Karnataka State Open University
Mukthagangothri, Mysore – 570 006.
Dept. of Studies and Research in Management

MBA IT Specialization
III Semester

E-commerce

Block 1

Preface

We are in the age of knowledge management and instant communication and consequently in the midst of an electronic revolution, the impact of which on the economy is much more profound than that caused by the Industrial revolution. This modern-day revolution, at the global level, has manifested itself in the form of many innovations and breakthroughs and giant leaps in internetworking technology. With these new opportunities, people can now transcend the barriers of time and distance with the Internet's speed.

With the inception of the Web, organizations and individuals are more and more making use of it to create new business ventures. The WWW is not only a definitive source of information, but an astounding business opportunity as well. People throughout the world are venturing out onto the Web for buying and selling goods and services. The Web has indeed proved to be a boon to business, drawing its power from the flow of easy and instantaneous transactions, worldwide. Online business is thriving and more and more corporate companies are joining the fray of electronic transactions. Thus ushered in, the era of 'E-commerce' has established a significant synergy between the use of digital information and computerized business.

Wish you happy reading !!!

Karnataka State Open University

Mukthagangothri, Mysore – 570 006.

Dept. of Studies and Research in Management

MBA. IT Specialization

III Semester

E-commerce

BLOCK 1

BLOCK1 INTRODUCTION

Electronic commerce is termed as E-commerce in short. E- Commerce is an action of conducting business transaction for selling goods, services and information via communication network.

First unit focuses on defining E-commerce, components of E-commerce, listing of trends and features that play a role on E-commerce. Unit two focuses on describing different categories of E-commerce. E-commerce is supported by basic underlying framework that identifies the task of hardware and software components and services provided by them explained in Unit 3. Unit 4 gives the detailed description on the important component of E-commerce i.e. Internet and Web. This block consists of 4 units and is organized as follows:

Unit 1- What Is E-commerce? The Difference between E-commerce and E-business, E-commerce: A Commercial Transaction, Technological Building Blocks Underlying E-commerce: the Internet, Web, and Mobile Platform, Major Trends in E-commerce, Unique Features of E-commerce Technology

Unit 2- Business-to-Consumer (B2C) E-commerce, Business-to-Business (B2B) E-commerce, Consumer-to-Consumer (C2C) E-commerce, Consumer-to-Business (C2B), E-commerce Mobile E-commerce (M-commerce), Social E-commerce, Local E-commerce: A Brief History, Understanding E-commerce: Organizing Themes, Academic Disciplines Concerned with E-commerce

Unit 3- The Internet, Technology Background , Internet – Key Technology concepts, TCP/IP, IP addresses, Domain names, DNS and URLs, Client Server Computing, Cloud computing model, Mobile platform

Unit 4- Hypertext, HTML, XML, Web servers and clients, Web browsers, Communication tools – E mail, messaging apps, online message boards, Internet Telephony

UNIT -1: INTRODUCTION TO E-COMMERCE

STRUCTURE

1.0 Objectives

1.1 Introduction

1.2 Difference between E-commerce and E-business

1.3 E-commerce: A Commercial Transaction

1.4 Technological Building Blocks Underlying E-commerce

1.5 Major Trends in E-commerce

1.6 Unique Features of E-commerce Technology

1.7 Check your progress

1.8 Summary

1.9 Keywords

1.10 Questions for self-study

1.11 References

1.0 OBJECTIVES

After studying this unit, you will be able to:

- ✓ Define E-commerce
- ✓ Categorize between E-commerce and E-business
- ✓ Explain technological components of E-commerce
- ✓ Gather major trends in E-commerce
- ✓ List the unique features of E-commerce

1.1 INTRODUCTION

E-commerce is a modern business methodology that addresses the needs of organization, merchants and consumers to cut costs simultaneously improving the quality of goods, services and information by increasing the speed of service delivery. It is basically moving trade to World Wide Web (www) through internet.

E-commerce doesn't require employing sales person and acquiring luxury showrooms thereby

1

spending less money. The faster customer response, improved service quality and minimizing product cycle time (Difference between product purchase-time to delivery time) are the main goals of E-commerce.

E-commerce involves the use of the Internet, the World Wide Web (Web), and mobile apps and browsers running on mobile devices to transact business. Although the terms Internet and Web are often used interchangeably, they are actually two very different things. The Internet is a worldwide network of computer networks, and the Web is one of the Internet's most popular services, providing access to billions of web pages. An app (short-hand for application) is a software application. The term is typically used when referring to mobile applications, although it is also sometimes used to refer to desktop computer applications as well. A mobile browser is a version of web browser software accessed via a mobile device. More formally, e-commerce can be defined as digitally enabled commercial transactions between and among organizations and individuals. Each of these components of our working definition of e-commerce is important.

Digitally enabled transactions include all transactions mediated by digital technology. For the most part, this means transactions that occur over the Internet, the Web, and/or via mobile devices. Commercial transactions involve the exchange of value (e.g., money) across organizational or individual boundaries in return for products and services. Exchange of value is important for understanding the limits of e-commerce. Without an exchange of value, no commerce occurs.

Advantages of E-commerce are:

- Provides 24*7 operation of trading
- Global reach of business is attained through internet
- Cost of acquiring, servicing and retaining is minimized
- An extended enterprise is easy to build since all players of E-commerce plays a role
- Intermediation or Brokerage is removed. **E.g.** ITC started website called e-Choupal.com
- It has power to provide best on both offline and online worlds
- It provides technology based customer interface
- Here customer controls the interaction
- Helps in collecting knowledge of customer behavior

2

Disadvantages of E-commerce are:

- Lack of security
- Inability to provide audit logs
- Lack of 3rd party verification in case of disputes
- Not suitable for perishable or very expensive goods

E-commerce opportunities for Industries are:

- Financial services: **E.g.** Birla Global Finance Ltd.
- Stock trading: **E.g.** Motilal Oswal
- Banking: **E.g.** ICICI
- Legal services: **E.g.** IntegrCom.com
- Professional services: **E.g.** HKS Architects (hksinc.com)
- Tour and travel: **E.g.** Trivago.in
- Health care: **E.g.** narayanahealth.org

1.2 DIFFERENCE BETWEEN E-COMMERCE AND E-BUSINESS

E-commerce: It involves commercial transactions through website over the internet for the activities such as online purchasing of product, online money transactions, online ticket booking and online customer care. The end customer will play a major role in the process of E-commerce. Customer communication is through the website and application.

E.g. Amazon, Myntra, Paytm

E-commerce sales can include every element of a sale: ordering a product, paying for a product, and having it delivered. It might also involve only part of the process. For example, a customer might order a product online to be picked up at the store. Payment might be conducted online or at the store when the item is picked up. Either way, the transaction still involved an element of e-commerce.

Many businesses also sell through virtual marketplaces in addition to their own websites. For example, a popular brand like Nike will sell shoes from its website, as well as through an online

3

retailer like Amazon. Whether you buy it from Nike's website or Amazon's, the transaction is still an example of e-commerce.

E-business: It involves business transactions over internet mainly for inventory management such as acquisition of raw materials and supply chain management. The information sharing is among the internal domains of the business. Website, Enterprise Resource planning (ERP) and Customer relationship management (CRM) is required for E-business.

Many processes that are described as e-business might be handled in-house through a company's network, or it might be something the company outsources to a provider that specializes in whatever service is desired. By producing them in-house, standard businesses may incorporate some elements of e-business into their plan—the two types of businesses are not mutually exclusive.

Sometimes the difference between a standard business and an e-business is just a matter of how business is conducted. For example, if you are an advisory firm helping people choose the right furniture, then you are a business, but if you run a website where people can compare furniture options, then you are an e-business.

E.g. E-auction, Hardware and software development site

E-commerce and e-business systems blur together at the business firm boundary, at the point where internal business systems link up with suppliers or customers as depicted in figure 1.1.
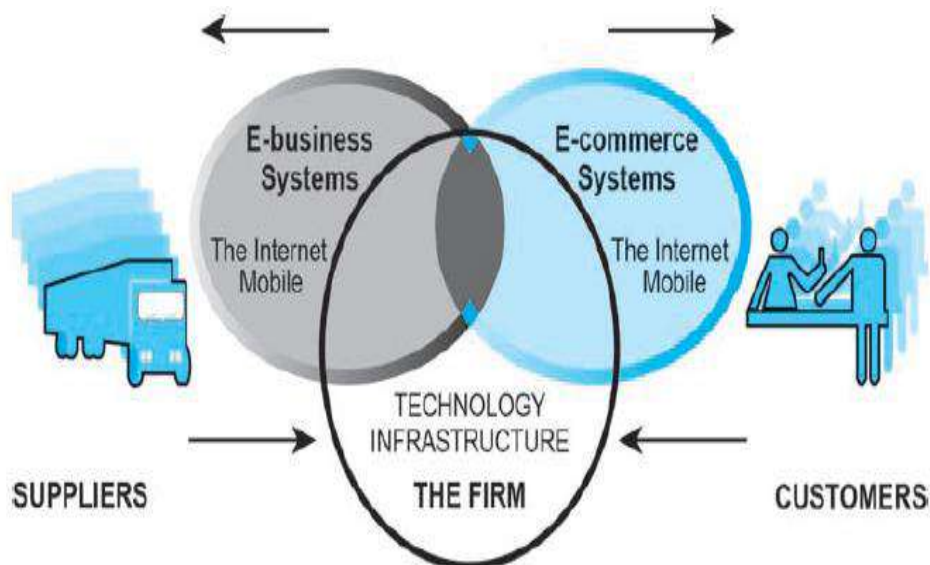

Fig. 1.1. The difference between e-commerce and e-business

4

1.3 E-commerce: A Commercial Transaction

E-commerce: A Commercial Transaction E-commerce defined simply, is the commercial transaction of services in an electronic format. In general terms, e-commerce is a business methodology that addresses the needs of organizations, traders and consumers to reduce costs while improving the quality of goods and services and increasing the speed of service delivery. It refers to all forms of transactions relating to commercial activities, including both organizations and individuals that are based upon the processing and transmission of digitized data, including text sound and visual images. A broad definition of ecommerce is: "The marketing, promoting, buying & selling of goods electronically, particularly via the Internet", which encompasses, interalia, "e-tailing (virtual shop fronts), EDI, which is B2B exchange of data; e-mail & computer faxing; [and] B2B buying and selling".

A narrower definition is "the trading of goods and services in which the final order is placed over the Internet". The Office of Tax Policy at the US Department of Treasury defines e-commerce most broadly as any transaction that occurs with the facilitation of electronic "tools and techniques". The Internet Tax Freedom Act (ITFA), 1998, on other hand provides the only legal definition of e-commerce as "any transaction conducted over the Internet or through Internet access, comprising the sale, lease, license, offer or delivery of property, goods, services or information, whether or not for consideration, and includes the provision of Internet access". The US Census Bureau measures e-commerce by looking at "the value of goods and services sold online whether over open networks such as the Internet, or over proprietary networks running systems such as EDI".

According to European Commission, e-commerce encompasses more than the purchase of goods online. It includes a disparate set of loosely defined behaviours, such as shopping, browsing the Internet for goods and services, gathering information about items to purchase and completing the transaction. It also involves the fulfilment and delivery of those goods and services and inquiries about the status of orders. Like any other sustained business activity it also means conducting consumer satisfaction surveys, capturing information about consumers and maintaining consumer databases for marketing promotions and other related activities. Interestingly, its Directive on E-commerce (2000/31/EC) defined the term 'commercial communication' instead of defining 'E-commerce'. Article 2(f) defined 'commercial

communication' as any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organization or person pursuing a commercial, industrial or craft activity or exercising a regulated profession.

The Gartner Group5 defines e-commerce as an evolving set of:

➢ Home-grown or packaged software applications that link multiple enterprises or individual consumers to enterprises for the purpose of conducting business.

➢ Business strategies aimed at optimizing relationships among enterprises and between individuals and enterprises through the use of information technologies.

➢ Business processes (such as procurement or selling or order status checking or payment) that, by definition, cross boundaries, and

➢ Technologies and tools that enable these applications, strategies and processes to be implemented and realised.

1.4 TECHNOLOGICAL BUILDING BLOCKS UNDERLYING E-COMMERCE

Technology is the backbone of e-commerce. Not only does it help connect sellers and customer on mobile and web platforms, but also enables the effective management of customer orders, deliveries, returns and payments of purchased goods. In fact, technology plays an important role throughout the e-commerce value chain, in areas such as recruitment, marketing, and advertising, among many others. Internet, Web and Mobile platform acts as a backbone for automating E-commerce.

Internet: The interconnection of computer networks built on common standards spread globally is called internet. TCP/IP was introduced when US defense department feared on nuclear attack of computers. In addition, IP (Internet Protocol) was introduced when the data needed to be passed on wired path. Earlier around 1960's internet was used to connect small number of mainframe computers and their users. The growth of internet globally evolved with increase in number of internet hosts with domain names. With the introduction of graphical user interface (GUI) for web in 1993, it took only 10 years to accumulate 53% of U.S. share. Internet helps in interconnecting 2 different individuals, messaging, mailing, document sharing and shopping.

Web: Web is a subset of Internet. It is the information system comprised of collection of documents and other resources that runs over Internet. These resources from any location can be accessed from browser by using web address called as Uniform Resource Locator (URL).

Earlier Internet was used for messaging, document sharing and remote computing. But the introduction of web in 1990's made internet more powerful with the collection of web pages. These web pages containing text, graphics, voice, animation and other interactive objects are created from Hypertext Markup Language (HTML). HTML pages can contain text, graphics, animations, and other objects. The Web introduced far more powerful and commercially interesting capabilities of direct relevance to commerce. The size of web is increasing exponentially day by day. In essence, the Web added color, voice, and video to the Internet, creating a communications infrastructure and information storage system that rivals television, radio, magazines, and libraries.

Mobile Platform: In the early years of e-commerce, the Web and web browsers were the only game in town. Today, in contrast, the Internet via a mobile app plays a vital role than by using a desktop computer and web browser. This is the devised technology of internet infrastructure. It allows software and services over the internet to be run on the mobile devices such as laptops, tablets and Smartphone. Lately, due to the emerging technologies and dependency over mobile devices, mobile platform play a vital role in improving E-commerce.

1.5 MAJOR TRENDS IN E-COMMERCE

Major trends in E-commerce based on 3 different perspectives are as follows:

1. **Business Perspective:**
   - *Retail E-commerce* shows a major growth in India, China & South Korea
   - With the excessive usage of mobile apps, *Mobile retail E-commerce* explodes
   - *Social E-commerce* based on social networks such as Instagram, Facebook and Pinterest take part in advertising and providing search, buy buttons that increases the customer product purchase.
   - With the increase in utilization of On-demand services such as Uber, Zomato etc helps in rise of *Local E-commerce*

- Small business and entrepreneurs are entering into E-commerce market place over the infrastructures created by well-established industries such as apple, facebook, google, ebay etc.

2. **Technological perspective:**
   - Since consumer is relied on the mobile devices for most of his day to day basis the mobile marketing, mobile advertising and online transactions have become popular.
   - Mobile messaging platforms such as Whatsapp, snapchat are also been used for advertising.
   - The companies are making investments in pay-per-click marketing mechanism to move ahead in future.
   - The cloud computing technology is evolving since software and content of consumer is expanding. The information is been stored in some "cloud" servers through internet and it is made available from any connected devices.
   - Internet of Things connecting large number of computers is getting evolved.
   - The large amount of data from online interaction is tracked by the firm initiating big data.
   - The useful data patterns are obtained from large amount of flooded information using big data analytics that result in acquiring customer interests and target.
   - Emerging artificial intelligence are being adopted by the companies by making recommendations for the customer purchases based on their searches and likes.

3. **Societal perspective:**
   - Self-publishing of user created contents, photos, videos and creative works over social network forums such as posts, blogs and tweets are increasing thereby connecting people.
   - Disclosing ones motives directly over a social network threatens privacy.
   - Adult's participation in social network like Facebook have become popular in all sectors of population.
   - Government is facing challenges for posing taxation over online trading.
   - The digital copyright owners have found a huge success by protecting intellectual property rights posing agreement over online distributors.

- Spamming and online security threats by hacking customer information are increasing.
- On-demand E-commerce services are creating a space for jobs.

Trends in ecommerce industry emerge from various things. How customers shop. What they buy and how they respond to marketing tactics employed by businesses. Within the last decade, a lot of new trends have emerged with a profounding influence. Ecommerce giants like Amazon, Walmart, and Alibaba have been at the forefront of adopting and benefiting from such trends.

The ecommerce industry is always changing and this year (2021-22) has been no different. More than ever, merchants are creating and/or improving their ecommerce businesses to meet customers where they are.

Let's discuss, the Ecommerce after COVID-19: Our world is changing. Ecommerce will only get bigger and better as the year moves on. New technologies will help it achieve that. The coronavirus has changed things all over the world, and it's expected that buying behavior is likely to boom. Even now, more and more people prefer buying things online because they are not willing to step out and risk exposure to new variants.

In 2021, retail e-commerce sales amounted to an estimated 4.9 trillion U.S. dollars worldwide. This figure is forecast to grow by 50 percent over the next four years, reaching about 7.4 trillion dollars by 2025. The quarantine had laid bare the importance of having an ecommerce business last year, and now, it's easy to say that if you don't have an ecommerce business, you will miss out on serious revenue.

As with all trends in e-commerce marketing, things start to fade after a point. Businesses need to revamp their strategy with every change. This is so that business always stay on top of the marketing game. It's also to show customers that no matter what trends, the product will always be in vogue!

1.6 UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY

Before E-commerce the marketing and trading of goods were sales driven and not focused on particular sector of customers. The customers were trapped as they could not compare for the best pricing and quality of the product. The lack of business transparency created differences in market information.

The arise of E-commerce helped merchants to gain more knowledge about customer behaviour by targeting different sectors of customer on fixing the different price segments for a product. There are 8 unique features of E-commerce challenging traditional business methods by enforcing new technological aspects.
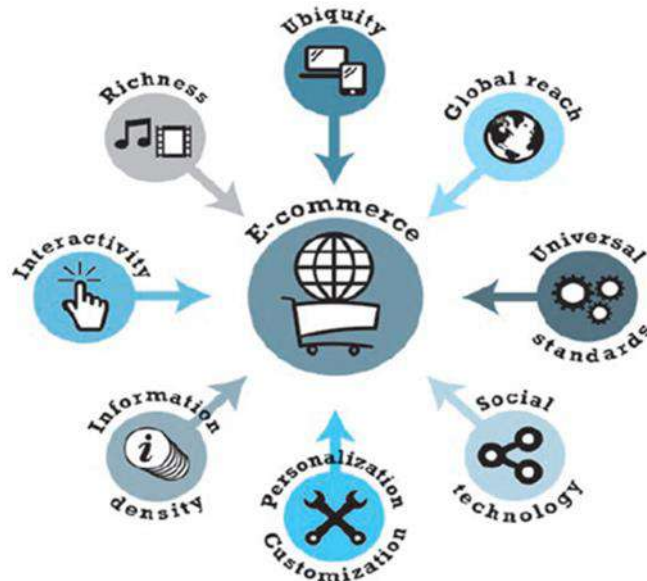

Fig. 1.2. Eight unique features of e-commerce technology

a. **Ubiquity:** In traditional business, the customer has to go to the market place spending his time and energy. But E-commerce is featured by Ubiqity where the customer is made availabe to purchase at all places, all time through mobile E-commerce creating *Marketspace*. This not only saves customer time and energy from travelling to the geographical location of the market place, but also reduces the mental effort of the customer to complete the task.

b. **Global Reach:** The total number of customers any business can attain is called reach. The traditional marketing was through telivision, radio and newspapers which is basically pertaining to some particular region. Hence the business can attain only local reach, whereas E-commerce makes the customers to be atrracted even outside the national boundary through internet with less cost.

c. **Universal standards:** The technical standards for conducting E-commerce over the internet shared all over the world is called Universal standards. It helps in,

> decreasing the *Market entry costs* as expenditure is mostly to get goods to market.

> Reducing *Search costs* as effort for finding the suitable product is made easier over internet

> Detecting *Product Price* as product description and pricing is shared with every customer.

> Finding suppliers, product delivery terms easily from anywhere in the world.

d. **Richness:** The complexity and content of message refers to richness of information. The E-commerce technology such as interactive media and customer targeted messaging using chatbot provides rich information resulting in trade of complex goods and services easily.

e. **Interactivity:** The two way communication between merchant and consumer or between 2 consumers represents the interactive feature of E-commerce. The consumer can directly chat with the merchant that gives them same face to face experience. The interactions are in terms of community forums, providing product comments, responsive websites and social networking sites by share and like of a product.

f. **Information density:** The quality and amount of information among all participants of E-commerce is called information density. The pricing transparency of the products removes the information disparity among the consumers at the same time cost transparency helps the consumer to find out at what cost the product has been purchased by merchants resulting in competitive trading techniques. The merchants makes use of customer information to target over different sectors of population for different product pricing over selling the same goods resulting in product price discrimination. The cost discrimination is also made based on quality and brand of a product.

g. **Personalization and customization:** Based on the previous purchases and interactions made with the customer, the merchant can collect the customer behaviour from information density. Hence personalization helps in targeting the specific individuals by messaging based on his interests. The customization mentions changing of delivered product or services based on customer requirement.

h. **Social Technology:** Previous to E-commerce, the contents were prepared by the experts at some location and it was consumed by the mass. But with the origination of social E-commerce technologies the user is given liberty to create his own content and share it world wide in the social network. The user is also given the privilege to channel their own content consumption.

1.7 CHECK YOUR PROGRESS

1. Electronic commerce (EC) is defined as the online exchange of _____ between firms, and also between firms and their customers.

    a. Money
    b. Services
    c. Goods
    d. All of the Above

2. What is the definition of e-commerce?

    a. The transmission of e-mail over the Internet
    b. Sales through catalog and telephone
    c. The conducting of business and communication transactions by electronic means
    d. Information provided by the U.S. Census Bureau

3. The dimension of E-commerce that enables commerce across national boundaries is called _____.

    a. Interactivity
    b. Global reach
    c. Richness
    d. Ubiquity

4. Which of the following is an example of E-business?

    a. Amazon's inventory control system
    b. Amazon.com website
    c. Amazon mobile app
    d. Amazon's Pinterest page

5. Which of the following is used to purchase products at different locations from any customer location at any time
   a. Marketplace
   b. Marketspace
   c. Social network
   d. The internet

Answers to check your progress:

   1. All of the Above
   2. The conducting of business and communication transactions by electronic means
   3. Global reach
   4. Amazon's inventory control system
   5. Marketspace

1.8 SUMMARY

In this unit we discussed the definition of E-commerce, advantages and disadvantages of E-commerce when applied over business, examples for industrial opportunities created by E-commerce. We also discussed, how a Commercial Transaction E-commerce and the commercial transaction of services in an electronic format. In addition, how E-commerce and E-business differ from each other. Later, technologies behind business over internet were explained along with the features that made E-commerce more popular.

1.9 KEYWORDS

2 **E-commerce**: It is a modern business methodology that addresses the needs of organization, merchants and consumers to cut costs simultaneously improving the quality of goods, services and information by increasing the speed of service delivery.

3 **E-business**: It involves business transactions over internet mainly for inventory management such as acquisition of raw materials and supply chain management.

4 **Internet**: The interconnection of computer networks built on common standards spread globally.

5   **Web**: the information system comprised of collection of documents and other resources that runs over Internet.

6   **Mobile Platform**: The devised technology of internet infrastructure which allows software and services over the internet to be run on the mobile devices.

7   **Reach**: The total number of customers any business can attain.

8   **Universal Standard**: The technical standards for conducting E-commerce over the internet shared all over the world.

9   **Richness**: The complexity and content of message refers to richness of information.

10 **Information Density**: The quality and amount of information among all participants of E-commerce is called information density.

1.10 QUESTIONS FOR SELF-STUDY

1. What is E-commerce? Suggest why it is important to study E-commerce.
2. Differentiate E-commerce from E-business
3. Describe different features of E-commerce.
4. Mention the benefits of Universal Standards.
5. Mention some business consequences resulted from growth from information density.
6. How does ubiquity of E-commerce impact consumers?
7. Discuss advantages and disadvantages of E-commerce.

