, and it's being used right now to transfer everything from friendly emails to hypersensitive data. The problem has gotten more prevalent with, always on, high-speed internet access. Attackers are always out there looking for that type of computers.

10.1.0 Security:

"**Security"** is the quality or state of being secure--to be free from danger.

Following are the types of security.

- **Physical security -** addresses the issues necessary to protect the physical items, objects or areas of an organization from unauthorized access and misuse.
- **Personal security -** addresses the protection of the individual or group of individuals who are authorized to access the organization and its operations.
- **Operations security-** protection of the details of a particular operation or series of activities.
- **Communications security -** concerned with the protection of an organization's communications media, technology, and content.
- **Network security -** is the protection of networking components, connections, and contents.
- **Information Security –** protection of information and its critical elements, including the systems and hardware that use, store, or transmit that information.

10.1.1 The Need for Security:

Industry Need for Information Security

An organization needs information security for four important reasons:

- ✓ To protect the organization's ability to function,
- ✓ To enable the safe operation of applications implemented on the organization's IT systems,
- ✓ To protect the data the organization collects and uses, and
- ✓ To safeguard the technology assets in use at the organization.

10.1.2 Creating a Security Strategy:

Creating a security strategy is one of the most important steps in planning our deployment. Our strategy should meet our organization's security needs and provide a secure messaging environment without being overbearing to our users.

In addition, our security strategy needs to be simple enough to administer. A complex security strategy can lead to mistakes that prevent users from accessing their mail, or it can allow users and unauthorized intruders to modify or retrieve information that we don't want them to access.

The five steps to developing a security strategy as follows:

- ✓ Identifying what we are trying to protect.

  For example, our list might include hardware, software, data, people, documentation, network infrastructure, or your organization's reputation.
- ✓ Determining what we are trying to protect it from.

  For example: unauthorized users, spammers, or denial of service attacks.
- ✓ Estimating how likely threats are to our system. If we are a large service provider, our chances of security threats could be greater than a small organization. In addition, the nature of our organization could provoke security threats.
- ✓ Implementing measures that will protect our assets in a cost-effective manner. For example, the extra overhead in setting up an SSL connection can put a performance burden on our Messaging deployment. In designing our security strategy, we need to balance security needs against server capacity.

- ✓ Continuously reviewing our strategy and make improvements each time a weakness is found.

Our security strategy should also plan for:

- ✓ Physical Security
- ✓ Server Security
- ✓ Operating System Security
- ✓ Network Security
- ✓ Messaging Security
- ✓ Application Security

- ✓ **Physical Security:**

Limit physical access to important parts of our infrastructure. For example, place physical limits on routers, servers, wiring closets, server rooms, or data centers to prevent theft, tampering, or other misuse. Network and server security become a moot point if any unauthorized person can walk into our server room an unplug our routers.

- ✓ **Server Security:**

Limiting access to important operating system accounts and data is also part of any security strategy. Protection is achieved through the authentication and access control mechanisms available in the operating system. In addition, we should install the most recent operating environment security patches and set up procedures to update the patches once every few months and in response to security alerts from the vendor.

- ✓ **Operating System Security:**

Reduce potential risk of security breaches in the operating environment by performing the following, often termed "system hardening:"

- **Minimize the size of the operating environment installation:** When installing an Oracle server in an environment that is exposed to the Internet, or any non trusted network, reduce the Oracle Solaris OS software installation to the minimum number of

packages necessary to support the applications to be hosted. Achieving minimization in services, libraries, and applications helps increase security by reducing the number of subsystems that must be maintained.

The Oracle Solaris Security Toolkit provides a flexible and extensible mechanism to minimize, harden, and secure Oracle Solaris systems. The primary goal behind the development of this toolkit is to simplify and automate the process of securing Oracle Solaris systems.

- **Track and monitor file system changes:** Within systems that require inclusion of security, a file change control and audit tool is indispensable as it tracks changes in files and detects possible intrusion. We can use a product such as Tripwire for Servers, or Oracle Solaris Fingerprint Database.

✓ **Network Security:**

The recommended deployment configuration, to support both horizontal scalability and service security, is to place the access layer of the architecture behind a firewall. In a two-tiered architecture, use two firewalls, creating a DMZ. This enables access to the information delivery elements, the calendar and messaging front ends, while protecting the main service elements on the internal network behind a second firewall. Such a configuration also enables the access layer and data layer elements to be scaled independently, accommodating traffic and storage elements. Limiting access to our network is an important part of our security strategy. Normally, overall access to networks is limited through the use of firewalls. However, email must be made available outside our site. SMTP (Simple Mail Transfer Protocol**)** is one such service.

To secure our network, we should:

- Turn off all operating system-provided services that listen on ports that we do not use.
- Replace telnet with Solid State Hybrid Drive, if possible.
- Place our application servers behind a packet filter, which drops external packets with an internal source IP address. A packet filter forbids all connections from the outside except for those ports that we explicitly specify.

- ✓ **Messaging Security:**

  Messaging Server offers the following sets of security features:

- **Protecting Messaging Components in our Deployment:** With this set of options, we can secure our MTA relays, message stores, web mail clients, and multiplexing services. In addition, we'll learn about third-party spam filter options.

- **Planning User Authentication:** These options enable you to determine how your users will authenticate to your mail servers, preventing unauthorized users from gaining access to our system.

- **Understanding Security Misconceptions:** Using this set of options, we can perform user authentication and protect the message itself by using authenticated SMTP and certificates for digital signatures, encryption, and Secure Sockets Layer (SSL).

10.1.3 Cyber-risk:

Before knowing the need for security in cyberspace, we should know what is Cyber-risk. The term "cyber-risk" covers any computer or internet-based threat. This includes: hacking attempts; malicious code planted on a computer (malware) or network of computers; stolen credentials used for an unauthorized login, known as "phishing"; denial-of-service attacks; or data intercepted on wireless networks or found on lost laptops and mobile phones.

The threats or risk come in the form of:

1. Computer Intrusion (hacking-passive or active)
2. Denial of service attacks (DOS)
3. Virus & Worms deployment.
4. Web defacement.
5. Spam.
6. Spoofing.
7. Proxy scan.
8. Distributed denial of service.

9. Malicious codes:
    -Virus
    -Bolts
10. Data theft and data manipulation.
    - Identity theft
    - Financial frauds.
11. Social engineering scams.

10.2 Cyber attacks:

Cyber attacks, also referred as cyber-warfare or cyber-terrorism in specific situations, is a type of offensive maneuver employed by both individuals and whole organizations that targets computer information systems, infrastructures, computer networks, and personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. Cyber-warfare or cyber-terrorism can be as harmless as installing spyware on a PC or as grand as destroying the infrastructure of entire nations. In the 21st century as the world becomes more technologically advanced and reliant upon computer systems, cyber attacks have become more sophisticated, dangerous, and the preferred method of attacks against large groups by "attackers."

Cyber attack can be in any of the following form-

- **Trojan Horse Attack: -** Trojan Horse arrives via email or software like free games. Trojan Horse is activated when the software or attachment is executed. Trojan Horse releases virus, monitors computer activity, installs backdoor, or transmits information to hacker.
- **Denial of Service Attacks :-** In a denial of service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle. In a distributed denial of service attack, hundreds of computers (known as a zombies) are compromised, loaded with DOS attack software and then remotely activated by the hacker.

- **Spamming Attacks: -** Sending out e-mail messages in bulk. It's electronic "junk mail." Spamming can leave the information system vulnerable to overload. Less destructive, used extensively for e-marketing purposes.

10.3 Cyber Security:

"Cyber security" is getting more and more mixed usage lately, so much it becoming almost as ambiguous as the term "cloud" was a few years back . The challenge information security executives and professionals are faced with is knowing − as the title implies − when and why the term should be used and how it should be presented, as a single word or two. While there isn't any recognized authority on the subject per se, there are at least some credible sources providing guidance that can help those of us in the industry to decide on "when, why and how" to use the term.

"Cyber security refers to preventative methods to protect information from being stolen, compromised or attacked in some other way. It requires an understanding of potential information threats, such as viruses and other malicious code. Cyber security strategies include identity management, risk management and incident management."

10.3.0 The general problems of Cyber security:

Many different problems are customarily grouped within the subject of "computer network security." While they share certain basic characteristics (e.g. the deliberate exploitation of a vulnerability in an information system for improper purposes), other characteristics that are legally important are not necessarily shared. The attackers, targets, victims, harms and possible defensive measures are legally relevant characteristics, but they vary among the forms of cyber attacks. As a result, it is likely best not to attempt to make legal policy recommendations aimed at cyber security generally.

For example, the failure of a business to safeguard the sensitive personal information of customers might be met with various legal responses directed at the enterprise with lax security such as legislated security standards, mandatory public disclosure of security.

The primary difficulty of cyber security isn't technology -- it's policy. The Internet mirrors real-world society, which makes security policy online as complicated as it is in the real world. Protecting critical infrastructure against cyber-attack is just one of cyberspace's many

security challenges, so it's important to understand them all before any one of them can be solved.

The list of bad actors in cyberspace is long, and spans a wide range of motives and capabilities. At the extreme end there's cyber war: destructive actions by governments during a war. Cyber war is conducted by capable and well-funded groups and involves military operations against both military and civilian targets. Along much the same lines are non-nation state actors who conduct terrorist operations. Although less capable and well-funded, they are often talked about in the same breath as true cyber war.

Much more common are the domestic and international criminals who run the gamut from lone individuals to organized crime. They can be very capable and well-funded and will continue to inflict significant economic damage.

- **Cyber space security Importance:**

Electronic computing and communication pose some of the most complex challenges engineering has ever faced. From controlling traffic lights to routing airplanes, computer systems govern virtually every form of transportation. Radio and TV signals, cell phones, and (obviously) e-mail all provide variety of examples, how communication depends on computers not only in daily life, but also for military, financial, and emergency services. Utility systems providing electricity, gas, and water can be crippled by cyberspace disruptions. Attacks on any of these networks would potentially have disastrous consequences for individuals and for society.

In fact, serious breaches of cyber security in financial and military computer systems have already occurred. Identity theft is a burgeoning problem. Viruses and other cyber-attacks plague computers small and large and disrupt commerce and communication on the Internet.

Historically, the usual approach to computer protection has been what is called "perimeter defense." It is implemented by placing routers and "firewalls" at the entry point of a sub-network to block access from outside attackers. Cyber security experts know well that the perimeter defense approach doesn't work. All such defenses can eventually be penetrated or bypassed. And even without such breaches, systems can be compromised, as when flooding Web sites with bogus requests will cause servers to crash in what is referred to as a "denial of service" attack or when bad guys are already inside the perimeter.

The problems are currently more obvious than the potential solutions. It is clear that engineering needs to develop innovations for addressing a long list of cyber security priorities. For one, better approaches are needed to authenticate hardware, software, and data in computer systems and to verify user identities. Biometric technologies, such as fingerprint readers, may be one step in that direction.

A critical challenge is engineering more secure software. One way to do this may be through better programming languages that have security protection built into the ways programs are written. And technology is needed that would be able to detect vulnerable features before software is installed, rather than waiting for an attack after it is put into use.

Another challenge is providing better security for data flowing over various routes on the Internet so that the information cannot be diverted, monitored, or altered. Current protocols for directing data traffic on the Internet can be exploited to make messages appear to come from someplace other than their true origin.

All engineering approaches to achieving security must be accompanied by methods of monitoring and quickly detecting any security compromises. And then once problems are detected, technologies for taking countermeasures and for repair and recovery must be in place as well.

Finally, engineers must recognize that a cyber security system's success depends on understanding the safety of the whole system, not merely protecting its individual parts. Consequently cybercrime and cyber terrorism must be fought on the personal, social, and political fronts as well as the electronic front.

Among other things, that means considering the psychology of computer users — if security systems are burdensome, people may avoid using them, preferring convenience and functionality to security. More research is needed on how people interact with their computers, with the Internet, and with the information culture in general. Cultural and social influences can affect how people use computers and electronic information in ways that increase the risk of cyber security breaches.

- **National Strategy to Secure Cyberspace:**

In the United States government, the **National Strategy to Secure Cyber space**, is a component of the larger National Strategy for Homeland Security. The National Strategy to Secure

Cyberspace was drafted by the Department of Homeland Security in reaction to the September 11, 2001 terrorist attacks. Released on February 14, 2003, it offers suggestions, not mandates, to business, academic, and individual users of cyberspace to secure computer systems and networks.

The National Strategy to Secure Cyberspace identifies three strategic objectives:

- ✓ Prevent cyber attacks against America's critical infrastructures;
- ✓ Reduce national vulnerability to cyber attacks; and
- ✓ Minimize damage and recovery time from cyber attacks that do occur.

To meet these objectives, the National Strategy outlines five national priorities: The first priority, the creation of a National Cyberspace Security Response System, focuses on improving the government's response to cyberspace security incidents and reducing the potential damage from such events. The second, third, and fourth priorities (the development of a National Cyberspace Security Threat and Vulnerability Reduction Program, the creation of a National Cyberspace Security Awareness and Training Program, the necessity of Securing Governments' Cyberspace) aim to reduce threats from, and vulnerabilities to, cyber attacks. The fifth priority, the establishment of a system of National Security and International Cyberspace Security Cooperation, intends to prevent cyber attacks that could impact national security assets and to improve the international management of and response to such attacks.

Ultimately, the National Strategy encourages companies to regularly review their technology security plans, and individuals who use the Internet to add firewalls and anti-virus software to their systems. It calls for a single federal center to help detect, monitor and analyze attacks, and for expanded cyber security research and improved government-industry cooperation.

There are seven key components that need to be included in truly effective cyber legislation:

1. Information Sharing:

The first element of any legislation must be to enable and foster information sharing between the public and private sectors, and among private-sector entities themselves.

Effective information sharing is a critical and fundamental part of today's cyber security measures. Various organizations and government agencies collect and analyze information regarding cyber threats and vulnerabilities.

2. Cyber Insurance:

Private-sector actors with responsibility for cyber security include those who write the computer codes, who build the hardware on which the code operates, who provide information transmission services, who build and maintain intrusion detection and prevention systems, and many others. Most, if not all, of these actors deny any liability for injuries to third parties who are affected by cyber security breaches as a result of the acts or omissions of the original actors.

3. Cyber-Supply-Chain Security:

One of the biggest holes in the U.S. cyber system is in the area of supply chain security, especially hardware and key infrastructure components. Software vulnerabilities, while still capable of causing substantial loss, can be fixed relatively easily by updating the code or, if need be, replacing the software entirely.

4. Cyber Self-Defense:

Presently, there are no well-defined rules to tell businesses what they can and cannot do to establish self-defense mechanisms in the cyber domain. The Department of Justice is trying to increase its capacity for prosecuting cyber attackers. The National Security Division of the Justice Department is creating new positions across the country in its National Security Cyber Specialist (NSCS) network for people who can competently prosecute cyber cases. As the ability to attribute involvement to specific players expands, law enforcement can prosecute not just those who steal the data, but those who use it as well.

5. Awareness, Education, and Training:

The American people recognize that there is a problem with securing the cyber domain. They hear about it regularly on the news, and know, abstractly, that it is there. The difficulty is that they receive mixed messages. What the public lacks is consistent, accurate, and up-to-date information. The federal government has tried to play a role here but has failed. That is no surprise.

6. Cyber Workforce:

While the above provision is aimed at the population in general, this one is aimed at the development of a workforce to serve the technology industry and the key government organizations that use cyber means for higher-order activities, such as cyber warfare, defense of specific technical industry intellectual property, and critical infrastructure defense.

7. Cyber security Beyond the Borders:

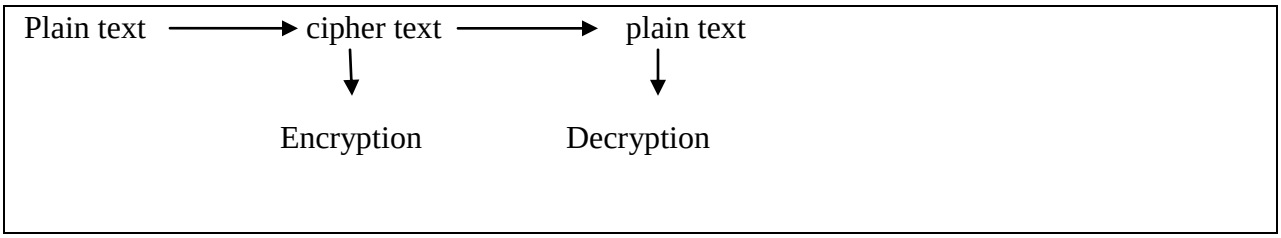
Cyber security is not now, and never will be, an issue that one country can solve alone. The solution will require a concerted—and ongoing—collaboration between the U.S. and like-minded free nations. Treaties and global governance do not contain bad actors, and should thus not be the focus of U.S. or international cyber security efforts. Instead, the U.S. must work with other friendly nations to alter bad cyber behavior by raising the costs of such behavior.

10.4 Designing for security in cyberspace:

There is no single answer to cyber-risk, but rather a combination of security best practice and policy, technical measures to discover and prevent breaches, and mitigation including backup plans and insurance in the event of a disaster.

Security in cyberspace can be designed in following ways-

- **Using intrusion alert programs:** They need to be operating constantly so that all unusual behavior on network is caught immediately.
- **Password:** Password should be charged with regular interval of time and it should ne alpha numeric and should be difficult to judge.
- **Using network scanning program**: We all should install all this software in our computer, so that we can get the information about warms and Trojan in the network, so it is very beneficial for our network system.
- **Encryption :** Encryption is the process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. As shown in the figure below, Encrypted data must be deciphered, or decrypted, before it can be read by the recipient.



Modern Encryption Methods:

- ✓ **Cryptographic Accelerator:** Coprocessor that calculates and handles the Random Number Generation.
  Eg: PCI coprocessor.
- ✓ **Authentication Token:** External device that interfaces with device to grant access. Two types: contact and Non Contact
  Eg: Credit Card, RSA Secure ID.
- ✓ **Biometric/ Recognition:** External device that measures human body factors to allow access.
  Eg: Fingerprint, Optical, Voice and Signature recognition.

Biometric method can be used by following devices:

- ✓ **By eye:** The iris of our eye is the colored part that surrounds our black pupil, the black part. Every iris is different. If a scan of a user's iris matches the one in the security system's memory, access is allowed.
- ✓ **By voice :** Another trait unique to every individual is his or her voice. The user speaks a specified word or sentence to gain access to a secured computer. Distinct patterns, tones, and other qualities in the voice must match the authorized user's voice in the computer's security system.
- ✓ **By fingerprint :** Another biometric option is the fingerprint and its unique identifying characteristics. Placed on a special reading pad, a designated finger's print is recognized by a computer. A similar biometric device scans a person's whole hand.
- ✓ **By blood vessels :** The blood vessels in a person's face radiate heat. The patterns of those vessels, and the heat scan, are completely individual and could be recognized and required for computer access.

There are several relatively simple steps that every organization can take to enhance its cyber security, beginning with the basics. Every extra measure strengthens an organization's security and makes it a little more difficult for attackers to penetrate. These should, as a start, include:

- Building a picture of where our data is stored, then protecting it based on its value to our organization.
- Implementing a password policy that requires and enforces strong passwords.
- Only allowing access where there is a clear business need.
- Requiring people to log in to systems as themselves – destroy all anonymous or generic accounts.

The Strategy is offering clear priorities for the European Union international cyberspace policy:

- **Freedom and openness:** The Strategy outlines the vision and principles on applying the EU core values and fundamental rights in cyberspace. Human Rights should also apply online and we will promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should promote democratic reform worldwide. The EU believes that increased global connectivity should not be accompanied by censorship or mass surveillance.

- **The laws, norms and EU core values apply as much in the cyberspace as in the physical world:** The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments. Developing cyber security capacity building: The EU will engage with international partners and organisations, the private sector and civil society to support global capacity building in third countries. It will include improving access to information and to an open Internet and preventing cyber threats.
- **Fostering international cooperation in cyberspace issues:** To preserve open, free and secure cyberspace is a global challenge, which the EU will address together with the relevant international partners and organizations, the private sector and civil society.

10.5 Unit Summary:

This unit introduces to:

- ✓ Cyberspace is a worldwide network of computers and the equipment that connects them, which by its very design is free and open to the public.
- ✓ Security is the quality or state of being secure--to be free from danger.
- ✓ Security Strategies:
  - Physical Security
  - Server Security
  - Operating System Security
  - Network Security
  - Messaging Security
- ✓ Cyber-risk covers any computer or internet-based threats.
- ✓ Cyber security refers to preventative methods to protect information from being stolen, compromised or attacked in some other way.

10.6 Keywords:

Cyberspace, Security in Cyberspace, Designing for Cyberspace.

10.7 Exercises:

1) What is cyberspace ?
2) What are the needs for security in cyberspace?
3) Explain the Strategies for securities in Cyberspace?
4) What do you mean by security? Explain various types of security.
5) Briefly explain Cyber Risk and Cyber Attack.
6) Explain the different forms of Cyber Attacks.
7) Explain the methods that can be followed to increase security in cyber space.

10.8 References:

1. Electronic Commerce – Elias Malady
2. Frontiers of Electronic Commerce – Kalakos Whinstone
3. E-Commerce – Mamta Bhusry
4. Electronic Commerce – Gary P.Schneider

Unit 11: How Much Risk Can You Afford? The Virus: Computer enemy Number one.

Structure:

11.0 Objectives:

After studying this unit you will be able to understand

- To know about Virus, Types of Virus
- Different kinds of Malware Viruses
- Protect system from Viruses

11.1 Computer virus:

A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their

keystrokes. However, not all viruses carry a destructive payload or attempt to hide themselves the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent.

A virus is a program with the capacity to propagate itself from computer to computer without any action from the computer user. It can also perform destructive actions on the computer it has infected when some trigger condition are met like successful infection, anniversary date, etc.

Viruses are a risk for email users as a large number of them were designed to use the lack of security features and bugs within Windows and Outlook to propagate.

11.1.0 Characteristics of Computer Viruses:

The characteristics of computer virus that is easy to why we feel and find out. Surely another computer performance than usual, because the virus is also the road on our computers. Here's one of the characteristics of Computer Virus Affected:

- ✓ Our computer is running slower than usual.
- ✓ Menu Run, Search hidden by the virus.
- ✓ CTRL + ALT + DEL cannot be used.
- ✓ Original folders on our computer hidden and replaced with virus files.
- ✓ Menu Tools -> Folder Options missing in Windows Explorer.
- ✓ Computers are often stopped or not responding.
- ✓ Computer suddenly restarts or crash, and this happened a few minutes.
- ✓ Computer applications are not running properly and often error.
- ✓ File Folder Icon Appears with but have a file type. Exe
- ✓ Hard drive or disk drive inaccessible.
- ✓ Print activity is not working properly.
- ✓ It often happens that strange error messages and does not usually.
- ✓ Often seen the menu or dialog box that is damaged.
- ✓ Duplication of names there are folders inside the folder.
- ✓ Computers are always issued a message of where the virus originated.

Neither of the above are common symptoms and characteristics of computers affected by viruses, but it can also occur as a result of interference with the hardware or software as well. The main solution is to install an antivirus that is always updated , the intention is that the antivirus can be updated. So a good antivirus is in fact not an expert or experts said, but a good antivirus is an antivirus that can be updated.

11.1.1 Programs which are NOT viruses:

- **Trojan horse:** A standalone program which does its damage immediately, while we are running it for another purpose (usually a game!).
- **Bomb:** A standalone program (like a Trojan horse) whose only effect is to destroy some part of our system (programs, data) but does not pretend to be another program while it runs.
- **Bug:** A legitimate program with some logic error which causes accidental damage to our system even though everything was done according to the manual.
- **User error:** A human error (which the human may deny!) which causes loss of data or programs, or damage to hardware, due to accident or entry of incorrect commands.

11.1.2 Viruses and worms:

The term virus is familiar to most users of computer equipment. This term is often used to describe all kinds of software that replicate from computer to computer, and even incorrectly for some other kinds of software that do not replicate. However, it is not widely known that there are two different groups of replicating software, viruses and worms. The difference between these two groups may not be obvious to the computer user who encounters a virus or worm, but the difference is significant from a technical point of view. A worm, for example, is able to use services provided by a modern networked environment much more efficiently than a virus. This results in an advantage that enables worms to spread much faster than viruses.

The name virus is borrowed from biological science. A biological virus is a passive element that floats around until it hits a suitable cell. The mechanisms of the matching cell are then used to reproduce the biological virus, to express it in a simplified way. The term virus is rather suitable for computer-based equivalents, as computer viruses are passive in the same way.

They attach to a carrier object and wait for the object to be transmitted to another computer. Once transmitted, they activate and start looking for other objects to infect.

A pure worm is more independent than a virus. A pure worm works by itself as an independent object. It does not need a carrier object to attach itself to. The worm can also spread by initiating telecommunications by itself. There is no need to wait for a human to send the file or document. There are also intermediate forms that resemble both viruses and worms. Many of the mass-mailing worms that have become widespread actually belong to this category.

They may spread attached to documents or other objects just like viruses, but still use email clients to mass mail themselves in a worm-like way. Another fact that separates these from pure worms is that the user must usually open an attachment in the mail before the worm activates. This slows down the replication speed compared to pure worms, as the worm must wait for actions from the receiver. This category of worms does, however, spread much faster than viruses because of the automatic transmission of the worm.

A computer environment must naturally meet some requirements to make worms possible. A worm's method of replication cannot work unless computers are networked in some way. It must be possible for a program to browse the network for other computers, connect to these computers and remotely install and start the worm without user intervention. This is the main reason for the fact that viruses were the most common form of malware in PC environments for a long time. The rapid growth of the Internet has provided worms with the functionality they need. Worms have actually caused almost all of the big “virus-incidents”.

Types of Computer virus:

- **Boot sector viruses :**

A boot sector virus infects the boot sector of floppy disks or hard drives. These blocks contain a small computer program that participates in starting the computer. A virus can infect the system by replacing or attaching itself to these blocks. These viruses replicate very slowly because they can only travel from one computer to another on a diskette. In addition, a boot attempt must be made on the target computer using the infected diskette before the virus can infect it. The virus may, however, reside on the diskette and infect new computers even if there is no operating system on it.

- **Traditional file viruses:**

This group of viruses replicates when attached to MS-DOS program files with the EXE or COM extensions. They cannot infect 32-bit EXE files used by newer versions of MS Windows. This group of viruses can replicate over any media that can transfer files, such as diskettes, local area networks, remote lines etc. Email did not play a significant role in spreading these viruses, as it was an unusual way of communicating in MS-DOS and Windows 3.x-based environments. These viruses, however, have a clear disadvantage compared to boot sector viruses; they require that program files be transmitted. In business environments this is usually done only as part of a maintenance procedure, not as part of everyday computer usage.

- **Document or macro viruses:**

Document or macro viruses are written in a macro language. Such languages are usually included in advanced applications such as word processing and spreadsheet programs. The vast majority of known macro viruses replicate using the MS Office program suite, mainly MS Word and MS Excel, but some viruses targeting other applications are known as well. Documents created using these applications are actually quite complex container files. The files work internally like miniature file systems. Separate so called "data streams" are created for the actual document data, data saved for undo operations, revisions of the document, embedded objects, macro procedures etc. It is usually easy for a virus to add its macros to the file using the application's own functions. High-level interfaces are available and the virus author does not need to understand how the macros are stored. The macro systems of these applications usually include features that make it possible to run certain macros automatically when a document is opened. Viruses use these features to activate when the virus is copied to a new computer.

- **32-bit file viruses :**

Previous file viruses were made for 16-bit program files used by MS-DOS. The 32-bit versions of Windows, such as Windows 95, 98 and NT, use a different and more complex format for the program files. Traditional files viruses cannot infect these files. A new group of file viruses emerged as the 32-bit operating systems became more popular. These viruses are by

nature similar to the previous file viruses with the exception that they can infect the new file format and work in 32-bit environments. This category is also called PE-viruses, because the new executable file format's name is PE (portable executable). The new format is also used by many other modules in the system, such as DLLs, system drivers etc. Some viruses infect these modules as well, but most stick to program files with the EXE extension.

- **Mail worms :**

A worm is by definition similar to a virus but more independent. The first wave of worms was seen when Internet mail became a standard way to communicate. An email client, and especially address books and mailing lists, provide a powerful way to reach a large number of recipients worldwide with very little effort. Modern, advanced email programs also provide this functionality through APIs that make it possible for computer programs to automatically send messages. All this together provides an environment that enables mail worms to spread much faster than viruses.

- **Pure worms:**

Pure worms have the potential to spread very quickly because they are not dependent on any human actions, but the current networking environment is not ideal for them. They usually require a direct real-time connection between the source and target computer when the worm replicates. A significant number of the computers connected to the Internet, however, are on-line only temporarily and perhaps behind dial-up connections. Servers are currently the main group of computers that meet these criteria. A larger number of machines, including workstations, may be suitable targets for a worm in local area networks that provide constant connectivity. Some technique to transfer and start the worm on the remote machine is also needed.

11.2 Malware Virus:

A malware virus is a catch-all term for any annoying or harmful software that makes its way onto a computer or a network without the owner's awareness. The word "malware" comes from the phrase "malicious software." Software is considered to be malware depending on what the intention of its creator was. Computer viruses, worms, Trojan horses, spyware or any other

form of unwanted software can be considered a malware virus. It is important to distinguish a malware virus from "bugs" or small defects in otherwise legitimate software.

A variety of purposes can be served by a malware virus, from simple pranks or vandalism, to making a financial profit for its creator. Throughout the early history of malware in the 1980s and 1990s, almost every malware virus was written for the sole purpose of playing a prank. Among the less-harmful viruses that circulated during this time was one that opened up all the text documents in a hard drive, and changed every instance of the word "and" to "not." A virus is technically defined as malware that requires intervention on the part of the computer user in order to function, such as opening up a malicious email attachment. Worms are variants of viruses, and may accomplish the same purpose, but are more insidious since they work on their own, without user intervention. One of the more infamous and dangerous types of malware viruses that have been seen is the Trojan horse virus. This is a group of viruses that make their way onto a computer, and act as something of a ticking time bomb. At the appointed time, they can erase a hard drive or steal confidential information before rendering the person's computer essentially inoperable. Trojan horse viruses typically present themselves as something that they are not, in order to gain access to a computer hard drive and conceal themselves. More recently, it has been common to see malware viruses that attempt to make a profit from stealing personal information from a computer user. Keystroke loggers are one example of this newer kind of malware. Their purpose is to keep track of every keystroke that is made on a computer, in order to mine data such as passwords, credit card numbers and other sensitive information. This financially motivated malware is often referred to as crime ware or spyware, and can be some of the most troublesome malware in existence.

Fortunately, there are many ways in which computer users can protect themselves from the threat of a malware virus. Anti-virus and anti-spam software are good places to start, and are recommended for those who own a computer that runs a Windows & trade; operating system. It is usually not considered necessary on computers with other operating systems, since most viruses are not written in a way that targets them.

11.2.0 Malware virus types:

The following are the important types of Malware viruses:

- **Trojan horses:**

The name Trojan horse is borrowed from Greek mythology. In the computer world the term refers to a program that contains hidden malicious functions. The program may look like something funny or useful such as a game or utility, but harms the system when executed. Many Trojans contain activation criteria that enable the Trojan to work for a while. The user is convinced that the program is safe and useful, and forwards it to other users before the malicious code strikes. Trojans lack a replication routine and thus are not viruses by definition. A Trojan is spread to other computers only through deliberate transfer by the users.

- **Backdoor Trojans:**

Backdoor Trojans are a special kind of Trojan that grant unauthorized access to computer systems. This type of Trojan is rather common and can pose a significant threat to business users.

These Trojans consist of two programs that interoperate: the silent server module planted in a victim's computer and the console used by a hacker. The silent server module acts as a spying tool. The console connects to it using networking protocols and transmits commands to it. This system can then be used to retrieve data from the target computer, modify data, alter system settings, execute programs and even record video and sound if the computer is equipped with multimedia capabilities.

- **Jokes:**

A joke program does something funny or tasteless, but does not harm the computer environment. The effect may be music or sounds, video or animations, interactive functions etc. Some jokes may disturb the computer's user interface and be rather annoying, but the effect is temporary and no permanent damage is done. If permanent damage is done, then the program is by definition a Trojan rather than a joke.

11.3 Virus spread:

Computer viruses are damaging, self-replicating programs which can spread from one computer to another via the Internet, a network, or a detachable computer device such as a printer, floppy disc, CD or USB drive. Over the last decade, the proliferation of Internet usage in offices and homes has propagated the spread of computer viruses and the demand for virus detection and virus removal software. Due to its dominance as the most widely-used operating system, Microsoft Windows is the most frequently targeted platform for virus creators.

The most commonly understood means of preventing computer viruses is to refrain from opening email attachments of an unknown origin or suspicious name. However, computer viruses can also be spread through text-based emails and instant messages, if the user clicks on an infected web address link within the message. Once inside a host computer, a virus may attach itself to an executable file within a certain program. Once the program is opened, the virus's code will execute and replicate itself. In order to avoid detection, many computer viruses employ stealthy hiding techniques which are written into their code, such as the ability to even interfere with anti-virus software.

There are a number of precautionary measures one can take to minimize their risk of contracting computer viruses. Popular anti-virus systems, Norton Anti Virus & trade; and Virus

Scan & reg ; from McAfee & reg are available for download and purchase via the Internet, while anti-virus systems such as AVG Anti-virus and security software are available for download on the Internet at no cost. Anti-virus systems need to be kept updated at all times in order to adequately block the latest computer viruses. Computer users should also refrain from opening suspicious email attachments, clicking on suspicious HTML links, and downloading programs of unknown origin on the Internet as much as possible. To prevent data loss in the event of virus infection, computer users should regularly backup their systems to a disk or separate hard-drive. Although anti-virus software is the best tool for detecting whether or not our computer is infected with a virus, there are a number of warning signs that are easy to spot. For example, if our computer is operating at a slower pace than usual, frequently freezes or crashes, restarts by itself, prevents access to certain discs or drives, or displays unusual error messages, we may be infected with a computer virus.

A virus is by definition a computer program that spreads or replicates by copying itself. There are many known techniques that can be used by a virus, and viruses appear on many platforms. However, the ability to replicate itself is the common criterion that distinguishes a virus from other kinds of software. The term virus is quite often misused. Some viruses contain routines that damage the computer system on which it runs. This so called payload routine may also display graphics, play sounds or music etc. This has lead to a situation where viruses are assumed to cause deliberate damage, even if there are many viruses that don't.

The term virus has, for these reasons, become a synonym for malicious software, which is incorrect from a technical point of view. The process of spreading a virus includes both technical features in the virus itself and the behavior of the computer user. Most viruses are by nature parasitic. This means that they work by attaching themselves to a carrier object. This object may be a file or some other entity that is likely to be transmitted to another computer.
The virus is linked to the host object in such a way that it activates when the host object is used. Once activated, the virus looks for other suitable carrier objects and attaches itself to them. This dependency on the human factor slows down the replication of viruses. Another closely related program type, a worm, reduces this dependency and is able to replicate much faster.

A virus always resides hidden in some useful object. A macro virus may, for example, infect an important document, but the user does not notice this as the document looks perfectly normal and may be used just like any other document. This means that it is hard for an ordinary

user to tell if a system is or is not infected. Special software is needed to examine the system and detect a virus infection.

- ✓ Trading, copying or pirating software on diskettes without knowing the source.
- ✓ Software salesmen giving demos on our computer from their diskettes.
- ✓ Computer repair personnel using diagnostic disks.
- ✓ Computer user groups and bulletin boards

11.3.0 When viruses activate:

- ✓ Every few times the computer is booted up ("Stoned" virus, every 8th boot).
- ✓ On a certain day of the year (March 6, "Michaelangelo" virus, destructive mutant of "Stoned").
- ✓ On a certain day of the week ("Sunday" virus).
- ✓ On a certain day of the month ("Friday the 13th", "Saturday the 14th" viruses).
- ✓ Every day EXCEPT one ("Israeli" or "Suriv03" virus, every day except Friday the 13th.)
- ✓ On a certain date only. (Jan. 1, 2000 "Century" will activate, write zeroes to all connected disks, effectively destroying all data and programs, destroying all directories, file allocation tables, boot records and partition tables, possibly causing the disk to have to be returned to the dealer for repair.)
- ✓ A certain period after infection ("Plastique" virus, one week).
- ✓ After infecting a certain number of files ("MIX/1" virus, six files).
- ✓ After a certain number of keystrokes ("Devil's Dance" virus, 2000 keystrokes; after 5000 destroys hard disk data and prints characteristic "Devil's Dance" message).
- ✓ At a particular time of day ("Teatime" virus, between 3:10 and 3:13 PM, trashes every 11th keystroke.)
- ✓ Any combination of the above, plus anything we can probably think of!

11.4 Protection from Virus:

Many computers, especially those running a Windows operating system, are at risk of contracting computer viruses. While some viruses are merely annoying, others can cause severe damage to our computer and may corrupt data beyond repair. To protect our computer from viruses, there are a few simple steps that can be taken. We must consider it a full time job; our

computer is never truly safe unless it is disconnected from the Internet and we never insert computer disks or software from unreliable sources.

Keeping a close eye on the health of our operating system and software is an important way to protect our computer from viruses. Ideally, we should use an operating system that is less susceptible to viruses, such as Linux or Macintosh. If we have a Windows operating system, make sure to keep up with updates and system patches so that viruses cannot exploit system vulnerabilities. Use security patches for web browsers as well, especially if we use Internet Explorer, or consider using a less vulnerable browser, like Mozilla Firefox or Opera. If our computer starts to run sluggishly or behave oddly, we may have a computer virus, and we should take steps to eliminate it.

Anti-virus software will help protect our computer as well, by maintaining a database of viruses and eliminating threats to our system as they arise, along with running periodic whole system scans. Anti-virus software can only effectively work if we keep it running at all times and update it frequently. Most software will automatically tell us when it needs updates. If we cannot afford anti-virus products, consider using anti-virus freeware from a reputable source.

We can also protect our computer from viruses by using a secure Internet connection and combining it with a firewall. Firewalls are easy to install; most computers have a setting which allows us to turn a firewall on and off, and if we make use of a wireless router, the router often has a firewall as well. If we are on a college or corporate network, the network administrators may take addition steps to protect the system from viruses so that the whole computer network will be healthy. Take advantage of anti-virus software and updates provided by our network, along with the firewall, which is often stronger than that on a personal computer.

Protect our computer from viruses by not installing untrustworthy software, clicking on pop-up ads, or opening unfamiliar e-mails, especially those that come with attachments. Use anti-virus scanning software to inspect incoming e-mail, and use the quarantine feature to isolate and eliminate incoming infected files. Make sure to scan disks that we use as well, to make sure that a virus is not contained on the disk, even it is from someone we know and trust.

A common belief is that viruses are written by teenage boys. This is true in part, but the situation is changing as new virus writing techniques enter the scene. Writing a working virus is not too difficult, but writing a successful virus is not an easy task. It is not enough to be a good programmer, and knowledge of how modern IT systems work on a larger scale is needed as well.

This has lead to a situation where more mature persons, even IT professionals, are involved as well. It is hard to provide accurate information about who is writing viruses and why. Most virus writers want to remain anonymous and their motives are rarely known.
There are several reasons for this.

- Most individuals realize that writing a virus is not ethically acceptable, even if it is legal. Most virus writers want to remain anonymous, or use a pseudonym if they give statements about their creation.
- Computer viruses are a new problem. There are still many countries where the laws do not address virus writing explicitly, even if significant improvements have taken place during in recent years.
- Even if writing a computer virus is illegal, the authorities often lack resources and skills to investigate and trace virus authors. These facts have led to a situation where most virus authors want to remain unknown, and the authorities are not willing to investigate a case due to unclear legislation or lack of resources.