1.11 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.
2. AdNabu,(2021), https://www.adnabu.com/ecommerce-marketing-trends

UNIT -2: TYPES OF E-COMMERCE

STRUCTURE

2.0 Objectives

2.1 Business-to-Consumer (B2C) E-commerce

2.2 Business-to-Business (B2B) E-commerce

2.3 Consumer-to-Consumer (C2C) E-commerce

2.4 Consumer-to-Business (C2B) E-commerce

2.5 Mobile E-commerce (M-commerce)

2.6 Social E-commerce

2.7 Local E-commerce

    2.7.1 A Brief History

2.8 Understanding E-commerce

    2.8.1 Organizing Themes

    2.8.2 Academic Disciplines Concerned with E-commerce

2.9 Check your progress

2.10 Summary

2.11 Keywords

2.12 Questions for self study

2.13 References

2.0 OBJECTIVES

After studying this unit, you will be able to:

- ✓ Explain different types of E-commerce
- ✓ Differentiate Business-to-Business and Consumer-to-Consumer
- ✓ Categorize between Social E-commerce and Local E-commerce
- ✓ Understand academic disciplines concerned with E-commerce
- ✓ Describe brief history of E-commerce
- ✓ Discuss about organizing themes

2.1   BUSINESS-TO-CONSUMER (B2C) E-COMMERCE

Online business selling to individual customer is called Business to Consumer E-commerce. The working of B2C model is as seen in the figure 2.1. B2C Model makes the customer to visit the virtual mall and complete the registration. The customer then selects product to buy which is passed on to the merchant to pass the order. Once, the payment is processed using Credit/debit card the product maintained in the inventory will be shipped for delivery and customer will receive the service. The merchant also maintains after sales service to retain customer or to ensure customer loyalty.
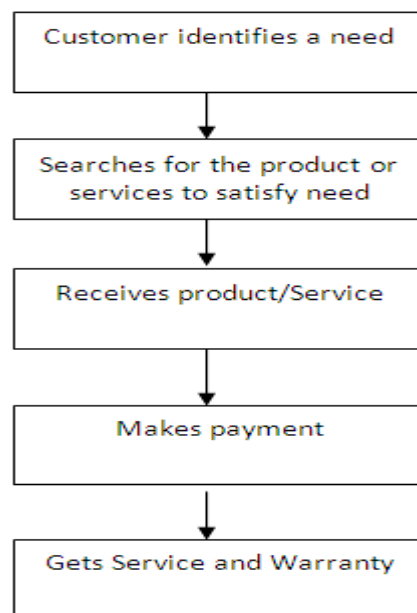
E.g. Flipkart

Fig.2.1 The working of B2C model

B2C e-commerce includes purchases of retail goods, travel and other types of services, and online content. B2C has grown exponentially since 1995 and is the type of e-commerce that most consumers are likely to encounter. It refers to a business platform, involving a business entity and consumers. It is a retail version of e-commerce known as e-tailing. Selling goods or services through web based shops. It is the most popular model of e-commerce as it has helped moving commercial transactions from public domain to private domain. B2C is about creating a better offline shopping experience – online.

2.2 BUSINESS-TO-BUSINESS (B2B) E-COMMERCE

Online business selling to another business is called Business to Business E-commerce. It can be represented as in Figure 2.2.
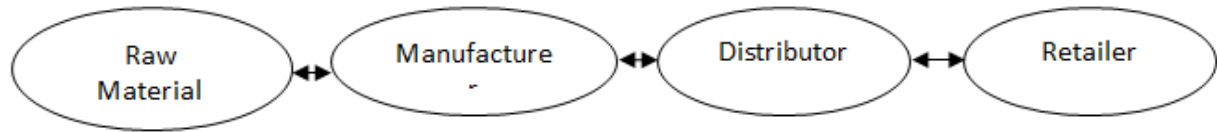

Fig. 2.2. Business-to-business (b2b) e-commerce

The common elements of B2B exchanges are:

➢ **Common marketplace** is an open place that makes business people comfortable to search a product.

➢ **Standardized documentation** is maintained since business people are trained.

➢ **Price quotes, Historical price and after sale information** is maintained.

➢ **Confidential transactions between businesses** have to be maintained as money involved between 2 businesses is very high and the trust needs to be maintained between them.

In B2B model, the business people will review the standardized document called as catalog in marketplace and identifies the specification for the product. Once the requirements are recognized, the request is posted for proposal by selecting the vendor based on his reputation. After receiving the filled purchase order the vendor prepares invoice for the purchase order followed by payment. Once the payment is successful, the shipment is arranged and the product is organized for inspection and reception. Salesforce, LinkedIn are some of the examples.

In B2B version of online transaction(s) the manufacturing organization takes a lead in setting up a business platform. This platform acts a business communication channel between the manufacturing/software developer entity and its vendors/suppliers, i.e., whatever was being done earlier in offline manner are now being done online. Thus a B2B platform acts as a business facilitator, negotiator and dealmaker, which facilitates, negotiates and clinches deal between independent or dependent business units.

The two primary business models used within the B2B arena: Net marketplaces, which include e-distributors, e-procurement companies, exchanges and industry consortia, and private industrial networks.

2.3   CONSUMER-TO-CONSUMER (C2C) E-COMMERCE

Individual Consumer selling product to another individual consumer is called Consumer to Consumer Ecommerce. In C2C model, the consumer goods ready to sell is placed for auction and market maker helps in preparing a product catalog, providing search engine and maintaining timely transfer of funds to the seller along with secured transactions for buyer. For example,

1. **Inforocket.com/ askme.com/ quora.com** – paid C2C model where experts are selected who can answer**.**
2. **Olx/ Quikr** – free C2C model used to sell any goods and services**.**
3. **Ola/ Uber** – on demand services.

In C2C e-commerce, the consumer prepares the product for market, places the product for auction or sale, and relies on the market maker to provide catalog, search engine, and transaction-clearing capabilities so that products can be easily displayed, discovered, and paid for.

Interestingly, with the passage of time these online models have also matured. A B2C model is no longer a 'business-to-consumer' model, it is integrating functionalities of other models like C2C or C2B also. It is far easier for a website that is successful at selling one product to branch into others. For example, Amazon has moved from selling books only to selling sea foods and other products as well. It is now hosting auctions, and courting eBay traders. Similarly, eBay is no longer a C2C platform but is also selling goods at fixed price, like e-tailer, B2C. Online market place is more dynamic and ready for all kinds of innovation. Yahoo! has made so many recent changes to its business that it is being called "the new google", while Google is using it's advertising formula to steer specialist buyers straight to specialist online sellers.

2.4 CONSUMER-TO-BUISNESS (C2B) E-COMMERCE

Consumer-to-business (C2B) is a business model where an end user or consumer makes a product or service that an organization uses to complete a business process or gain competitive advantage. The C2B methodology completely transposes the traditional business-to-consumer (B2C) model, where a business produces services and products for consumer consumption. The C2B approach evolved from the growth of popular consumer-generated media and content across different consumer segments, such as websites, blogs, podcasts, videos and social networks.

It is an innovative retail-marketing platform, where a business entity offers a variety of packages or options to entice the online customer. Here the business entity/ service provider bids for consumer. It is often referred to as 'reverse auction'. Such models are widely prevalent in tourism and travel industry. The tour operators, hotels and airlines not only give deep discounts to the consumers but also give them option to negotiate the prices. It is a pro-active version of e-commerce as it offers deals, packages or bundle of products at competitive prices.

In the C2B model, a consumer provides a business with a fee-based opportunity to market a product or service on the consumer's website or blog. In this type of relationship, a website owner is paid to review the product or service through blog posts, videos or podcasts. In most cases, paid advertisement space is also available on the consumer website.

2.5 MOBILE E-COMMERCE (M-COMMERCE)

Nowadays, most of consumer's time is spent over mobile devices for booking services, making online payments and searching online contents. Hence, mobile devices play a vital role in E-commerce. The process of using mobile devices involving cellular and wireless networks for online transactions over the internet is called as Mobile E-commerce. Currently, M-commerce adds on a major trend in upgrading E-commerce.

The steady shift of consumer behavior to online shopping from retail stores hasn't been lost on wireless electronic device manufacturers. Mobile electronic commerce is yet another way to purchase online items from electronic storefronts or online services from automated service providers. Computer-mediated networks enable these transaction processes through electronic

store searches and electronic point-of-sale capabilities. Other mobile devices include dash-top mobile devices, personal digital assistants or smartphones.

Device vendors target younger generations who use mobile phones more than any other age group, prompting online vendors to collaborate with big names in the telecommunications industry to promote the advancement of e-commerce to m-commerce such that users can shop online from their phones. Most of these advances are accomplished through sophisticated application designs that are constantly emerging and evolving.

One of the features of m-commerce sites is the adaptation of websites to make them easier to use with smaller screen sizes. There are a number of adaptations that can be made including the removal of large graphics and the optimization of fonts for easier viewing and ergonomics.

2.6 SOCIAL E-COMMERCE

E-commerce generated by social networks and online connections is called as Social E-commerce. Demand in creating Facebook, Instagram, Pinterest and YouTube accounts, liking and disliking of the social contents, development of collective online tool for shopping, building online connections through friend recommendations, creating virtual shops over social network, buy button and shopping tabs upholds E-commerce.

The social E-commerce is also collaborated with mobile devices by creating an app for Facebook, YouTube and Instagram to keep the consumers engaged through messages. This variation of Social E-commerce is called as **Conversational commerce**.

Social e-commerce is often intertwined with m-commerce, particularly as more and more social network users access those networks via mobile devices. A variation of social e-commerce known as conversational commerce leverages the mobile connection even further. Conversational commerce involves the use of mobile messaging apps such as Facebook Messenger, WhatsApp, Snapchat, Slack, and others as a vehicle for companies to engage with consumers.

Understanding Social Commerce: Social commerce professionals create and post messages and interactive features that promote online sales and other e-commerce initiatives. Some of the marketing tactics social commerce employs include:

- ➢ Inviting users to vote on product style or choices
- ➢ Offering personalized buyer options
- ➢ Applying large and striking graphics to attract viewer clicks
- ➢ Using videos to show the product in use and from multiple angles
- ➢ Encouraging user-submitted photos, commentary, and feedback
- ➢ Using celebrity endorsements of the product line
- ➢ Linking directly to the checkout or shopping cart
- ➢ Offering promotions or giveaways to users who share the product on their feeds

Social commerce encourages social shopping tools such as forums and communities where buyers and sellers discuss their online shopping experiences and compare notes.

Special Considerations:

Social commerce is a growing and changing field of online marketing that works in conjunction with social media and online shopping growth. Fashion and shopping-related blogs use social commerce and media to entice shoppers to purchase linked items online.

For example, many popular fashion blogs have Instagram accounts that allow followers to like, share, and comment on the offered product. The tagged article frequently links directly to the store's shopping cart or check-out desk.

2.7 LOCAL E-COMMERCE

Engaging the consumer to E-commerce based on his/her geographic location is called Local E-commerce. The local shops or merchants use various marketing strategies to attract their regular customers for their shops creating a better business. For example,

- ➢ **Reliance mart** – Providing discount coupons for the next purchase.
- ➢ **Med Plus** – providing points on each purchase that could be summed up for the discount.

2.7.1 A Brief History

E-commerce is said to be,

- • Started in 1970 when pharmaceutical firm known as Baxter Healthcare created a B2B model using telephone based modem for hospitals to reorder supplies from Baxter.

21

- In 1980 PC based remote order entry system was introduced based on Electronic Data Interchange (EDI) standards that helped the firm to exchange commercial documents and perform digital transactions.
- In 1981 the first large scale B2C model based digital transaction system called as '**Minitel'** was introduced. It is a French videotext system with 8inch screen.
- In 1994, AT&T, Volvo, sprint started Banner based advertisements and in 1995 First sales of banner ad space was done by Netscape & Infoseek.
- Around 2006, the E-commerce services such as ticket booking travel services, retail products and online banking was added on.

Overall, E-commerce is divided into 3 periods,
1. **1995-2000 :** Period of Invention
2. **2001-2006 :** Period of Consolidation
3. **2007 :** Period of Reinvention

1. **Period of Invention**: This period of E-commerce involved selling of simple Retail products over internet since there was no bandwidth for complex products. The marketing was carried using simple static ads and static web pages were used to represent brand for large companies. The search engines were not powerful. Around 2000 stock market found a great fall as most of the companies disappeared due to .com crash.

E-commerce created a milestone in the commercial history where Internet was connected to Personal computers creating Local area network. Universal communications was made possible by creating freely accessible HTML pages with cheap computers.

E-commerce also played a major role economically at early times. As the products of different brands are made available to customers over internet by creating a market space,

- There is an equal distribution of price, cost and quality reducing information asymmetry.
- Decreases search and marketing cost.
- Intermediate costs spent over distributors and retailers are removed.
- The collection of customer details on every search made over market space helps merchants to conduct customer targeted marketing with less effort.

- Price changing cost of a product is low.

- Fiction free Ecommerce is managed by adjusting the price of the product on demand.

- The new firm can easily build brand name recognition by expanding the customer base.

- New technologies applied creates an informative and community like features. The customer once dependent on particular company web interface would less likely switch to other competitors.

2. **Period of Consolidation**: This period of E-commerce is technology as well as business driven. Strengthening the brands became more important than creating new brands in this era. Financing companies moved on to capital markets. Along with retail services, travel and financial services were added on. The business upgraded with presence of broadband network and cheap Personal computers. Better search engines were implied for marketing over internet. Ads were based on user queries, rich media and video. Behavioral target on customer was carried on through websites and email. Multiple websites were created for each product.

3. **Period of Reinvention**: This period of E-commerce shows the growth of blogs, video, photo sharing apps and wikis for content. The use of mobile devices became common which helped to incorporate local goods and services in E-commerce. On demand services were supported by mobile apps and cloud computing by selling unused assets such as cars, spare rooms and personal time. Hence, this period of E-commerce was considered to be business oriented, technological as well as sociological. Entertainment content is considered as a major source in this period. Marketing was pursued through social networks, word of mouth, virtual marketing and use of analytical tools for personal marketing. Firms having static web pages were moved on to apps and social network for expanding their brand.

2.8 UNDERSTANDING E-COMMERCE

Understanding E-commerce at one attempt has become burdensome. Hence, it is acknowledged into 3 perspectives – Technological, Business and Society.

2.8.1 Organizing Themes

i. *Technology:* Understanding E-commerce based on the infrastructure incorporated. Due to the development of digital computing and communication technology, understanding E-commerce requires the basic knowledge of information technology and fundamentals of computer science. It needs the wide knowledge gathering not only on web and internet but also cloud computing, desktop computers, mobile devices, local area network, different databases, client server computing, data mining technologies. These technologies are applied over the different business cycle such as supply chain management, resource planning and customer relationship management. One must also be aware of concepts such as packet switching communication, TCP/IP protocol, HTML5, CSS and software programming like Flash and javascript for client side and PHP, java for server side of client/ server computing to understand E-commerce better over technological perspective.

ii. *Business:* Understanding E-commerce based on Return on Investment for a company. Once the technology is applied over business, it becomes commercial creating interest and excitement on E-commerce and presenting business with new ways of production and transaction. Strategies and plans for new firms need to be changed. One need to have the knowledge of digital markets, digital goods, business models, firm and industry, value chains, value webs, industry structures, consumer behavior and financial analysis to understand E-commerce in business perspectives.

iii. *Society:* Impact of globalized E-commerce is putting pressure on a society to enforce laws of nations. It affects individual privacy of the customer by gathering his information for behavioral marketing. The intellectual property right is influenced by sharing digital copy of copyrighted contents such as music, books and videos. The issue of equity, equal access and content regulations will take hold of welfare policy.

2.8.2 Academic Disciplines Concerned with E-commerce

There are 2 perspectives of E-commerce: Technical and Behavioral

1. **Technical**:

- The *computer scientist* sees E-commerce as one of the salient application of Internet. They are involved in development of computer hardware, software and improvement of standards, encryption, databases and operations.
- The *operational management scientist* builds mathematical models to apply for the business and improvise them.
- The *information technology team* is concerned about data mining, business analytics, search engine and artificial intelligence.

2. **Behavioral**:

- The *information scientists* are interested in E-commerce because of its involvement in industry value chains, structure and corporate strategy.
- *Economists* are concerned about online consumer behavior, digital goods pricing and identical features of digital electronic market. They also corporate with market scholars to collect consumer response to market and ad campaigns, understand the firms potential to brand, segment markets, target consumers and position products to achieve good Return on Investment. (ROI)
- *Marketing scholars* are focused in marketing ways, development of brand and extension of the firm, understand online consumer behavior, analyze the capability of E-commerce technologies to divide and target consumer groups.
- *Management scholars* are concerned on entrepreneurial behavior and challenges taken by newly started firms developing organizational structures in less time.
- *Finance and accounting scholars* are interested on valuation and accounting practices of E-commerce.
- *Psychologists* are focused on study of Internet usage, web usage as a social network and communication tool.
- *Legal scholars* are focused on preserving intellectual property, privacy and content regulations.

2.9 CHECK YOUR PROGRESS

1. eBay, Amazon.com belongs to which of the below segments
   a. B2B
   b. B2C
   c. C2B
   d. C2C

2. The primary source of financing during early years of E-commerce was _____
   a. Bank loans
   b. Venture capital fund
   c. Large retail firms
   d. Initial public offering

3. Which of the following is not a technology to gather consumer information?
   a. Spy ware
   b. Cookies
   c. Gmail
   d. Anonymizers

4. _____ is a set of planned activities for getting profit in a market place.
   a. Business model
   b. Profit model
   c. Business plan
   d. Revenue plan

5. The best product to sell in B2C E-commerce are _____.
   a. Small products
   b. Digital products
   c. Fresh products
   d. Perishable products

Answers to check your progress:

1. b) B2C, they involve in the process of selling goods and services directly to the consumers.
2. b) Venture capital fund, small money invested over a firm.
3. d) Anonymizers, it is a proxy server that acts as a shield between client computer and the internet.

4. a) Business Model

5. b) Digital products, they can be sold and distributed repeatedly without replenishing inventory.

2.10   SUMMARY

In this unit we discussed the different business models such as B2C E-commerce, B2B E-commerce, C2C E-commerce, Mobile E-commerce, Social E-commerce and Local E-commerce. We discussed process involved in different types of E-commerce by mentioning some examples. In general terms, e-commerce is a business methodology that addresses the needs of organizations, traders and consumers to reduce costs while improving the quality of goods and services and increasing the speed of service delivery. The evolution of E-commerce in 3 periods is talked over. We also discussed on different perspectives of understanding the E-commerce based on organizing themes and academic disciplines.

2.11   KEYWORDS

1. **Business-to-Consumer E-commerce (B2C)**: Online business selling to individual customer is called Business to Consumer E-commerce.

2. **Business-to-Business E-commerce (B2B)**: Online business selling to another business is called Business to Business E-commerce.

3. **Consumer-to-Consumer E-commerce (C2C)**: Individual Consumer selling product to another individual consumer is called Consumer to Consumer Ecommerce.

4. **Mobile E-commerce:** The process of using mobile devices involving cellular and wireless networks for online transactions over the internet is called as Mobile E-commerce.

5. **Social E-commerce:** E-commerce generated by social networks and online connections is called as Social E-commerce.

6. **Local E-commerce:** Engaging the consumer to E-commerce based on his/her geographic location is called Local E-commerce.

7. **Conversational commerce**: The process of engaging the consumers through messages over mobile devices by creating an app for Facebook, YouTube and Instagram.

2.12 QUESTIONS FOR SELF-STUDY

1. Explain major types of E-commerce.
2. Describe the basic themes required for understanding E-commerce.
3. Discuss on major academic disciplines contributing to E-commerce.
4. Explain 3 periods of E-commerce evolution.
5. What is conversational E-commerce? Explain.

2.13 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.
2. AdNabu,(2021), https://www.adnabu.com/ecommerce-marketing-trends.
3. Wei J, editor. Mobile electronic commerce: Foundations, development, and applications. CRC press; 2014 Nov 20.

UNIT -3: E-COMMERCE INFRASTRUCTURE

STRUCTURE

3.0 OBJECTIVES

After studying this unit, you will be able to:

- ✓ Understand key concepts and background of Internet Technology
- ✓ Define the terms IP address, Domain names, DNS and URLs
- ✓ Describe what is the use of domain names
- ✓ Explain client server computing model and cloud computing model.
- ✓ Describe Mobile Platform in detail.

3.1 THE INTERNET

The internet is derived from the word internetwork. It is an interconnected network of computers called as hosts providing services for individuals, linking business, educational institutions and government agencies. It is not controlled or owned by any organizations. The services provided are such as email, messaging, shopping, research, music, video etc.

It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope that are linked by a broad array of electronic and optical networking technologies. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

One of the popular services provided by Internet is web. Web is a collection of pages containing graphics, contents, video, audio and other attractive objects created from a programming language called as HTML. Web browser is used to host the web pages and navigation from one page to another happens on the click of hyperlinks.

Most traditional communications media, such as telephone and television services, are reshaped or redefined using the technologies of the Internet, giving rise to services such as Voice over Internet Protocol (VoIP) and Internet Protocol television (IPTV). Newspaper publishing has been reshaped into Web sites, blogging, and web feeds. The Internet has enabled or accelerated the creation of new forms of human interactions through instant messaging, Internet forums, and social networking sites.

The origins of the Internet reach back to the 1960s when the United States funded research projects of its military agencies to build robust, fault-tolerant and distributed computer networks. This research and a period of civilian funding of a new U.S. backbone by the National Science Foundation spawned worldwide participation in the development of new networking technologies and led to the commercialization of an international network in the mid 1990s, and resulted in the following popularization of countless applications in virtually every aspect of modern human life. As of 2009, an estimated quarter of Earth's population uses the services of the Internet.

3.2 TECHNOLOGY BACKGROUND

It was stated that the Internet was started 55 years ago and it is divided into 3 phases.

1. **Innovation Phase (1961-1974):** This phase started with the fundamentals of Internet. The concepts like packet switching, global computer network, common communication protocol called as TCP/IP and common addressing scheme for all computers connected to the network were introduced. Client/server computing was implemented on hardware and software to share files, run applications and send messages. In this phase, internet was basically implemented to connect large mainframe computers on different college campus.

2. **Institutionalization Phase (1975-1995):** In this phase, Internet was made of use by US Department of Defense (DOD) and National Science Foundation (NSF). They provided funds and authorization for the development of Internet. Later the wide area packet switched network with distributed control called as Advanced Research Project Agency network (ARPANET), the hyperlink concept of navigating from one page to another, the concept of making internet available to all called as 'civilian internet', the idea of giving names to network address called as Domain name system (DNS) for easy understanding of the clients was commercially introduced. 'Netscape' a first commercial web browser was initiated during this time.

3. **Commercialization Phase (1995 onwards):** The private corporations took over the expansion of internet over military and colleges resulting in establishment of fully commercial civilian network. This period was the beginning of E-commerce providing services for retail stores and auctions. The discussions were made over future needs of security and functionality over internet technology.

3.3 INTERNET- KEY TECHNOLOGY CONCEPTS

In 1995, Federal Networking Council (FNC) termed Internet as network that supports Transmission Control Protocol (TCP), uses IP Addressing Scheme where information system is logically linked together by a globally unique address space and provides voice and data services

to the public. The basic concepts required to understand Internet is packet switching, TCP/IP communication protocol and client/ server computing.

Packet Switching: It is a segmentation of digital message into several individual units called as packets. These packets are dispersed along several paths from the source and reassembled at the destination point.

Earlier, the communication was through the dedicated network between one end to another end of the terminal called as circuit switching network. Here, the point to point network has to be setup before the communication can proceed and large amount of communication time is wasted for pause between words and assembling the circuit segments. This drawback led to the introduction of packet switching network.

In packet switching network, the messages are divided into segments called as packets. Each packet is appended with other information such as source address, destination address, length of the message, total number of packets sent, error control bits and flow control bits. These packets are dispersed along different paths through special purpose computers called as routers that interconnects different computer networks to make up an internet. Each router guides the packets for taking up the next path based on the program written over it called as routing algorithm ensuring packet reaches the destination computer where all the packets are assembled to get the message. This process helps in using any spare capacity over a network unlike dedicated circuit switching network.
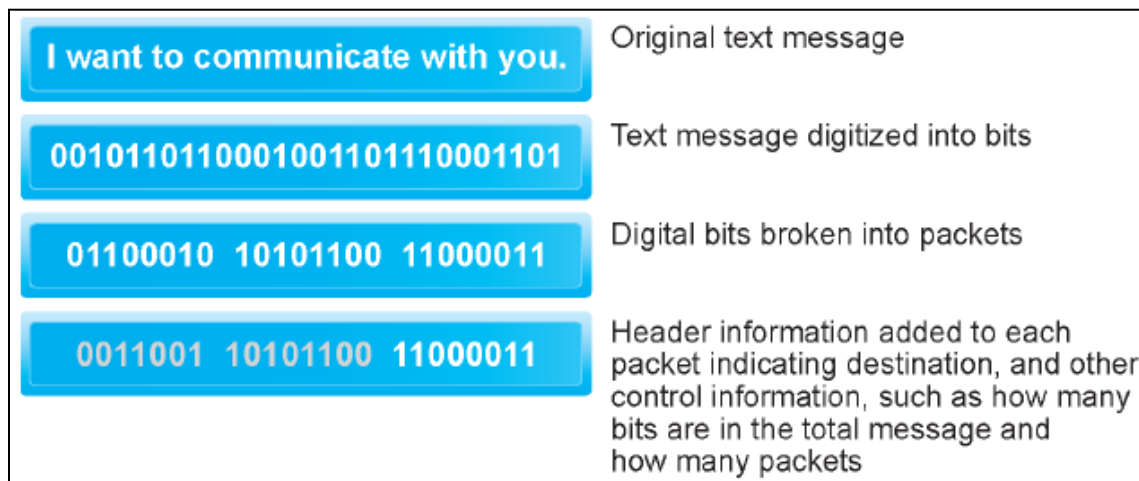

Fig.3.1: Segmented digital message

3.4 TCP/IP

The packet switching network had a great concept of using a spare capacity of the network, but there was no standard rule that agreed upon for the process of packet segmentation, routing the packets in a proper route and reassembling the packets received at the destination. Hence, a set of rules and standards were introduced termed as protocol to control ordering, compression, routing and reassembling of the packets.