However, some successful investigations have been performed. The targets have usually been the authors of the most successful and widespread viruses, which have also caused the most damage.

Another visible phenomenon is the forming of virus writing groups. These groups consist of a varying number of members with a common hobby: writing viruses or performing hacking-related activities. Group members are usually active on the Internet under pseudonyms. Because of efficient networking, the members of a virus-writing group may be located anywhere in the world but still work together on common virus projects.

New viruses or hacking tools made by the group are usually clearly labeled with the group's name. Different groups tend to compete about who can write the most advanced viruses or other hacking tools, or attain the most publicity.

The motives of most virus writers remain unknown. There are however some motives that can be identified by examining virus samples or talking to known or anonymous virus authors.

- **Challenge and curiosity.** There are no courses or good books about how to write viruses. Many programmers want to see if they can do it, and do not necessarily realize that the virus may cause significant damage.

- **Fame and power.** Even if the author remains anonymous, it probably gives a kick to read about the virus in headlines. The virus, and possibly the damage it has caused makes other people work and react in some way.
- **Protest and anarchy.** A virus is quite a powerful way to cause intentional damage. There have been cases where a virus is intended to harm a school's network.
- **Proof of concept.** Someone may for example want to prove that a certain replication technique works. This type of virus may also appear on new platforms or applications capable of hosting viruses.
- **Political motives.** A virus may be used to spread a political message. This may, for example, be protests against totalitarian governments, multinational corporations etc. Organized political parties do not use viruses.

Many viruses contain some information about the author of the virus. This information should be used with great care, especially if the indicated author is the real name of an existing person. Virtually no one puts his or her own name in a virus, and any real name in a virus is probably an attempt to harm the reputation of that person. One should also be very careful when drawing conclusions about the virus author based on political messages in the virus. The apparent party or person behind the message may or may not be the real author of the virus. The author may just as well be someone who wants that party to look like a virus writer.

11.4.0 Most commonly use Anti-viruses:

- **McAfee, Inc.** formerly McAfee Security is an American global computer security software company headquartered in Santa Clara, California, and the world's largest dedicated security technology company. As of February 28, 2011, McAfee is a wholly owned subsidiary of Intel. In early 2014, Intel announced it would rebrand McAfee as Intel Security in 2014.
- **Symantec Corporation** is an American computer security, backup and availability solutions software corporation headquartered in Mountain View, California, United States. It is a Fortune 500 company and a member of the S&P 500 stock market index.
- **Kaspersky Lab** is a Russian multi-national computer security company, co-founded by Eugene Kaspersky and Natalia Kaspersky in 1997. Kaspersky Lab is a developer of secure content and threat management systems and the world's largest privately held vendor of software security products. Kaspersky Lab is headquartered in Moscow.

11.5 Conclusions:

Adapting to new architectures:

The computer systems used by business and home users have developed tremendously over the past ten years. Both system architecture and the way we use computers is totally different from the late 1980s and early 1990s. But the virus problem is still there, worse than ever. As a matter of fact, viruses and worms have been able to adopt and benefit from the new features that modern computer environments offer.

11.6 Unit Summary:

This unit introduces to

- A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".
- Types of Computer virus:
  - ✓ Boot sector viruses
  - ✓ Traditional file viruses
  - ✓ Document or macro viruses

- ✓ 32-bit file viruses
- ✓ Worms

- A malware virus is a catch-all term for any annoying or harmful software that makes its way onto a computer or a network without the owner's awareness.
- Other kinds of Malware:
  - ✓ Trojan horses
  - ✓ Backdoor Trojans
  - ✓ Jokes

11.7 Keywords:

Computer Virus, Types of Virus, Malware Virus.

11.8 Exercises:

1) What is Virus and Explain Types of Virus?
2) Write a note on Malware Virus?
3) How to protect computer from Viruses?
4) How the Computer Viruses will be spread. Explain
5) Write a note on Trojan Virus?
6) Briefly explain the different types of Anti-virus Softwares ?

11.9 References:

1. Electronic Commerce – Elias Malady
2. Frontiers of Electronic Commerce – Kalakos Whinstone
3. E-Commerce – Mamta Bhusry
4. Electronic Commerce – Gary P.Schneider

Unit 12: Security Protection and Recovery. Marketing on the Internet. Cyber frauds, Financial frauds, e-mail frauds.

Structure:

12.0 Objectives:

After studying this unit you will be able to understand:

- To know about the protection of Securities.
- Internet Marketing and its uses.
- Different kinds of Frauds.
- Different methods of Backups etc.

12.1 Introduction of Security Protection and Recovery:

Data or Security Protection and Recovery is the fourth Core Infrastructure Optimization capability. The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Standardized level in Data Protection and Recovery.

Challenges	Solutions	Benefits
Business Challenges	**Projects**	**Business Benefits**
No standard data management policy, which creates isolated islands of data throughout the network on file shares, nonstandard servers, personal profiles, Web sites, and local PCs.	Implement backup and restore solutions for critical servers	Effective data management strategy drives stability in the organization and improves productivity.
Poor or non-existent archiving and backup services makes achieving regulatory compliance difficult.	Consolidate and migrate file and print servers to simplify backup and restoration.	Standards for data management enable policy enforcement and define SLAs, improving the business relationship to IT.
Lack of disaster recovery plan could result in loss of data and critical systems.	Deploy data protection tools for critical servers.	Strategic approach to data management enables better data recovery procedures, supporting the business with a robust platform. Organization is closer to implementing regulatory compliance
IT Challenges		**IT Benefits**
Hardware failure or corruption equates to catastrophic data loss..		Mission-critical application data are kept in a safe place outside of the IT location.
Server administration is expensive.		Basic policies have been established to guarantee access to physical media (tapes, optical devices) when necessary.
IT lacks tools for backup and restore management.		

The Standardized Level in the Infrastructure Optimization Model addresses key areas of Data Protection and Recovery, including Defined Backup and Restore Services for Critical Servers. It requires that our organization has procedures and tools in place to manage backup and recovery of data on critical servers.

12.1.0 Backup and Restore Services for Critical Servers:

Backup and recovery technologies provide a cornerstone of data protection strategies that help organizations meet their requirements for data availability and accessibility. Storing, restoring, and recovering data are key storage management operational activities surrounding one of the most important business assets: corporate data.

Data centers can use redundant components and fault tolerance technologies (such as server clustering, software mirroring, and hardware mirroring) to replicate crucial data to ensure high availability. However, these technologies alone cannot solve issues caused by data corruption or deletion, which can occur due to application bugs, viruses, security breaches, or user errors.

There may also be a requirement for retaining information in an archival form, such as for industry or legal auditing reasons; this requirement may extend to transactional data, documents, and collaborative information such as e-mail. Therefore, it is necessary to have a data protection strategy that includes a comprehensive backup and recovery scheme to protect data from any kind of unplanned outage or disaster, or to meet industry requirements for data retention.

The following guidance is based on the Windows Server System Reference Architecture implementation guides for Backup and Recovery Services.

Phase 1: Assess

The Assess Phase examines the business need for backup and recovery and takes inventory of the current backup and recovery processes in place. Backup activities ensure that data are stored properly and available for both restore and recovery, according to business requirements. The design of backup and recovery solutions needs to take into account business requirements of the organization as well as its operational environment.

Phase 2: Identify

The goal of the Identify Phase of our backup and recovery solution is to identify the targeted data repositories and prioritize the critical nature of the data. Critical data should be defined as data required for keeping the business running and to comply with applicable laws or regulations. Any backup and recovery solutions that are deployed must be predictable, reliable, and capable of complying with regulations and processing data as quickly as possible.

Challenges that we must address in managing data include:

- Managing growth in the volumes of data.
- Managing storage infrastructure to improve the Quality of Service (QoS) as defined by Service Level Agreements (SLAs), while reducing complexity and controlling costs.
- Integrating applications with storage and data management requirements.
- Operating within short, or nonexistent, data backup windows.
- Supporting existing IT systems that cannot run the latest technologies.
- Managing islands of technology that have decentralized administration.
- Assessing data value so that the most appropriate strategies can be applied to each type of data.

While the backup and restoring of all organizational data is important, this topic addresses the backup and restore policies and procedures we must implement for critical services to successfully move from a Basic level to a Standardized level.

Phase 3: Evaluate and Plan

In the Evaluate and Plan Phase, we should take into account several data points to determine the appropriate backup and recovery solution for our organization. These requirements can include:

- How much data to store.
- Projected data growth.
- Backup and restore performance.
- Database backup and restore needs.
- E-mail backup requirements.
- Tables for backups and restores.

- Data archiving (off-site storage) requirements.
- Identification of constraints.
- Select and acquire storage infrastructure components.
- Storage monitoring and management plan.
- Testing the backup strategy.

- **Backup Plan:**

In developing a backup and recovery plan for critical servers we need to consider these factors:

- **Backup Modes:**

The backup mode determines how the backup is carried out in relation to the data that is being backed up.

There are two ways in which data backups can take place:

- ✓ **Online Backups.** Backups are made while data is still accessible to users.
- ✓ **Offline Backups.** Backups are made of data that is first rendered inaccessible to users.

- **Backup Types:**

Various types of backups can be used for online and offline backups. An individual environment's SLA, backup window, and recovery time requirement determine which method or combination of methods is optimal for that environment.

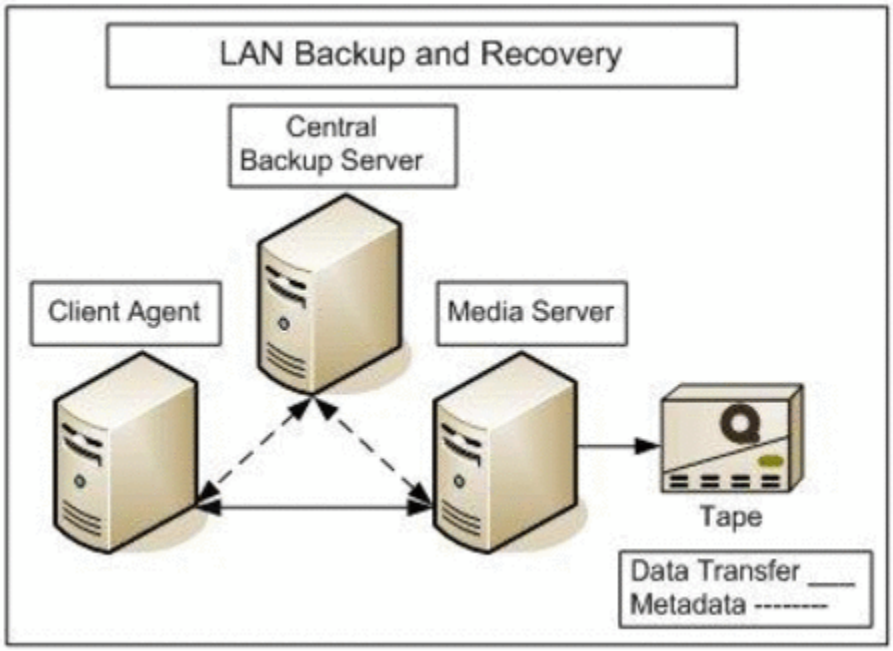
- ✓ **Full Backup.** Captures all files on all disks.
- ✓ **Incremental Backup.** Captures files that have been added or changed since the last incremental backup.
- ✓ **Differential Backup.** Captures files that have been added or changed since the last full backup.

- **Backup Topologies:**

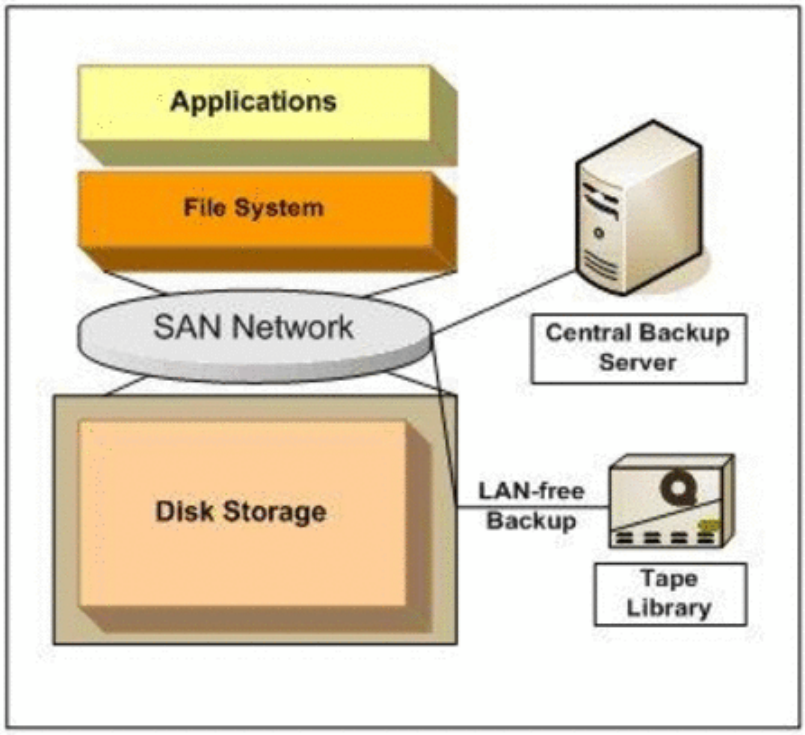
Originally, the only type of storage technology that required backup involved hard disks connected directly to storage adapters on servers. Today, this kind of storage is known as direct-attached storage, or DAS. The backup and recovery landscape has changed markedly with the development of technologies such as Storage Area Network (SAN) and Network Attached

Storage (NAS). SAN environments in particular provide a significant opportunity to optimize and simplify the backup and recovery process.

- ✓ **Local Server Backup and Recovery (DAS).** Each server is connected to its own backup device.
- ✓ **LAN-Based Backup and Recovery (NAS).** This is a multi-tier architecture in which some backup servers kick off jobs and collect metadata about the backed-up data (also known as control data) while other servers (designated as media servers) perform the actual job of managing the data being backed up.



- ✓ **SAN-Based Backup and Recovery.** In this topology we have the ability to move the actual backup copy operation from the production host to a secondary host system.



- **Service Plan:**

We have to consider many factors when designing our backup and recovery service. Among the factors to consider are:

- ✓ Fast backup and fast recovery priorities – Recovery Time Objective (RTO).
- ✓ The frequency with which data changes.
- ✓ Time constraints on the backup operation.
- ✓ Storage media.
- ✓ Data retention requirements.
- ✓ Currency of recovered data – Recovery Point Objective (RPO).

- **Recovery Plan:**

Even the best backup plan can be ineffective if we don't have a recovery plan in place. Following are some of the elements of a good data recovery plan.

- **Verify Backups:**

Verifying backups is a critical step in disaster recovery. We can't recover data unless we have a valid backup.

A good safeguard is to back up any existing log files before we restore a server. If data is lost or an older backup set is restored by mistake, the logs help to recover.

A drill measures our ability to recover from a disaster and certifies our disaster recovery plans. Create a test environment and attempt a complete recovery of data. Be sure to use data from production backups, and to record how long it takes to recover the data. This includes retrieving data from off-site storage.

Phase 4: Deploy

After the appropriate storage infrastructure components are in place and the backup and recovery service plan is defined, our organization can install the storage solution and associated monitoring and management tools into the IT environment.

12.2 Marketing on the Internet:

Internet marketing is the fastest growing and most exciting branch of marketing today, as the world becomes ever more connected, keeping up with developments and trends is vital for marketers trying to reach new audiences who are more discerning, fragmented and cynical than ever.

Marketing efforts done solely over the Internet. This type of marketing uses various online advertisements to drive traffic to an advertiser's website. Banner advertisements, pay per click (PPC), and targeted email lists are often methods used in Internet marketing to bring the most value to the advertiser. Internet marketing is a growing business mainly because more and more people use the internet every day. Popular search engines such as Google and Yahoo have been able to capitalize on this new wave of advertising.

Technology and software are changing at such a high rate that it seems almost impossible to keep up with trends. Products and services are evolving and adapting to the online sphere. The web is constantly shifting, growing and changing everything is fleeting.

Internet marketing – often called online marketing or e-marketing is essentially any marketing activity that is conducted online through the use of internet technologies. It comprises not only advertising that is shown on websites, but also other kinds of online activities like email and social networking. Every aspect of internet marketing is digital, meaning that it is electronic information that is transmitted on a computer or similar device, though naturally it can tie in with traditional offline advertising and sales too.

12.2.0 Principles of Internet marketing:

Internet marketing has three cornerstone principles:

- **Immediacy:** The web changes at a blistering pace and online audiences, whose attention spans are short, expect on-the-minute updates and information to keep the favour and attention of this group, we must respond to online messages and interact with communities as quickly as possible.

- **Personalization:** Customers online are no longer faceless members of a broad target audience – they are individuals who want to be addressed personally use the wealth of personal information available online to our benefit by targeting the relevant people precisely and personally.

- **Relevance:** Communication online must be interesting and relevant to the reader, otherwise it will simply be ignored. With all the information that is competing for our audience's attention, we must find a way to stand out and engage readers. The best way to do this is by giving them exactly what they want, when they want it. Throughout this course, we will learn tips and techniques for making all our online communication more immediate, personal and relevant.

12.2.1 Uses of Internet Marketing:

- Market and competitors are already there. If we market and sell products or services to a middle-class clientele, we need to extend our strategy to include the internet.

- Web users expect the highest convenience and information at their fingertips, all companies need a website as their central point of contact. If our details don't come up in a web search, we will be ignored.
- Customers are fickle, they will not expend a lot of energy to find us online. Even worse, if our competitor is easy to find online, our potential customers will happily turn to them.
- Since South Africans are using, socializing and buying on the web and especially because current advertising spend is still very low now is an excellent time to move our marketing into the online sphere and capitalize on a new and connected audience.
- Audiences want to interact with and converse about our brand and products give them the opportunity to do it in a mediated space, and become part of the discussion.
- Online marketing is almost always cheaper and more targeted than traditional.

12.3 Cyber frauds:

The development of the internet and digital technologies represent a major opportunity , transforming businesses and providing new tools for everyday communication. According to survey data from the Office for National Statistics (ONS), 80 per cent of households in Great Britain had an internet connection in 2012, up from 77 percent in 2011 (ONS, 2012a). Internet users are spending increasing amounts of time online and undertaking a greater range of online and social networking activities (Ofcom, 2012). In terms of business, online retail spending in 2012 accounted for around 10 percent of all retail spend each month in Great Britain.

A crime in which the perpetrator develops a scheme using one or more elements of the Internet to deprive a person of property or any interest, estate, or right by a false representation of a matter of fact, whether by providing misleading information or by concealment of information.

As increasing numbers of businesses and consumers rely on the Internet and other forms of electronic communication to conduct transactions; illegal activity using the very same media is similarly on the rise. Fraudulent schemes conducted via the Internet are generally difficult to trace and prosecute, and they cost individuals and businesses millions of dollars each year.

Definitions:

According to a U.S. JUSTICE DEPARTMENT Web site devoted to the topic, Internet fraud refers to any type of scheme in which one or more Internet elements are employed in order to put forth "fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme." As pointed out in a report prepared by the National White Collar Crime Center and the Federal Bureau of Investigation (FBI) in 2001, major categories of Internet fraud include, but are not limited to, auction or retail fraud, Securities fraud, and Identity Theft.

Securities fraud, also called investment fraud, involves the offer of bogus stocks or high-return investment opportunities, market manipulation schemes, pyramid and Ponzi schemes, or other "get rich quick" offerings. Identity theft, or identity fraud, is the wrongful obtaining and use of another person' personal data for one's own benefit; it usually involves economic or financial gain for the perpetrator.

However, the internet also presents opportunities to cyber criminals. The nature of some 'traditional' crime types has been transformed by the use of computers and other information communications technology (ICT) in terms of its scale and reach, with risks extending to many aspects of social life, such as:

- Financial transactions;
- Sexual offending;
- Harassment and threatening behavior; and
- Commercial damage and disorder.