One of the chief Protocols for Internet is Transmission Control Protocol/ Internet Protocol (TCP/ IP). TCP establishes connection between the computers and manages the packets to get received at the destination in a correct order without any packet loss. IP manages the addressing scheme for the packets to be routed over different paths to reach a destination.

TCP/IP architecture is composed of 4 different layers as shown below,

1. **Network Interface Layer:** This layer is responsible for sending and receiving the packets from the network medium.
2. **Internet Layer:** This layer is responsible for packaging, addressing and routing the packets in the Internet.
3. **Transport Layer:** This layer helps in creating a communication with other applications by sequencing and acknowledging the packets to and from the applications.
4. **Application Layer:** The set of protocols in this layer helps in providing services to the user and exchange of data. Some of those protocols are Border Gateway Protocol (BGP), Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP).
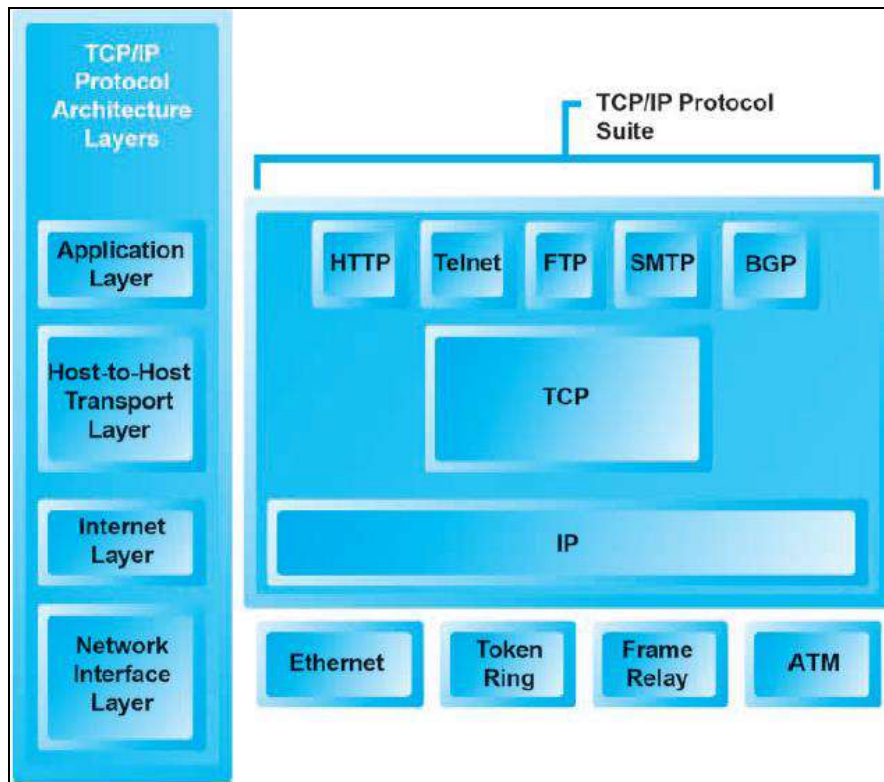
Fig. 3.2 TCP/IP Model

3.5 IP ADDRESSES

IP Address is used to communicate between the computers and helps in identification of individual computer over an Internet. When an user joins the internet using dail-up or cable modem, the computer is assigned with a temporary IP address by Internet Service Provider (ISP) whereas some of the universities are provided connected over Local Area Network (LAN) are assigned with a permanent IP address.

An Internet Protocol address (also known as an IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

The designers of the Internet Protocol defined an IP address as a 32-bit number consisting of 4 octets and this system, known as Internet Protocol Version 4 (IPv4), is still in use today.

34

However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995. IPv6 was standardized as RFC 2460 in 1998 and its deployment has been ongoing since the mid-2000s.

IP addresses are binary numbers, but they are usually stored in text files and displayed in human-readable notations, such as 172.16.254.1 (for IPv4), and 2001:db8:0:1234:0:567:8:1 (for IPv6).

Eg. 74.125.73.106 (IP address) will get you Google!

The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries (Internet service providers) and other entities. (http://en.wikipedia.org/wiki/IP_address)

The Internet Protocol (IP) is part of the TCP/IP suite and is the most widely used internetworking protocol. As with any protocol standard, IP is specified in two parts:

- The interface with a higher layer (e.g., TCP), specifying the services that IP provides

- The actual protocol format and mechanisms.

There are 2 types of IP Address- **IPv4** and **IPv6**

- **IPv4:** It is a 32 bit address that appears as a sequence of 4 numbers separated by periods such as **a.b.c.d**. Each number (**a/b/c/d**) ranges from 0-255. There can be 2^{32} addresses generated from IPv4. IP address is comprised of 2 components called *Host address* that identifies an individual host on specific network segment and *Network address* that identifies the TCP/IP network containing the host.

- **IPv6:** It is a 128 bit address that appears as a sequence of 4 numbers separated by periods such as **a.b.c.d**. Each number (**a/b/c/d**) ranges from 0-255. There can be 2^{128} addresses generated from IPv6.

3.6 DOMAIN NAMES

It is very difficult to remember 32 bit or 128 bit IP address for identification of a computer and to establish communication. Hence there was a need for easily remembered names for these addresses which led to the initiation of Domain names.

Domain name is an internet resource name globally made known to Web servers and online organizations providing all destination information. It is comprised of 2 components separated by a period such as *example.com.* It is used to identify single IP address or group of IP addresses.

Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name.

3.7 DNS and URLs

DNS: Domain Name System is termed as DNS. It is an internet system for mapping the numeric address with an alphanumeric name. When user needs to load a webpage, the alphanumeric name given over the browser need to be converted to corresponding IP address to locate the website. Namespace can be of two types -

- **Flat namespace:** In a flat name space, a name is assigned to an address. A name in this space is a sequence of characters without structure.

- **Hierarchical namespace:** In a hierarchical name space, each name is made of several parts. The first part can define the nature of the organization, the second part can define the name of an organization, and the third part can define departments in the organization, and so on. In this case, the authority to assign and control the name spaces can be decentralized.

DNS is hierarchical in structure with root server at the top as shown in Figure 3.3. The next level contains top domain domains to identify organization type or geographical location such as *.com, .org, .gov, .uk, .ca.* For every top level domains can have second level domains and third level domains as well to identify the organization or an individual.

In the namespace design, the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127. For the Internet, the top of the naming hierarchy is managed by an organization called ICANN (Internet Corporation for Assigned Names and Numbers).
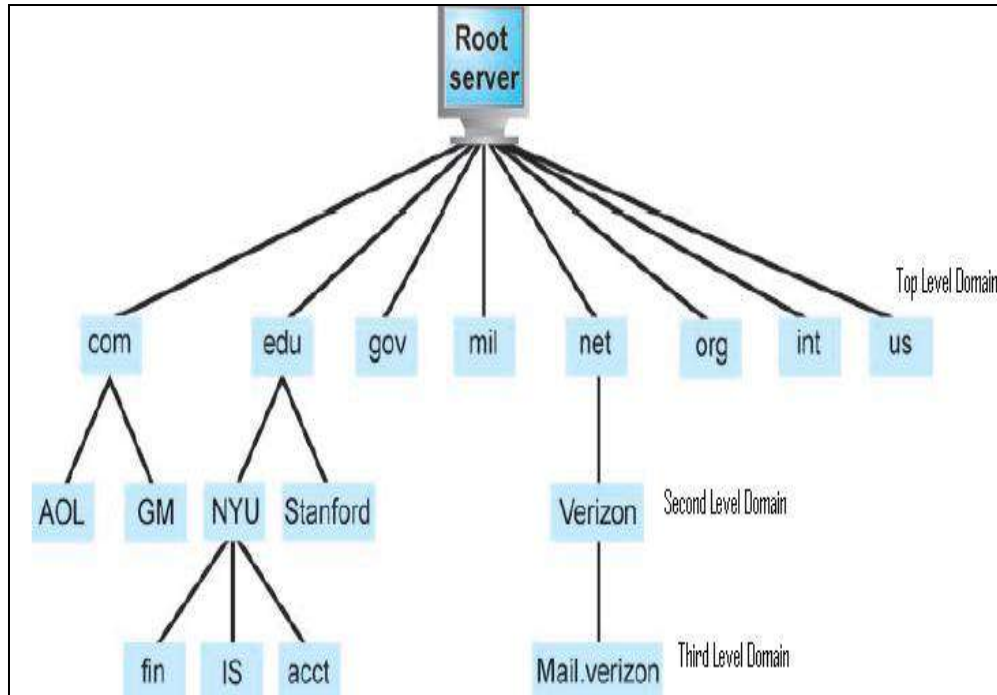
Fig. 3.3 Hierarchal structure of Domain Name System

Some simple terms used in DNS namespace-

- **Label:** Each node in the tree has a label, which is a string with a maximum of 63 characters. The root label is a null string (empty string).

- **Domain Name:** Each node in the tree has a domain name. A full domain name is a sequence of label separated by dots (.). The domain names are always read from the node up to the root. The last label is the label of the root (null).

- **Fully Qualified Domain Name:** If a label is terminated by a null string, it is called a fully qualified domain name (FQDN). An FQDN is a domain name that contains the full name of a host. It contains all labels, from the most specific to the most general, that uniquely define the name of the host. For example, the domain name *challenger.ate.tbda.edu*.

- **Partially Qualified Domain Name:** If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN). A PQDN starts from a node, but it does not reach the root. It is used when the name to be resolved belongs to the same site as the client. Here the resolver can supply the missing part, called the suffix, to create an

FQDN. For example, if a user at the *jhda.edu.* site wants to get the IP address of the *challenger* computer; he or she can define the partial name ***challenger.***

URLs: Uniform Resource Locator is termed as URL. It is an address provided to the web browser to identify the location of the content in web. The domain name is also a part of the URL. Each page is assigned a **URL** (**Uniform Resource Locator**) that effectively serves as the page's worldwide name. URLs have three parts: the protocol (also known as the **scheme**), the DNS name of the machine on which the page is located, and the path uniquely indicating the specific page (a file to read or program to run on the machine). As an example, the URL of the page shown is http://www.abc.in/index.html.

For example, if the URL is given as www.example.com, www refers to hostname, example.com refers to domain name. Here DNS will map the www.example.com to an IP address 192.0.2.1. The process of mapping takes place as shown below,

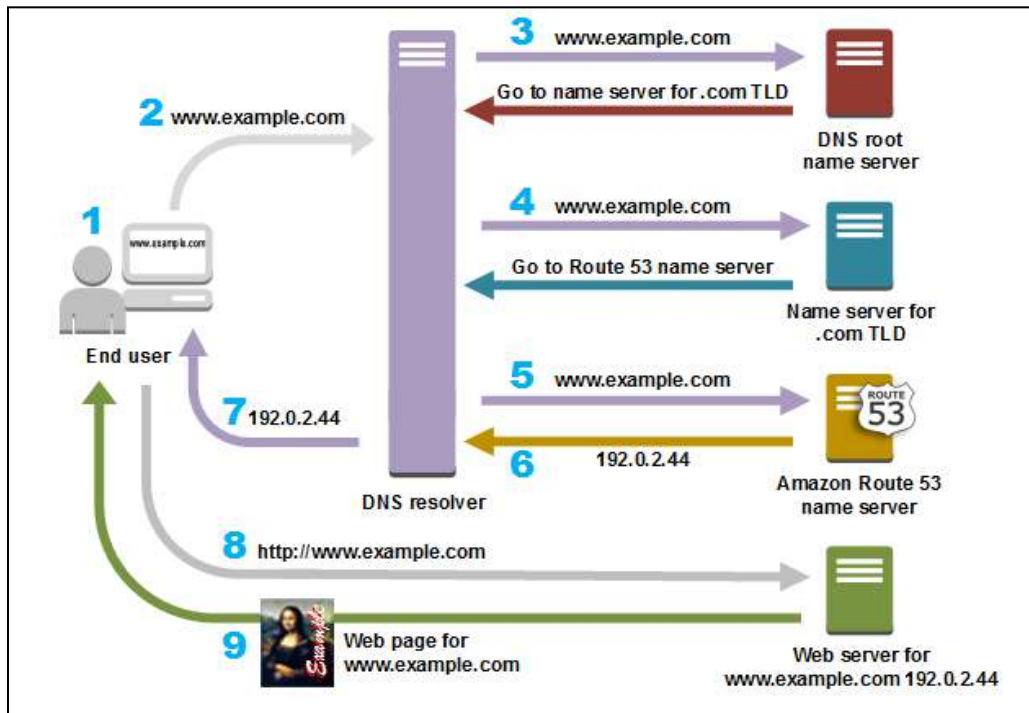
Fig. 3.4 Mapping of DNS to IP

When the user types www.example.com on the web browser and clicks on enter button, DNS resolver managed by Internet Service Provider (ISP) will take up the URL and pass it on to the root server. The request is again passed on to the Top Level Domain (TLD) server for .com

38

domains. The name servers associated with the example.com is a response for this request. Now the request is passed on to the corresponding name server where the associated IP address for the URL is obtained and responded back to the DNS resolver which is taken up by the web browser and opens up the content of www.example.com.

3.8 CLIENT SERVER COMPUTING

During 1960's the computing was centralized and the task was entirely done at the single main frame computer connected to the users by terminals. Due to the insufficient computing power for graphics and other functionalities and development of personal computers and LAN around 1970 and 1980 client server model was initiated.

Client server computing is a model of computing where client computer is connected to the network of one or more computers called as servers dedicated to perform different functions. Client computer is a powerful desktop computer which is a part of the network. Server computer is a networked computer dedicated to perform different functions that the client needs such as file storage, software application and printing.
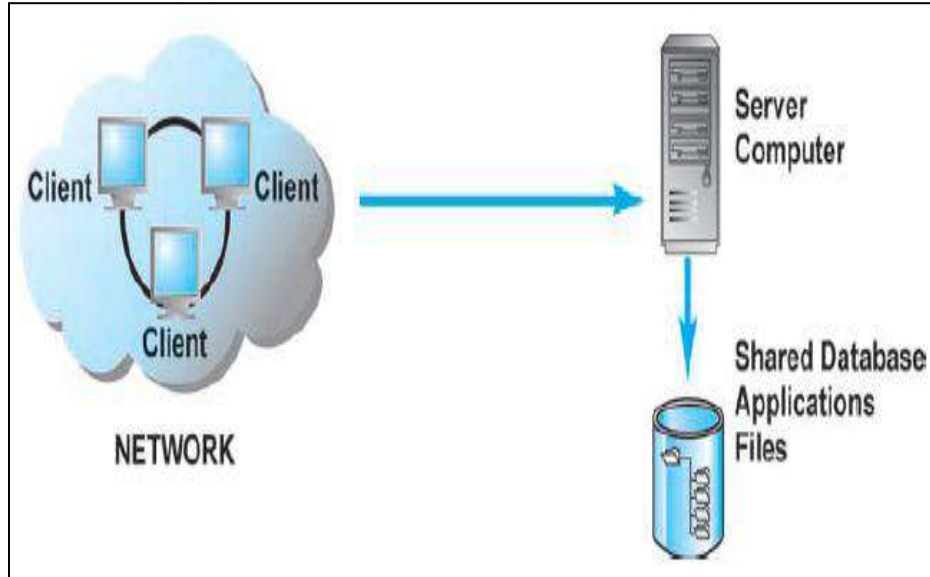

Fig. 3.5 Client Server model

Here the expansion is easy by adding any number of server and client computers. If the server goes down backup servers can take up the task and if client is inoperable then other part of the

network keeps working unaffected. The load is balanced across the servers and hence the hardware and software at the client side can be kept simple.

Client-server architecture: architecture of a computer network in which many clients (remote processors) request and receive service from a centralized server (host computer). Client computers provide an interface to allow a computer user to request services of the server and to display the results the server returns. Servers wait for requests to arrive from clients and then respond to them. Ideally, a server provides a standardized transparent interface to clients so that clients need not be aware of the specifics of the system (i.e., the hardware and software) that is providing the service. Clients are often situated at workstations or on personal computers, while servers are located elsewhere on the network, usually on more powerful machines. This computing model is especially effective when clients and the server each have distinct tasks that they routinely perform. In hospital data processing, for example, a client computer can be running an application program for entering patient information while the server computer is running another program that manages the database in which the information is permanently stored. Many clients can access the server's information simultaneously, and, at the same time, a client computer can perform other tasks, such as sending e-mail. Because both client and server computers are considered independent devices, the client-server model is completely different from the old mainframe model, in which a centralized mainframe computer performed all the tasks for its associated "dumb" terminals, which merely communicated with the central mainframe.

3.9 CLOUD COMPUTING MODEL

Cloud computing is a process of providing computer processing, software, storage and other services as a shared pool of virtualized resources over an Internet. The resource and services can be accessed whenever needed from any connected device and location. The characteristics of cloud computing are,

- **On-demand self-service**: The server time and resource required by the consumer for computations can be accessed by their own whenever required.

- **Universal network access**: The cloud resource can be accessed by any standard network, internet devices or mobile network.

- **Location-independent resource pooling**: The resources required for the computation need to be served to multiple users. The virtual copy of the same resource is shared to the users based on their demand without disclosing the actual location of the resource.

- **Rapid Elasticity**: The resource required for computation can be increased, decreased or managed based on the demand created by the user.

- **Measured service**: The charges made for the service provided to the user is based on the amount of resources already been used.

Types of Cloud computing based on what service is provided to the customer:

1. **Infrastructure as a Service (IaaS)**: Here the customer uses network, storage and processing power to run their information systems from the third party service providers called as cloud service providers. The customers are charged for the storage and computation power used from the third party servers.

   For example, Amazon uses Amazon web Services (AWS) that offers Simple Storage Service (S3) for storing customer data and Elastic cloud computing (EC2) for computation.

2. **Software as a Service (SaaS)**: Here vendors host the software as a service over cloud infrastructure and make accessible to the customer through network. The customer is charged for the service as annual subscription.

   For example, Google apps provides a collection of business application and Salesforce.com maintains customer relationship management (CRM) along with related software services over the internet.

3. **Platform as a Service (PaaS)**: Here the customer uses infrastructure and programming platform provided over cloud as a service to run the applications.

   For example, IBM provides Bluemix for application development and testing over the cloud environment.

Types of Cloud computing based on who owns the service provided to the customer:

- **Public Cloud:** The third party service providers owns and manages the service such as storage, processing and network provided to the customer. The customer pays for the amount of resources and computing power used. The enterprise that do not own their own

software or hardware resources and requires less security over the computing data uses this type of cloud.

Example: Google Drive, Dropbox and Apple iCloud.

- **Private cloud:** The cloud infrastructure is maintained merely for single organization for providing services such as storage, network and processing. These services are hosted internally by in house IT or externally by private third party service providers. The enterprise here requires strict data security and control over the data used.

  Example: Financial and Healthcare companies.

- **Hybrid cloud:** The private cloud infrastructure is used only for the core business activities whereas the less critical computing or extra processing capacity requires the public infrastructure is called Hybrid cloud. These clouds are owned by in house IT, private host or third party service providers.

3.10 MOBILE PLATFORM

The mobile devices such as Smartphone, laptop, tablet and iPad have become the primary source for accessing the internet nowadays for shopping, bill payment and other services which shows that the mobile devices act as a basic platform for E-commerce. This is because the mobile devices are lighter, can be carried anywhere and accessible any time using applications that doesn't require complex operating system. Smartphone have found the drastic improvements in technology with varying operating systems such as Microsoft, Apple iPhone iOS and java/Linux. The high power consuming hardware in personal computers is replaced by less power draining flash memory chips with storage up to 128 GB in Smartphone.

3.11 CHECK YOUR PROGRESS

1. What does Arpanet stand for?
   a. Advanced Research Project Agency Network
   b. Advanced Research Programmed Auto Network
   c. Advanced Research Project Automatic Network
   d. Advanced Research Project Authorized Network

2. The special purpose computers through which the packets are dispersed along different path is called

      a. Switches

      b. Hub

      c. Routers

      d. Firewall

3. IPv6 is comprised of _____ bit address

      a. 256

      b. 32

      c. 64

      d. 128

4. Which of the following device converts hostname into IP address?

      a. DNS Server

      b. Hub

      c. DHCP Server

      d. Firewall

5. What is a DNS Client called as?

      a. DNS handler

      b. DNS resolver

      c. DNS updater

      d. None of the above

6. The entire hostname has a maximum of _____ characters

      a. 255

      b. 127

      c. 63

      d. 31

7. Which of the following is a type of cloud computing service?

      a. Service-as-a-Software (SaaS)

      b. Software-and-a-Server (SaaS)

      c. Software-as-a-Service (SaaS)

      d. Software-as-a-Server (SaaS)

8. Which of the following is an example of the cloud?

a. Amazon Web Services (AWS)

b. Dropbox

c. Cisco WebEx

d. All of the Above

9. The _____ allows systems and services to be accessible by a group of organizations.

a. Public cloud

b. Private cloud

c. Community cloud

d. Hybrid cloud

10. URL is _____

a. Source address

b. Users address

c. Web Address

d. An attribute

Answers to check your progress:

1. a) Advanced Research Project Agency Network
2. c) Routers
3. d) 128
4. a) DNS Server
5. b) DNS resolver
6. a) 255
7. c) Software-as-a-service
8. d) All of the above
9. a) Public cloud
10. c) Web Address

3.12 SUMMARY

In this unit we discussed the definition of Internet and technology background of the internet. We also discussed the definitions and functionalities of several key concepts of Internet

such as Packet switching, TCP/IP, IP Address, Domain names, DNS and URL's. Later we described on the different computing models such as Client server model, Cloud computing model and its types. Finally, we described how E-commerce is impacted by the mobile platform.

3.13 KEYWORDS

1. **Internet:** It is an interconnected network of computers called as hosts providing services for individuals, linking business, educational institutions and government agencies.
2. **Packet switching:** It is a segmentation of digital message into several individual units called as packets.
3. **TCP/IP:** Transmission Control Protocol/ Internet Protocol (TCP/ IP) is an Internet Protocol that establishes connection between the computers and manages the packets to get received at the destination in a correct order without any packet loss.
4. **IP Address:** IP Address is used to communicate between the computers and helps in identification of individual computer over an Internet.
5. **Domain Names:** Domain name is an internet resource name globally made known to Web servers and online organizations providing all destination information.
6. **DNS:** Domain Name System is an internet system for mapping the numeric address with an alphanumeric name.
7. **URL:** Uniform Resource Locator is an address provided to the web browser to identify the location of the content in web.
8. **Client Server Computing:** Client server computing is a model of computing where client computer is connected to the network of one or more computers called as servers dedicated to perform different functions.
9. **Cloud Computing:** Cloud computing is a process of providing computer processing, software, storage and other services as a shared pool of virtualized resources over an Internet.

3.14 QUESTIONS FOR SELF STUDY

1. Explain key technology concepts behind the Internet.
2. Explain 3 different types of cloud computing model.

3. Why is packet switching essential to the Internet?

4. Define TCP/IP, Domain name, DNS, URL and IP Address with example.

5. Explain the impact of mobile platform on E-commerce.

6. Explain client server computing model.

3.15 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

2. Techopedia (December 15, 2016), https://www.techopedia.com/definition/1327/domain-name

3. Cisco, https://www.thousandeyes.com/learning/techtorials/dns-domain-name-system

4. AWS, https://aws.amazon.com/route53/what-is-dns/

UNIT -4: INTERNET AND WEB

STRUCTURE

4.0 OBJECTIVES

After studying this unit, you will be able to:

- ✓ Define the terms Hypertext, HTML and XML
- ✓ Explain Web servers and clients
- ✓ Describe the role of server
- ✓ Explain Web browsers.
- ✓ List and explain different communication tools.
- ✓ Discuss about different messaging apps available
- ✓ Define Internet Telephony

4.1 HYPERTEXT

The web address typed on the web browser software in Personal computer fetches the web pages required from the server where the resource is hosted through network using Hypertext Transfer Protocol (HTTP). Hypertext is way of formatting the pages associated with the links that connect one document to another and connecting the pages with other media like graphics, sound, video and animation files. When the hyperlink is clicked over the page, the graphics get opened or the video gets played.

The web address typed over the browser is composed of several parts such as HTTP, domain name, directory path and document name.

<div align="center">

http://domainname/directorypath/filename

</div>

- **HTTP**: Hypertext transfer protocol is used to fetch and display the page requested by the user from the hosted server

- **Domain name**: It specifies the name of the organization server where the resource is hosted. Most of the times the domain name will very near to the name of the organization.

- **Directory path**: The actual path where the resource is resided over the hosted server.

- **Document name**: The name of the document requested.