New forms of criminal activity have also been developed, targeting the integrity of computers and computer networks such as the spread of malware and hacking. Threats exist not just to individuals and businesses, but to national security and infrastructure.

The cyber threat has been assigned a 'Tier One' threat status in the national security strategy (HMSO, 2010) – one of the highest priorities for action. To assist in tackling the cyber threat, £860 million of public funding was set aside as part of a five-year National Cyber Security Programme.

Improvement in detecting a Cyber Crime:

The national cyber security strategy (Cabinet Office, 2011) sets out the key objectives that the Government intends to achieve by 2015 in relation to cyber security and cyber crime, to both tackle the threats and reap the benefits of cyberspace.

In 2013 the new National Crime Agency (NCA) brought together specialist law enforcement capability into a National Cyber Crime Unit (NCCU) to address some of the most serious forms of cyber crime. The new Serious and Organized Crime Strategy, issued alongside the launch of the NCA, sets out the framework and direction for those tackling on serious and organized crimes, which can also include cyber crimes.

It is critical for policy makers to have knowledge of the scale and nature of cyber crime, how it is changing over time and whether interventions to tackle the problem are having an impact. This will help to drive forward policy decisions with a sound evidence base in this area and is vital in the context of emerging forms of cyber crime and technological developments.

- Collates a comprehensive evidence base regarding cyber crime, that is identifying data, analysis and research from published academic, industry and government sources.
- Considering the reliability, objectivity and quality of available evidence, indicating the extent that available data sources can be relied on.
- Focus on cyber-dependent crime and specific forms of cyber-enabled crimes fraud and theft, and sexual offending against children. These are areas where there is more, higher-quality evidence available than for other forms of cyber crime.

12.4 Financial Fraud:

Financial fraud can be broadly defined as an intentional act of deception involving financial transactions for purpose of personal gain. **Fraud is a crime**, and is also a civil law violation. Many fraud cases involve complicated financial transactions conducted by 'white collar criminals' such as business professionals with specialized knowledge and criminal intent.
An unscrupulous investment broker may present clients with an opportunity to purchase shares in precious metal repositories.

For example, Management status as a professional investor gives him credibility, which can lead to justified credibility among potential clients. Those who believe the opportunity to be legitimate contribute substantial amounts of cash and receive authentic-looking bond

documentation in return. If the investment broker is fully aware that no such repositories exist and still receives payments for worthless bonds, then victims may sue him for fraud.

Fraudsters can contact their potential victims through many methods, which include face- to-face interaction, by post, phone calls, sms or emails. The difficulty of checking identities and legitimacy of individuals and companies, the ease with which fraudsters can divert visitors to dummy sites and steal personal financial information, the international dimensions of the web and ease with which fraudsters can hide their true location, all contribute to making internet fraud the fastest growing area of fraud.

"Get-Rich-Quick" schemes are plans which offers high or unrealistic rates of return for a small amount of investment while at the same time promising that such investment is easy and risk-free.

Illegal schemes or scams are often advertised through spam or 'cold-calling'. Some forms of advertising for these schemes market books or compact discs about getting rich quick rather than asking participants to invest directly in a concrete scheme. It is clearly possible to get rich quickly if one is prepared to accept very high levels of risk - this is the premise of the gambling industry. However, gambling offers the near-certainty of completely losing the original stake over the long term, even if it offers some wins along the way. Nevertheless, many people long for instant wealth, and find these schemes appealing.

The following financial fraud activities are prohibited under relevant legislations.

- ✓ Illegal Deposit Taking
- ✓ Illegal Internet Investment Scheme
- ✓ Illegal Foreign Exchange Trading Scheme
- ✓ Unauthorized Withdrawals
- ✓ Unauthorized Use of Credit or Debit Card
- ✓ Misuse of Bank Negara Malaysia and Senior Officers' Names and Positions

12.5 E-mail fraud:

Email fraud is the intentional deception made for personal gain or to damage another individual through email. Almost as soon as email became widely used, it began to be used as a means to defraud people. Email fraud can take the form of a "con game" or scam. Confidence

tricks tend to exploit the inherent greed and dishonesty of their victims. The prospect of a 'bargain' or 'something for nothing' can be very tempting. Email fraud, as with other 'bunco schemes' usually targets naive individuals who put their confidence in get-rich-quick schemes such as 'too good to be true' investments or offers to sell popular items at 'impossibly low' prices. Many people have lost their life savings due to fraud. The fact is that 80 to 90 percent of emails are spam.

12.5.0 Forms of E-mail Frauds:

- **Spoofing:**

Email sent from someone pretending to be someone else is known as spoofing. Spoofing may take place in a number of ways. Common to all of them is that the actual sender's name and the origin of the message are concealed or masked from the recipient. Many, if not most, instances of email fraud do use at least minimal spoofing, as most frauds are clearly criminal acts. Criminals typically try to avoid easy traceability.

- **Phishing for data:**

Some spoof messages purport to be from an existing company, perhaps one with which the intended victim already has a business relationship. The 'bait' in this instance may appear to be a message from 'the fraud department

- **Bogus offers:**

Email solicitations to purchase goods or services may be instances of attempted fraud. The fraudulent offer typically features a popular item or service, at a drastically reduced price. Items may be offered in advance of their actual availability. For instance, the latest video game may be offered prior to its release, but at a similar price to a normal sale.

- **Requests for help:**

The "request for help" type of email fraud takes this form: an email is sent requesting help in some way. However, a reward is included for this help, which acts as a "hook". The reward may be a large amount of money, a treasure, or some artifact of supposedly great value.

The con man tells the "mark" (victim) that he is "allowed" to supply money, for which he should expect a generous reward when the prisoner returns. The confidence artist claims to have chosen the victim for their reputation for honesty.

12.5.1 Avoiding E-mail fraud:

Due to the widespread use of web bugs in email, simply opening an email can potentially alert the sender that the address to which the email is sent is a valid address. This can also happen when the mail is 'reported' as spam, in some cases: if the email is forwarded for inspection, and opened, the sender will be notified in the same way as if the addressee opened it.

Email fraud may be avoided by:

- ✓ Keeping one's email address as secret as possible.
- ✓ Using a spam filter.
- ✓ Noticing the several spelling errors in the body of the "official looking" email.
- ✓ Ignoring unsolicited emails of all types and simply deleting them.
- ✓ Ignoring offers from unknown sources. The contents of an email are not a formal or binding agreement.

Many frauds go unreported to authorities, due to feelings of shame, guilt, or embarrassment.

12.6 Unit Summary:

This unit introduces to,

- Internet marketing is marketing efforts done solely over the Internet.
- Principles Internet marketing
  - ✓ Immediacy
  - ✓ Personalization
  - ✓ Relevance
- Cyber frauds Online theft of credit card number, expiration date, and other information for criminal use.
- Financial fraud can be broadly defined as an intentional act of deception involving financial transactions for purpose of personal gain.

- Email fraud is the intentional deception made for personal gain or to damage another individual through email.

12.7 Keywords :

Internet Marketing, CyberFraud, Financial Frauds, E-Mail Frauds and Protection & Recovery.

12.8 Exercises:

1) Write note on Security Protection.
2) Explain the different phases of Backup and Restore services.
3) What do you mean by Marketing on Internet?
4) Explain the uses of the Internet marketing.
5) What is Financial Frauds and its types?
6) Write a note on Cyber Fraud.
7) Explain the forms of E-Mail Frauds?

12.9 References:

1. Electronic Commerce – Elias Malady
2. Frontiers of Electronic Commerce – Kalakos Whinstone
3. E-Commerce – Mamta Bhusry
4. Electronic Commerce – Gary P.Schneider

Unit-13: Online Shopping, Internet Marketing Techniques

Structure:

13.0 Objectives:

After studying this unit you will be able to understand

- To know about online shopping.
- Different features of Online Shopping
- Different methods of Online payment
- Internet Marketing
- To know about Internet Marketing Techniques.

13.1 Online shopping:

Online shopping or online retailing is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the Internet using a web browser. Alternative names are: e-web-store, e-shop, e-store, Internet shop, web-shop, web-store, online store, online storefront and virtual store. Mobile commerce (or m-commerce) describes purchasing from an online retailer's mobile optimized online site or app.

An online shop evokes the physical analogy of buying products or services at a bricks-and-mortar retailer or shopping center, the process is called business-to-consumer (B2C) online

shopping. In the case where a business buys from another business, the process is called business-to-business (B2B) online shopping. The largest of these online retailing corporations are Alibaba , Amazon.com and eBay.

Retail success is no longer all about physical stores, this is evident because of the increase in retailers now offering online store interfaces for consumers. With the growth of online shopping, comes a wealth of new market footprint coverage opportunities for stores that can appropriately cater to offshore market demands and service requirements.

13.1.0 Online Shopping Features:

The following are the important features of Online Shopping :

- **Make it easy and obvious to start the buying process:**

Not only should there be a "buy" button that's easy to find, but there should be buttons in various places throughout the website. For example, putting buttons next to the image is a logical place, but we should also make it possible for people to add images to their cart at the thumbnail view too.

- **Require as little as possible from the user:**

Don't require a user to supply a ton of information just to buy something from us. They shouldn't have to register for an account before they can buy something. Embrace "gradual engagement" as much as possible, don't ask them anything unless we absolutely have to, and only when it's necessary (and natural) in the process.

- **Provide constant feedback and status updates:**

People like to know where they are in the checkout process, and how much time they have left until their order has been placed. They also like getting confirmation that they just completed an action, like "You just added 2 items to your shopping cart."

- **Show the total as you go:**

One big mistake is to hide the order total until the very end, when the user has decided to check out. This is the wrong time to spring a big price-tag on them because they might decide that it's easier to just bail out rather than try to figure out how to get rid of some of the items.

Buyers like to know their total as early-on in the process as possible. This includes estimated shipping charges as well. By letting them know what they've spent early on, we'll avoid giving them sticker shock at the end, and they're more likely to finish the checkout process.

- **Cart contents should be obvious:**

Our users shouldn't have to wait until the "checkout" process before they can see what they've added to the cart. The shopping cart contents should be easy to view no matter where we are in the website. The user shouldn't have to leave our images just to see what they've already selected.

People like "active carts" – meaning that the information displayed on the page that we're on changes dynamically based on other shopping activity (i.e. having a smart navigation link that knows exactly how much is in their cart.)

- **Don't require information to be entered twice:**

Did you ever call the cable or phone company and have to enter our account number before they'll connect us and then when we are finally connected with a real person, they ask us the account number again? We hate that, right? So why would us require our customers to do this? Be mindful of these instances, and avoid them. (One simple place to start: shipping & billing information.)

- **Keep the checkout process as short as possible:**

The shorter the process, the more people will complete the checkout process. This is a fact. Remove steps, and simplify everything wherever possible. One great way to shorten the process is to have a "Batch add to cart" feature, so our users can add many images to the cart at the same time.

13.1.1 Methods of Payment of Online Marketing:

Online shoppers commonly use a credit card or a PayPal account in order to make payments. However, some systems enable users to create accounts and pay by alternative means, such as:

- Billing to mobile phones and landlines.

- Cash on delivery (C.O.D.)
- Cheque / Check
- Debit card
- Direct debit in some countries
- Electronic money of various types
- Gift cards
- Postal money order
- Wire transfer/delivery on payment
- Invoice, especially popular in some markets/countries.
- Bit coin or other crypto currencies

Some online shops will not accept international credit cards. Some require both the purchaser's billing and shipping address to be in the same country as the online shop's base of operation. Other online shops allow customers from any country to send gifts anywhere.
The financial part of a transaction may be processed in real time (e.g. letting the consumer know their credit card was declined before they log off), or may be done later as part of the fulfillment process.

13.1.2 Advantages of Online Marketing:

- **Convenience:**

Online stores are usually available 24 hours a day, and many consumers have Internet access both at work and at home. Other establishments such as internet cafes and schools provide internet access as well. In contrast, visiting a conventional retail store requires travel and must take place during business hours.

In the event of a problem with the item (e.g., the product was not what the consumer ordered, the product was not satisfactory), consumers are concerned with the ease of returning an item in exchange for either the correct product or a refund. Consumers may need to contact the retailer, visit the post office and pay return shipping, and then wait for a replacement or refund. Some online companies have more generous return policies to compensate for the traditional advantage of physical stores.

- **Information and reviews:**

Online stores must describe products for sale with text, photos, and multimedia files, whereas in a physical retail store, the actual product and the manufacturer's packaging will be available for direct inspection which might involve a test drive, fitting, or other experimentation. Some online stores provide or link to supplemental product information, such as instructions, safety procedures, demonstrations, or manufacturer specifications. Some provide background information, advice, or how-to guides designed to help consumers decide which product to buy. Some stores even allow customers to comment or rate their items. There are also dedicated review sites that host user reviews for different products. Reviews and even some blogs give customers the option of shopping for cheaper purchases from all over the world without having to depend on local retailers.

In a conventional retail store, clerks are generally available to answer questions. Some online stores have real-time chat features, but most rely on e-mails or phone calls to handle customer questions.

- **Price and selection:**

One advantage of shopping online is being able to quickly seek out deals for items or services provided by many different vendors (though some local search engines do exist to help consumers locate products for sale in nearby stores). Search engines, online price comparison services and discovery shopping engines can be used to look up sellers of a particular product or service.

Shipping costs (if applicable) reduce the price advantage of online merchandise, though depending on the jurisdiction, a lack of sales tax may compensate for this.

Shipping a small number of items, especially from another country, is much more expensive than making the larger shipments bricks-and-mortar retailers order. Some retailers (especially those selling small, high-value items like electronics) offer free shipping on sufficiently large orders.

Another major advantage for retailers is the ability to rapidly switch suppliers and vendors without disrupting users' shopping experience.

13.1.3 Disadvantages of Online Marketing:

- **Fraud and security concerns:**

Given the lack of ability to inspect merchandise before purchase, consumers are at higher risk of fraud than face-to-face transactions. Merchants also risk fraudulent purchases using stolen credit cards or fraudulent repudiation of the online purchase. However, merchants face less risk from physical theft by using a warehouse instead of a retail storefront.

Secure Sockets Layer (SSL) encryption has generally solved the problem of credit card numbers being intercepted in transit between the consumer and the merchant. However, one must still trust the merchant (and employees) not to use the credit card information subsequently for their own purchases, and not to pass the information to others. Also, hackers might break into a merchant's web site and steal names, addresses and credit card numbers, although the Payment Card Industry Data Security Standard is intended to minimize the impact of such breaches. Identity theft is still a concern for consumers. Computer security has thus become a major concern for merchants and e-commerce service providers, who deploy countermeasures such as firewalls and anti-virus software to protect their networks.

Phishing is another danger, where consumers are fooled into thinking they are dealing with a reputable retailer, when they have actually been manipulated into feeding private information to a system operated by a malicious party.

Quality seals can be placed on the Shop web page if it has undergone an independent assessment and meets all requirements of the company issuing the seal. The purpose of these seals is to increase the confidence of online shoppers. However, the existence of many different seals, or seals unfamiliar to consumers, may foil this effort to a certain extent.

A number of resources offer advice on how consumers can protect themselves when using online retailer services. These include:

- ✓ Sticking with known stores, or attempting to find independent consumer reviews of their experiences; also ensuring that there is comprehensive contact information on the website before using the service, and noting if the retailer has enrolled in industry oversight programs such as a trust mark or a trust seal.
- ✓ Before buying from a new company, evaluate the website by considering issues such as: the professionalism and user-friendliness of the site; whether or not the company lists a telephone number and street address along with e-contact information; whether a fair and

reasonable refund and return policy is clearly stated; and whether there are hidden price inflators, such as excessive shipping and handling charges.

- ✓ Ensuring that the retailer has an acceptable privacy policy posted. For example note if the retailer does not explicitly state that it will not share private information with others without consent.
- ✓ Ensuring that the vendor address is protected with SSL (Secure Sockets Layer) when entering credit card information. If it does the address on the credit card information entry screen will start with "HTTPS".
- ✓ Using strong passwords, without personal information. Another option is a "pass phrase," which might be something along the lines: "I shop 4 good a buy!!" These are difficult to hack, and provides a variety of upper, lower, and special characters and could be site specific and easy to remember.

Although the benefits of online shopping are considerable, when the process goes poorly it can create a thorny situation. A few problems that shoppers potentially face include identity theft, faulty products, and the accumulation of spyware. Whenever users purchase a product, they are required to put in their credit card information and billing/shipping address. If the website is not secure, customer information can be accessible to anyone who knows how to obtain it. Most large online corporations are inventing new ways to make fraud more difficult. However, criminals are constantly responding to these developments with new ways to manipulate the system. Even though online retailers are making efforts to protect consumer information, it is a constant fight to maintain the lead. It is advisable to be aware of the most current technology and scams protect consumer identity and finances.

Product delivery is also a main concern of online shopping. Most companies offer shipping insurance in case the product is lost or damaged. Some shipping companies will offer refunds or compensation for the damage, but this is up to their discretion.

- **Lack of full cost disclosure:**

The lack of full cost disclosure may also be problematic. While it may be easy to compare the base price of an item online, it may not be easy to see the total cost up front. Additional fees such as shipping are often not be visible until the final step in the checkout

process. The problem is especially evident with cross-border purchases, where the cost indicated at the final checkout screen may not include additional fees that must be paid upon delivery such as duties and brokerage. Some services include estimates of these additional cost, but nevertheless, the lack of general full cost disclosure remains a concern.

- **Privacy:**

Privacy of personal information is a significant issue for some consumers. Many consumers wish to avoid spam and telemarketing which could result from supplying contact information to an online merchant. In response, many merchants promise to not use consumer information for these purposes,

Many websites keep track of consumer shopping habits in order to suggest items and other websites to view. Brick-and-mortar stores also collect consumer information. Some ask for a shopper's address and phone number at checkout, though consumers may refuse to provide it. Many larger stores use the address information encoded on consumers' credit cards (often without their knowledge) to add them to a catalog mailing list. This information is obviously not accessible to the merchant when paying in cash.

- **Product suitability:**

Many successful purely virtual companies deal with digital products, (including information storage, retrieval, and modification), music, movies, office supplies, education, communication, software, photography, and financial transactions. Other successful marketers use drop shipping or affiliate marketing techniques to facilitate transactions of tangible goods without maintaining real inventory.

Some non-digital products have been more successful than others for online stores. Profitable items often have a high value-to-weight ratio, they may involve embarrassing purchases, they may typically go to people in remote locations, and they may have shut-ins as their typical purchasers. Items which can fit in a standard mailbox such as music CDs, DVDs and books—are particularly suitable for a virtual marketer.

Products such as spare parts, both for consumer items like washing machines and for industrial equipment like centrifugal pumps, also seem good candidates for selling online. Retailers often need to order spare parts specially, since they typically do not stock them at

consumer outlets in such cases, e-commerce solutions in spares do not compete with retail stores, only with other ordering systems. A factor for success in this niche can consist of providing customers with exact, reliable information about which part number their particular version of a product needs, for example by providing parts lists keyed by serial number.

Products less suitable for e-commerce include products that have a low value-to-weight ratio, products that have a smell, taste, or touch component, products that need trial fittings most notably clothing and products where color integrity appears important. Nonetheless, some web sites have had success delivering groceries and clothing sold through the internet is big business.

- **Aggregation:**

High-volume websites, such as Yahoo!, Amazon.com, and eBay, offer hosting services for online stores to all size retailers. These stores are presented within an integrated navigation framework, sometimes known as virtual shopping malls or online marketplaces.

13.1.4 Impact of reviews on consumer behavior:

One of the great benefits of online shopping is the ability to read product reviews, written either by experts or fellow online shoppers. The Nielsen Company conducted a survey in March 2010 and polled more than 27,000 Internet users in 55 markets from the Asia-Pacific, Europe, Middle East, North America, and South America to look at questions such as

How do consumers shop online?

What do they intend to buy?

How do they use various online shopping web pages? and

The impact of social media and other factors that come into play when consumers are trying to decide how to spend their money on which product or service.