Example: http://www.megacorp.com/content/features/23263.html

- ➢ www.megacorp.com - Domain
- ➢ content/features – Directory path
- ➢ 23263.html – Document name

4.2 HTML

The most widely used web page formatting language is HTML (Hypertext Markup Language). It was introduced based on Generalized Markup Language (GML) developed in 1960's. The set of markup tags are provided to format the web pages. The web browser will interpret these tags into a page display. The HTML defines the style and structure of the web page including heading, text formatting, positioning, tables and graphics. From the day HTML was launched, the browsers are adding the features continuously to refine the layout of the page displayed. Hence,

when E-commerce website is designed it has to be taken care that it is supported by all the browsers even in the older versions. The recent version HTML5 introduces features such as drag and drop, video playback, mobile websites and responsive websites with adaptive web delivery. The HTML design can be done on the software tools such as notepad, dreamviewer.

The HTML originally invented by Tim Berners-Lee in 1989,was strongly based on Standard Generalized Mark-up Language (SGML),.It is an internationally agreed language used for describing how pages of text,graphics and other information are organized formatted and linked together.

HTML is the official language of the World Wide Web and was first developed in 1990. HTML is a product of SGML (Standard Generalized Markup Language). SGML is a complex, technical specification describing markup language. HTML was originally created to allow the users who were not specialized in SGML to publish and exchange scientific and other technical documents. HTML especially facilitated this exchange by incorporating the ability to link documents electronically using *hyper*links. Thus the name *Hyper*text Markup Language.

HTML is a language for describing web pages.

- HTML stands for **H**yper **T**ext **M**arkup **L**anguage
- HTML is a **markup** language
- A markup language is a set of markup **tags**
- The tags **describe** document content
- HTML documents contain HTML **tags** and plain **text**
- HTML documents are also called **web pages**

4.2.1 HTML Tags

HTML mark up tags are usually called HTML tags:

- HTML tags are keywords surrounded by **angle brackets**   like <html>
- HTML tags normally **come in pairs** like and
- An HTML element starts with a **start tag / opening tag**
- An HTML element ends with an **end tag / closing tag**
- Start and end tags are also called **opening tags** and **closing tags**
- The **element content** is everything between the start and the end tag

- Some HTML elements have **empty content**
- Empty elements are **closed in the start tag**
- Most HTML elements can have **attributes**
- The HTML Tags are case in sensitive.

Tags are used to represent various elements of web page like Header, Footer, Title, Images etc.

Tags are of two types: **Container Tags, Empty Tags.**

4.2.2 Writing HTML Using Notepad or TextEdit

HTML can be edited by using a professional HTML editor like:
- Adobe Dreamweaver
- Microsoft Expression Web
- CoffeeCup HTML Editor

However, for learning HTML we recommend a text editor like Notepad (PC) or TextEdit (Mac).

Follow the 4 steps below to create your first web page with Notepad.

Step 1: Start Notepad

Step 2: Edit HTML file with Notepad

Step 3: Save HTML like -> Select Save as. filename: filename.html. in Notepad's file menu.

Step 4: Run the HTML in any Browser.

4.2.3 HTML Page Structure

Basic HTML Document Code Structure

```
<!-- This is a comment -->
<!DOCTYPE html>
<html> <head><title>Title of the page</title></head>
     <body>
            <h1>This a heading</h1>
             <p>This is a paragraph.</p>
             <p>This is another paragraph.</p>
     </body>  </html>
```

4.3   XML

XML is eXtensible Markup language unlike HTML. HTML is used for the "look and feel" and display of data on the page whereas XML is used to describe data and information. XML is rich in syntax and extensible by allowing the user to create his own tags. It transforms the data into new formats such as importing the data from the database and displaying it as a table.
The enterprises can use XML to describe invoices, payroll and financial information and shared throughout the organization via intranet.

Example,

```
<? xml version="1.0"?>
<note>
    <from>Jack</from>
    <to>Mary</to>
     <subject>Ecommerce</subject>
     <body>Ecommerce is a trade and business over internet</body>
</note>
```

The first line in above example is XML declaration specifying the version of document. The next line '<note>' defines the root, next 4 lines defines the 4 child elements of the root element (<to>, <from>, <subject>, <body>) and last line defines end of the root element '<note>'.
The XML format called as Really Simple Syndication (RSS) helps user to include text, articles, blogs, audio files and digital content for data sharing over internet. When the RSS aggregator software is installed in the computer, it scans and gathers the information from articles, blogs and websites.
Example: Feedly, Reeder, and NewsBlur.

4.4   WEB SERVERS AND CLIENTS

Web server: It is a software that delivers the web page written in HTML to the client computers over a network when installed and request for the service is made using HTTP. Apache is the most widely used Web server software on Linus and Unix platform. Internet Information Service

(IIS) plays a significant role on Microsoft platform. Every web server computer over an internet is provided with IP address.

The web server also provides other functionalities such as,

- Security service: This is to provide authentication and authorization of the person to access the particular website. The payment transactions are associated with SSL and TLS protocol for secure transmission of information over the network.

- File Transfer Protocol (FTP): This protocol is used to transfer the files to and from the server.

- Search Engine: This is used to search entire web for the particular document. The web server software associates the index with each web page to make easy keyword search over the content and delivering all likely matching web pages.

- Data capture: The log file maintained at the server will keep track of number of times a particular web site is accessed, the details of user who accessed the website, date and time of the access, length of the access and information on specific pages that were accessed. This information can be later used by the site manager to analyze and specify the most popular web site.

Apart from web servers, there are several other servers performing a particular task such as database servers, ad servers, mail servers and video servers.

Web server operations:

- All the communications between a web client and a web server use the HTTP

- When a web server begins execution, it informs the Operating System (OS) under which it is running & it runs as a background process

- A web client or browser, opens a network connection to a web server, sends information requests and possibly data to the server, receives information from the server and closes the connection.

- The primary task of web server is to monitor a communication port on host machine, accept HTTP commands through that port and perform the operations specified by the commands.

- When the URL is received, it is translated into either a filename or a program name.

General characteristics of web server:

- The file structure of a web server has two separate directories
- The root of one of these is called **document root** which stores web documents
- The root of the other directory is called the **server root** which stores server and its support software's
- The files stored directly in the document root are those available to clients through top level URLs
- The secondary areas from which documents can be served are called **virtual document trees.**
- Many servers can support more than one site on a computer, potentially reducing the cost of each site and making their maintenance more convenient. Such secondary hosts are called **virtual hosts.**
- Some servers can serve documents that are in the document root of other machines on the web; in this case they are called as **proxy servers**

Example:

Apache

- Apache is the most widely used Web server.
- The primary reasons are as follows: Apache is an excellent server because it is both fast and reliable.
- Furthermore, it is open-source software, which means that it is free and is managed by a large team of volunteers, a process that efficiently and effectively maintains the system.
- Finally, it is one of the best available servers for Unix-based systems, which are the most popular for Web servers.
- Apache is capable of providing a long list of services beyond the basic process of serving documents to clients.
- When Apache begins execution, it reads its configuration information from a file and sets its parameters to operate accordingly.

Internet Information Services (IIS)

- Microsoft IIS server is supplied as part of Windows—and because it is a reasonably good server—most Windows-based Web servers use IIS.

- With IIS, server behavior is modified by changes made through a window-based management program, named the IIS snap-in, which controls both IIS and File Transmission Protocol (ftp).

- This program allows the site manager to set parameters for the server.

- Under Windows XP and Vista, the IIS snap-in is accessed by going to *Control Panel, Administrative Tools, and IIS Admin.*

Web client: The web client is a computing device that is capable of requesting a document from the server using HTTP and displaying the HTML pages. Web client can be any mobile devices, printer, refrigerator and home lighting systems,

4.5 WEB BROWSERS

Browser is a software used to display web pages. When a user requests for the web page from particular website, the web browser will fetch the necessary content from web server and displays it on the user's device.

Example: Google chrome, Internet Explorer, Mozilla Firefox, Microsoft Edge and Safari.

A **web browser** is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video, or other piece of content. Hyperlinks present in resources enable users to easily navigate their browsers to related resources.

Although browsers are primarily intended to access the World Wide Web, they can also be used to access information provided by Web servers in private networks or files in file systems. Some browsers can be also used to save information resources to file systems.

While developing a site, we should try to make it compatible to as many browsers as possible. Especially site should be compatible to major browsers like Explorer, FireFox, Netscape, Opera and Safari.

Internet Explorer

Internet Explorer (IE) is a product from software giant Microsoft. This is the most commonly used browser in the universe. This was introduced in 1995 along with

Windows 95 launch and it has passed Netscape popularity in 1998.

Netscape

Netscape is one of the original Web browsers. This is what Microsoft designed Internet Explorer to compete against. Netscape and IE comprise the major portion of the browser market. Netscape was introduced in 1994.

Mozilla

Mozilla is an open-source Web browser, designed for standards compliance, performance and portability. The development and testing of the browser is coordinated by providing discussion forums, software engineering tools, releases and bug tracking. Browsers based on Mozilla code is the second largest browser family on the Internet today, representing about 30% of the Internet community.

Konqueror

Konqueror is an Open Source web browser with HTML 4.01 compliance, supporting Java applets, JavaScript, CSS 1, CSS 2.1, as well as Netscape plugins. This works as a file manager as well. It supports basic file management on local UNIX file systems, from simple cut/copy and paste operations to advanced remote and local network file browsing.

Firefox

Firefox is a new browser derived from Mozilla. It was released in 2004 and has grown to be the second most popular browser on the Internet.

Safari

Safari is a web browser developed by Apple Inc. and included in Mac OS X. It was first released as a public beta in January 2003. Safari has very good support for latest technologies like Extensible Hypertext Markup Language (XHTML), Cascading Style Sheets (CSS2) etc.

Opera

Opera is smaller and faster than most other browsers, yet it is full- featured. Fast, user-friendly, with keyboard interface, multiple windows, zoom functions, and more. Java and non Java-enabled versions available. Ideal for newcomers to the Internet, school children, handicap and as a front-end for CD-Rom and kiosks.

Lynx

Lynx is a fully-featured World Wide Web browser for users on Unix, Virtual Memory System (VMS), and other platforms running cursor-addressable, character-cell terminals or emulators.

4.6 COMMUNICATION TOOLS

It is a tool that allows people to connect globally either one to one or one to many basis. Some of them include E-mail, messaging apps, online message boards and internet telephony.

4.6.1 E-mail

Electronic mail is the most widely used communication tool since the earlier days. E-mail is associated with a set of protocols that supports text, image, audio and video to be sent from one person to another via internet. Along with the embedded text in a mail, the files such as documents, audio, video and image files are sent as an attachment inserted as a part of e-mail message.

4.6.2 Messaging apps

Instant messaging allows to share messages in real time. Unlike E-mail that takes several seconds to reach the recipients, the text appears more instantly on the receiver side using instant messaging. The sender will create a buddy list they want to communicate with and type a text message that is received by the buddies instantly and the buddies can respond to the sender the same way while both keeping online. Although text is the primary mechanism, it also provides voice and video chat functionality. It is cheaper when compared to SMS and MMS texting.

Example: Skype, Yahoo Messenger, Google hangouts.

Other messaging apps such as Facebook messenger, WhatsApp, snapchat, Kik, Viber are more widely used providing competition to Instant Messaging.

4.6.3 Online message boards

Online message boards referred as forums, bulletin board or discussion group is a web application that enables users to communicate with each other. The messaging boards provides a separate thread for the members of the board. Firstly, the board administrator has to grant permission for the members of the boards to start their own

thread and reply to the other people's thread. The board administrator has the authority to edit, delete, modify or move any thread on the message board. Here the members have to visit the board to get the updates on the new posts.

4.6.4 Internet Telephony

When the existing telephone system is built over from scratch using internet and packet switching technology over network with TCP/IP, it would make it less expensive and more efficient. And thus internet telephony was introduced and called as IP telephony in short. It is a technology that use Voice over Internet Protocol (VoIP) and packet switching network to transmit voice, fax and other audio over internet. VoIP can be used over basic handset and mobile devices. Currently it has become more popular since it is provided as a triple play (Voice, Internet and TV) in a single package.

Example: Skype

4.7 CHECK YOUR PROGRESS

1. Which is the correct syntax for web address
    a. http://directorypath/domainname/filename
    b. http://domainname/directorypath/filename
    c. http://domainname/filename/directorypath
    d. http://filename/directorypath/domainname

2. HTML stands for -
    a. HighText Machine Language
    b. HyperText and links Markup Language
    c. HyperText Markup Language
    d. None of these

3. Which internet language is used for including text, articles, blogs for data sharing over internet?
    a. RSS

b. RDF

        c. WSDL

        d. OWL

4. Software that requests data from web server is called _____

        a. Users

        b. Hosts

        c. Clients

        d. Programs

5. Which of the following allow us to access E-mail from anywhere?

        a. Forum

        b. Web blog

        c. Message board

        d. Webmail interface

Answers to Check Your Progress

1. b) http://domainname/directorypath/filename
2. c) HyperText Markup Language
3. a) RSS
4. c) Clients
5. d) Webmail interface

4.8 SUMMARY

In this unit we started with the key terminologies such as Hypertext discussing the syntax of web address. Then we discussed different languages for the purpose of designing webpage, holding and transferring the data called HTML and XML. We also had a discussion on Web server, web clients and web browsers. Later we mentioned some of the communication tools with their functionality.

4.9 KEYWORDS

1. **Hypertext:** Hypertext is way of formatting the pages associated with the links that connect one document to another and connecting the pages with other media like graphics, sound, video and animation files.

2. **HTML:** It is a web formatting language used to define the style and structure of the web page.

3. **XML:** XML is used to describe data and information.

4. **Web server:** It is a software that delivers the web page written in HTML to the client computers over a network.

5. **Web client:** The web client is a computing device that is capable of requesting a document from the server using HTTP and displaying the HTML pages.

6. **Web Browser:** Web Browser is a software used to display web pages.

4.10 QUESTIONS FOR SELF-STUDY

1. List the differences between HTML and XML.

2. Explain Web servers, Web clients and Web browsers.

3. What is the significance of Hypertext? Explain the syntax of web address with example.

4. Describe different communication tools.

5. Define Browser and explain different types of Browsers.

4.11 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

2. Programming the World Wide Web: Robert W. Sebesta, 4th Edition, Pearson Education, 2008.

3. Web Programming Building Internet Applications – Chris Bates, 3rd Edition, Wiley India, 2006.

Karnataka State Open University
Mukthagangothri, Mysore – 570 006.
Dept. of Studies and Research in Management

MBA IT Specialization
III Semester

E-commerce

Block 2

Karnataka State Open University

Mukthagangothri, Mysore – 570 006.

Dept. of Studies and Research in Management

MBA. IT Specialization

III Semester

E-commerce

BLOCK 2: CONSTRUCTION OF E-COMMERCE PRESENCE

BLOCK 2 INTRODUCTION

This block speaks of how an e-commerce idea (a website or an application) be put up across the marketplace. That is, how to convert an idea into a money-generating product. The block also conveys what are the different approaches towards the conversion, what is the software and hardware needed, site tools etc. It conveys the various security issues that the e-commerce product face and what is its viable solution for prevention. Also, once the product is ready to the market, what are the different ways of payments that could be presented to the customers for accessing the services. The last unit will convey the various business strategies and the various business to customer models.

This block consists of 4 units and is organized as follows:

Unit 5- E-commerce presence – Building an e-commerce idea, Systematic approach, Choosing software and hardware, E-commerce site tools

Unit 6- E-commerce security E-commerce System environment, Security threats, Technology solutions

Unit 7- E-commerce payment systems: Management policies, E-commerce payment systems, Electronic billing presentment and payment

Unit 8- E-commerce Business Strategies: E-commerce business models, Major B2C Business models, B2B Business models

UNIT 5: E-COMMERCE PRESENCE

STRUCTURE

5.0 OBJECTIVES

After studying this unit, you will be able to:

- ✓ Learn how to convert an idea into an e-commerce presence
- ✓ Define and imagine an e-commerce presence in the market
- ✓ Explain the Systems Development Life Cycle
- ✓ Describe factors to consider in developing an e-commerce presence
- ✓ Choose and use the right kind of software and hardware for your product
- ✓ Discuss about other e-commerce site tools

5.1 INTRODUCTION

In the previous units, you learned about the technological foundation for e-commerce. We learnt and understood about the internet, the web and the mobile platform. In this chapter you

will know and understand the important factors that a manager should consider while building an e-commerce presence. We learn how an idea can be converted to an e-commerce website or an application. We discuss the various software and hardware needed for the successful running of this e-commerce product. These days, software and hardware prices have gradually reduced but are more powerful than at the advent of the early e-commerce days. We also discuss the merging of mobile devices and the social network platforms like facebook.com (now called "meta") that adds to the complexity of having the e-commerce presence into three platforms: The web, the mobile and the social networks.

5.2 IMAGINE THE E-COMMERCE PRESENCE

Before we begin to build a website or an application of our own, we need to provide answers to a few questions. The questions list is as follows:

1. What is the idea?
2. Where is the money for running the site or app coming from?
3. Who is the target for whom we are creating the product?
4. Where is this target coming from?
5. Where is the content coming from and what type of content is it?

The answers to these questions are important.

1. The idea is the concept or ideology behind running the e-commerce website or app. We should know the pros and cons of converting the idea into to a product. It is the vision that runs in the background and with whose hope that we can accomplish and how to accomplish towards the conversion of an e-commerce presence.

The vision of the e-commerce presence plays an important role. If you open any website, through the home page we can make out what the vision of the company is. For example: Amazon wants to be the biggest marketplace in the world, Facebook wants the world to be more open and connected and for Google it's to organize the world's information and make the information available easily and accessible globally.

2. Once the mission and vision is defined, we need to start thinking about where the money will come for running our e-commerce presence. A preliminary idea of the business and revenue

2

models should be created. We need to also think how the general idea will generate revenue. The basic revenue model alternatives are advertising, subscriptions, transaction fees, sales, and affiliate revenue.

Many a time's one single business model will be a logical combination of one or more of the above alternate revenue models. As an example – facebook.com runs advertising in the right side of their website. Google search engine has an ads feature – which ranks at the top of their website.

3. We need to know for whom we are creating the product. The target audience is extremely important for the launch of any website or application. We should also know where best we can reach this target audience.

The target audience can be described in a number of ways: demographics, behavior patterns (lifestyle), current consumption patterns (online vs. offline purchasing), digital usage patterns, content creation preferences (blogs, social networks, sites like Pinterest), and buyer personas (profiles of your typical customer).

Understanding the demographics of your target audience is usually the first step. Demographic information includes age, income, gender, and location.
We take an example of Harley Davidson motorcycles to understand about the importance of demographics.
People from the age of 34 and all the way till 65 purchase motorcycles. These men travel with women during the rides. The Harley Davidson website has a collection of women's clothing and several web pages devoted to women riders. The love for motorcycles and the brand, and the lifestyle associated with touring highways of America on a powerful cycle is the one that drives Harley Davidson customers together.

4. The chances of the product's success will depend greatly on the characteristics of the market that you are about to enter. The marketplace for the target audience is a very important factor.
This does not just depend on your entrepreneurial brilliance and the brains behind it. Enter into a declining market filled with strong competitors, and you will multiply your chances of failure. Enter into a market that is emerging, growing, and has few competitors, and you stand a better chance. Enter a market where there are no players, and you will either be rewarded handsomely with a profitable monopoly on a successful product no one else thought of (Apple) or you will be quickly forgotten because there isn't a market for your product at this point in time

5. Websites are like books: they're composed of a lot of pages that have content ranging from text, to graphics, photos, and videos. People or customers visit our website only for the content that we showcase. This acts as a major force and foundation for the revenue generation and ultimate success of the e-commerce presence.

There are basically two types of content: static and dynamic content:

The static content is text and images that do not change frequently over a period of time. Dynamic content is content that changes regularly, say, daily or hourly. Dynamic content can be created by you, or increasingly, by bloggers and fans of your website and products. User generated content has a number of advantages: it's free, it engages your customer fan base, and search engines are more likely to catalog your site if the content is changing. Other sources of content, especially photos, are external websites that aggregate content such as Pinterest.

Know yourself: Conduct a SWOT analysis

Finally, before investing the time and effort along with the idea to join your website or application into the market, it's important first of all to know ourselves. A SWOT (Strength, Weakness, Opportunity, Threats) analysis helps us for that.

STRENGTHS
- Current sites do not address market needs
- Unique approach
- Easy navigation
- Better personalization
- Customer base growing
- High-value market segment
- Superior social strategy

WEAKNESSES
- Limited financial resources
- No prior online experience
- No existing user base
- No media attention
- No Web design expertise
- No computer background

OPPORTUNITIES
- Ability to address large market with unmet needs
- Potential to capture significant share of this market
- Potential to develop related sites

THREATS
- Approach could be copied by competitors
- Advertisers may not want to try a new site
- Rapid pace of technological development
- Low market entry costs

Fig.5.1: SWOT Analysis

5.3 BUILDING AN E-COMMERCE PRESENCE: A SYSTEMATIC APPROACH

E-commerce has moved from a PC-centric activity on the web to a mobile and tablet-based. Though 70% of e-commerce retail and travel revenues happen through the desktop computers, an increase in using smartphones and tablets for purchase is observed.

But still, we need to give significance to these "touch points" where a customer seeks for the product's service.

The e-commerce presence can be classified into four types. They are:

1. Website/App
2. Social Media
3. E-mail
4. Offline media.

There are different platforms for each of this presence. The figure 5.2 illustrates the various e-commerce presences with their platforms.

Fig.5.2: E-Commerce presence MAP
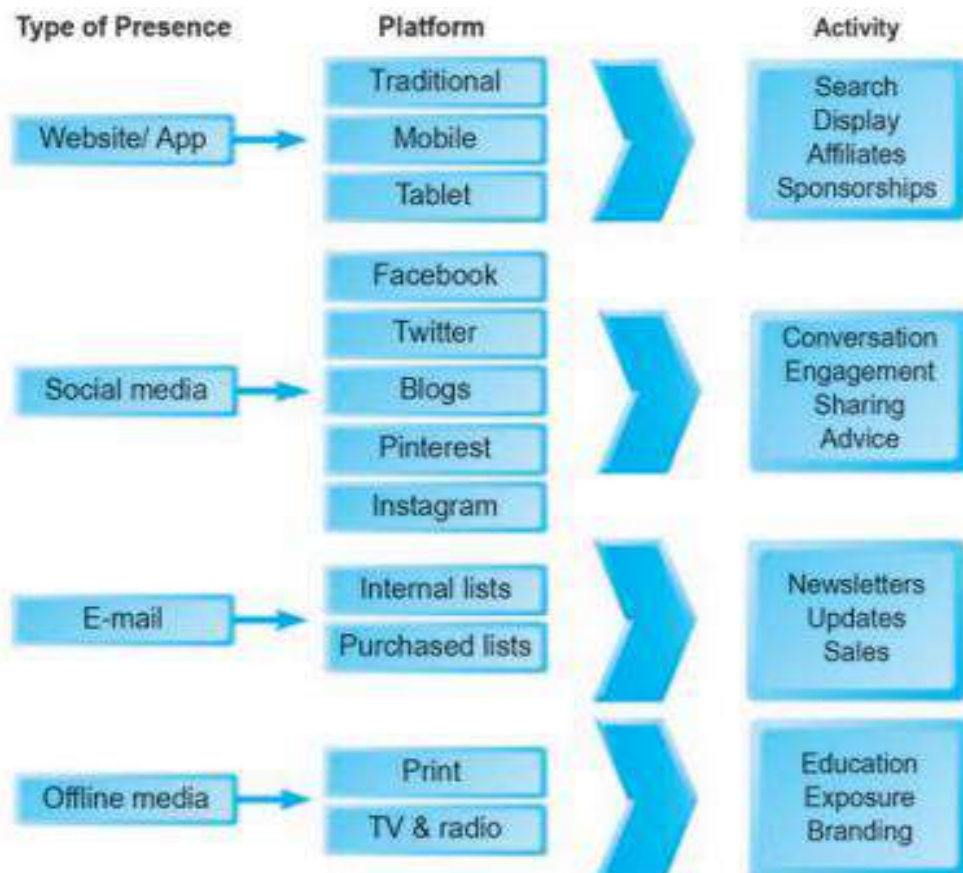
For instance, in the case of websites and/or apps, there are three different platforms: traditional desktop, tablets, and smartphones, each with different capabilities. And for each type of e-commerce presence there are related activities you will need to consider. For instance, in the case of websites and apps, you will want to engage in search engine marketing, display ads, affiliate programs, and sponsorships. Offline media, the fourth type of e-commerce presence, is included here because many firms use multiplatform or integrated marketing where print, television, or radio ads refer customers to websites and apps.

Also, it is advised to develop a timeline with milestones for the development of a startup.
There are five phases that summarizes the e-commerce presence. They are:

1. Planning
2. Website Development
3. Web implementation
4. Social media plan
5. Social media implementation
6. Mobile plan.