According to the research, reviews on electronics (57%) such as DVD players, cell phones or PlayStations, and so on, reviews on cars (45%), and reviews on software (37%) play an important role in influencing consumers who tend to make purchases online. Furthermore, 40% of online shoppers indicate that they would not even buy electronics without consulting online reviews first.

13.2 Internet Marketing:

Internet marketing or online marketing refers to advertising and marketing efforts that use the Web and email to drive direct sales via electronic commerce, in addition to sales leads from Web sites or emails. Internet marketing and online advertising efforts are typically used in conjunction with traditional types of advertising like radio, television, newspapers and magazines.

13.2.0 Specialized Areas of Internet Marketing:

Internet marketing can also be broken down into more specialized areas such as Web marketing, email marketing and social media marketing:

- Web marketing includes e-commerce Web sites, affiliate marketing Web sites, promotional or informative Web sites, online advertising on search engines, and organic search engine results via search engine optimization (SEO)
- Email marketing involves both advertising and promotional marketing efforts via e-mail messages to current and prospective customers
- Social media marketing involves both advertising and marketing (including viral marketing) efforts via social networking sites like Facebook, Twitter, YouTube and Digg.

13.3 How to Create An Internet Marketing Strategy:

Online and brick-and-mortar businesses require Internet marketing strategies. A comprehensive Internet marketing strategy can launch or increase sales substantially for a business. Internet marketing requires a knowledge of social media, Search Engine Optimization (SEO), blogs, email lists, affiliate marketing and more. If we do not already recognize these terms, may want to learn more about Internet marketing. If we are ready to launch a business or a product, then we should research, create and track a marketing strategy online as well as in print.

Read the following steps to find out how to create an Internet marketing strategy:

- **Develop our brand name and image before communicating with our market:** In today's marketing world, a brand name and image is as important as the strategy itself.

Our brand makes us recognizable amongst competitors, so pick a name, trademark, website, letterhead and business plan before launching a strategy.

- **Study our competitors:** Study them from their website through their sales process, including their marketing strategies. Identify the past and ongoing marketing strategies of our largest competitors, so we know what works in our given market.
- **Study our market:** Decide if we are part of a niche market. If so, we will want to center our strategy on that demographic, instead of all Internet consumers.
- **Choose our ideal consumer**: Decide who our demographic is, in order to target it with our strategy. Focus the majority of our online marketing budget on our ideal demographic.
- **Mimic the successful marketing strategies of our competitors:** Our market research should tell us how many followers our competitors have on Facebook, how many people they send their email list to and how many people comment on their blog entries. This means that the demographic responds well, and these campaigns should be the first on our list for our strategy.
- **Create a multi-faceted Internet marketing strategy:** In order to increase our brand recognition we should launch several marketing campaigns at once.

The following are marketing strategies that we should look at starting within a few weeks of each other:

- ✓ Create social media accounts and assign someone to launch interesting material every day. In order to attract followers, social media accounts and blogs must be consistently updated.
- ✓ Create or pay someone to write SEO articles. Articles that mention popular keywords related to our product, but also offer tips or advice are a great way to introduce people to our product. They also help our website to show up on the first pages of an Internet search. Do not scrimp on the money we spend for SEO articles, Google has created a way to list top quality articles first.
- ✓ Collect or buy email lists. People who have stores have most likely collected emails throughout the years, which can be used for email blasts. If we do not have any emails,

we can buy them from marketing companies or neighboring markets. Send an initial blast and monthly blasts updating our customers on new products.

- ✓ Create videos of people using our product, how to sure people vouching for our product. We can launch these videos via our website, You Tube, Video, Face book or other places in order to draw interest to our website.
- ✓ Buy ads on sites that cater to our market. Communicate our brand image, videos or other product info on banner ads. If we don't have the skills to craft a well-designed ad, hire a graphic designer to create a good advertise.

- **Set up tracking capabilities for all of our campaigns:** The easiest way to do this is to set up a Google Analytics account through our main Google account. Create a campaign for each face of our strategy so that we can look back later and see which ones had the best Return on Investment (ROI).

  Consider buying print ads that cater to our market that also launch at the same time as our Internet marketing campaign. Track this ad by buying a similar domain name that redirects to your site. Let a Google Analytics campaign track the success of the print ad, in comparison to our Internet marketing, through this other domain.
- **Launch our campaign in the same few days and weeks.** Be consistent, if our method requires communication with customers. Follow through with all of our orders as quickly as possible, in order to create good reviews on our website and other marketplaces.
- **Evaluate our ROI and repeat any strategies that were successful, if and when we launch new products.** Some campaigns are ongoing and we can try to slowly or virally increase our following.
- ✓ As online marketing strategies begin, also consider affiliate marketing. With this type of marketing, other people advertise our products. All products that are sold leading from their site will give them a portion of the profit. This is a good way to increase our online ads without paying for them in advance.
- ✓ Sign up for trial versions of email blast software, such as Constant Contact, Vertical Response. These programs allow us to make email blasts using templates, and we can pay with monthly or yearly installments.

13.3.0 Top 10 Internet Marketing Strategies:

Internet marketing can attract more people to our website, increase customers for our business, and enhance branding of our company and products. If we are just beginning our online marketing strategy the top 10 list below will get us to started on a plan that has worked for many.

- ✓ Start with a web promotion plan and an effective web design and development strategy.
- ✓ Get ranked at the top in major search engines, and practice good Search Optimization Techniques.
- ✓ Learn to use Email Marketing Effectively.
- ✓ Dominate our marketing niche with affiliate, reseller, and associate programs.
- ✓ Request an analysis from an Internet marketing coach or Internet marketing consultant.
- ✓ Build a responsive opt-in email list.
- ✓ Publish articles or get listed in news stories.
- ✓ Write and publish online press releases.
- ✓ Facilitate and run contests and give aways via our web site.
- ✓ Blog and interact with our visitors.

By following the above tips we'll be on our way to creating a concrete internet marketing strategy that could boost our business substantially.

13.4 Internet Marketing Techniques:

Each of the following five internet marketing techniques can be implemented without a considerable investment (except perhaps time). While some of them might be more accurately described as internet marketing advice rather than internet marketing techniques each of them can have a positive impact on our internet marketing initiatives.

- **Track and analyze our web site traffic:**

Most web hosts offer traffic analysis data to their clients, and it is arguably the most important tool at our disposal in measuring the effectiveness of our internet marketing techniques and overall website performance. By taking the time to understand this data, we can begin to understand the motivations and interests of our audience.

Are many of them leaving on one particular page?

Perhaps we should make some changes to keep their interest. Are most of them looking at one particular part of our site?

Perhaps we should make it a more featured area. Since this data updates on a regular basis, we are also able to gauge the effectiveness of any changes that we make. These are the most basic examples, as there are many more useful bits of information available what search terms our visitors are using to find us, what sites are bringing us the most traffic, how long our visitors are staying, etc. Maintaining a successful website is an ongoing process, and visitor data is crucial to getting optimum results.

- **Request links from non-competing, quality companies related to our industry:**

This is a simple but effective piece of internet marketing advice. Links allow us to get quality traffic while increasing the prestige of our business. Visitors that enter our site from a link that they find on another site are predisposed to believe that they will find something of value there if not, why would the site take the time and effort to link to it?

The added benefit to link building internet marketing techniques is that they can give a tremendous boost to our link popularity, which is a major factor in determining how our site gets ranked in search engines.

- **Write informative articles about our business or products and make them available to online publications and webmasters:**

There are numerous sites that will allow us to offer original informational articles for others to publish. In fact, our own company routinely publishes articles containing internet marketing advice. Such an exchange benefits for us in several ways.

First, all of these sites require anyone who is reprinting our article to provide a link back to our site, which can provide highly targeted visitors (visitors that most likely already have a good impression of us from our article).

Another way to boost our link popularity, which is vitally important to our search engine rankings (as discussed above and in our last issue). Moreover, if we offer a service, a reputation is our most valuable asset. Widely distributed articles can help to establish us as an expert in our field and help us to gain credibility with our future clients. Although internet marketing

techniques such as these may require a considerable time investment, the payoff can be well worth the trouble.

- **Give our website visitors a clear call to action:**

If our site isn't intended to sell a product or gain a customer, then what is it for? Our internet marketing techniques should have a clear purpose, meaning that every page on our site should focus on getting the visitor to take an action. This could be purchasing something online, filling out a form or sending an email, making a phone call, or even simply moving on to the next step in the process. Our website should be more than a static billboard proclaiming that we are open for business it should compel our visitors to follow a specific path that leads to a sale. The answer can be as simple as placing a prominent offer on our pages.

- **When it comes to our site, don't overlook the obvious:**

As previously mentioned, this might fall better into the category of internet marketing advice, rather than internet marketing techniques. However, it is important that we compare our website to an actual store. Is everything clean and organized, or is everything messy and cluttered? Many websites give bad first impressions with issues that could easily be avoided. Broken links are a sign of sloppiness that are fairly common. To combat this, there are several websites that will automatically scan our site and identify any broken links. Does our site maintain its look and functionality with most browsers? People are sometimes dismayed to learn that their site (which looks great in Internet Explorer) doesn't maintain its look or functionality with other popular browsers such as Firefox. The time and resources required to fix these problems are small when compared with the cost of tarnishing our professional image.

13.5 Unit Summary:

This unit introduces that:

- Online shopping is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the Internet using a web browser.
- Advantages:
  - ✓ Convenience
  - ✓ Information and reviews

- ✓ Price and selection

- Disadvantage:
  - ✓ Fraud and security concerns
  - ✓ Lack of full cost disclosure
  - ✓ Privacy
  - ✓ Product suitability
  - ✓ Aggregation

- Internet Marketing Techniques:
  - ✓ Track and analyze your web site traffic.
  - ✓ Request links from non-competing, quality companies related to your industry
  - ✓ Write informative articles about your business or products and make them available to online publications and webmasters
  - ✓ Give your website visitors a clear call to action

13.6 Keywords:

Online Shopping, Feature, Advantage and Disadvantage of Online Shopping.

Internet Marketing, Strategies and Techniques

13.7 Exercises:

1) What is Online Shopping? Explain Features
2) Explain advantage and disadvantages of Online Shopping?
3) Write a note on Internet Marketing?
4) How to Create an Internet Marketing Strategy?
5) Explain Internet Marketing Techniques.

13.8 References:

1. Electronic Commerce – Elias Malady
2. Frontiers of Electronic Commerce – Kalakos Whinstone
3. E-Commerce – Mamta Bhusry
4. Electronic Commerce – Gary P.Schneider

Unit-14: Legal and Ethical Issues, Legal infrastructure for E- Commerce in India

Structure:

14.0 Objectives:

After studying this unit you will be able to understand

- To get brief knowledge of E- Commerce
- Legal and ethical issues in E-commerce
- E-business and legal issues
- E-commerce in India.

14.1 Introduction:

All most all the countries now enjoy Internet access, and a recent survey reported that there are approximately 20 million Internet hosts worldwide. The number of Internet users in the world are currently more than 100 million people.

The exponential growth of the Internet and online activity raise a number of new regulatory issues and legal questions.

- How does copyright apply to digital content?
- How can national laws apply to activities in cyberspace?
- Can privacy and data protection exist on the Web?
- Can electronic commerce really be secure?
- Should governments tax cyber trade?
- Can cyberspace be regulated by one, or by many authorities?

In seeking to apply the law to the Internet, problems arise owing to the fact that most laws largely apply to the pre-cyberspace world.

In the modern era of electronic technology, many people want to get their work done quickly with little effort. In traditional commerce, it's not easy to start a business. You must implement strategies that follow rules and regulations enforced by government. Electronic commerce makes it possible to do almost any kind of business in a very simple way. What makes it simple? The reason is that existing legal frameworks and enforcement mechanisms are not strong.

E-commerce presents a world of opportunity for doing businesses, reaching global markets and purchasing without leaving the home or office. E-commerce can provide opportunities to improve business processes, just as phones, faxes and mobile communications have in the past. However, just as any new business tool has associated issues and risks so does e-commerce.

It's important to understand the legal issues and potential risks to ensure a safe, secure environment for trading with customers and other businesses.

The issue of law on the Internet is a complex one. Between the two all-or-nothing extremes lies a broad spectrum of possibilities. Many people revel in the freedom to express themselves and the freedom from prohibitions such as zoning restrictions that the Internet apparently affords. With no law at all, however, the Internet would be no place to conduct business or pleasure. Laws give people certainties about their rights and responsibilities: they make life more predictable.

"Without predictability, business will not be able to act efficiently, or price services effectively," said Thomas Vartanian, a Washington, D.C.-based lawyer.

14.2 E-Commerce:

E-Commerce is the ability of a company to have a dynamic presence on the Internet which allowed the company to conduct its business electronically, in essence having an electronic shop. Products can be advertised, sold and paid for all electronically without the need for it to be processed by a human being. In other words Electronic commerce (E-Commerce) is a conducting business using one of many electronic methods, usually involving telephones, computers (or both).

E-Commerce is not about the technology itself, it is about doing business using the technology. Due to the vastness of the internet advertising and the website can be exposed to hundreds of people around the world for almost nil cost and with information being able to be changed almost instantly the site can always be kept up to date with all the latest products to match with consumers demands.

The biggest advantage of E-Commerce is the ability to provide secure shopping transactions via the internet and coupled with almost instant verification and validation of credit card transactions. This has caused E-Commerce sites to explode as they cost much less than a store front in a town and has the ability to serve many more customers.

14.2.0 Benefits of E-Commerce:

An E-Commerce website offers many advantages to most types of businesses of all types and sizes. The main advantages are

- **Access to a Global market:**

The internet allows companies to have access to a global market rather than just the potential customers in the surrounding area of there physical location. Due to the fact that the website is open 24-hours a day time differences between countries are no longer a problem.

- **Cutting out the middleman:**

Businesses can sell direct to the consumer rather than having to sell to a supplier and then them sell it on, this means the company can usually offer the product at a discount compared to there retailers because only one company has to make profit rather than two or more.

- **A level playing field:**

A small business can compete and show itself as a professional company as much as a large ones as budgets for setting up a professional site are relatively cheap to the amount of return we can get on them.

- **Open 24 hours a Day:**

Because of the fully automated payment and order processing systems of the site never be closed even office/warehouse is closed. Orders can be dispatched during opening hours while orders can be taken 24 hours a day, this has great advantages for people who might be at work or busy during normal working hours.

- **Greater Customer Satisfaction:**

` An E-Commerce website can be a powerful tool for building customer loyalty if it is effective enough, a well designed website puts the customer in charge of the relationship, they can buy, browse, ask for help or track the progress of order they have placed where they want and when they want.

- **Reduced Marketing Costs:**

Word of mouth can be incredibly powerful on the Web through e-mail recommendations and search engine rankings. We can achieve a great deal through growth by treating customers well, keeping them informed about our activities and benchmarking our self against competitors. Also with the internet advertisement being relatively cheap, we can reach many more people at a cheaper cost than using conventional advertising methods.

- **Better Customer Information:**

We can quickly and easy to analyze our customers by location and area as well as the products they buy as we will have to request a customers name and address from them when processing a transaction. As well as we being more informed about our customers, your customers are also more informed as generally on E-Commerce sites there is more information

on a product including reviews etc to help customers choose the right product for them. This works in the best interest for the site as it cuts down on the amount of returned goods.

- **Security:**

E-Commerce suits offered by companies come with built in security in the software and with the purchase of a dent SSL certificate and some good server configuration we can safely know that all the details of our customers will be safe and secure. We can get approved certificates to show that our site is secure and meets up the certain standards, this lets our customers know that they are safe to shop at our site and the data will not end up in the wrong hands.

14.2.1 Implications Of E-Commerce:

When using the Internet and E-Commerce is is important to remember that there are many legal, moral and ethical issues to consider.

- **Ethical & Morel Implications:**

Businesses entering the e-commerce world will be facing a new set of ethical challenges. It is easy for businesses to become sidetracked in the technical challenges of operating in this way and to pay little attention to the ethical implications.

There are many ethical implications for businesses to run into that would normally be addressed when doing business face to face, for example selling tobacco and alcohol to an under age minor over the internet, this is impossible to regulate easily and affectively as it would be if the person walked into a store, not only is this in ethical but it is also illegal.

- **Legal Implications:**

The central issues of E-Commerce and the law include the development of E-Commerce, the role of consumers and regulation of e-commerce in regards to consumer protection.

E-commerce is a new way of conducting business that takes place on the Internet, it has become an important way in which consumers purchase goods across the world as well as due to internet technology progressing rapidly in the last few years.

Although E-Commerce has a big effect on the global trade, governments also have a large effect on the growth of E-Commerce on the internet by regulating is accordingly. As

Governments set regulations for E-Commerce organizations managers are starting to worry if the regulations will be to tight or may reduce the market in the online trade. .

- **Security Implications:**

There are a few security implications that come about when setting an E-Commerce website, especially when handling sensitive information such as credit card information and personal details such as address. Many parts will have to be protected well including communication between the customer and the website server and the server itself from any hacker trying to intercept information or from trying to retrieve existing information from databases.

- **Customer & Server:**

To secure data between the customer and the web server there is a system called SSL (Secure Socket Layer) which encrypts the information between them so no one else can read it. The theory of it is quite basic and uses the following steps:

- ✓ User want to send data to the server, before it leaves it is encrypted with a unique key for the session.
- ✓ The server receives this information then encrypts the information one more time this time using its own unique session, this is completely different from the users unique key. It then sends back the data.
- ✓ The users computer now unlocks the data with the key it locked it with earlier, the data is still encrypted but now only with the servers key. The users computer then sends the data back.
- ✓ The server then receives this information and unlocks it with its key and now has the unencrypted data of what the user was sending to the server. This type of encryption comes in different strengths depending on the SSL certificate.

- **Server Security:**

As well as security between the consumer and server there is also security needed on the server(s) as well, especially if sensitive information is stored under customers accounts, such as credit card information and other personal information.

Servers will have to be protected to withstand any hack attempts to retrieve the information that is stored. Prevention measures such as firewalls, checking for root kits, antivirus systems and others should be put in place, as well as encryption of the data if possible so should a hacker gain entry the information he see's is useless to him or her.

14.3 Setting up an E- Commerce:

There are a number of steps that need to be taken and considered when setting up an E-Commerce website. Some of these steps are below:

- **Choosing A Company Name;**

When setting up an E-Commerce site is it important to choose a sensible company name, a name such as "Jelly Penos Peppers Currys" with a domain jellypenospepperscurrys.com probably isn't the best idea as most people will not remember the company name let alone the domain name. At the very least we want a company name that is memorable because then even if a customer can't remember our companies domain name at the very least he or she can search for our company in a popular search engine.

- **Potential Customers:**

In order to setup a successful site we need to analyze and research the potential for the products that we wish to sell and to find out if the market is already saturated with similar ideas, if we cannot offer anything different to other well known companies what will make customers attracted to our site, in short, nothing.

We need to know the type of customer we are aiming for and what they require, for example if we are aiming at business users we may have E-Commerce software that allows different logins to do different things to the company account etc, plus everything would have to have a VAT invoice.

- **Financial Resources:**

The financial costs involved in setting up an E-Commerce site range from almost nothing to many thousands of pounds, it all depends on what we want the site to do and how customized we would like the package.

- **Training & Development:**

Depending on the scale of the system, training may not be needed, if for example we were a large scale business with an existing ordering system we would get the E-Commerce system to integrate with the old one so it is easy and familiar to staff.

14.4 Legal and Ethical Issues:

- **Electronic Transaction:**

Some federal, state and territory governments encourage the adoption of electronic commerce by enacting and enabling legalization. Even the electronic transfer of land is covered, "Importantly, the Act is similar in all material respects to those operating both in other States and at the Federal level, so people can be confident that electronic transactions carry the same legal weight nationwide".

Moreover the bill is expected to boost electronic commerce as an effective tool for businesses to increase their efficiency. This may reduce administrative duties, storage and operational costs for businesses.

New legislation brings some questions such as,

- ✓ For how long will these acts be valid?
- ✓ What are the boundaries of these acts?
- ✓ Who should be forced to follow the rules?

Most of these questions are unanswerable today. Global companies have the responsibility to deal with some of the legal issues such as how to form contracts, abide by consumer protection laws, create privacy policies and protect databases.

- **Privacy & Security:**

While shopping on the Internet, most people typically do not think about what is happening in the background. Web shopping is generally very easy. We click on a related site, go into that site, buy the required merchandise by adding it to our cart, enter our credit card details and then expect delivery within a couple of days. This entire process looks very simple but a developer or businessmen knows exactly how many hurdles need to be jumped to complete the order. Customer information has to pass through several hands so security and privacy of the

information are a major concern. The safety and security of a customer's personal information lies within the hands of the business.

In traditional and online trading environments, consumers are entitled to have their privacy respected. Websites should provide the customers with choices regarding the use of their personal information, and incorporate security procedures to limit access to customer information by unauthorized parties. Privacy policies and procedures should be clearly explained to customers. Although respecting consumer privacy rights is a legal requirement, it also represents good business practice.

- **Copyright & Trademark:**

Many attempts have been made to address the issues related to copyrights on digital content. E-commerce has a tremendous impact on copyright and related issues, and the scope of copyrights is affecting how e-commerce evolves. It is essential that legal rules are set and applied appropriately to ensure that digital technology does not undermine the basic doctrine of copyright and related rights. If someone uses a trademark in such a way as to dilute the distinctive quality of the mark or trade on the owner's reputation, the trademark owner may seek damages.

Some Web-based applications have enabled large-scale exploitation of music samples and audio formats. Software that is available free of cost on the Net allows the transfer of songs and videos without the authorization of rights holders (e.g. Napster, MP3 Providers).
Moreover, CD burners and portable MP3 players allow copyright violations to occur rather easily.

- **Online Terms, Conditions, Policies and Laws:**

At the moment, most online privacy policies are produced by private businesses for individual companies. Governments are developing legislation to support and strengthen the privacy protection measures of many businesses. These initiatives are aimed at regulating the storage, use and disclosure by businesses of personal information.

Privacy legislation is designed to protect a person's personal information. The privacy laws of their host country affect overseas companies. Every organization should be very careful while applying terms and conditions for the electronic transaction for Internet users. Privacy and

security policies not only reflect the organizations practice but also the rules and regulations for doing business with the company.

Major issues regarding the legalization of electronic transactions include the following.

- ✓ Ensure proper online contracts.
- ✓ Record retention obligations.
- ✓ Original documentation, in terms of TAX and VAT requirements.
- ✓ Import/export regulations.
- ✓ Exchange control regulation.
- ✓ Foreign data protection law.

- **Legislation Dilemma:**

Electronic transactions separate e-business from traditional types of businesses. When a transaction takes place, Who has jurisdiction?

Who has the authority to apply law over the transaction?

For example, if we buy a laptop in our local computer store, we know our legal rights. If the computer does not work when we take it home, and the store refuses to settle up, then we can probably take the dispute to our local small claims court. But if we buy the same computer online, from a vendor on the other side of the world, perhaps through a dealer based in yet a third country, then our rights are a lot less clear. Which country's protection laws apply: ours, those in the vendor's home country, or those of the intermediary? Without knowing which particular set of laws apply, it's impossible to know whom to sue..

A little legislation can go a long way toward helping parties to establish better boundaries to work within. When a transaction that takes place between two different parties located in two different countries goes wrong then a number of complex questions arise. This is not the first time the question of extra-territorial jurisdiction over Web content has been raised.

14.5 E-Business and Legal Issues:

The technological basis of e-commerce is basically Web client/server middleware, or what is called three-tier architectures. The client tier is the Web browser involving some type of form processing. The middle tier is the Web server, often with transaction processing. The Web

server in turn links to the third tier, a database processing the order information. Some of the issues are strictly Internet-related, such as domain names and trademarks, linking and framing, Click ware (and shrink ware), and meta tag use. Others are traditional issues applied to the Internet, such as copyright, contracts, consumer protection, privacy, taxation, regulated industries and jurisdiction.

E-commerce site development, its advertising, electronic transaction, money transactions and such involve many legal issues, which need to be taken into account step by step. Before developing an e-commerce site a registered domain and a registered trademark should be established. There must be some copyright protection on the site. The business must ensure that it displays the terms and condition/policies within its site. Security involving the privacy of a user's data is always one of the main concerns while doing business online. Defining rules and regulations for the advertisement of the site by placing banners on other known sites is another. It is of great value when dealing with such complex issues to consult an attorney who specializes in the issues of cyber space.

14.6 Legal Infrastructure for E-Commerce in India:

The Parliament of India passed its cyber law in the form of the Information Technology Act, 2000, which provides the legal infrastructure for e-commerce. The Act received the assent of the President of India and became the law of the land on 17 October 2000.

The objective of the Information Technology Act, 2000 would be to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information. The act would also facilitate electronic filing of documents with various government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 for related matters.

The Act thereafter stipulates numerous provisions in order to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act further states that unless otherwise agreed to, the acceptance of a contract expressed by electronic means of communication shall have legal validity and

enforceability. The Act would facilitate electronic intercourse in trade and commerce, eliminate barriers and obstacles to electronic commerce that result from the celebrated uncertainties relating to writing and signature requirements over the Internet. The objectives of the Act also aim to promote and develop the legal and business infrastructure necessary for implementing electronic commerce.

Chapter II of the Act stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify the electronic record by the use of a public key of the subscriber.

Chapter III contains details about e-governance and provides, among other things, that where any law provides that information or other matters shall be in writing, typewritten or printed form, then, not withstanding anything contained in such a law, that requirement should be satisfied if the information or matter is:

a) Rendered or made available in an electronic form;
b) Accessible to make it usable for subsequent reference.

That chapter also provides details about the legal recognition of digital signatures. The various provisions give further elaboration about the use of electronic records and digital signatures in government agencies. The Act also refers to publication of rules and regulations in an Electronic Gazette.

Chapter IV gives a scheme for the regulation of certifying authorities. The Act provides for a controller of certifying authorities who shall perform the function of supervising the activities of certifying authorities as well as setting standards and conditions governing the certifying authorities. The controller also specifies the various forms and the content of digital signature certificates. The Act acknowledges the need to recognize foreign certifying authorities and it further details the various provisions for granting the license to issue digital signature certificates. The duties of subscribers are also covered. The Act also covers penalties and adjudication for various types of offences and mentions the power and qualifications for the adjudicating officer.

A provision in Chapter X foresees a Cyber-Regulations Appellate Tribunal where appeals against the orders passed by Adjudicating Officers could be referred. The tribunal would not be bound by the principles of the Code of Civil Procedure, but would follow the principles of

natural justice and have the same powers as a civil court. Any appeal against an order or decision of the Cyber-Regulations Appellate Tribunal would be made to the High Court.

Chapter XI covers various offences and stipulates that the investigation must be by a police officer only, and that officer should have the rank of deputy superintendent of police or higher. These offences include tampering with computer source documents, publishing obscene information in electronic form, breach of confidentiality and privacy, misrepresentation, publishing a digital signature certificate that is false in certain particulars and publication for fraudulent purposes.

Hacking and penalties if found guilty have been defined in Section 66. For the first time, punishment for hacking has been designated as a cyber crime. The Act also provides for constituting the Cyber-Regulations Advisory Committee, which would advise the government about any rules or other matter connected with the Act. The Act also has four schedules which amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them conform with provisions of the IT Act. Overall, the Information Technology Act, 2000 is considered.

14.6.0 Analysis of E-commerce elements of Legal Infrastructure:

Analysis of other elements related to ICT and e-commerce shows the diversity of approaches and a wide range in the scope and breadth of policy, laws and regulations. Much of the work concerning the legal and regulatory frameworks for e-commerce in South Asia has been done in India and Pakistan. Both countries have sought to legalize the electronic format and granted legality to electronic commerce transactions.

India has incorporated some aspects relating to cybercrime into its cyber law. Certain acts have been stipulated as cybercrimes with punishment in the form of imprisonment and fines. While India and Pakistan have covered some aspects in their e-commerce laws, there are still large areas that require appropriate attention. Additional objective examination of cyberlaws and e-commerce laws around the world shows that some extremely important issues need to be fully addressed by any nation. Related areas that concern ICT either directly or indirectly have been addressed by the other South Asian countries.

- **Telecommunication regulation policy:**

In terms of a general overall framework or guideline in the form of a Telecommunication Regulation Policy, the countries of South Asia have a variety of situations. Bangladesh has a policy, but it does not include complete privatization. Public and private sector entities are supposed to work together. A licensing scheme remains. Bhutan has the Telecommunications Act, 2000 and it stipulates that the sole provider of telecommunications is state owned. In India, there are private and public holdings for the ICT industry.

The four remaining South Asian countries have policies, but these would include more elements than just regulation. Maldives has the Telecommunications Policy covering 2001-2005. Nepal has had a Telecommunications Policy since 1996. Changes and reform concerning ICT in Pakistan began with the Pakistan Telecommunication (Re-Organization) Act 1996. As of 2004, Sri Lanka has had a National Telecommunications Policy.

- **Consumer protection:**

India has the Consumer Protection Act 1986, however, nothing in the Act refers explicitly to e-commerce consumers. It provides for the regulation of trade practices, the creation of national and state level Consumer Protection Councils, consumer disputes redress forums at the National, State and District level to redress disputes, class actions and for recognized consumer associations to act on behalf of consumers. The Act provides a detailed list of unfair trade practices, but it is not exhaustive.

Similarly, Maldives has had a consumer protection act since 1996 and Nepal has a consumer protection act, but there is no provision for e-commerce consumers. The Consumer Protection Act, 1998 of Nepal came into force on 13 April 1999 and establishes the Consumer Protection Council. Pakistan has consumer protection acts in some provinces, but with no provision for e-commerce consumers. Sri Lanka has a Consumer Protection Act 1979, which is not yet applicable to e-commerce, but policy to do so exists. The Act provides for consumer protection, regulation of internal trade and the establishment of fair trade practices.

- **Protection of intellectual property:**

Five countries in South Asia are party to the World Intellectual Property Organization (WIPO) Convention: Bangladesh acceded in 1985; Bhutan acceded in 1994; Maldives joined in

2004; Nepal joined in 1997; and Sri Lanka joined in 1978. Bhutan and Nepal are also members of the Paris Union. Bangladesh, and Sri Lanka are members of both the Paris Union and the Berne Union. As of this writing, Sri Lanka was the only country in South Asia to become party to the Trademark Law Treaty in 1996. Bangladesh Copyright Law, 2000 does provide for IT protection. The Copyright Act of India provides protection to computer programs, but specifically excludes computer software from the ambit of its protection. The Copyright (Amendment) Act, 1992 of Pakistan provides protection to computer programs. Sri Lanka provides protection under Code of Intellectual Property Act Number 52 of 1979 as amended by (Amendment) Act 13 of 1997. Computer software is protected by copyright law as described in the Code of Intellectual Property Act and Act Number 14 of 2000. However, it appears that the protection does not extend to computer programs/databases.

- **Cybercrimes and cyber-evidence:**

Cybercrime and the acceptance of cyber-evidence have become major concerns for all countries as part of globalization and the spread of e-commerce. However, there are some basic issues yet to be resolved, such as types of computer crime, set of procedural powers, specific definitions and scope of cybercrime, lack of a common understanding about the problem and how to respond, issues of sovereignty, problems of dual criminality.

- **Recommendations:**

There are several issues that need to be addressed in order to have harmonization of legal and regulatory systems for e-commerce that could be acceptable to all countries in South Asia:

- ✓ Telecommunication liberalization
- ✓ Recognition of electronic documents
- ✓ Consumer protection for e-commerce consumers
- ✓ Electronic funds transfer
- ✓ Dispute resolution
- ✓ Liability of Internet service providers (ISP)
- ✓ Domain names
- ✓ Intellectual property protection

- ✓ Privacy
- ✓ Cybercrime

Addressing these issues by creating e-commerce laws in each South Asian country would help promote the growth of an e-commerce regime in South Asia. Once a law is in place, an extremely important role is played by entities entrusted with implementation of existing laws enacted by the parliament.

Indian experience has shown that it is easy to enact law on paper. However, it is extremely difficult to enforce laws in actual practice. There are numerous challenges that require appropriate awareness among citizens about e-commerce laws. This is so because at the end of the day, the e-commerce laws are basically targeted to protect and help those citizens.

There is an urgent need in countries of South Asia to ensure that their lawmakers and policy makers are appropriately sensitized about the various nuances and legal issues that impact e-commerce. This is important in order to prevent the passage of some policy which may have no relation to the existing realities. The result might be implementation that is likely to create more obstacles or harm than achieve any good.

- **Law enforcement and cyber law:**

Another issue that requires attention is the fact that law enforcement agencies and the police need to be duly trained about the various issues relating to e-commerce laws. While some acts have been designated as cybercrimes in India, with punishment by imprisonment and fine, a large number of cybercrimes that have already emerged still have not been regulated by the e-commerce laws of South Asian countries. Since the enactment of the Information Technology Act 2000 in India, there is the start of some awareness about cyber law and cybercrime related issues. There is a need for the government to come up with strong training and awareness programmes on all related issues pertaining to cyber law and cybercrime. The Government needs to target all statutory authorities who have been constituted under the Information Technology Act for training and orientation. These statutory authorities include the Adjudicating Officers as well as the various Certifying Authorities. At present the Adjudicating Officers in India are not aware about how to proceed in adjudicating claims for damages by way of compensation.

The Information Technology Act 2000 stipulates that cybercrime in India shall only be investigated by a police officer not below the rank of Deputy Superintendent of Police (DSP). There is no orientation given to the police officers in an organized, systematic basis. Special training programmes are needed for those police officers who are designated to deal with cybercrime.

This area needs to be seriously and urgently addressed. Cyber law training also needs to be given to the government departments and the relevant officers engaged in e-commerce and e-governance activities. This is essential, as the preamble of the Information Technology Act specifically states that the objective of this law is to promote e-commerce and electronic filing of documents with government agencies.

- **Concluding observations:**

This study has suggested that there is a need to improve Internet density, and this could be achieved through the entry of private parties into the field of telecommunications. This should be encouraged as a matter of policy. Greater cooperation among SAARC-member countries could enable exchange of information and experiences related to the establishment and successful implementation of e-commerce legal and regulatory systems.

Comprehensive dissemination of information should be made to the public about existing e-commerce laws. Education and training for officials in enforcement agencies, the judiciary, the police force, and so forth is needed with a top priority given to the various legal issues relating to e-commerce.

14.7 Unit Summary:

This unit introduces to:

- E-Commerce is the ability of a company to have a dynamic presence on the Internet which allowed the company to conduct its business electronically, in essence having an electronic shop.
- Legal and Ethical Issues
    - ✓ Legislation Dilemma
    - ✓ Electronic Transaction
    - ✓ Privacy & Security

- ✓ Copyright & Trademark
- ✓ Online Terms, Conditions, Policies and Laws

- Setting up an E- Commerce
  - ✓ Choosing A Company Name
  - ✓ Potential Customers
  - ✓ Financial Resources
  - ✓ Training & Development

14.8 Keywords:

Legal and Ethical Issues, E- Commerce – Benefits, Setting up E- Commerce, Legal Infrastructure.

14.9 Exercise:

1) What is E- Commerce and its benefits?
2) What are the Implications of the E-commerce.
3) Explain the setting up an E- Commerce.
4) Explain the legal and ethical issues?
5) Write a note Legal infrastructure in India.
6) Briefly explain the analysis of E-Commerce elements of Legal Infrastructure.

14.10 References:

1. Electronic Commerce – Elias Malady
2. Frontiers of Electronic Commerce – Kalakos Whinstone
3. E-Commerce – Mamta Bhusry
4. Electronic Commerce – Gary P.Schneider

Unit 15: International Cyber Law (IT Act 2000 and the latest Cyber Law)

Structure:

15.0 OBJECTIVES:

- To know about Cyber law meaning.
- Brief idea about International Cyber Law
- Different authorities of International Cyber law
- IT Act 2000 and its latest cyber law

15.1 Introduction to Cyber Law:

Cyber law is a new phenomenon having emerged much after the onset of Internet. Internet grew in a completely unplanned and unregulated manner. Even the inventors of Internet could not have really anticipated the scope and far reaching consequences of cyberspace. The growth rate of cyberspace has been enormous. Internet is growing rapidly and with the

population of Internet doubling roughly every 100 days, Cyberspace is becoming the new preferred environment of the world.

With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. In response to the absolutely complex and newly emerging legal issues relating to cyberspace, Cyber Law or the law of Internet came into being. The growth of Cyberspace has resulted in the development of a new and highly specialized branch of law called Cyber Laws – Laws of internet and the World Wide Web.

There is no one exhaustive definition of the term "Cyber law". However, Cyber law is a term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to, or emanating from, any legal aspects or issues concerning any activity in Cyberspace comes within the ambit of Cyber law.

Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation. Some leading topics include internet access and usage, privacy, freedom of expression, and jurisdiction. Cyber law is the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware and Information Systems (IS). The introduction of new digital information and communications technologies has given birth to a new legal domain, commonly called Information and Communication Technology Law or more fashionably - Cyber Law.

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly “cyberspace”, i.e. the Internet. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a chapter XI entitled “Offences” in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

"Computer law" is a third term which tends to relate to issues including both Internet law and the patent and copyright aspects of computer technology and software.

Electronic commerce has led to specific legal problems, for example with regard to evidence, liability, consumer protection or payment. The convergence between broadcasting, telecommunications and digital information technology has created a new platform for public information with all the related legal issues.

Practically every country in the world has issued specific legislation or developed case law in this area. The domain has acquired sufficient stability to fit into a common structure. A logical consequence of this evolution is the publication of an International Encyclopedia of Cyber Law. The Encyclopedia consists primarily in a series of national monographs, treating the different legal subjects related to information and communication technology on the basis of a common standard outline.

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Cyber law encompasses laws relating to:

- Cyber Crimes
- Electronic and Digital Signatures
- Intellectual Property
- Data Protection and Privacy

15.2 International Cyber Law or Cyber Crime:

There is no commonly agreed single definition of “cybercrime”. Broadly speaking, it refers to illegal internet-mediated activities that often take place in global electronic networks. Cybercrime is "international" or "transnational" – there are ‘no cyber-borders between countries' International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with

cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. No matter in developing or developed countries, governments and industries has gradually realized the colossal threats of cybercrime on economic and political security and public interests. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale. U.S.-China's cooperation is one of the most striking progress recently because they are the top two source countries of cybercrime.

Cybercrime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web. There isn't really a fixed definition for cyber crime.

The Indian Law has not given any definition to the term 'cyber crime'. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law. But "Cyber Security" is defined under Section (2) (b) means protecting information, equipment ,devices computer, computer resource, communication device and information stored there in from unauthorized access, use, disclosure, disruption, modification or destruction.

Information and communication technology (ICT) plays an important role in helping ensure interoperability and security based on global standards. General countermeasures have been adopted in cracking down cybercrime, such as legal measures in perfecting legislation and technical measures in tracking down crimes over the network, Internet content control, using public or private proxy and computer forensics, encryption and plausible deniability, etc. Due to the heterogeneity of law enforcement and technical countermeasures of different countries.

15.3 Types of Cyber Crimes:

- **Hacking:**

Hacking is not defined in the amended IT Act, 2000. Hacking means unauthorized attempts to bypass the security mechanisms of an information system or network. Also, in simple

words Hacking is the unauthorized access to a computer system, programs, data and network resources. The term “hacker” originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.

- **Law & Punishment:**

Under Information Technology amendment Act, 2008, Section 43(a) read with section 66 is applicable and Section 379 & 406 of Indian Penal Code, 1860 are also applicable. If crime is proved under IT Act, accused shall be punished for imprisonment, which may extend to three years or with fine, which may extend to five hundred thousand rupees or both. Hacking offence is cognizable, bail able, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

- **Data Theft:**

Data Theft is a growing problem, primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices, capable of storing digital information such as flash drives, iPods and even digital cameras. The damage caused by data theft can be considerable with today’s ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices. According to Information Technology amendment Act, 2008, crime of data theft under Section 43 (b) is stated as - If any person without permission of the owner or any other person, who is in charge of a computer, computer system of computer network - downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, then it is data theft.