PHASE	ACTIVITY	MILESTONE
Phase 1: Planning	Envision e-commerce presence; determine personnel	Mission statement
Phase 2: Website development	Acquire content; develop a site design; arrange for hosting the site	Website plan
Phase 3: Web implementation	Develop keywords and metatags; focus on search engine optimization; identify potential sponsors	A functional website
Phase 4: Social media plan	Identify appropriate social platforms and content for your products and services	A social media plan
Phase 5: Social media implementation	Develop Facebook, Twitter, and Pinterest presence	Functioning social media presence
Phase 6: Mobile plan	Develop a mobile plan; consider options for porting your website to smartphones	A mobile media plan

Fig.5.3: E-Commerce presence Timeline

5.3.1 Factors to consider in developing an E-commerce Presence

Developing an e-commerce presence is not an easy task. Development can be done in two ways. In the first there is your team of people with various talents who develop it. Or in the second case, we outsource the development to a different team and set of people.

There are various factors to consider in developing an e-commerce presence. They are: Management, Software, Hardware architecture, Design, Telecommunications, Human Resources.
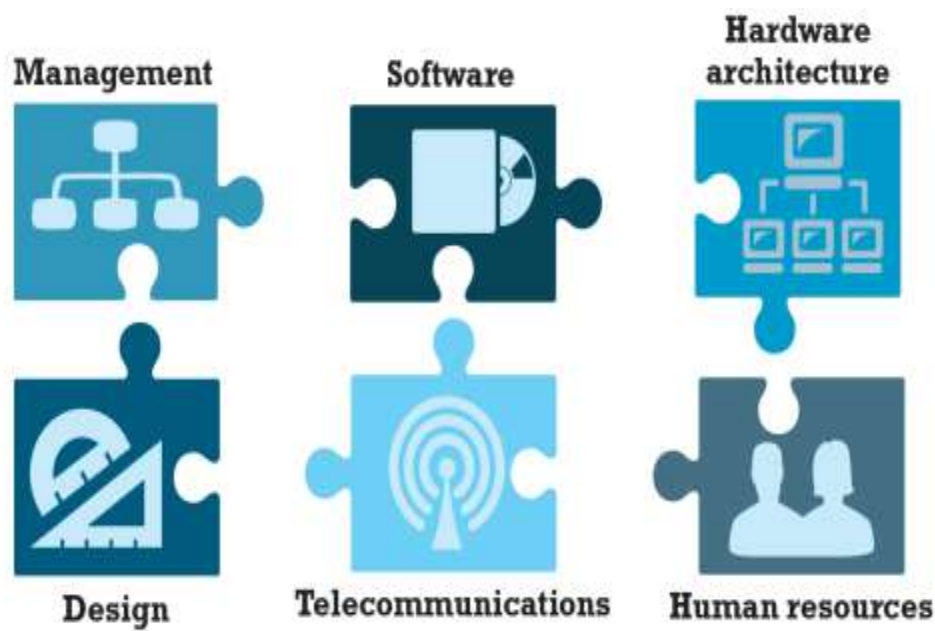
Fig.5.4: Factors to consider in developing an E-Commerce presence

Management is about the skills needed to manage every aspect for the development of the presence.

We discuss software and hardware in detail below:

Design conveys the various ways in which the factors have to interact for a successful running of the e-commerce presence.

- ➤ Telecommunications – are the different ways and methods in which the various components communicate with each other.
- ➤ Human resources – is about managing both resources (people v/s non-people entities)

5.3.2 The systems development life cycle

The Systems Development Life cycle (SDLC) is a methodology for understanding the business objectives of any system and designing an appropriate viable solution. The development of the cycle does not guarantee that success will be obtained, but still it is better than having no proper plan for development.

There are 5 major steps involved in the systems development life cycle. They are:

1. System Analysis / Planning – do the planning for the complete product.
2. Systems design – design individual components separately
3. Building the system - Combine and integrate the individual components to a single workable software product.
4. Testing – Perform various kinds of testing. The testing can be done to individual components and for the complete software.
5. Implementation – Run the components as a group so that the complete functionality of the software is achieved.
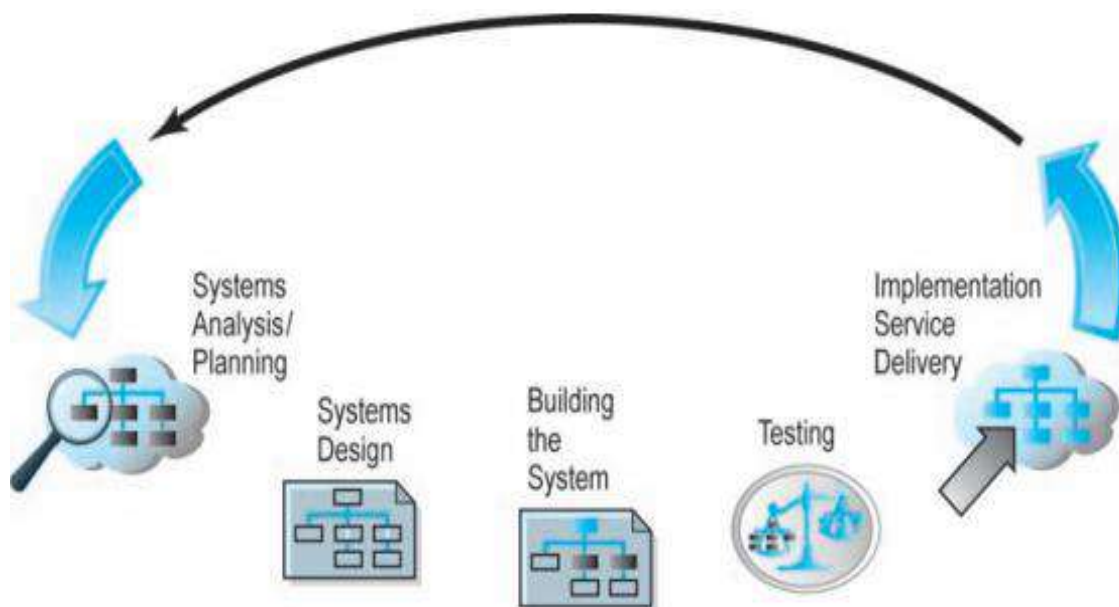

Fig.5.4: Websites System Development Life Cycle

5.4 CHOOSING THE SOFTWARE

We should be careful while selecting the software that we choose to start the startup or the e-commerce presence. Also, the software that we choose should be scalable both horizontally and vertically.

Most of the software used in startups is based on the following architectures:

1. Two-tier architecture
2. Multi-tier architecture.

The type of the tier that we need to choose is based on our consumer demands and needs. The following other kinds of software are also needed for the startup:

1. Web server software – Examples: Apache HTTP Server, Apache Tomcat server
2. Application servers – Software that runs the applications.

APPLICATION SERVERS

Web application servers are software programs that provide the specific business functionality required of a website. The basic idea of application servers is to isolate the business applications from the details of displaying web pages to users on the front end and the details of connecting to databases on the back end. Application servers are a kind of middleware software that provides the glue connecting traditional corporate systems to the customer as well as all the functionality needed to conduct e-commerce. In the early years, a number of software firms developed specific separate programs for each function, but increasingly, these specific programs are being replaced by integrated software tools that combine all the needed functionality for an e-commerce site into a single development environment, a packaged software approach. In most cases choosing open source software is considered viable than proprietary software. The various open source software options are detailed in the figure 5.4

Open source software is software developed by a community of programmers and designers, and is free to use and modify. The advantage of using open source web building tools is that you get exactly what you want, a truly customized unique website. The disadvantage is that it will take several months for a single programmer to develop the site and get all the tools to work together seamlessly.

FUNCTIONALITY	OPEN SOURCE SOFTWARE
Web server	Apache (the leading web server for small and medium businesses)
Shopping cart, online catalog	Many providers: osCommerce, Zen Cart, AgoraCart, X-cart, AspDotNetStorefront
Credit card processing	Credit card acceptance is typically provided in shopping cart software but you may need a merchant account from a bank as well.
Database	MySQL (the leading open source SQL database for businesses)
Programming/scripting language	PHP is a scripting language embedded in HTML documents but executed by the server, providing server-side execution with the simplicity of HTML editing. Perl is an alternative language. JavaScript programs are client-side programs that provide user interface components. Ruby on Rails (RoR, Rails) and Django are other popular open source web application frameworks.
Analytics	Analytics keep track of your site's customer activities and the success of your web advertising campaign. You can also use Google Analytics if you advertise on Google, which provides good tracking tools; most hosting services will provide these services as well. Other open source analytic tools include Piwik, CrawlTrack, and Open Web Analytics.

Fig.5.4: Open source software options

5.5 CHOOSING THE HARDWARE

Whether you host your own site or outsource the hosting and operation of your site, you will need to understand certain aspects of the computing hardware platform. The hardware platform refers to all the underlying computing equipment that the system uses to achieve its e-commerce functionality. Your objective is to have enough platform capacity to meet peak demand (avoiding an overload condition), but not so much platform that you are wasting money.

10

The scalability of the hardware that we need to procure again is based on two needs:

1. The Demand side
2. The supply side

There are various ways of vertical and horizontal scaling techniques. They are:

1. Use a faster computer
2. Create a cluster of computers to run in parallel.
3. Usage of appliance servers.
4. Segment workload
5. Batch requests – single batch, multiple batch
6. Manage connections – single or multiple connections.
7. Aggregate user data – into data pools, so that relevant and related can be pooled in.
8. Cache – store frequently used data in cache than in any other memory.

5.6 OTHER E-COMMERCE

TOOLS FOR SEARCH ENGINE OPTIMIZATION

A website is only as valuable from a business perspective as the number of people who visit. The first stop for most customers looking for a product or service is to start with a search engine, and follow the listings on the page, usually starting with the top three to five listings, then glancing to the sponsored ads to the right. The higher you are on the search engine pages, the more traffic you will receive. Page 1 is much better than Page 2. So how do you get to Page 1 in the natural (unpaid) search listings? While every search engine is different, and none of them publish their algorithms for ranking pages.

TOOLS FOR INTERACTIVITY AND ACTIVE CONTENT

The more interactive a website is, the more effective it will be in generating sales and encouraging return visitors. Although functionality and ease of use are the supreme objectives in site design, you will also want to interact with users and present them with a lively, "active" experience. You will want to personalize the experience for customers by addressing their individual needs, and customize the content of your offerings based on their behavior or

11

expressed desires. In order to achieve these business objectives, you will need to consider carefully the tools necessary to build these capabilities. Simple interactions such as a customer submitting a name, along with more complex interactions involving credit cards, user preferences, and user responses to prompts, all require special programs.

Brief description of some commonly used software tools for achieving high levels of site interactivity are as given below:

- **Common Gateway Interface (CGI)**: a set of standards for communication between a browser and a program running on a server that allows for interaction between the user and the server

- **Active Server Pages (ASP)** a proprietary software development tool that enables programmers using Microsoft's IIS package to build dynamic pages.

- **ASP.NET:** successor to ASP Java a programming language that allows programmers to create interactivity and active content on the client computer, thereby saving considerable load on the server.

- **Java**: a programming language that allows programmers to create interactivity and active content on the client computer, thereby saving considerable load on the server

- **Java Server Pages (JSP)**: like CGI and ASP, a web page coding standard that allows developers to dynamically generate web pages in response to user requests.

- **JavaScript:** a programming language invented by Netscape that is used to control the objects on an HTML page and handle interactions with the browser.

- **ActiveX:** a programming language created by Microsoft to compete with Java

- **VBScrip**t: a programming language invented by Microsoft to compete with JavaScript

- **ColdFusion:** an integrated server-side environment for developing interactive web applications **PHP:** open source, general purpose scripting language

- **Ruby on Rails (RoR/ Rails):** open source web application framework based on Ruby programming language

12

5.7 CHECK YOUR PROGRESS

1. The idea plays an important role towards starting the company / product. State True or False.

2. We have to scale the software and hardware as per the demand and needs of the customers. State True or False.

3. Its important many a times to have an idea that can be converted to a product across a _____ marketplace.

4. Customers play an important role in running any business model. State True or False.

5. The _____ audience is important to run any business model.

6. The _____ analysis helps us to know our strengths and weakness before entering the market with our idea as a product.

7. Expand the acronym SDLC.

Answers to Check Your Progress:

1. True
2. True
3. sparse
4. True
5. target
6. SWOT
7. Systems Development Life Cycle

5.8 SUMMARY

In this unit, we discussed how to convert an idea to a e-commerce product. We also learnt about the stakeholders who run the product. It was made aware about the Systems Development life cycle. We discussed what is the software and hardware needs for running the product. We also observe and learn about other e-commerce site tools.

5.9 KEYWORDS

- **Vision** – The idea and ideology behind which a product can be created.
- **Business model** – The model that converts an idea to a business viable product. The product generates revenue.
- **Target audience** – It is our customers or consumers who seek-peek and consume our services.
- **Software** – The software tools needs to run a successful product. These tools are installed into the hardware.
- **Hardware** – The source of tools needed to run the software and in turn manage the product's scalability
- **SDLC** – The different phases of systems development life cycle.

5.10 QUESTIONS FOR SELF STUDY

1. What are the main factors to consider when developing an e-commerce presence?
2. Name the four main kinds of e-commerce presence and the different platforms for each type.
3. Define the systems development life cycle and discuss the various steps involved in creating an e-commerce site.
4. Explain the need of picking the right hardware and software for running the e-commerce presence.
5. How is scalability of software and hardware managed in any e-commerce presence?

5.11 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

UNIT 6- E-COMMERCE SECURITY

STRUCTURE

6.0 OBJECTIVES

After studying this unit, you will be able to:

- ✓ Understand what is security with respect to e-commerce.
- ✓ What is the role of security in running a successful e-commerce product.
- ✓ What are the different kinds of security threats.
- ✓ Define hacking
- ✓ Explain about Cyber vandalism
- ✓ Describe about hactivism
- ✓ What are the technology solutions for overcoming these security threats.

6.1 INTRODUCTION

The Internet and Web are increasingly vulnerable to large-scale attacks and potentially large-scale failure. Increasingly, these attacks are led by organized gangs of criminals operating

globally—an unintended consequence of globalization.

Even more worrisome is the growing number of large-scale attacks that are funded, organized, and led by various nations against the Internet resources of other nations. Anticipating and countering these attacks has proved a difficult task for both business and government organizations. However, there are several steps you can take to protect your websites, your mobile devices, and your personal information from routine security attacks.

6.2 E-COMMERCE SYSTEM ENVIRONMENT

For most law-abiding citizens, the Internet holds the promise of a huge and convenient global marketplace, providing access to people, goods, services, and businesses worldwide, all at a bargain price. For criminals, the Internet has created entirely new—and lucrative—ways to steal from the more than 1.6 billion Internet consumers worldwide in 2016. From products and services, to cash, to information, it's all there for the taking on the Internet.

It's also less risky to steal online. Rather than rob a bank in person, the Internet makes it possible to rob people remotely and almost anonymously. Rather than steal a CD at a local record store, you can download the same music for free and almost without risk from the Internet.

Cybercrime is becoming a more significant problem for both organizations and consumers. Bot networks, DDoS attacks, Trojans, phishing, ransomware, data theft, identity fraud, credit card fraud, and spyware are just some of the threats that are making daily headlines.

Criminals who steal information on the Internet do not always use this information themselves, but instead derive value by selling the information to others on the so-called underground or shadow economy market. Data is currency to cybercriminals and has a "street value" that can be monetized. For example, in 2013, Vladislav Horohorin (alias "BadB") was sentenced to over 7 years in federal prison for using online criminal forums to sell stolen credit and debit card information (referred to as "dumps"). At the time of his arrest, Horohorin possessed over 2.5 million stolen credit and debit card numbers.

6.2.1   What is good e-commerce security?

To understand this question, we need to find the answer for what is a secure commercial transaction?

Anytime you go into a marketplace you take risks, including the loss of privacy (information

about what you purchased). Your prime risk as a consumer is that you do not get what you paid for. As a merchant in the market, your risk is that you don't get paid for what you sell. Thieves take merchandise and then either walk off without paying anything, or pay you with a fraudulent instrument, stolen credit card, or forged currency.

E-commerce merchants and consumers face many of the same risks as participants in traditional commerce, albeit in a new digital environment. Theft is theft, regardless of whether it is digital theft or traditional theft. Burglary, breaking and entering, embezzlement, trespass, malicious destruction, vandalism—all crimes in a traditional commercial environment—are also present in e-commerce. However, reducing risks in e-commerce is a complex process that involves new technologies, organizational policies and procedures, and new laws and industry standards that empower law enforcement officials to investigate and prosecute offenders. The figure 6.1 illustrates the multi-layered nature of e-commerce security.

Fig.6.1: Multi-Layered Nature of E-Commerce Security

6.2.1 Dimensions of e-commerce security

The below are the dimensions of e-commerce security with their meanings:

1. **Integrity** - the ability to ensure that information being displayed on a website or transmitted or received over the Internet has not been altered in any way by an unauthorized party.

2. **Nonrepudiation** - the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions.

3. **Authenticity** - the ability to identify the identity of a person or entity with whom you are dealing on the Internet.

4. **Confidentiality -** the ability to ensure that messages and data are available only to those who are authorized to view them

5. **Privacy** - the ability to control the use of information about oneself

Table 6.1: Dimensions of e-commerce security

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

6.3 SECURITY THREATS

To understand the various security threats that can happen, we should understand the structure of a typical e-commerce transaction. The Figure 6.2 provides the structure and illustrates a typical e-commerce transaction with a consumer using a credit card to purchase a product.
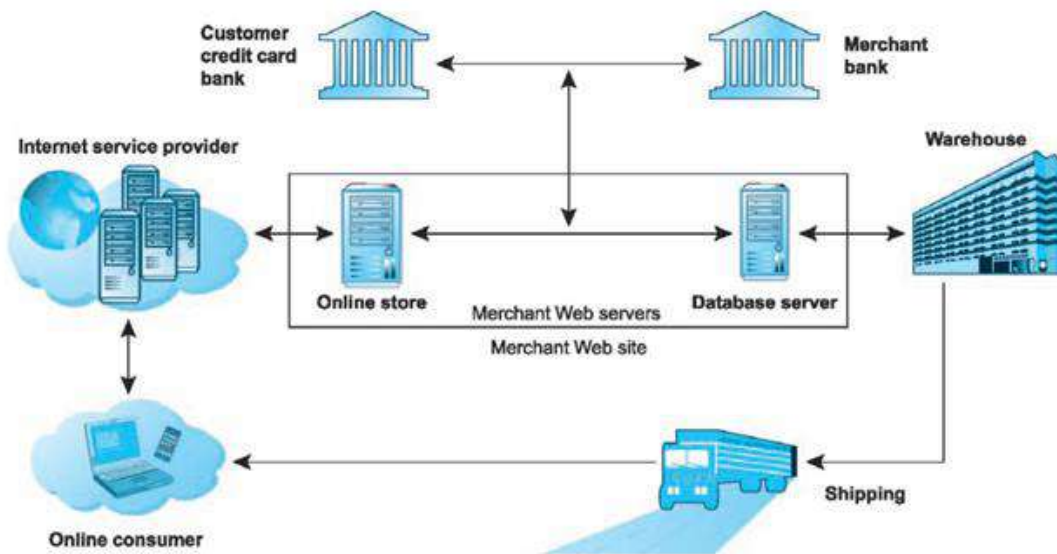
Fig. 6.2: The structure of an e-commerce transaction.
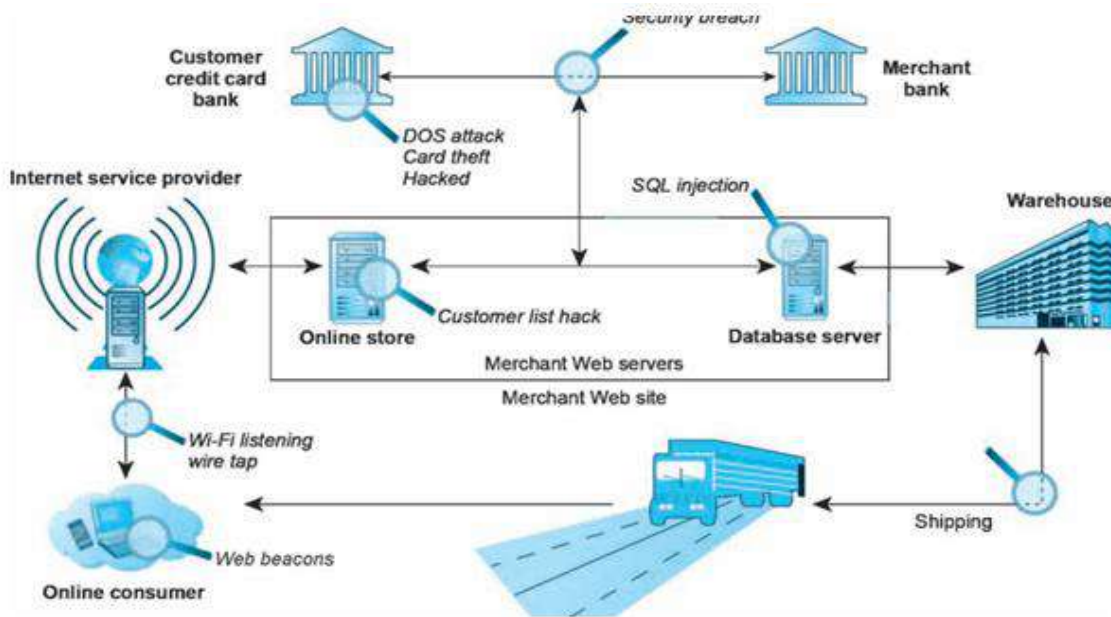

Fig. 6.3: The vulnerable points of an e-commerce transaction.

Also Figure 6.3 discusses the various ways in which this e-commerce transaction be hampered with security threats and breaches.

The various security threats with their meanings is given below:

1. **Malicious code (also called malware)** - includes a variety of threats such as viruses, worms, Trojan horses, and bots

2. **Exploit kit** - collection of exploits bundled together and rented or sold as a commercial product

3. **Maladvertising** - online advertising that contains malicious code

4. **drive-by download** - malware that comes with a downloaded file that a user requests

5. **Virus** - a computer program that has the ability to replicate or make copies of itself, and spread to other files

6. **Worm** - malware that is designed to spread from computer to computer

7. **Ransomware (also called scareware)** - malware that prevents you from accessing your computer or files and demands that you pay a fine or a ransom

8. **Trojan horse** - appears to be gentle and kind, but then does something other than expected. Often a way for viruses or other malicious code to be introduced into a computer system

9. **backdoor** - feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer

10. **bot** - type of malicious code that can be covertly installed on a computer when connected to the Internet. Once installed, the bot responds to external commands sent by the attacker

11. **botnet** - collection of captured bot computers

12. potentially unwanted program (PUP) - program that installs itself on a computer, typically without the user's informed consent

6.3.1 Hacking, Cybervandalism, and hacktivism

A hacker is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term cracker is typically used to denote a hacker with criminal intent. These hackers are people who gain unauthorized access by finding weakness or vulnerable points present in websites and Operating systems.

Today, hackers have malicious intentions to disrupt, deface, or destroy sites or to steal personal or corporate information they can use for financial gain (data breach). This is also called as cyberwar or cyber vandalism.

Hacktivism adds a political plot to the story. Hacktivists typically attack governments, organizations, and even individuals for political purposes, employing the tactics of cyber vandalism, distributed denial of service attacks, data thefts, and doxing (gathering and exposing personal information of public figures, typically from emails, social network posts, and other documents).

6.4   TECHNOLOGY SOLUTIONS

At first glance, it might seem like there is not much that can be done about the onslaught of security breaches on the Internet. Reviewing the security threats in the previous section, it is clear that the threats to e-commerce are very real, widespread, global, potentially devastating for individuals, businesses, and entire nations, and likely to be increasing in intensity along with the growth in e-commerce and the continued expansion of the Internet. But in fact a great deal of progress has been made by private security firms, corporate and home users, network administrators, technology firms, and government agencies. There are two lines of defense: technology solutions and policy solutions.

In this section, we consider some technology solutions: The first line of defense against the wide variety of security threats to an e-commerce site is a set of tools as shown in figure 6.4 that can make it difficult for outsiders to invade or destroy a site.

Fig. 6.4: Tools available to achieve site security

To know how to secure the e-commerce site, we need to understand a few terminologies. They are:

1. Encryption – A process of transforming plain text or data to cipher texts that cannot be read by anyone other than the sender and the receiver.

The purpose of encryption is 2-folds:

- To secure stored information.
- To secure information transmission.

Encryption enables 4 of the 6 dimensions mentioned in table 6.1.

➢ Message integrity—provides assurance that the message has not been altered.

➢ Nonrepudiation—prevents the user from denying he or she sent the message.

➢ Authentication—provides verification of the identity of the person (or computer) sending the message.

➢ Confidentiality—gives assurance that the message was not read by others.

There are different ways of encryption schemes. They are:

1. Symmetric key cryptography

2. Public key cryptography

3. Digital envelopes

4. Digital certificates and Public key infrastructure

Also, there are different algorithms that help the encryption process. To brief a few algorithms:

1. Data Encryption Standard (DES) - developed by the National Security Agency (NSA) and IBM. Uses a 56-bit encryption key

2. Advanced Encryption standard – AES - the most widely used symmetric key algorithm, offering 128-, 192-, and 256-bit keys

6.5 CHECK YOUR PROGRESS

1. Define the term: Integrity.
2. List any 2 encryption algorithms.
3. There are _____ number of dimensions to e-commerce security.
4. Define the term: Virus.
5. Viruses spreads itself by creating copies of the bad program to multiple instances. State True or False?

Answers to Check Your Progress:

1. Integrity - the ability to ensure that information being displayed on a website or transmitted or received over the Internet has not been altered in any way by an unauthorized party.
2. AES and DES algorithms.
3. 06 dimensions
4. A computer program that has the ability to replicate or make copies of itself, and spread to other files
5. True.

6.6 SUMMARY

Through this Unit we were able to learn the e-commerce system environment, the multiple dimensions to e-commerce security, the different kinds of security threats, learn about cybervandalism and hacktivism.

Also, we learnt about the different encryption schemes with their algorithms.

6.7 KEYWORDS

- **White hats** - "good" hackers who help organizations locate and fix security flaws
- **Black hats** - hackers who act with the intention of causing harm
- **Grey hats** - hackers who believe they are pursuing some greater good by breaking in and revealing system flaws
- **Privacy** - the ability to control the use of information about oneself
- **Hacker** – A person who breaks into a system or an organizational site.
- **Worm** - malware that is designed to spread from computer to computer

6.8 QUESTIONS FOR SELF STUDY

1. Explain the multiple dimensions to e-commerce security.
2. Illustrate with a diagram the e-commerce system environment.
3. List and explain any 4 security threats with their meanings.
4. Explain hacker, cybervandalism and hacktivism.
5. Explain any 2 encryption based security dimensions in detail.
6. List any antivirus software that you know and explain its need and usage.

6.9 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.
2. http://williamstallings.com/Cryptography/

UNIT 7- E-COMMERCE PAYMENT SYSTEMS

STRUCTURE

7.0 Objectives

7.1 Management policies

7.2 E-commerce payment systems

7.3 Electronic billing presentment and payment

7.4 Check your progress

7.5 Summary

7.6 Keywords

7.7 Questions for self-study

7.8 References

7.0 OBJECTIVES

After studying this unit, you will be able to:

- ✓ E-commerce management policies
- ✓ Identify the major e-commerce payment systems in use today.
- ✓ Explain about patent law
- ✓ Discuss about encryption
- ✓ Describe the features and functionality of electronic billing presentment and payment systems.

7.1 MANAGEMENT POLICIES

Worldwide, in 2016, companies are expected to spend over €76 billion on security hardware, software, and services, up 8% from the previous year (Gartner, 2016). However, most CEOs and CIOs believe that technology is not the sole answer to managing the risk of e-commerce. The technology provides a foundation, but in the absence of intelligent management policies, even the best technology can be easily defeated. Public laws and active enforcement of cybercrime statutes also are required to both raise the costs of illegal behaviour on the Internet and guard against corporate abuse of information.

Let's consider briefly the development of management policy.

A SECURITY PLAN: MANAGEMENT POLICIES

In order to minimize security threats, e-commerce firms must develop a coherent corporate policy that takes into account the nature of the risks, the information assets that need protecting, and the procedures and technologies required to address the risk, as well as implementation and auditing mechanisms. **Figure 7.1** illustrates the key steps in developing a solid security plan.
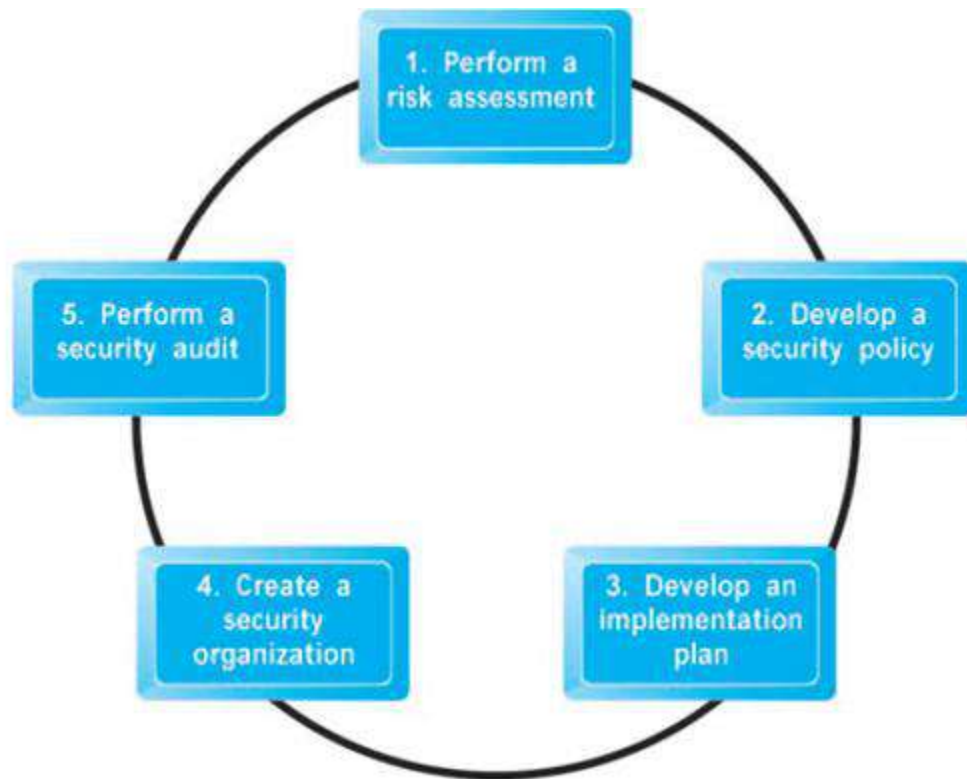
Fig.7.1: E-Commerce Security Plan

A security plan begins with **risk assessment**—an assessment of the risks and points of vulnerability. The first step is to inventory the information and knowledge assets of the e-commerce site and company. What information is at risk? Is it customer information, proprietary designs, business activities, secret processes, or other internal information, such as price schedules, executive compensation, or payroll? For each type of information asset, try to estimate the dollar value to the firm if this information were compromised, and then multiply that amount by the probability of the loss occurring. Once you have done so, rank order the results. You now have a list of information assets prioritized by their value to the firm.

Based on your quantified list of risks, you can start to develop a **security policy**— a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying

the mechanisms for achieving these targets. You will obviously want to start with the information assets that you determined to be the highest priority in your risk assessment. Who generates and controls this information in the firm? What existing security policies are in place to protect the information? What enhancements can you recommend to improve security of these most valuable assets? What level of risk are you willing to accept for each of these assets? Are you willing, for instance, to lose customer credit card data once every 10 years? Or will you pursue a 100-year hurricane strategy by building a security edifice for credit card data that can withstand the once-in-100-year disaster? You will need to estimate how much it will cost to achieve this level of acceptable risk. Remember, total and complete security may require extraordinary financial resources. By answering these questions, you will have the beginnings of a security policy.

Next, consider an **implementation plan**—the steps you will take to achieve the security plan goals. Specifically, you must determine how you will translate the levels of acceptable risk into a set of tools, technologies, policies, and procedures. What new technologies will you deploy to achieve the goals, and what new employee procedures will be needed?

To implement your plan, you will need an organizational unit in charge of security, and a security officer—someone who is in charge of security on a daily basis. For a small e-commerce site, the security officer will likely be the person in charge of Internet services or the site manager, whereas for larger firms, there typically is a dedicated team with a supporting budget. The **security organization** educates and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security.

The security organization typically administers access controls, authentication procedures, and authorization policies. **Access controls** determine which outsiders and insiders can gain legitimate access to your networks. Outsider access controls include firewalls and proxy servers, while insider access controls typically consist of login procedures (usernames, passwords, and access codes).

Authentication procedures include the use of digital signatures, certificates of authority, and PKI. Now that e-signatures have been given the same legal weight as an original pen-and-ink version, companies are in the process of devising ways to test and confirm a signer's identity. Companies frequently have signers type their full name and click on a button indicating their understanding that they have just signed a contract or document.

Biometric devices can also be used to verify physical attributes associated with an individual, such as a fingerprint or retina (eye) scan or speech recognition system. (**Biometrics** is the study of measurable biological, or physical, characteristics.) A company could require, for example, that an individual undergo a fingerprint scan before being allowed access to a website, or before being allowed to pay for merchandise with a credit card. Biometric devices make it even more difficult for hackers to break into sites or facilities, significantly reducing the opportunity for spoofing. Newer Apple iPhones (5S and later) feature a fingerprint sensor called Touch ID built into the iPhone's home button that can unlock the phone and authorize purchases from the iTunes, iBooks, and App Stores without requiring users to enter a PIN or other security code. According to Apple, the system does not store an actual fingerprint, but rather biometric data, which will be encrypted and stored only on a chip within the iPhone, and will not be made available to third parties.

Security tokens are physical devices or software that generate an identifier that can be used in addition to or in place of a password. Security tokens are used by millions of corporation and government workers to log on to corporate clients and servers.

One example is RSA's SecurID token, which continuously generates six-digit passwords. **Authorization policies** determine differing levels of access to information assets for differing levels of users. **Authorization management systems** establish where and when a user is permitted to access certain parts of a website. Their primary function is to restrict access to private information within a company's Internet infrastructure.

Although there are several authorization management products currently available, most operate in the same way: the system encrypts a user session to function like a passkey that follows the user from page to page, allowing access only to those areas that the user is permitted to enter, based on information set at the system database.

By establishing entry rules up front for each user, the authorization management system knows who is permitted to go where at all times.

The last step in developing an e-commerce security plan is performing a security audit. A **security audit** involves the routine review of access logs (identifying how outsiders are using the site as well as how insiders are accessing the site's assets). A monthly report should be produced that establishes the routine and non routine accesses to the systems and identifies unusual patterns of activities. As previously noted, tiger teams are often used by large corporate sites to

evaluate the strength of existing security procedures. Many small firms have sprung up in the last five years to provide these services to large corporate sites.

Tech Laws Of India

The information technology sector is the largest and fastest-growing industry in India. Over the years, this sector has witnessed huge investment along with a considerable amount of growth contributing to the improved economy of the nation. Tech laws of India is now emerging as the "digital hub" of the world, with it being the largest employer in the private sector.

The incredible inclination with progressive nature in the field of Information Technology and the growth of the information service sector has drastically changed the world economy giving rise to a new system based on intellectuals, resulting in the new areas and scope of research & development, employment, productivity, efficiency, and enhanced attributes of growth.

The Information Technology industry in the last few decades has shown a tremendous contribution to the global economy. To estimate the prospects of the industry, the knowledge about the contribution and the driving factors forms the base.

Information Technology Sector – Indian Perspective

India has become the digital capabilities hub of the world with around 75% of global digital talent present in the country. In light of the increasing IT adoption, the IT sector treats as a separate entity of business model to an integrate model for providing the basic IT infrastructure and applications to keep business on track. Hence, in the current scenario, IT is treated as a business partner which helps in providing solutions to business problems connected with software.

India's software industry is one of the world's successful information technology industries. It has taken a long journey in setting up its base during the 1980s march for being the hub for many global firms by 2019 and still marching. India became the potential hub for the IT industry and almost all the giants of the IT industry started setting up their operations in India. The IT industry has witnessed tremendous transformation since 2000, in customizing to mass customization of products and services for their end-users.

Market Size

IT & BPM industry's revenue is estimated to be around US$ 191 billion in 2020, growing at 7.7% and expected to cross US$ 350 billion by 2025. The digital economy estimates to reach Rs 69,89,000 crore (US$ 1 trillion) by 2025. The total number of employees grew to 1.02 million cumulatively for four Indian IT majors (including TCS, Infosys, Wipro, HCL Tech) as of December 31, 2019.

Investments/ Developments

India is the largest employer in the software sector and has attracted a significant amount of investors from different countries. The computer software and hardware sector in India have been able to attract cumulative Foreign Direct Investment (FDI) inflow worth US$ 44.91 billion in the last two decades. The sector is ranked second in FDI inflow.

Role of Legal Advancement in Booming the IT Industry

- The development of the Indian IT sector dates back to 1974, when a mainframe manufacturer, Burroughs asked Tata Consultancy Services (TCS), to send software programmers for installing system software for a U.S. client. Until then, there was no proper governance of the IT Sector in private companies and the policies were not very effective.

- There was a huge outflow of skilled Indians to the western countries for taking up jobs due to the lack of job opportunities in the country. This gave a good opportunity to the IT sector to establish its base in the United States of America and several European countries. The first software export zone SEEPZ was set up in Mumbai/Bombay in 1973. Around 80 per cent of India's software exports were out of SEEPZ, Bombay in the 1980s.

- The immigration laws in the United States of America were relaxed in 1965 which attracted a large number of skilled Indian professionals aiming for research. The Indian economy remained hostile to the software industry through the 1970s. Import tariffs is as high as 135% on hardware and 100% on software and the software industry that did not consider an "industry",

- Indian Information Technology organizations developed as an industry during the '70s but didn't attract investment in the IT field due to restricting imports of computer peripherals, high import tax, strict Foreign Exchange and Regulation Act (FERA) limiting its allocation.

- The government of India's policy towards the IT sector has a complete new turn in 1984 – New Computer Policy (NCP-1984) will introduce. The policies gave the software sector the status of Industry-opening doors for FDI and other investments. The IT industry was freed from license-permit raj, permission for foreign companies to set up wholly-owned, export-dedicated units, and a scheme to set up a series of software parks that would offer infrastructure at less than market costs.

- In 1991 the Department of Electronics forms a corporation as Software Technology Parks of India (STPI) that, being owns by the government, could provide VSAT communications without moving away from its monopoly

- India and the European Union agreed to bilateral cooperation in the field of science and technology. A joint EU-India group of scholars was formed to further promote joint research and development.

- The IT industry is an employer to both technical and non-technical graduates and has a great potential to create huge foreign exchange inflows for India. India exports software and services to approximately 95 countries around the world. Countries get benefits by outsourcing their work to India due to low labour costs.

- The GOI started providing various incentives like tax holidays and competitive duty structures, reduction in the international communication cost, and infrastructure facilities to support IT Parks. These factors created huge opportunities in the IT sector leading to a boom in the sector.

- With an increase in technological advancement and internet usage, a lot of avenues for crimes coming up, with new laws enacts to curb such practices. Having said that, one of the major advances in the legal regime was the enactment of the Information Technology Act, 2000.

- As of February 2020, there were 417 approved SEZs across the country with 274 from IT & BPM and 143 as exporting SEZs.

Status of data privacy in consonance with the Information Technology sector

As we all know that the information technology market has advanced with the improvement in the field of technology and telecommunication networks. The capacity to collect, process, and

store data has also increased. No doubt, such advancement in the IT sector has proved to be very emphatic, however, it has its own negative and devastating impacts covering a wide range of ethical and social issues. One such impact is the breach of data privacy. Data privacy is the collection, processing, and storing of personal and sensitive personal data. When such information is for an illegal purpose, it amounts to breach and the data collectors will liable for the same.

Under the Privacy of data, the consent-base system will follow in India wherein the data controller allow to use, process, and transfer the information to a third party once the consent of the person receives. This has led to a breach of privacy data and has given greater autonomy to data controllers.

Since India does not have a comprehensive data protection mechanism, the main enactment that deals with the protection of data is the Information Technology Act, 2000. Under the IT Act and the IT Rules, what is primarily sought to protect is 'personal information' and 'sensitive personal data or information'

Information under the privacy laws are categorised into two types:-

1. Personal Information or Data

2. Sensitive Personal information Data

Personal Information or data

Personal information is the details which enable the identification of a person. Further, personal information includes all the data about or relating to a person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

The name, address, email id, contact details, bank account details, etc. fall under the category of personal information.

Sensitive Personal Information Data

Sensitive Personal Information Data is under Rule 3 of the 2011 rules. This definition is inclusive and gives an exhaustive list of what are the types of sensitive personal information

data. Therefore, Sensitive information is a type of personal information. This information is of vital importance to a person's life

Race or ethnic origin, religion, political affiliations, sexual orientation, criminal history, and trade union or association memberships are all considered sensitive information. Any information about biometrics, genetics, or medical history is also treated as sensitive information.

The strongest legal protection provided to personal information in India is through section 43A of the Information Technology Act, 2000[3] and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011- The Rules provides for a comprehensive structure for Reasonable Security practices and gives a procedure of compliances to follow by the data processors.

Private Policy: Needs and Requirements

The Body Corporate must have a privacy policy for handling of and deal with personal information including sensitive personal data or information published on the official website of the Body Corporate where the information providers have easy access to it. Such a policy should have clear and accessible statements of the Body Corporate's practice and policy.

It should also lay down the types of personal and sensitive information or data collected via password; financial physical, physiological, and mental health condition; sexual orientation; medical records and history; biometric information; or any other information as required under the contract. As biometrics provide high accuracy and are less exposed to damages, most of the companies rely upon it.

The website shall contain clear information

- Private policy

- Name and details of the Grievance Officer

- The third-party shall not disclose the information or data any further.

- It shall not publish the obtained personal information and sensitive data or information.

- They have implemented security practices and standards for example IS/ISO/IEC 27001.

- They have Comprehensive documented information programmes. A security program is a document set of the company's information security policies, procedures, guidelines, and standards. The security program should provide a roadmap for effective security management practices and controls. Having a security program will help the company ensure the confidentiality, integrity, and availability of your client and customer information, as well as your organization's essential data.

- An information security policy that contains managerial, technical, operational and physical security control measures that commensurate with the information assets protecting with the nature of business

Standards Set for Reasonable Security Forces

- The International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such standard under Rule 8.

- Any industry association or an entity formed by such an association, whose members are self -regulating by following other than IS/ISO/IEC codes of best practices for data protection), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

The Judgement was given by the Hon'ble Court in the case of Justice K. S. **Puttaswamy (Retd.) and Anr. vs Union of India and Ors**, in 2012 is considered to be the milestone in the history of data privacy and protection. The Court ruled that the Right to Privacy is a Fundamental Right and an integral part of Article 21. The Court also held that "Informational Privacy" is an essential facet in the Right to Privacy.

IT Laws and Regulations in Connection with IPR

The IT industry has a very deep connection with the IPR legislation. In the fast-moving pace of inventing new software, every IT industry works to its maximum to get their protection.

The Information Technology sector mainly composes of software, web designing, and data operations. Further, the new software develops every second by hard-working engineers who put in immense effort to make use of this software for innovations.

Under the IPR regime, the work is protected under three laws:

1. Patent Law
2. Copyright Law
3. Trademark Law

Patent Law

A patent grants monopoly for the exploitation of an invention. The holders of a patent are granted the exclusive right to prevent others from using, commercializing, or importing the patented products or processes. To protect such software, patents are crucial. Patent protection is to any field of technology without discrimination. Additionally, granting of the patent will ensure that these computer programs protect from being copied illegally. Additionally, from unauthorized use. Further, in India, only when the software attaches to hardware can have a patent. Making it difficult for all software to be patented. However, it is pertinent that we make a distinction between a computer programme. Further, software to encourage innovations in the IT sector.

Copyright law

Under Section 2(o) of the Copyright Act, a literary work includes a computer programme. Further, Section 13 states that copyright subsists in a literary work. Thus, it would subsist on a computer programme too. Additionally, Article 10 of the TRIPs also talks about computer programmes. Further, computer programmes have a source code and an object code which are copyrightable under the Indian Copyright Act.

Labour Laws in Information Technology Industry

It is a misconception that the IT industry exempts from employment and labour laws. But in the reality, these laws apply to the IT and ITES companies although the Factories Act, 1946; the Industrial Disputes Act, 1947, and certain State labour laws do not apply to IT Industries. Apart from that, all the other labour laws apply to IT Industries as well.

Following are some important employment laws that bind software companies.

1. *Shops and Establishments Act*

   The Shops and Establishments Act has enhancement by every state in India. IT and ITES companies in a particular State are covered within the definition of 'commercial establishments' under the Shops & Establishments Act of the State.

2. The Employees' Provident Fund & Miscellaneous Provisions Act, 1952

The Employees Provident Fund Act provides for financial security and stability to employees. Additionally, in an event that the employee temporarily or no longer fit to work or at retirement. Moreover, Employee Provident Fund (EPF) implements by the Employees Provident Fund Organization (EPFO) of India.

3. The Employees' State Insurance Act, 1948

The ESI Act is self-financing social security protecting workers and their dependents in contingencies. Such as sickness, maternity, death, disablement, or occupational disease. Further, being a self-financing scheme, the ESI funds will primarily build-out of contributions from employers. Additionally, employees payable monthly at a fixed percentage of wages paid.

4. The Employees' Compensation Act, 1923

This Act provides for compensation to workmen and employees for various injuries, even death, incurred during their employment.

5. The Payment of Bonus Act, 1965

The Act lays down a scheme for the calculation of bonus, payment of maximum. Further, the minimum bonus, deductions from the bonus, etc. Recently, the wage threshold for determining the eligibility of employees has been revised from Rs. 10,000 to Rs. 21,000 per month, thereby bringing a larger pool of employees under the coverage of the Act.

6. Equal Remuneration Act, 1976

The Act provides that employers cannot discriminate against men and women in matters of recruitment. Additionally, by notification in March 1977, the Government has 'Data processing and tabulating services'. Under the ambit of the Act thereby bringing IT and ITES industries in its sweep

7. Industrial Employment (Standing Orders) Act, 1946

The object of the Act is to require employers in industrial establishments. Additionally, it is to define with sufficient precision the rules and conditions of employment. Under them and to make them known to workmen/employees. Some states such as Karnataka have exempted the IT and ITES companies from the application of this Act.

8. The Maternity Benefit Act, 1961

The Maternity Benefit Act enacts for the benefit of working pregnant women. Who are, or have given birth, or suffered a miscarriage. This Act is on the moral that when a woman gives birth. She does it not only for herself but for the whole society.

9. The Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013

The Act makes it the responsibility of the Employer to protect women against sexual harassment. The Act has laid down procedures for dealing with complaints and enquiries, protection of victims. Additionally prescribes punishment for sexual harassment, and also punishes false complaints of harassment. Noncompliance with this Act may invite a fine of up to Rs 50,000/- upon the employer. Further, cancellation of license to carry out business activities.

In addition to the above enactments, other laws such as the Employment Exchanges (Compulsory Notification of Vacancies) Act, 1959, the Minimum Wages Act, the Payment of Gratuity Act are also applicable to the IT and ITES companies.

Government Policies and Controls on Encryption

Encryption and cryptographic techniques for preserving the security of online communication have become increasingly contested in India. Rapid digitalization in the past decade has led to the proliferation of domestic and foreign online communication services that use encryption and, consequently, pose challenges to national security bodies and law enforcement agencies (LEAs). To help overcome these challenges, the Indian government issued controversial new rules in February 2021 that require messaging communication providers to supply information regarding the originators of messages. Many providers argue that this requirement significantly weakens the end-to-end (E2E) encryption they deploy.

The contestation between maintaining higher degrees of online security and issuing new rules to grant technological exceptions for security agencies and LEAs is not specific to India. Conflicts between LEAs and companies that use encryption to protect personal data and communication have become public in many countries. For example, in 2016, there was a contentious public debate in the United States when the Federal Bureau of Investigation asked Apple to provide a backdoor to the smartphone of a suspected criminal by breaking its encryption protections. Apple

refused. While the bureau found a workaround, this did not create a durable solution to the issue.[3] In 2019, the Australian government passed a law that enables government agencies to force businesses to break encryption. The law has faced opposition from those arguing that this approach will weaken encryption and have adverse economic consequences. And in October 2020, the LEAs of the Five Eyes intelligence-sharing pact (which includes Australia, Canada, New Zealand, the United Kingdom, and the United States) issued a statement that called on technology companies to find a solution to the issue of E2E encryption. India supported this statement.

On the one hand, thanks to digitalization, India's security agencies and LEAs now have access to significantly more types of data—via mobile devices, over-the-top (OTT) platforms, and cloud storage, for example; they therefore can tap into more personal information for surveillance and investigation purposes. And for service providers, advances in encryption offer obvious benefits in terms of ensuring confidentiality, protecting the security of online communications and transactions, and authenticating the identities of individuals. But security agencies and LEAs argue that as more forms of secure and confidential communication become widely available, malicious actors are increasingly using them as shields to conceal criminal or terrorist activities. They further assert that the demands to cope with the negative effects of digitalization currently outweigh the advantages.

While other countries are dealing with similar issues, the solutions to India's concerns must reflect its particular legal and market structures and its security and law enforcement imperatives. The growth of mobile phone usage, internet access, and broadband networks has led to the significantly increased usage of OTT services for messaging, voice calls, and other forms of communication. Many of the industry's major companies, such as WhatsApp and Signal, use E2E encryption. OTT messaging services are provided by businesses who are not telecom service providers. Therefore, these services function very differently from traditional infrastructure, such as phone lines and towers.