- **Law & Punishment:**

Under Information Technology amendment Act, 2008, Section 43(b) read with Section 66 is applicable and under Section 379, 405 & 420 of Indian Penal Code, 1860 are also applicable. Data Theft offence is cognizable, bail able, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

- **Spreading Virus or Worms:**

In most cases, viruses can do any of damage, the creator intends them to do. They can send your data to a third party and then delete your data from your computer. They can also ruin/mess up our system and render it unusable without a re-installation of the operating system. Most have not done this much damage in the past, but could easily do this in the future. Usually the virus will install files on your system and then will change our system so that virus program is run every time when we start our system. It will then attempt to replicate itself by sending itself to other potential victims.

- **Law & Punishment:**

Under Information Technology amendment Act, 2008, Section 43(c) and 43(e) read with Section 66 is applicable and under Section 268 of Indian Penal Code, 1860 are also applicable. Spreading of Virus offence is cognizable, bail able, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

- **Identity Theft:**

Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order access resources or obtain credit and other benefits in that person's name. Information Technology amendment, 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft. Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white collared criminals are a lot less brutal. But the ramifications of an identity theft are still scary.

- **Law & Punishment:**

Under Information Technology amendment Act, 2008, Section 66-C and Section 419 of Indian Penal Code, 1860 also applicable. Identity Theft offence is cognizable, bail able, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

- **E-Mail Spoofing:**

E-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e-mail originated from different source. E-mail spoofing is sending an e-mail to another person in such a way that it appears that the e-mail was sent by someone else. A spoof email is one that appears to originate from one source but actually has been sent from another source. Spoofing is the act of electronically disguising one computer as another for gaining as the password system. It is becoming so common that we can no longer take for granted that the e-mail we are receiving is truly from the person identified as the sender. Email spoofing is a technique used by hackers to fraudulently send email messages in which the sender address and other parts of the email header are altered to appear as though the email originated from a source other than its actual source. Hackers use this method to disguise the actual email address from which phishing and spam messages are sent and often use email spoofing in conjunction with Web page spoofing to trick users into providing personal and confidential information.

- **Law & Punishment:**

Under Information Technology amendment, 2008, Section 66-D and Section417, 419 & 465of Indian Penal Code, 1860 also applicable. Email spoofing offence is cognizable, bail able, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

In terms of cybercrime, we may often associate it with various forms of Internet attacks, such as hacking, Trojans, malware (keyloggers), botnet, Denial-of-Service (DoS), spoofing, phishing, and vishing. Though cybercrime encompasses a broad range of illegal activities, it can be generally divided into five categories:

- **Intrusive Offences:**

✓ **Illegal Access:** "Hacking" is one of the major forms of offences that refer to unlawful access to a computer system.

✓ **Data Espionage:** Offenders can intercept communications between users (such as e-mails) by targeting communication infrastructure such as fixed lines or wireless, and any Internet service.

For example : e-mail servers, chat or VoIP communications.

✓ **Data Interference:** Offenders can violate the integrity of data and interfere with them by deleting, suppressing, or altering data and restricting access to them.

- **Content-related offences:**

✓ **Pornographic Material:** Sexually related content was among the first content to be commercially distributed over the Internet.

✓ **Racism, Hate Speech, Glorification of Violence:** Radical groups use mass communication systems such as the Internet to spread propaganda.

✓ **Religious Offences:** A growing number of websites present material that is in some countries covered by provisions related to religious offences.

For example : anti-religious written statements.

✓ **Spam:** Offenders send out millions of e-mails to users, often containing advertisements for products and services.

- **Copyright and trademark-related offences:**

✓ **Common copyright offences:** cyber piracy, software piracy, piracy of music or movies.

✓ **Trademark violations:** A well-known aspect of global trade. The most serious offences include phishing and domain or name-related offences, such as cyber squatting.

- **Computer-related offences:**

✓ **Fraud:** online auction fraud, advance fee fraud, credit card fraud, Internet banking

✓ **Forgery:** manipulation of digital documents.

- ✓ **Identity theft:** It refers to stealing private information including Social Security Numbers (SSN), passport numbers, Date of birth, addresses, phone numbers, and passwords for non-financial and financial accounts.

- **Combination offences:**
- ✓ **Cyber terrorism:** The main purposes of it are propaganda, information gathering, preparation of real-world attacks, publication of training material, communication, terrorist financing and attacks against critical infrastructure.
- ✓ **Cyber warfare:** It describes the use of ICTs in conducting warfare using the Internet.
- ✓ **Cyber laundering:** Conducting crime through the use of virtual currencies, online casinos and etc.

15.3.0 Threats of Cyber Law:

Similar to conventional crime, economic benefits, power, revenge, adventure, ideology and lust are the core driving forces of cybercrime. Major threats caused by those motivations can be categorized as following:

Economic security, reputation and social trust are severely challenged by cyber fraud, counterfeiting, impersonation and concealment of identity, extortion, electronic money laundering, piracy and tax evasion.

Public interest and national security/integrity can be threatened by dissemination of offensive material, for example pornographic, defamatory or inflammatory/intrusive communication cyber stalking/harassment, Child pornography and pedophilia, electronic vandalism/terrorism.

Privacy, domestic and even diplomatic information security are harmed by unauthorized access and misuse of ICT, denial of services, and illegal interception of communication.

Domestic, as well as international security are threatened by cybercrime due to its transnational characteristic. No single country can really handle this big issue on their own. It is imperative for us to collaborate and defend cybercrime on a global scale.

15.3.1 International trends:

As more and more criminals are aware of potentially large economic gains that can be achieved with cybercrime, they tend to switch from simple adventure and vandalism to more targeted attacks, especially platforms where valuable information highly concentrates, such as computer, mobile devices and the Cloud. There are several emerging international trends of cybercrime.

- **Platform switch:**

Cybercrime is switching its battle ground from Windows-system PCs to other platforms, including mobile phones, tablet computers, and VoIP. Because a significant threshold in vulnerabilities has been reached. PC vendors are building better security into their products by providing faster updates, patches and user alert to potential flaws. Besides, global mobile devices' penetration—from smart phones to tablet PCs—accessing the Internet by 2013 will surpass 1 billion, creating more opportunities for cybercrime. The massively successful banking Trojan, Zeus is already being adapted for the mobile platform. SMS phishing, is another method cyber criminals are using to exploit mobile devices, which users download after falling prey to a social engineering ploy, is designed to defeat the SMS-based two-factor authentication most banks use to confirm online funds transfers by customers. VoIP systems are being used to support vishing (telephone-based phishing) schemes, which are now growing in popularity.

- **Social engineering scams:**

It refers to a non-technical kind of intrusion, in the form of e-mails or social networking chats, that relies heavily on human interaction and often involves fooling potential victims into downloading malware or leaking personal data. Social engineering is nevertheless highly effective for attacking well-protected computer systems with the exploitation of trust. Social networking becomes an increasingly important tool for cyber criminals to recruit money mules to assist their money laundering operations around the globe. Spammers are not only spoofing social networking messages to persuade targets to click on links in emails they are taking advantage of users' trust of their social networking connections to attract new victims.

- **Highly targeted**:

The newest twist in "hyper targeting" is malware that is meant to disrupt industrial systems such as the Stuxnet network worm, which exploits zero-day vulnerabilities in Microsoft. The first known copy of the worm was discovered in a plant in Germany. A subsequent variant led to a widespread global outbreak.

- **Dissemination and use of malware**:

Malware generally takes the form of a virus, a worm, a Trojan horse, or spyware. In 2009, the majority of malware connects to host Web sites registered in the U.S.A. (51.4%), with China second (17.2%), and Spain third (15.7%). A primary means of malware dissemination is email. It is truly international in scope.

- **Intellectual property theft (IP theft)**:

It is estimated that 90% of the software, DVDs, and CDs sold in some countries are counterfeit, and that the total global trade in counterfeit goods is more than $600 billion a year. In the USA alone, IP theft costs businesses an estimated $250 billion annually, and 750,000 jobs.

15.4 International Cyber Law legislative responses and cooperation:

- **International responses*:***

✓ **Group of Eight :**

Group of Eight (G8) is made up of the heads of eight industrialized countries: the U.S., the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada.

In 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cybercrime, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis.

✓ **United Nations:**

In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of

information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology.

- ✓ **ITU:**

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cyber security issues. The ITU was the lead agency of the World Summit on the Information Society (WSIS).

In 2003, Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cybercrime.

In 2005, the Tunis Commitment and the Tunis Agenda were adopted for the Information Society.

- ✓ **Council of Europe :**

Council of Europe is an international organisation focusing on the development of human rights and democracy in its 47 European member states.

In 2001, the Convention on Cybercrime, the first international convention aimed at Internet criminal behaviors, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member states. But only 25 countries ratified later. It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cybercriminal offences qualification, provision for laws empowering law enforcement and enabling international cooperation.

- **Regional responses*:***
- ✓ **APEC:**

Asia-Pacific Economic Cooperation (APEC) is an international forum that seeks to promote promoting open trade and practical economic cooperation in the Asia-Pacific Region. In 2002, APEC issued Cyber security Strategy which is included in the Shanghai Declaration. The strategy outlined six areas for co-operation among member economies including legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education.

- ✓ **OECD:**

The Organisation for Economic Co-operation and Development (OECD) is an international economic organisation of 34 countries founded in 1961 to stimulate economic progress and world trade. In 1990, the Information, Computer and Communications Policy (ICCP) Committee created an Expert Group to develop a set of guidelines for information security that was drafted until 1992 and then adopted by the OECD Council. In 2002, OECD announced the completion of "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security".

- ✓ **European Union:**

In 2001, the European Commission published a communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".

In 2002, EU presented a proposal for a "Framework Decision on Attacks against Information Systems". The Framework Decision takes note of Convention on Cybercrime, but concentrates on the harmonization of substantive criminal law provisions that are designed to protect infrastructure elements.

- ✓ **Commonwealth:**

In 2002, the Commonwealth of Nations presented a model law on cybercrime that provides a legal framework to harmonize legislation within the Commonwealth and enable international cooperation. The model law was intentionally drafted in accordance with the Convention on Cybercrime.

- ✓ **ECOWAS:**

The Economic Community of West African States (ECOWAS) is a regional group of west African Countries founded in 1975 it has fifteen member states. In 2009, ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law.

- ✓ **Gulf Cooperation Council (GCC):**

In 2007, the Arab League and Gulf Cooperation Council (GCC) recommended at a conference seeking a joint approach that takes into consideration international standards.

- ✓ **Voluntary industry response:**

During the past few years, public-private partnerships have emerged as a promising approach for tackling cyber security issues around the globe. Executive branch agencies (e.g., the Federal Trade Commission in US), regulatory agencies (e.g., Australian Communications and Media Authority), separate agencies (e.g., ENISA in the EU) and industry (e.g., MAAWG, …) are all involved in partnership. In 2004, the London Action Plan was founded, which aims at promoting international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses.

15.5 IT Act 2000 (Information technology Act):

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank

The Information Technology Act 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on October 17, 2000. This act is being opposed by Save Our Voice campaign and other civil society organizations in India. User-review and consumer social networking site MouthShut.com has filed a write petition in the Supreme Court of India to repeal and nullify parts of IT Act 2000

15.5.0 Cyber Law Cases in India :

- **UTI Bank hooked up in a phishing attack:**

Fraudsters of cyberspace have reared its ugly head, the first of its kind this year, by launching a phishing attack on the website of Ahmedabad-based UTI Bank, a leading private

bank promoted by India's largest financial institution, Unit Trust of India (UTI).

A URL on Geocities that is almost a facsimile version of the UTI Bank's home page is reported to be circulating amongst email users. The web page not only asks for the account holder's information such as user and transaction login and passwords, it has also beguilingly put up disclaimer and security hazard statements.

“In case we have received any e-mail from an address appearing to be sent by UTI Bank, advising us of any changes made in our personal information, account details or information on our user identity and password of our net banking facility, please do not respond. It is UTI Bank's policy not to seek or send such information through email. If we have already disclosed our password please change it immediately, “ the warning says.

If any unsuspecting account holder enters his login identity, password, transaction identity and password in order to change his details as 'advised' by the bank, the same info is sent vide mail form.

After investigation, we found that Mailform is a service of PC Svet, which is a part of the Czech company PES Consulting. The Webmaster of the site is a person named Petr Stastny whose e-mail can be found on the web page. Top officials at UTI Bank said that they have reported the case to the Economic Office Wing, Delhi Police. The bank has also engaged the services of Melbourne-based Fraud Watch International, a leading anti-phishing company that offers phishing monitoring and take-down solutions. "We are now in the process of closing the site. Some of these initiatives take time, but customers have been kept in the loop about these initiatives", said V.K.Ramani, President - IT, UTI Bank.

As per the findings of UTI Bank's security department, the phishers have sent more that 1,00,000 emails to account holders of UTI Bank as well as other banks. Though the company has kicked off damage control initiatives, none of the initiatives are cent percent foolproof. "Now there is no way for banks to know if the person logging-in with accurate user information is a fraud," said Ramani. However, reliable sources within the bank and security agencies confirmed that the losses due to this particular attack were zilch.

The bank has sent alerts to all its customers informing about such malicious websites, besides beefing up their alert and fraud response system. "Engaging professional companies like Fraud Watch help in reducing time to respond to attacks," said Sanjay Haswar, Assistant Vice President, Network and Security, UTI Bank.

- **City principal seeks police help to stop Cyber crime:**

Principals across the city seem to be taking a cue from principal of Bombay Scottish School, Mahim. After students began posting insults against him on Orkut, instead of punishing them he decided to call in cyber cell cops to talk to students. Now, other school principals have decided to bring in the cyber cell police to speak at their schools. They feel students and parents need to be educated against the legal and moral consequences of cyber crime.

Admitting to the existence of some mischievous students who misuse the internet and also stray into restricted sites due to lack of supervision, principals feel the cyber cell can play a huge role in educating students and warning them. Principal Rekha Vijaykar, GHK School, Santacruz, said that with more and more exposure to the internet, students had started misusing the freedom and hence needed to be monitored. "Monitoring and educating students against the pitfalls of visiting restricted sites is the responsibility of parents. However, the school too has to play an active role," she said.

Principal Alka Lokre of J M Bajaj School, Nagothane concurred. "Students need to be oriented with soul searching and conscience questioning which will help restrain them from misusing modern amenities," she said. As a solution, Principal Fr Dr Francis Swamy of Holy Family School, Andheri, said that apart from educating students, parents and teachers also needed to be roped in for the success of any initiative against internet abuse. "Without the support of parents, no awareness programme can succeed. Parents need to be sensitised to the problem on hand and should be active in stopping their children from maligning anyone," he said.

Principal Paul Machado of Campion School went a step further, highlighting the long term effect of such uncontrolled freedom to students. "Parents must understand that today their children are misusing the internet to abuse others. Tomorrow, they may become victims of it too. Hence, parents need to be taken into confidence too to stem this rot." Apart from the above, all principals lauded the move by Dr D P N Prasad, Bombay Scottish principal, to invite the cyber cell to speak on cyber crime and said that they would also be inviting the cell officials to speak on the subject in their schools.

15.6 Unit Summary:

This unit introduces the

- Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. Cyber law is a term used to describe the legal issues related to use of communications technology, particularly “cyberspace”, i.e. the Internet.
- Cybercrime is "international" or "transnational" – there are ‘no cyber-borders between countries' International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement.

- Types of Cyber Crimes:
  - ✓ Hacking
  - ✓ Data Theft
  - ✓ Spreading Virus or Worms
  - ✓ Identity Theft
  - ✓ E-Mail Spoofing
- Other Forms:
  - ✓ Intrusive Offences
  - ✓ Content-related offences
  - ✓ Copyright and trademark-related offences
  - ✓ Computer-related offences
  - ✓ Combination offences
- International Cyber Law legislative responses and cooperation
  - ✓ International responses
  - ✓ Regional responses

15.7 Keywords :

Cyber Law, Cyber Crime, International Cyber Law, and IT Act 2000.

15.8 Exercises :

1. What is Cyber Law and Explain.
2. Write a short note on International Cyber Law.
3. Explain the different threats of Cyber Law.
4. Explain the types of Cyber crime?
5. Mention different International Cyber Law legislatives.
6. Write a note on IT Act.

15.9 References:

1. Electronic Commerce – Elias Malady
2. Frontiers of Electronic Commerce – Kalakos Whinstone
3. E-Commerce – Mamta Bhusry
4. Electronic Commerce – Gary P.Schneider

Unit 16: The E-cycle of Internet Marketing case study

Structure:

16.0 OBJECTIVES:

- To Know about E-cycle.
- How e-cycle effect on Internet marketing ?
- Different Case studies of Internet marketing.

16.1 Introduction of E-cycle and Internet Marketing:

E-cycle is the practice of reusing, donating or redistributing an electronic item until the end of its life cycle and then recycling the item when it is no longer usable. E-cycling is generally practiced to reduce the amount of electronic components that are discarded when users purchase new components.

The U.S. Environmental Protection Agency (EPA) lists e-cycle as a new term that refers to the process of collecting, distributing, brokering, repairing or reusing used electronic components without discarding them until the expiry of their life cycle. The e-cycling process allows people to reduce, reuse and recycle obsolete electronic items.

The used electronic items or equipment are called electronic waste (e-waste). Items that can be e-cycled include the following:

- Televisions
- Microwave ovens
- Computer peripherals
- Vacuum cleaners
- Mobile phones
- DVDs
- CDs
- Stereos
- Computers

In most cases, electronic items that are functional, such as computers and mobile phones, can be circulated to another person or organization. Other non-functioning electronic items can be repaired, resold or donated. With technological advancements, new electronic devices replace existing ones, making older versions obsolete. Organizations have started investing in e-cycling facilities, due to technology's increasing rate of obsolescence.

Discarding electronic devices is a serious threat to the environment because of the toxic substances involved in their components

- **Internet Marketing:**

Internet marketing, or online marketing, refers to advertising and marketing efforts that use the Web and email to drive direct sales via electronic commerce, in addition to sales leads from Web sites or emails. Internet marketing and online advertising efforts are typically used in conjunction with traditional types of advertising like radio, television, newspapers and magazines.

- **E- marketing:**

Identifying, understanding collaboratively creating and meeting a segment of human and social needs, wants, desires, wishes digitally.

Advantages of Internet Marketing:

Just as Internet research becomes an increasingly important tool during the purchasing process, more marketers are seeing the advantages, too. It's a win-win situation. Marketing departments are investing more in online marketing today because it's

- ✓ Attractive to a significant segment of the demographics for most customer profiles. It can effectively reach our target customer.
- ✓ Faster and less expensive to conduct direct marketing campaigns.

For example, an email campaign or online newsletter compared with traditional printing and direct-mail costs.

- ✓ More economic to communicate via email, online chat, and video conferencing than long distance phone calls or toll-free numbers offered by our company.
- ✓ Measurable, which means that successes are identifiable and repeatable.
- ✓ Set up for real-time results monitoring, and it can handle real-time tweaks and on the-fly changes.
- ✓ Open 24-hours a day, which means that even potential customers with insomnia can be reached at some point during the buying process.
- ✓ Targeted, allowing we to pinpoint using geography, contextual relevance, and other useful parameters to reach a very specifically defined audience. (Online reviews are used more by expert Internet users or in niche product markets.)
- ✓ Continuously available, letting us to give away white papers or free webinars to gather good sources of leads over time. Products with high price points and long sales cycles require many "touches" and follow-up with a potential customer.

16.1.0 Reasons for going Internet Marketing:

1.New economy:

Internet has created a new economy, which by its explosive growth and sheer size already changed our perception of traditional way of doing business. Companies like Amazon and Ebay have successfully created domination on areas, where just few years ago traditional brick-and-mortar companies were kings. However, in order to be successful on the net, we don't have to be

a giant like them. Many small and mid-size companies managed to build online businesses quite profitably. In fact, studies show that small and mid-size companies will be the main growth force of e-commerce in coming years.