7.2 E-COMMERCE PAYMENT SYSTEMS

For the most part, existing payment mechanisms such as cash, credit cards, debit cards, checking accounts, and stored value accounts have been able to be adapted to the online environment, albeit with some significant limitations that have led to efforts to develop alternatives. In

addition, new types of purchasing relationships, such as between individuals online, and new technologies, such as the development of the mobile platform, have also created both a need and an opportunity for the development of new payment systems. In this section, we provide an overview of the major e-commerce payment systems in use today.

Table 7.1 lists some of the major trends in e-commerce payments in 2016–2017.

- Payment by credit and/or debit card remains the dominant form of online payment.
- Mobile retail payment volume skyrockets.
- PayPal remains the most popular alternative payment method online.
- Apple, Google, Samsung, and PayPal extend their reach in mobile payment apps.
- Large banks enter the mobile wallet and P2P payments market.
- Square gains further traction with a smartphone app, credit card reader, and credit card processing service that permits anyone to accept credit card payments.
- Google refocuses Google Wallet, which had met with tepid response, solely on sending and receiving money.
- Mobile P2P payment systems such as Venmo take off.

Worldwide, online payments by consumers represented a market of almost €2.35 trillion in 2016. Institutions and business firms that can handle this volume of transactions (mostly the large banking and credit firms) generally extract 2%–3% of the transactions in the form of fees. Given the size of the market, competition for online payments is spirited. New forms of online payment are expected to attract a substantial part of this growth.

The primary form of online payment is still the existing credit and debit card system. Alternative payment methods such as PayPal continue to make inroads into traditional payment methods. Mobile payments are also expected to grow significantly. **Figure 7.2** illustrates the percentage of consumers that use various alternative payment methods in 2016. However, none of these alternative payment methods have become substitutes for the bank and credit cards, but instead provide consumers with alternative methods of accessing their existing bank and credit accounts.
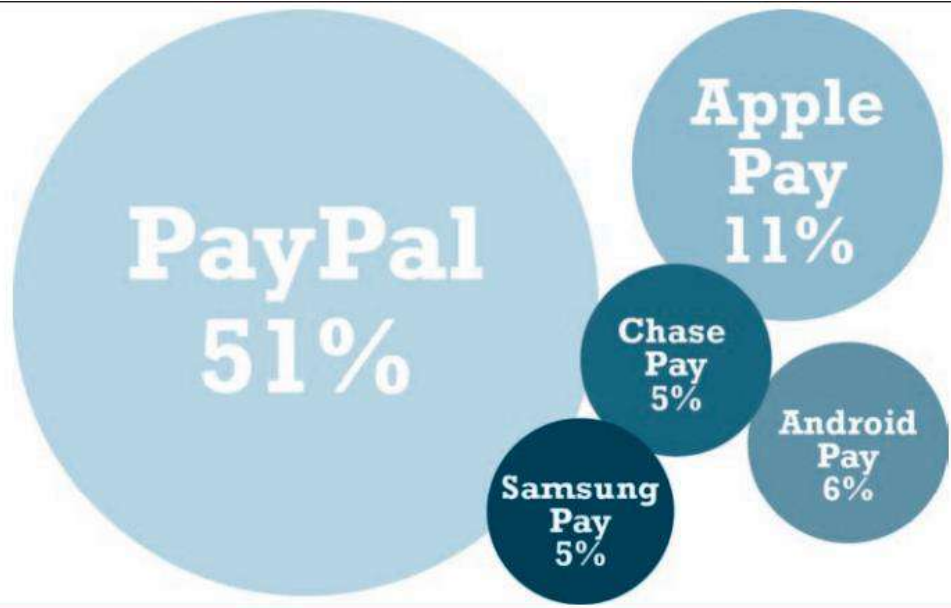
Fig 7.2 Alternative payment methods

In developing countries, e-commerce payments can be very different depending on traditions and infrastructure. Credit cards are not nearly as dominant a form of online payment as they are in the United States. If you plan on operating an e-commerce site in Europe, Asia, or Latin America, you will need to develop different payment systems for each region. For instance, in Denmark, Norway, and Finland payment is primarily with debit or credit cards, while in Sweden, payment after being tendered an invoice and by bank transfer are very popular in addition to credit/debit cards. In the Netherlands, the online payments service iDEAL is the most popular retail e-commerce payment method. In Italy, consumers rely heavily on both credit cards and PayPal. In Japan, although credit card is the primary payment method, many consumers still pick up and pay for goods using cash at local convenience stores.

ONLINE CREDIT CARD TRANSACTIONS

Because credit and debit cards are the dominant form of online payment, it is important to understand how they work and to recognize the strengths and weaknesses of this payment system. Online credit card transactions are processed in much the same way that in-store purchases are, with the major differences being that online merchants never see the actual card being used, no card impression is taken, and no signature is available. Online credit card transactions most closely resemble Mail Order-Telephone Order (MOTO) transactions. These types of purchases are also called Cardholder Not Present (CNP) transactions and are the major

reason that charges can be disputed later by consumers. Because the merchant never sees the credit card, nor receives a hand-signed agreement to pay from the customer, when disputes arise, the merchant faces the risk that the transaction may be disallowed and reversed, even though he has already shipped the goods or the user has downloaded a digital product. **Figure 7.3** illustrates the online credit card purchasing cycle.
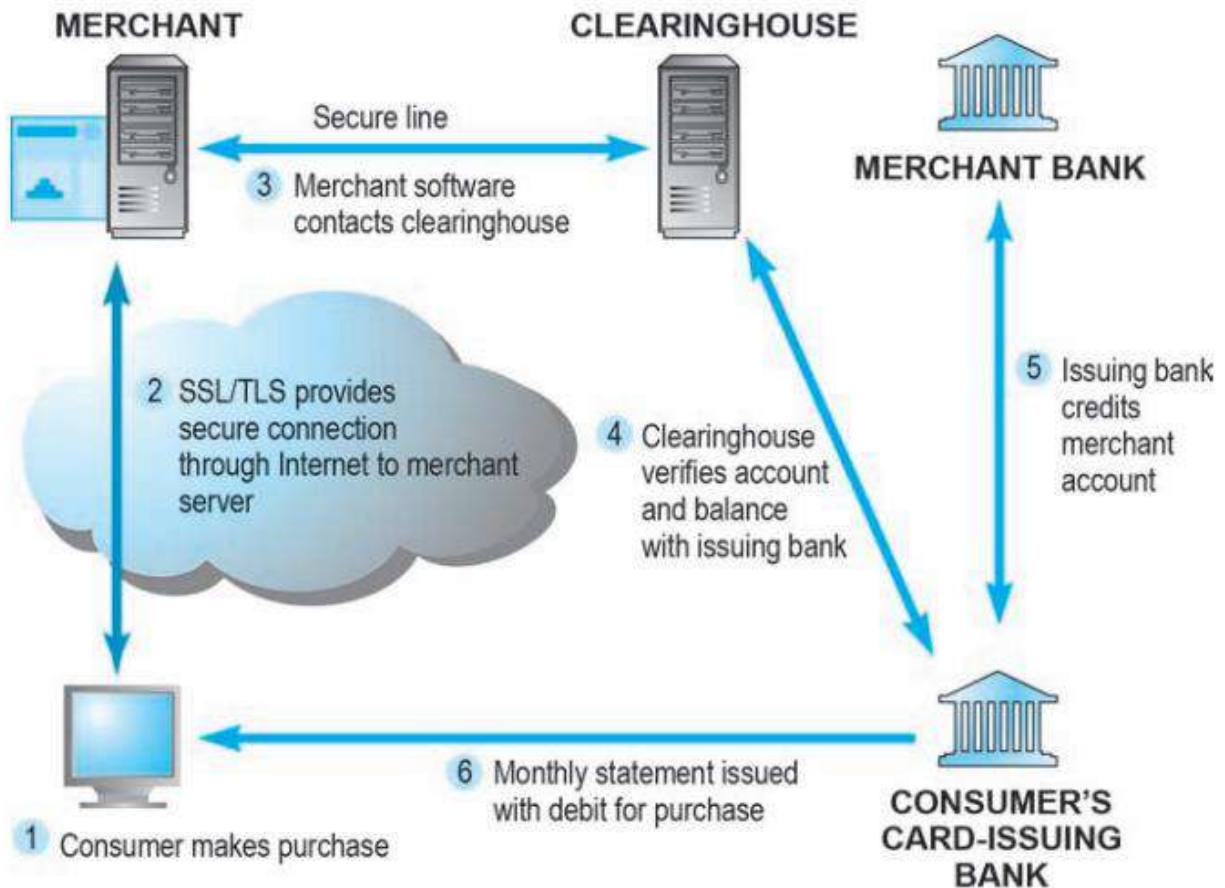
Fig. 7.3. Online credit card purchasing cycle

There are five parties involved in an online credit card purchase: consumer, merchant, clearinghouse, merchant bank (sometimes called the "acquiring bank"), and the consumer's card issuing bank. In order to accept payments by credit card, online merchants must have a merchant account established with a bank or financial institution. A **merchant account** is simply a bank account that allows companies to process credit card payments and receive funds from those transactions.

As shown in Figure 7.3, an online credit card transaction begins with a purchase (1). When a consumer wants to make a purchase, he or she adds the item to the merchant's shopping cart. When the consumer wants to pay for the items in the shopping cart, a secure tunnel through the Internet is created using SSL (Secure Socket Layer) /TLS (Transport Layer Security). Using encryption, SSL/TLS secures the session during which credit card information will be sent to the merchant and protects the information from interlopers on the Internet (2). SSL does not authenticate either the merchant or the consumer. The transacting parties have to trust one another.

Once the consumer credit card information is received by the merchant, the merchant software contacts a clearinghouse (3). As previously noted, a clearinghouse is a financial intermediary that authenticates credit cards and verifies account balances. The clearinghouse contacts the issuing bank to verify the account information (4). Once verified, the issuing bank credits the account of the merchant at the merchant's bank (usually this occurs at night in a batch process) (5). The debit to the consumer account is transmitted to the consumer in a monthly statement (6).

Credit Card E-commerce Enablers

Companies that have a merchant account still need to buy or build a means of handling the online transaction; securing the merchant account is only step one in a two-part process. Today, Internet payment service providers (sometimes referred to as payment gateways) can provide both a merchant account and the software tools needed to process credit card purchases online.

For instance, Authorize.net is an Internet payment service provider. The company helps a merchant secure an account with one of its merchant account provider partners and then provides payment processing software for installation on the merchant's server. The software collects the transaction information from the merchant's site and then routes it via the Authorize.net "payment gateway" to the appropriate bank, ensuring that customers are authorized to make their purchases. The funds for the transaction are then transferred to the merchant's merchant account. Cyber Source is another well-known Internet payment service provider.

Limitations of Online Credit Card Payment Systems

There are a number of limitations to the existing credit card payment system. The most important limitations involve security, merchant risk, administrative and transaction costs, and social equity.

The existing system offers poor security. Neither the merchant nor the consumer can be fully authenticated. The merchant could be a criminal organization designed to collect credit card numbers, and the consumer could be a thief using stolen or fraudulent cards. The risk facing merchants is high: consumers can repudiate charges even though the goods have been shipped or the product downloaded.

The banking industry attempted to develop a secure electronic transaction (SET) protocol, but this effort failed because it was too complex for consumers and merchants alike. The rate of online credit card fraud is expected to reach $4 billion in 2016, up from $2 billion in 2011. As banks switch to EMV cards with computer chips, offline credit card fraud becomes more difficult, encouraging criminals to focus on online fraud.

The administrative costs of setting up an online credit card system and becoming authorized to accept credit cards are high. Transaction costs for merchants also are significant—roughly 3% of the purchase plus a transaction fee of 20–35 cents per transaction, plus other setup fees.

Credit cards are not very democratic, even though they seem ubiquitous. Millions of young adults do not have credit cards, along with millions of others who cannot afford cards or who are considered poor risks because of low incomes.

ALTERNATIVE ONLINE PAYMENT SYSTEMS

The limitations of the online credit card system have opened the way for the development of a number of alternative online payment systems. Chief among them is PayPal.

PayPal (purchased by eBay in 2002 and then spun-off as an independent company again in 2015) enables individuals and businesses with e-mail accounts to make and receive payments up to a specified limit.

Paypal is an example of an **online stored value payment system**, which permits consumers to make online payments to merchants and other individuals using their bank account or credit/debit cards. It is available in 202 countries and 25 currencies around the world. PayPal builds on the existing financial infrastructure of the countries in which it operates. You establish a PayPal account by specifying a credit, debit, or checking account you wish to have charged or paid when conducting online transactions. When you make a payment using PayPal, you e-mail the payment to the merchant's PayPal account. PayPal transfers the amount from your credit or checking account to the merchant's bank account.

The beauty of PayPal is that no personal credit information has to be shared among the users, and the service can be used by individuals to pay one another even in small amounts. However, one issue with PayPal is its relatively high cost. For example, when using a credit card as the source of funds, to send or request money, the cost ranges from 2.9% to 5.99% of the amount (depending on the type of transaction) plus a small fixed fee (typically $0.30) per transaction. PayPal is discussed in further depth in the case study at the end of the chapter. Although PayPal is by far the most well-known and commonly used online credit/debit card alternative, there are a number of other alternatives as well. Pay with Amazon is aimed at consumers who have concerns about entrusting their credit card information to unfamiliar online retailers. Consumers can purchase goods and services at non-Amazon websites using the payment methods stored in their Amazon accounts, without having to re-enter their payment information at the merchant's site.

Amazon provides the payment processing. Visa Checkout (formerly V.me) and MasterCard's Master Pass substitute a user name and password for an actual payment card number during online checkout. Both Master Pass and Visa Checkout are supported by a number of large payment processors and online retailers. However, they have not yet achieved the usage of Paypal.

Bill Me Later (owned by PayPal as well) also appeals to consumers who do not wish to enter their credit card information online. Bill Me Later describes itself as an open-ended credit account. Users select the Bill Me Later option at checkout and are asked to provide their birth date and the last four digits of their social security number.

They are then billed for the purchase by Bill Me Later within 10 to 14 days. Bill Me Later is currently offered by more than 1,000 online merchants.

WU Pay (formerly eBillme, and now operated by Western Union) offers a similar service. WU Pay customers who select the WU Pay option at firms such as Sears, Kmart, and other retailers do not have to provide any credit card information. Instead they are e-mailed a bill, which they can pay via their bank's online bill payment service, or in person at any Western Union location. Dwolla is a similar cash-based payment network for both individuals and merchants. It bypasses the credit card network and instead connects directly into a bank account. In 2015, Dwolla eliminated its transaction and processing fees, changing its focus from consumer-to-consumer

payments to larger businesses. Dwolla has its own network that bypasses the Automated Clearing House (ACH), the traditional system for processing financial transactions in the United States, and in 2015, signed up major U.S. bank BBVA Compass. Earlier in the year, the U.S. Treasury had selected Dwolla (along with PayPal) to process payments to federal agencies, and in October 2015, the Chicago Mercantile Exchange chose Dwolla

to replace ACH. Dwolla now processes nearly $2 billion a year and has over 1 million accounts. Like Dwolla, Stripe is another company that is attempting to provide an alternative to the traditional online credit card system. Stripe focuses on the merchant side of the process. It provides simple software code that enables companies to bypass much of the administrative costs involved in setting up an online credit card system, and instead lets companies begin accepting credit card payments almost immediately without the need to obtain a merchant account or use a gateway provider. Stripe recently introduced merchant apps that can accept NFC payments. Unlike PayPal, the customer doesn't need a Stripe account to pay, and all payments are made directly to the company rather than being routed through a third party.

MOBILE PAYMENT SYSTEMS: YOUR SMARTPHONE WALLET

The use of mobile devices as payment mechanisms is already well established in Europe and Asia and is now exploding in the United States, where the infrastructure to support mobile payment is finally being put in place.

Near field communication (NFC) is the primary enabling technology for mobile payment systems. **Near field communication (NFC)** is a set of short-range wireless technologies used to share information among devices within about 2 inches of each other (50 mm). NFC devices are either powered or passive. A connection requires one powered device (the initiator, such as a smartphone), and one target device, such as a merchant NFC reader, that can respond to requests from the initiator. NFC targets can be very simple forms such as tags, stickers, key fobs, or readers. NFC peer-to-peer communication is possible where both devices are powered. Consumers can swipe their NFC-equipped phone near a merchant's reader to pay for purchases. In September 2014, Apple introduced the iPhone 6, which is equipped with NFC chips designed to work with Apple's mobile payments platform, Apple Pay. Building on Apple Passbook and Touch ID biometric fingerprint scanning and encryption that Apple previously introduced in September 2012, Apple Pay is able to be used for mobile payments at the point-of-sale at a

physical store as well as online purchases using an iPhone. Other competitors in NFC-enabled mobile payments include Android Pay, Samsung Pay, PayPal, and Square. Surveys reveal that about 20%–30% of smartphone users have downloaded mobile wallet apps, but that only about 20% of these adopters have made a payment in the last month using these apps. The promise of riches beyond description to a firm that is able to dominate the mobile payments marketplace has set off what one commentator has called a goat rodeo surrounding the development of new technologies and methods of mobile payment.

SOCIAL/MOBILE PEER-TO-PEER PAYMENT SYSTEMS

In addition to using a mobile device as a vehicle for e-commerce and as a payment method at physical point-of-sale, another type of mobile payment transaction is becoming increasingly popular: social/mobile peer-to-peer payments. Services such as Venmo, Square Cash, Snapcash, the newly refocused Google Wallet, and the new Facebook Messenger Payment service all enable users to send another person money through a mobile application or website, funded by a bank debit card. There is no charge for this service. Currently, these services are the most popular among Millennials, which is the key demographic driving their growth. Venmo, owned by PayPal, is particularly popular, with its success in part due to its integration with Facebook and its social network newsfeed, which lets users see when friends are paying other friends or paying for products and services. In 2015, Venmo processed an estimated $8 billion in transactions and is growing at over 200% annually. In 2016, Facebook and PayPal announced that Facebook subscribers could use PayPal to purchase goods and services, with notifications coming through Facebook Messenger. Analysts forecast that mobile P2P will grow to $174 billion, worth 30% of total P2P payment volume, by 2020. That's up from $5.6 billion, or just 1%, in 2014.

DIGITAL CASH AND VIRTUAL CURRENCIES

Although the terms digital cash and virtual currencies are often used synonymously, they actually refer to two separate types of alternative payment systems. **Digital cash** typically is based on an algorithm that generates unique authenticated tokens representing cash value that can be used "in the real world." Bitcoin is the best known example of digital cash. Bitcoins are encrypted numbers (sometimes referred to as cryptocurrency) that are generated by a complex

algorithm using a peer-to-peer network in a process referred to as "mining" that requires extensive computing power.

Like real currency, Bitcoins have a fluctuating value tied to open-market trading. Like cash, Bitcoins are anonymous—they are exchanged via a 34-character alphanumeric address that the user has, and do not require any other identifying information. Bitcoins have recently attracted a lot of attention as a potential money laundering tool for cybercriminals and illicit drug markets like Silk Road, and have also been plagued by security issues, with some high-profile heists. Nonetheless, there are companies now using Bitcoins as a legitimate alternative payment system.

Virtual currencies, on the other hand, typically circulate primarily within an internal virtual world community, such as Linden Dollars, created by Linden Lab for use in its virtual world, Second Life. Virtual currencies are typically used for purchasing virtual goods.

7.3 ELECTRONIC BILLING PRESENTMENT AND PAYMENT

In 2007, for the first time, the number of bill payments made online exceeded the number of physical checks written in the United States. In the $19 trillion U.S. economy with a $13.3 trillion consumer sector for goods and services, there are billions of bills to pay. According to the U.S. Postal Service, U.S. households received about 21 billion bills in 2015 via the mail. No one knows for sure, but some experts believe the life-cycle cost of a paper bill for a business, from point of issuance to point of payment, ranges from $3 to $7. This calculation does not include the value of time to consumers, who must open bills, read them, write checks, address envelopes, stamp, and then mail remittances. The billing market represents an extraordinary opportunity for using the Internet as an electronic billing and payment system that potentially could greatly reduce both the cost of paying bills and the time consumers spend paying them. Estimates vary, but online payments are believed to cost between only 20 to 30 cents to process.

Electronic billing presentment and payment (EBPP) systems are systems that enable the online delivery and payment of monthly bills. EBPP services allow consumers to view bills electronically using either their desktop PC or mobile device and pay them through electronic funds transfers from bank or credit card accounts.

More and more companies are choosing to issue statements and bills electronically, rather than mailing out paper versions, especially for recurring bills such as utilities, insurance, and subscriptions.

MARKET SIZE AND GROWTH

In 2002, 61% of bill payments in the United States were made by check, and only 12% by online bill payments. In 2015, in contrast, online bill payments accounted for more than 55% of all bill payments, while paper checks now account for less than 20%. Among online households, almost three-quarters pay at least one bill online each month, and almost half receive at least one bill electronically each month. Mobile bill payments are surging, with 33% U.S. households in 2015 paying at least one bill on a mobile device. Most consumers cited the convenience and time saved by using mobile bill payment.

One major reason for the surge in EBPP usage is that companies are starting to realize how much money they can save through online billing. Not only is there the savings in postage and processing, but payments can be received more quickly (3 to 12 days faster, compared to paper bills sent via regular mail), thereby improving cash flow. Online bill payment options can also reduce the number of phone calls to a company's customer service line. In order to realize these savings, many companies are becoming more aggressive in encouraging their customers to move to EBPP by instituting a charge for the privilege of continuing to receive a paper bill.

Financials don't tell the whole story, however. Companies are discovering that a bill is both a sales opportunity and a customer retention opportunity, and that the electronic medium provides many more options when it comes to marketing and promotion. Rebates, savings offers, cross-selling, and upselling are all possible in the digital realm, and much less expensive than mailed envelopes stuffed with offers.

EBPP BUSINESS MODELS

There are four EBPP business models: online banking, biller-direct, mobile, and consolidator.

➢ The online banking model is the most widely used today. Consumers share their banking or credit card credentials with the merchant and authorize the merchant to charge the consumer's bank account. This model has the advantage of convenience for the consumer because the payments are deducted automatically, usually with a notice from the bank or the merchant that their account has been debited.

➢ In the biller-direct model, consumers are sent bills by e-mail notification, and go to the merchant's website to make payments using their banking credentials. This model has the advantage of allowing the merchant to engage with the consumer by sending coupons or rewards. The biller-direct model is a two-step process, and less convenient for consumers.

➢ The mobile model allows consumers to make payments using mobile apps, once again relying on their bank credentials as the source of funds. Consumers are notified of a bill by text message and authorize the payment. An extension of this is the social-mobile model, where social networks like Facebook integrate payment into their messaging services. The mobile model has several advantages, not least of which is the convenience for consumers of paying bills while using their phones, but also the speed with which bills can be paid in a single step. This is the fastest growing form of EBPP. In 2016, Facebook and PayPal announced a deal in which Facebook users can pay for purchases on Facebook using PayPal (Demos, 2016). Consumers will not have to leave Facebook in order to purchase and pay for products.

➢ In the consolidator model, a third party, such as a financial institution or a focused portal such as Intuit's Paytrust, Fiserv's MyCheckFree, Mint Bills, and others, aggregates all bills for consumers and permits one-stop bill payment. This model has the advantage of allowing consumers to see all their bills at one website or app. However, because bills come due at different times, consumers need to check their portals often. The consolidator model faces several challenges. For billers, using the consolidator model means an increased time lag between billing and payment, and also inserts an intermediary between the company and its customer.

Supporting these primary business models are infrastructure providers such as Fiserv, Yodlee, FIS Global, ACI Worldwide, MasterCard RPPS (Remote Payment and Presentment Service), and others that provide the software to create the EBPP system or handle billing and payment collection for the biller. **Figure 7.4** categorizes the major players in the EBPP marketspace.
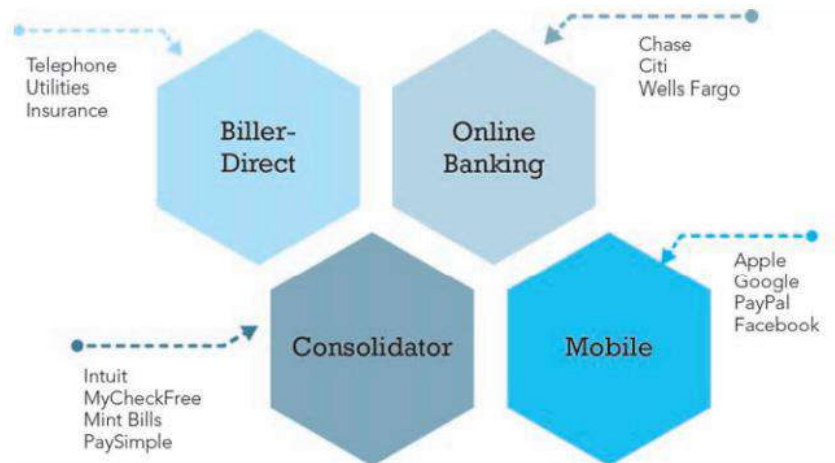
Fig. 7.4 Major players in the EBPP marketspace

7.4 CHECK YOUR PROGRESS

---

1. Write the key steps in developing a security plan.

2. Write the major e-commerce payment systems in use today.

3. Write a note on digital cash.

4. What is Electronic billing presentment and payment (EBPP) systems?

5. Who are the Major players in the EBPP marketspace?

Answers to Check Your Progress:

1. Perform a risk assessment—an assessment of the risks and points of vulnerability.

   Develop a security policy—a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets.