2. Internet is a perfect venue for business:

In order to make a sale we need visitors to come to our shop. On the Internet, our shop could be only a click away from our prospective customers. With proper marketing our Internet storefront can have more buyers than us ever can get in a brick and mortar shop.

3. Company's image:

Whether we sell products or services online or not, in today's world we have to have a corporate presence on the Internet. Otherwise, as we must have noticed that people simply don't take our business seriously if we tell them that our company does not have a website. A nice corporate site definitely increases the image of a company especially if it has great product or service related content to go with.

4. Provide better customer support:

Customer accusation and retention is one of the key factors of business value chain. Thanks to Internet technology, business can provide customer support more effectively. This means better customer satisfaction and increase of profitability.

5. Make information more easily available to customers:

Just a couple of years ago, companies used to require days to deliver products or services update information to their customers. Things have changed since then. Today we can add or make any changes to our company and product related content virtually in a matter of couple of hours, publish on our site and share with the whole world.

6. Cut costs:

New technologies allow we to take virtually any part of our business online, that include supply chain management, billing, shipping, procurement etc. Streamlining these business

processes through online systems will allow companies to cut costs significantly in almost every sphere of any business.

For example: companies can reduce more than five percents of their maintenance, repair and operation costs by adopting e-business solutions. This five percent savings can turn into 50% of a company's net profit!

7. Ability to do business 24 hours:

How else we can continue making sales, while our stuffs are sleeping! The biggest advantages of online shops are that they are open 24 hours a day year round. Thanks to Internet off time, when our shop is generally closed, sales in some cases can be more than our regular business hours!

8. Low start up costs:

Building a web site does not require big investments. There are many low cost tools available today, which can help us create sites from very scratch. Many business portals allow us to build web sites from templates. For less than 100$/month we can have a full-fledged corporate e-business site with all e-commerce features!

9. We physical presence could be in any location:

The World Wide Web allows us to do business from any part of the world. Our physical location, except for few cases is not that important since we conduct our business online.

10. Go global:

Thanks to Internet we can instantly become a global player. In fact, we don't have to invest large sums of money to do this. There are literally hundreds of vertical and horizontal e-marketplaces available on the net. These marketplaces allow us for a nominal fee to get access to a large audience of prospective customers from all over the world.

The right determinant of e-business success is the same like any off line business. We have to have a great idea, we have to have a business plan, there should be a value proposition for prospective clients and we should have belief in it and our ability!

16.2 E-CYCLE OF INTERNET MARKETING:

- **BUSINESS PLANNING:**

A **business plan** is a formal statement of a set of business goals, the reasons they are believed attainable, and the plan for reaching those goals. It may also contain background information about the organization or team attempting to reach those goals. Business plans may also target changes in perception and branding by the customer, client, taxpayer, or larger community. When the existing business is to assume a major change or when planning a new venture, a 3 to 5 year business plan is required, since investors will look for their annual return in that time frame. Written document identifying our business goals & how we will achieve them.

Elements of Business Planning:

- ✓ Mission / Vision
- ✓ Product
- ✓ Competition
- ✓ Target audience
- ✓ Marketing
- ✓ Sales plan
- ✓ Operation
- ✓ Technology

- **Product :**

A product is anything that can be offered to a market that might satisfy a want or need. In retailing, products are called merchandise. In manufacturing, products are bought as raw materials and sold as finished goods. Commodities are usually raw materials such as metals and agricultural products, but a commodity can also be anything widely available in the open market. In project management, products are the formal definition of the project deliverables that make up or contribute to delivering the objectives of the project. In insurance, the policies are

considered products offered for sale by the insurance company that created the contract. The elements of the product to be considered in Internet Marketing,

- ✓ Emphasize on viability, quality & integrity
- ✓ Physical vs. Service

- **Pricing:**

Pricing is the process of determining what a company will receive in exchange for its product. Pricing factors are manufacturing cost, market place, competition, market condition, brand, and quality of product. Pricing is also a key variable in microeconomic price allocation theory. Pricing is a fundamental aspect of financial modeling and is one of the four Ps of the marketing mix. The other three aspects are product, promotion, and place. Price is the only revenue generating element amongst the four Ps, the rest being cost centers. However, the other Ps of marketing will contribute to decreasing price elasticity and so enable price increases to drive greater revenue and profits. Pricing is the manual or automatic process of applying prices to purchase and sales orders, based on factors such as: a fixed amount, quantity break, promotion or sales campaign, specific vendor quote, price prevailing on entry, shipment or invoice date, combination of multiple orders or lines, and many others. Automated systems require more setup and maintenance but may prevent pricing errors. The needs of the consumer can be converted into demand only if the consumer has the willingness and capacity to buy the product. Thus pricing is very important in marketing.

Element of the Internet Marketing:

- ✓ Frequent purchase plans
- ✓ On-line auctions

- **Place:**

In Internet Marketing where a product and inventory information is provided by multiple third parties, whereas transactions are processed by the marketplace operator. Online marketplaces are the primary type of multichannel ecommerce. In an online marketplace, consumer transactions are processed by the marketplace operator and then delivered and fulfilled by the participating retailers or wholesalers (often called Drop shipping).In general, because

marketplaces aggregate products from a wide array of providers, selection is usually more wide, availability is higher, and prices are more competitive

The Important elements of the Internet Marketing,

- ✓ Exchange of information between businesses and delivery companies
- ✓ Ensure prompt delivery of physical goods to customers
- ✓ Related to fulfillment

- **Promotion:**

Internet advertising, uses the Internet to deliver promotional marketing messages to consumers. It includes email marketing, search engine marketing, social media marketing, many types of display advertising (including web banner advertising), and mobile advertising. Like other advertising media, online advertising frequently involves both a publisher, who integrates advertisements into its online content, and an advertiser, who provides the advertisements to be displayed on the publisher's content. Other potential participants include advertising agencies who help generate and place the ad copy, an ad server who technologically delivers the advertises and tracks statistics, and advertising affiliates who do independent promotional work for the advertiser.

Elements of the Internet Marketing:

- ✓ AIDA (Attention, Interest, Desire, and Action)
- ✓ Get prospective visitors' attention
- ✓ Create interests in a product
- ✓ Build a desire in the product
- ✓ Banners

- **Personalization:**

Personalization is an extreme form of price differentiation. Whereas product differentiation tries to differentiate a product from competing ones, personalization tries to make a unique product offering for each customer.

- ✓ Combination of Promotion & Product
- ✓ For customers to receive personalized information
- ✓ 'Artificial Intelligence' incorporated into Internet Marketing

- ✓ Identification
- ✓ Determining buyers' buying pattern
- ✓ Marketing attractive products
- ✓ How to add personalization
- ✓ Keywords
- ✓ Collaborative filtering
- ✓ Rule-based

16.3 Case Studies of Internet Marketing:

Case No.1:

Though this company's website had been in existence since 2004, it had never been able to achieve any significant ranking in popular search engines. Their website was rarely ever found via search engines so they never had many web visitors.

The company was heavily invested in Yellow Pages advertising but they realized that more and more of their potential clients prefer to use the Internet to find service organizations. They threw money at a new website and waited for the Internet leads to come flying in. After two years had passed, they could not attribute a single new client to the money and effort they had spent on their website.

They questioned their web development company as to why they were not getting any new customers from their site. They learned that their website was rarely visited. Their web developer was unapologetic. He had delivered a website as promised - completed his end of the bargain. He had built the "store" - it was not his fault that no one entered the store. He was just happy to collect his annual "rent" on the store without customers.

The Solution:

Web Partners was tapped to assist the company in formulating a comprehensive search engine marketing strategy that would increase qualified website traffic, search engine referrals and customer acquisition. In essence, make their website do what all websites should be wired to do increase sales by bringing in new clients and strengthening existing client relationships.

Web Partners observed and evaluated the website. This included studying and

experimenting with frequently associated keywords and phrases. Following this analysis, a search engine optimization approach was formulated, tested, and refined.

Results:

Significant results were achieved within just five months from the start of the Web Partners engagement. Traffic greatly increased by 3000%, this led to a substantial increase in sales even as Yellow Pages expenditures were reduced.

Since then, the company website has consistently occupied the top 10 search engine results for associated keywords and phrases in every major search engine and online directory. It has occupied the number one spot in Google for key searches over the past two years. The approach gave the company a significant online advantage over its rivals.

Case No.2:

Ko Marketing started working with John Deere in 2003 they continue to be a client, the Website had virtually no search engine optimization, and the Website technology dated back to 1995. The Website is highly dynamic, providing users with a powerful way to search through John Deere's dealers' used equipment inventories, by location, zip code, equipment type, and in multiple languages.

We identified basic issues with the Website that were preventing Machinefinder.com from improving its search engine visibility.

- ✓ No keyword strategy was in place for determining which keywords had the most value to target for improved rankings.
- ✓ One element to maximizing search engine visibility is to ensure that our HTML code is optimized so that search engines understand each page. On this site, basic page tagging, such as HTML page titles, header (H1) text, etc., needed to be done
- ✓ There was not enough content that appealed to users and search engines.
- ✓ Equipment listings could not be indexed by search engines because they were only available for viewing using the site's search functionality.
- ✓ URL structures are important to gaining search engine visibility, so we made it a high priority to change dynamic URLs with multiple query variables and on-URL session tickets to static URLs. Foreign-language URLs could not be adequately crawled and

indexed by search engines.

- ✓ Individual John Deere dealer pages could not be crawled and indexed.
- ✓ The site had the potential to gain many more back links (links pointing to a website) than were currently present.
- ✓ Pay Per Click activities were being managed in-house with resources that did not have time to extend and optimize the campaigns.
- ✓ Pay Per Click campaigns were not set up to track any user actions, limiting the ability to effectively target spending by keyword.

The Steps Taken:

- **Keyword Research** – The SEO process began with extensive keyword research to identify the most valuable combination of words people used to find the used equipment listed on the site. There are over 40 equipment categories and many sub-categories contained within each of those larger buckets. We worked with the John Deere Agricultural Remarketing team to identify potential keywords based on their deep industry experience, used keyword research tools, and surveyed the competitive landscape.

- **Page Tagging** – The Website needed a small update in order to accommodate the process of applying page titles, meta description tags, and keyword tags. We worked with the Website development team to create a quick administrative add-on to allow the Deere team to assign these variables to individual pages.

- **Content Creation** – The Website had almost no pages beyond the basic search interfaces and user registration pages. We created 50 new pages of content to target the basic equipment categories and address some of the additional content needs.

- **Unlocking the Equipment Listings** – Because the individual equipment listings (over 60,000 individual equipment pieces at the time, changing daily) were "locked" behind the equipment search interface, we had the challenge of making the individual URLs accessible to search engines. One step that we took was to create a Google Site Map and

automate the process of refreshing the equipment listings. This first required that we re-write the URLs for the individual equipment listings in order to make them friendlier to search engine robots. Another step that we took was to use the same file to submit equipment listings to Google Base.

- **URL Structure –** Because of the legacy technology platform of the site (dating back to 1995) we were very limited in our ability to completely re-write the URLs of the Website, without having the entire site re-developed. We made the changes that we could, and the end result was a URL structure that was a bit more friendly, but not 100% where we wanted it to be. Technology limitations of an existing site are always one of the challenges we face, and we work with the Web development team at a client to find the most appropriate solution.

- **Foreign Language URLs** – In order to give search engines access to the content in the 12 non-English languages that the site supports, we created a URL structure to present the localized content to search engines appropriately. In order to make a stronger connection to the content we added on-site navigation to get to these localized pages.

- **Foreign Language Optimization** – The process for localization of the page content is managed by each territory separately. We needed to provide the country managers with the education and training to conduct keyword research, tag pages, and localize page content. We started by conducting our own foreign-language keyword research. We then presented the data to the individual country managers, and then provided individual training for how to take over the process and take control of localizing the content with search engines in mind.

- **Individual Dealer Pages –** We worked with Deere and the Web development team to create a new format for the Web pages that represent each individual Deere dealer on the Machinefinder.com Website. The new page layout and content components were more appealing to search engines, providing more valuable content to crawl and index. URLs were also re-written to gain maximum indexing exposure.

- **Link Building**– The longevity of the site and the Deere brand name provided a nice initial base of links pointing to the site. However, a concentrated effort to generate additional links had not yet been undertaken. We took a highly-customized approach to the link building campaign, making sure to target high-quality links from Websites that were thematically-related to the Machinefinder.com site, approaching each opportunity with the appropriate outreach.

- **Pay Per Click Management** – Ko Marketing took over the management of the PPC campaigns in Google, Yahoo!, and MSN. We established over 30 new campaigns within each engine, added keyword depth, removed under-performing/overly-generic keywords, and wrote new ad copy versions to test simultaneously. As important, we established actions that needed to be tracked on the Website and added the appropriate Website analytics and tracking tools.

- **On-Going Recommendations**– As part of an on-going monthly program, Ko Marketing continues to provide content evaluation, recommendations for new content & new content types, identify new link opportunities, and manage the overall SEO program for the site. We have worked with the client every month for over three years to continually improve Website optimization, facilitating the steady growth of Website traffic and visibility.

The Results:

Quality traffic from search engines has consistently improved over the more than four years we have been working with this client.

- The initial optimization **quadrupled the search engine traffic** to the site.
- The index of pages in search engine databases went from a few hundred pages to **50,000 to 60,000 indexed pages** at any given time.
- The PPC campaigns **dramatically improved**, producing increased results, including measurable performance on an individual keyword level.

- Most importantly, the John Deere dealers who list their equipment on the Website have experienced a pronounced increase in direct inquiries for specific pieces of used equipment!

Our significant success in providing the needed SEO and PPC results, and our ability to do so within the limiting corporate guidelines for the Website, continues to satisfy this client above and beyond all expectations. The client continues to entrust its search engine optimization and pay per click management to KoMarketing today.

Case Study: Moving into New Global Markets

One high-tech company, spun out of a major research university, develops high performance cell-analysis systems at a fraction of the cost of competitors. This new start-up company needed to break into an existing and highly competitive market: life-science research equipment.

They needed to build a U.S. presence and break into the international community for their market. The strategy entailed SEO and ongoing paid search in the United States, South America, Europe, and the Asia-Pacific region. Landing page testing and analysis was part of the package, ensuring that the target market for each country found just what they needed, when they needed it.

Advanced strategies with Google Analytics were applied, to measure progress in new geographic markets. The company adapted this same data to inform offline marketing decisions and new target areas. By applying the online sales engine metrics tools, they are able to follow their online traffic all the way into their CRM system. This way, they know which efforts have the biggest payoff in each country.

After working on these efforts for 2 years, they saw their cost per lead decrease by64% and their conversion rate more than double. The results from their online lead tracking combined with in-depth website analysis is guiding their Internet marketing strategy for the coming year.

Case Study: Manufacturing Company Improves Sales

A manufacturer and installation service company for custom security systems needed to expand its reach and drive new sales. The new website just wasn’t pulling in the target number or quality of leads they were hoping to garner, despite aggressive marketing efforts. The strategy to

drive more traffic involved focusing on the Google Ad Words account to help the company realize return for its advertising expenses. The advertising funds weren't being spent as wisely as they could have been. The Ad Words account was reorganized to focus on the keywords that would deliver the best leads back to the company. Expensive keywords that weren't entirely relevant to the business were eliminated, making advertising an effective driver of sales leads.

The impact of online advertising was further increased by more effective landing pages. Many savvy marketers miss the importance of a landing page that delivers, in a compelling way, the exact information a person is seeking when clicking an ad. The website copy was also improved, adding keyword-rich text throughout, to improve search engine visibility. The effort also included redesigning the company's website and appropriately indexing the website with Google, to support organic search results.

The end effect was that the organic search rankings improved dramatically. More important, they began driving sales for the first time from their website, achieving just under $2 million in online sales by the end of their first full year with the new strategy. This translated to nearly $20 in sales for every $1 spent on advertising. The following year, continuing optimizations allowed for an additional 40% increase in revenue with only a 30% increase in advertising spend.

Case Study: Large Childcare Provider Increases Web Conversions

A large provider of early education and care services to children between 6 weeks and 12 years of age wanted to leverage the web to deliver new business leads in a slow economy. With multiple brands, more than 1,100 schools (corporate and franchise) serving over 100,000 children in the United States and internationally, the company was using its brand websites as the primary point of contact to communicate both with prospects and existing customers. Initial efforts after the initial website launch involved website analytics, paid search, and SEO, although the company was unsatisfied with the outcome of those efforts. They wanted to improve both their online presence and marketing efficiency.

Paid search improvements were tackled first; website-based lead generation was the primary measure of success for the project. A costly website redesign was avoided by identifying ways to rearrange and edit existing website content for increased effectiveness. Paid search was also

integrated more fully into existing online marketing efforts, as part of a comprehensive online strategy.

Conversion rates were improved by applying usability improvements. These came from directly assessing website visitor behavior and interviewing both users and the sales team. Paid search campaigns were moved beyond just Google to Yahoo! And MSN, and the conversion rates improved by creating geo targeted landing pages.

The result from these usability, landing page, and paid search campaign changes was that the cost per conversion steadily declined in all three paid search programs and conversion rates increased overall by 35% over a 2-year period. In addition, advertising costs were reduced by 5% for a competitive keyword marketplace.

Case Study: Major Software Company Grows Sales

One of the world's leading organizations in optimizing application performance, this computer industry leader provides software, experts, and best practices to ensure applications work well and deliver business value. Supporting 46 of the top 50 Fortune 500 companies, and 12 of the top 20 most visited U.S. websites, the diversity of their products, services, and target audiences demands a measured, integrated visibility strategy.

Their initial goal was to appear on "page one" for search engine results listings and paid search results. They also were posing great questions among themselves, such as "How can we build upon and improve our existing online marketing efforts?" Many strategic online elements were already in place: a successful website, analytics tools, a paid search program, and a talented team poised to implement a profitable visibility strategy. A plan focusing on earning the top spots in online search for multiple languages emerged. Additional objectives included elevating specific company solutions and reinforcing an international presence.

Three key components drove the success of their new online marketing initiative:

• A review of the infrastructure for search engine optimization: Search engine visibility improved significantly for non branded terms through implementation of a structured strategy for URL taxonomies, page redirection, page design, link building, and more. With numerous complex websites within the corporate global network, evaluating and leveraging existing content is key, as both the organization and its websites continue to grow.

• Integrating online lead tracking into their CRM system: Integrating search marketing activities with lead source tracking now links how customers are finding the company online and the effectiveness of their online marketing activities in converting online interest into sales.
• Paid search arbitrage: Building on existing successful paid search campaigns, the next level adds depth using a word market strategy and provides a strategy for the aggressive optimization of individual campaign elements, particularly landing page optimization.

You learn more about the word market in the section "Speak Your Audience's Language: The Real Search Engine Optimization" "The Audience Is Listening (What Will You Say?)."
The company has deepened their level of expertise in the area of search marketing. In addition to investing in online marketing efforts, they are now getting a return on those efforts through metrics: tracking, analyzing, and measuring data. Their newly created online sales engine uses the web to drive and convert customers.

16.4 Unit Summary:

This unit introduces the

- E-cycle is the practice of reusing, donating or redistributing an electronic item until the end of its life cycle and then recycling the item when it is no longer usable.
- Internet marketing, or online marketing, refers to advertising and marketing efforts that use the Web and email to drive direct sales via electronic commerce, in addition to sales leads from Web sites or emails.
- Reasons for Online Marketing
- E-cycle on Internet Marketing.

16.5 Keywords:

E-Cycle, Internet Marketing

16.6 Exercise:

1. What is E- Cycle?
2. What is Internet Marketing?
3. Explain advantages of Internet marketing.
4. Explain E cycle on Internet Marketing?
5. Give the reasons for going Online Marketing.

16.7 References:

1. Electronic Commerce – Elias Malady
2. Frontiers of Electronic Commerce – Kalakos Whinstone
3. E-Commerce – Mamta Bhusry
4. Electronic Commerce – Gary P.Schneider