   Create an implementation plan—a plan that determines how you will translate the leves of acceptable risk into a set of tools, technologies, policies, and procedures.

   Create a security team—the individuals who will be responsible for ongoing maintenance, audits, and improvements.

2. **Digital cash** typically is based on an algorithm that generates unique authenticated tokens representing cash value that can be used "in the real world."

3. Online credit card transactions, PayPal, Mobile payment systems, Digital cash.

4. Electronic billing presentment and payment (EBPP) systems are a form of online payment systems for monthly bills. EBPP services allow consumers to view bills electronically and pay them through electronic funds transfers from bank or credit card accounts.

5. Major players in the EBPP marketspace include: online banking, biller-direct systems, mobile payment systems, and consolidators.

7.5 SUMMARY

In this unit, we have examined e-commerce security and payment issues. First, we will have identified the major security risks and their costs, and describe the variety of solutions currently available. Then, we have looked at the major payment methods and consider how to achieve a secure payment environment.

7.6 KEYWORDS

- **Implementation plan -** the action steps you will take to achieve the security plan goals
- **Security organization -** educates and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security
- **Access controls -** determine who can gain legitimate access to a network
- **Authentication procedures -** include the use of digital signatures, certificates of authority, and public key infrastructure
- **Security token -** physical device or software that generates an identifier that can be used in addition to or in place of a password
- **Digital cash -** an alternative payment system in which unique, authenticated tokens represent cash value
- **Virtual currency -** typically circulates within an internal virtual world community or is issued by a specific corporate entity, and used to purchase virtual goods

7.7 QUESTIONS FOR SELF-STUDY

1. What features or abilities does an intrusion prevention system use to protect a network?

2. Differentiate between the security dimension of confidentiality and the concept of online privacy.

3. What are the general technologies and tools needed by merchants and users to implement a mobile   payment system?

4. What risks do Bitcoin users face?

5. What is nonrepudiation and why is it an important dimension of e-commerce security? What technologies are used to establish nonrepudiation?

7.8 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

2. http://williamstallings.com/Cryptography/

3. https://vakilsearch.com

4. https://carnegieindia.org/

UNIT 8- E-commerce Business Strategies

STRUCTURE

8.0 Objectives

8.1 E-commerce business models

8.2 Major B2C Business models

8.3 B2B Business models

8.4 Check your progress

8.5 Summary

8.6 Keywords

8.7 Questions for self-study

8.8 References

8.0 OBJECTIVES

After studying this unit, you will be able to:

- ✓ Identify the key components of e-commerce business models.
- ✓ Describe the major B2C business models.
- ✓ Describe the major B2B business models.
- ✓ Define E-tailer
- ✓ Understand key business concepts and strategies applicable to e-commerce.

8.1 E-COMMERCE BUSINESS MODELS

A **business model** is a set of planned activities (sometimes referred to as *business processes*) designed to result in a profit in a marketplace. A business model is not always the same as a business strategy, although in some cases they are very close insofar as the business model explicitly takes into account the competitive environment. The business model is at the centre of the business plan. A **business plan** is a document that describes a firm's business model. A business plan always takes into account the competitive environment. An **e-commerce business model** aims to use and leverage the unique qualities of the Internet, the Web, and the mobile platform.

EIGHT KEY ELEMENTS OF A BUSINESS MODEL

If you hope to develop a successful business model in any arena, not just e-commerce, you must make sure that the model effectively addresses the eight elements listed in **Figure 8.1**. These elements are value proposition, revenue model, market opportunity, competitive environment, competitive advantage, market strategy, organizational development, and management team. Many writers focus on a firm's value proposition and revenue model. While these may be the most important and most easily identifiable aspects of a company's business model, the other elements are equally important when evaluating business models and plans, or when attempting to understand why a particular company has succeeded or failed. In the following sections, we describe each of the key business model elements more fully.
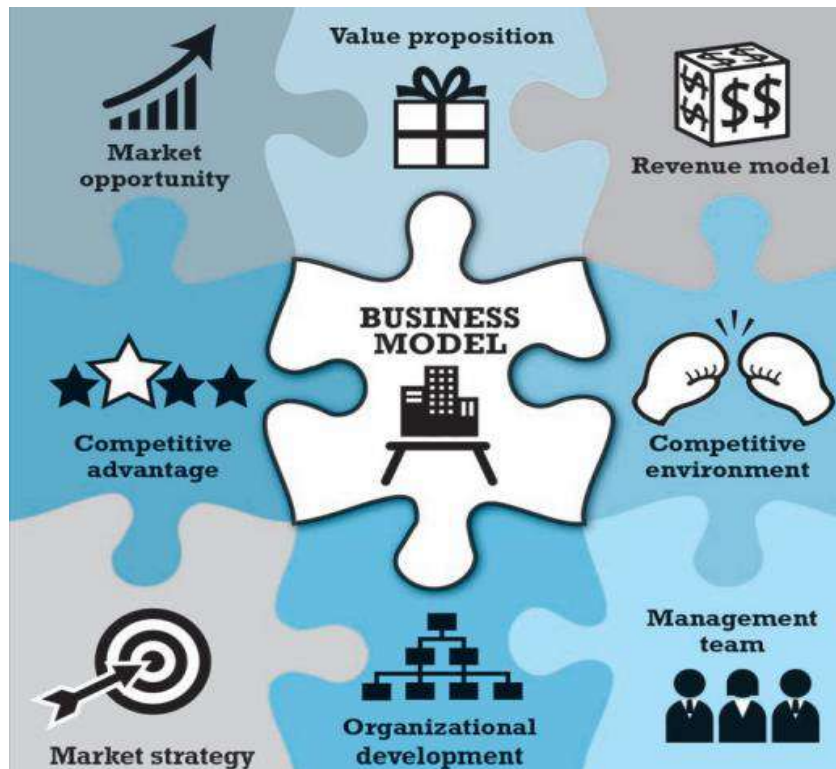

Fig. 8.1 A business model has eight key elements. Each element must be addressed if you hope to be successful.

Value Proposition

A company's value proposition is at the very heart of its business model. A **value proposition** defines how a company's product or service fulfils the needs of customers. To develop and/or

analyse a firm's value proposition, you need to understand why customers will choose to do business with the firm instead of another company and what the firm provides that other firms do not and cannot. From the consumer point of view, successful e-commerce value propositions include personalization and customization of product offerings, reduction of product search costs, reduction of price discovery costs, and facilitation of transactions by managing product delivery.

For instance, before Amazon existed, most customers personally traveled to book retailers to place an order. In some cases, the desired book might not be available, and the customer would have to wait several days or weeks, and then return to the bookstore to pick it up. Amazon makes it possible for book lovers to shop for virtually any book in print from the comfort of their home or office, 24 hours a day, and to know immediately whether a book is in stock. Amazon's Kindle takes this one step further by making e-books instantly available with no shipping wait. Amazon's primary value propositions are unparalleled selection and convenience.

Revenue Model

A firm's **revenue model** describes how the firm will earn revenue, generate profits, and produce a superior return on invested capital. We use the terms *revenue model* and *financial model* interchangeably. The function of business organizations is both to generate profits and to produce returns on invested capital that exceed alternative investments. Profits alone are not sufficient to make a company "successful". In order to be considered successful, a firm must produce returns greater than alternative investments. Firms that fail this test go out of existence. Although there are many different e-commerce revenue models that have been developed, most companies rely on one, or some combination, of the following major revenue models: advertising, subscription, transaction fee, sales, and affiliate.

In the **advertising revenue model**, a company that offers content, services, and/or products also provides a forum for advertisements and receives fees from advertisers. Companies that are able to attract the greatest viewership or that have a highly specialized, differentiated viewership and are able to retain user attention ("stickiness") are able to charge higher advertising rates. Yahoo, for instance, derives a significant amount of revenue from display and video advertising.

In the **subscription revenue model**, a company that offers content or services charges a subscription fee for access to some or all of its offerings. For instance, the digital version of *Consumer Reports* provides online and mobile access to premium content, such as detailed

ratings, reviews, and recommendations, only to subscribers, who have a choice of paying a $6.95 monthly subscription fee or a $30.00 annual fee.

Experience with the subscription revenue model indicates that to successfully overcome the disinclination of users to pay for content, the content offered must be perceived as a high-value-added, premium offering that is not readily available elsewhere nor easily replicated. Companies successfully offering content or services online on a subscription basis include eHarmony (dating services), Ancestry (genealogy research), Microsoft's

Xbox Live (video games), Pandora, Spotify, and Apple Music (music), Scribd and Amazon's Kindle Unlimited program (e-books), and Netflix and Hulu (television and movies). Recently, a number of companies have been combining a subscription revenue model with a freemium strategy. In a **freemium strategy**, the companies give away a certain level of product or services for free, but then charge a subscription fee for premium levels of the product or service. See the case study, *Freemium Takes Pandora Public*.

In the **transaction fee revenue model**, a company receives a fee for enabling or executing a transaction. For example, eBay provides an auction marketplace and receives a small transaction fee from a seller if the seller is successful in selling the item. E*Trade, a financial services provider, receives transaction fees each time it executes a stock transaction on behalf of a customer.

In the **sales revenue model**, companies derive revenue by selling goods, content, or services to customers. Companies such as Amazon, L.L.Bean, and Gap all have sales revenue models. A number of companies are also using a subscription-based sales revenue model. Birchbox, which offers home delivery of beauty products for a $10 monthly or $100 annual subscription price, is one example. Dollar Shave Club, which sells razor blades by subscription and was recently acquired by Unilever for $1 billion, is another.

In the **affiliate revenue model**, companies that steer business to an "affiliate" receive a referral fee or percentage of the revenue from any resulting sales. For example, MyPoints makes money by connecting companies with potential customers by offering special deals to its members. When they take advantage of an offer and make a purchase, members earn "points" they can redeem for freebies, and MyPoints receives a fee. Community feedback companies typically receive some of their revenue from steering potential customers to websites where they make a purchase. **Table 8.2** summarizes these major revenue models.

Table 8.2 Revenue models

REVENUE MODEL	EXAMPLES	REVENUE SOURCE
Advertising	Yahoo	Fees from advertisers in exchange for advertisements
Subscription	eHarmony Consumer Reports Online Netflix	Fees from subscribers in exchange for access to content or services
Transaction Fee	eBay E*Trade	Fees (commissions) for enabling or executing a transaction
Sales	Amazon L.L.Bean Birchbox iTunes	Sales of goods, information, or services
Affiliate	MyPoints	Fees for business referrals

Market Opportunity

The term **market opportunity** refers to the company's intended **marketspace** (i.e.,an area of actual or potential commercial value) and the overall potential financial opportunities available to the firm in that marketspace. The market opportunity is usually divided into smaller market niches. The realistic market opportunity is defined by the revenue potential in each of the market niches where you hope to compete.

For instance, let's assume you are analysing a software training company that creates online software-learning systems for sale to businesses. The overall size of the software training market for all market segments is approximately €65 billion.

The overall market can be broken down, however, into two major market segments: instructor-led training products, which comprise about 70% of the market (€45.5 billion in revenue), and computer-based training, which accounts for 30% (€19.5 billion).

There are further market niches within each of those major market segments, such as the FT 500 online training market and the small business computer-based training market. Because the firm is a start-up firm, it cannot compete effectively in the large business, online training market (about €13.65 billion). Large brand-name training firms dominate this niche. The start-up firm's

real market opportunity is to sell to the thousands of small business firms that spend about €5.85 billion on online software training. This is the size of the firm's realistic market opportunity.

Competitive Environment

A firm's **competitive environment** refers to the other companies selling similar products and operating in the same marketspace. It also refers to the presence of substitute products and potential new entrants to the market, as well as the power of customers and suppliers over your business. We discuss the firm's environment later in the chapter. The competitive environment for a company is influenced by several factors: how many competitors are active, how large their operations are, what the market share of each competitor is, how profitable these firms are, and how they price their products.

Firms typically have both direct and indirect competitors. Direct competitors are companies that sell very similar products and services into the same market segment. For example, Priceline and Travelocity, both of whom sell discount airline tickets online, are direct competitors because both companies sell identical products— cheap tickets. Indirect competitors are companies that may be in different industries but still compete indirectly because their products can substitute for one another. For instance, automobile manufacturers and airline companies operate in different industries, but they still compete indirectly because they offer consumers alternative means of transportation. CNN, a news outlet, is an indirect competitor of ESPN, not because they sell identical products, but because they both compete for consumers' time online.

The existence of a large number of competitors in any one segment may be a sign that the market is saturated and that it may be difficult to become profitable. On the other hand, a lack of competitors could signal either an untapped market niche ripe for the picking, or a market that has already been tried without success because there is no money to be made. Analysis of the competitive environment can help you decide which it is.

Competitive Advantage

Firms achieve a **competitive advantage** when they can produce a superior product and/or bring the product to market at a lower price than most, or all, of their competitors. Firms also compete

on scope. Some firms can develop global markets, while other firms can develop only a national or regional market.

Firms that can provide superior products at the lowest cost on a global basis are truly advantaged.

Firms achieve competitive advantages because they have somehow been able to obtain differential access to the factors of production that are denied to their competitors— at least in the short term. Perhaps the firm has been able to obtain very favourable terms from suppliers, shippers, or sources of labour. Or perhaps the firm has more experienced, knowledgeable, and loyal employees than any competitors. Maybe the firm has a patent on a product that others cannot imitate, or access to investment capital through a network of former business colleagues or a brand name and popular image that other firms cannot duplicate. An **asymmetry** exists whenever one participant in a market has more resources—financial backing, knowledge, information, and/or power—than other participants. Asymmetries lead to some firms having an edge over others, permitting them to come to market with better products, faster than competitors, and sometimes at lower cost.

For instance, when Apple announced iTunes, a service offering legal, downloadable individual song tracks for 99 cents a track that would be playable on any digital device with iTunes software, the company had better-than-average odds of success simply because of Apple's prior success with innovative hardware designs, and the large stable of music firms that Apple had meticulously lined up to support its online music catalog. Few competitors could match the combination of cheap, legal songs and powerful hardware to play them on.

One rather unique competitive advantage derives from being a first mover. A **first-mover advantage** is a competitive market advantage for a firm that results from being the first into a marketplace with a serviceable product or service. If first movers develop a loyal following or a unique interface that is difficult to imitate, they can sustain their first-mover advantage for long periods. Amazon provides a good example. However, in the history of technology-driven business innovation, most first movers often lack the **complementary resources** needed to sustain their advantages, and often follower firms reap the largest rewards. Indeed, many of the success stories we discuss in this book are those of companies that were slow followers—

businesses that gained knowledge from the failure of pioneering firms and entered into the market late.

Some competitive advantages are called "unfair." An **unfair competitive advantage** occurs when one firm develops an advantage based on a factor that other firms cannot purchase. For instance, a brand name cannot be purchased and is in that sense an "unfair" advantage. Brands are built upon loyalty, trust, reliability, and quality. Once obtained, they are difficult to copy or imitate, and they permit firms to charge premium prices for their products.

In **perfect markets**, there are no competitive advantages or asymmetries because all firms have access to all the factors of production (including information and knowledge) equally. However, real markets are imperfect, and asymmetries leading to competitive advantages do exist, at least in the short term. Most competitive advantages are short term, although some can be sustained for very long periods. But not forever. In fact, many respected brands fail every year.

Companies are said to **leverage** their competitive assets when they use their competitive advantages to achieve more advantage in surrounding markets. For instance, Amazon's move into the online grocery business leverages the company's huge customer database and years of e-commerce experience.

Market Strategy

No matter how tremendous a firm's qualities, its marketing strategy and execution are often just as important. The best business concept, or idea, will fail if it is not properly marketed to potential customers.

Everything you do to promote your company's products and services to potential customers is known as marketing. **Market strategy** is the plan you put together that details exactly how you intend to enter a new market and attract new customers. For instance, Twitter, YouTube, and Pinterest have a social network marketing strategy that encourages users to post their content for free, build personal profile pages, contact their friends, and build a community. In these cases, the customer becomes part of the marketing staff!

Organizational Development

Although many entrepreneurial ventures are started by one visionary individual, it is rare that one person alone can grow an idea into a multi-million dollar company. In most cases, fast-growth companies—especially e-commerce businesses—need employees and a set of business

procedures. In short, all firms—new ones in particular— need an organization to efficiently implement their business plans and strategies.

Many e-commerce firms and many traditional firms that attempt an e-commerce strategy have failed because they lacked the organizational structures and supportive cultural values required to support new forms of commerce.

Companies that hope to grow and thrive need to have a plan for **organizational development** that describes how the company will organize the work that needs to be accomplished. Typically, work is divided into functional departments, such as production, shipping, marketing, customer support, and finance. Jobs within these functional areas are defined, and then recruitment begins for specific job titles and responsibilities. Typically, in the beginning, generalists who can perform multiple tasks are hired. As the company grows, recruiting becomes more specialized. For instance, at the outset, a business may have one marketing manager. But after two or three years of steady growth, that one marketing position may be broken down into seven separate jobs done by seven individuals.

For instance, eBay founder Pierre Omidyar started an online auction site, according to some sources, to help his girlfriend trade Pez dispensers with other collectors, but within a few months the volume of business had far exceeded what he alone could handle. So he began hiring people with more business experience to help out. Soon the company had many employees, departments, and managers who were responsible for overseeing the various aspects of the organization.

Management Team

Arguably, the single most important element of a business model is the **management team** responsible for making the model work. A strong management team gives a model instant credibility to outside investors, immediate market-specific knowledge, and experience in implementing business plans. A strong management team may not be able to salvage a weak business model, but the team should be able to change the model and redefine the business as it becomes necessary.

Eventually, most companies get to the point of having several senior executives or managers. How skilled managers are, however, can be a source of competitive advantage or disadvantage. The challenge is to find people who have both the experience and the ability to apply that experience to new situations. To be able to identify good managers for a business start-up, first

consider the kinds of experiences that would be helpful to a manager joining your company. What kind of technical background is desirable? What kind of supervisory experience is necessary? How many years in a particular function should be required? What job functions should be fulfilled first: marketing, production, finance, or operations? Especially in situations where financing will be needed to get a company off the ground, do prospective senior managers have experience and contacts for raising financing from outside investors?

Table 8.3 summarizes the eight key elements of a business model and the key questions that must be answered in order to successfully develop each element.

Table 8.3 Key elements of a business model

COMPONENTS	KEY QUESTIONS
Value proposition	Why should the customer buy from you?
Revenue model	How will you earn money?
Market opportunity	What marketspace do you intend to serve, and what is its size?
Competitive environment	Who else occupies your intended marketspace?
Competitive advantage	What special advantages does your firm bring to the marketspace?
Market strategy	How do you plan to promote your products or services to attract your target audience?
Organizational development	What types of organizational structures within the firm are necessary to carry out the business plan?
Management team	What kinds of experiences and background are important for the company's leaders to have?

RAISING CAPITAL

Raising capital is one of the most important functions for a founder of a start-up business and its management team. Not having enough capital to operate effectively is a primary reason why so many start-up businesses fail. Many entrepreneurs initially "bootstrap" to get a business off the ground, using personal funds derived from savings, credit card advances, home equity loans, or from family and friends. Funds of this type are often referred to as **seed capital**. Once such funds are exhausted, if the company is not generating enough revenue to cover operating costs, additional capital will be needed. Traditional sources of capital include incubators, commercial banks, angel investors, venture capital firms, and strategic partners. One of the most important aspects of raising capital is the ability to boil down the elements of the company's business plan into an **elevator pitch**, a short two-to-three minute (about the length of an elevator ride, giving

rise to its name) presentation aimed at convincing investors to invest. **Table 8.4** lists the key elements of an elevator pitch.

Table 8.4 Key elements of an elevator pitch

ELEMENT	DESCRIPTION
Introduction	Your name and position; your company's name, and a tagline in which you compare what your company does to a well-known company. Example: "My name is X, I am the founder of Y, and we are the Uber/Amazon of Z."
Background	The origin of your idea and the problem you are trying to solve.
Industry size/market opportunity	Brief facts about the (hopefully very large) size of the market.
Revenue model/numbers/ growth metrics	Insight into your company's revenue model and results thus far, how fast it is growing, and early adopters, if there are any.
Funding	The amount of funds you are seeking and what it will help you achieve.
Exit strategy	How your investors will achieve a return on their investment.

Incubators (sometimes also referred to as accelerators) such as Rocket Internet typically provide a small amount of funding, but more importantly, also provide an array of services to start-up companies that they select to participate in their programs, such as business, technical, and marketing assistance, as well as introductions to other sources of capital. Well-known European incubator programs include INiTs (Austria), Accelerace (Denmark), Numa (Le Camping) (France), and SeedRocket (Spain).

Obtaining a loan from a commercial bank is often difficult for a start-up company without much revenue, but it may be worthwhile to investigate programs offered by the U.S. Small Business Administration, and its state or local equivalents. The advantage of obtaining capital in the form of a loan (debt) is that, although it must be repaid, it does not require an entrepreneur to give up any ownership of the company.

Angel investors are typically wealthy individuals (or a group of individuals) who invest their own money in an exchange for an equity share in the stock in the business. In general, angel

investors make smaller investments (typically €1 million or less) than venture capital firms, are interested in helping a company grow and succeed, and invest on relatively favorable terms compared to later stage investors. The first round of external investment in a company is sometimes referred to as Series A financing.

Venture capital investors typically become more interested in a start-up company once it has begun attracting a large audience and generating some revenue, even if it is not profitable. **Venture capital investors** invest funds they manage for other investors such as investment banks, pension funds, insurance companies, or other businesses, and usually want to obtain a larger stake in the business and exercise more control over the operation of the business. Venture capital investors also typically want a well-defined "exit strategy," such as a plan for an initial public offering or acquisition of the company by a more established business within a relatively short period of time (typically 3 to 7 years), that will enable them to obtain an adequate return on their investment. Venture capital investment often ultimately means that the founder(s) and initial investors will no longer control the company at some point in the future.

Crowdfunding involves using the Internet to enable individuals to collectively contribute money to support a project. The concepts behind crowdfunding have been popularized by Kickstarter and Indiegogo, but they could not be used for equity investments in for-profit companies due to various laws and regulations. In Europe, the European Commission has indicated an intention to support crowdfunding and has issued several reports aimed at promoting understanding this form of financing at the EU level and laying the groundwork for possible future action, as well as a guide to crowdfunding for small and medium enterprises as part of its effort to inform citizens about both its benefits and risks.

CATEGORIZING E-COMMERCE BUSINESS MODELS: SOME DIFFICULTIES

There are many e-commerce business models, and more are being invented every day. The number of such models is limited only by the human imagination, and our list of different business models is certainly not exhaustive. However, despite the abundance of potential models, it is possible to identify the major generic types (and subtle variations) of business models that have been developed for the e-commerce arena and describe their key features. It is important to realize, however, that there is no one correct way to categorize these business models.

Our approach is to categorize business models according to the different major e-commerce sectors—B2C and B2B—in which they are utilized. You will note, however, that fundamentally similar business models may appear in more than one sector. For example, the business models of online retailers (often called e-tailers) and e-distributors are quite similar. However, they are distinguished by the market focus of the sector in which they are used. In the case of e-tailers in the B2C sector, the business model focuses on sales to the individual consumer, while in the case of the e-distributor, the business model focuses on sales to another business. Many companies use a variety of different business models as they attempt to extend into as many areas of e-commerce as possible.

A business's technology platform is sometimes confused with its business model. For instance, "mobile e-commerce" refers to the use of mobile devices and cellular and wide area networks to support a variety of business models. Commentators sometimes confuse matters by referring to mobile e-commerce as a distinct business model, which it is not. All of the basic business models we discuss below can be implemented on both the traditional Internet/Web and mobile platforms. Likewise, although they are sometimes referred to as such, social e-commerce and local e-commerce are not business models in and of themselves, but rather subsectors of B2C and B2B e-commerce in which different business models can operate.

You will also note that some companies use multiple business models. For instance, Amazon has multiple business models: it is an e-retailer, content provider, market creator, e-commerce infrastructure provider, and more. eBay is a market creator in the B2C and C2C e-commerce sectors, using both the traditional Internet/ Web and mobile platforms, as well as an e-commerce infrastructure provider.

Firms often seek out multiple business models as a way to leverage their brands, infrastructure investments, and assets developed with one business model into new business models.

Finally, no discussion of e-commerce business models would be complete without mention of a group of companies whose business model is focused on providing the infrastructure necessary for e-commerce companies to exist, grow, and prosper. These are the e-commerce enablers. They provide the hardware, operating system software, networks and communications technology, applications software, web design, consulting services, and other tools required for e-commerce.

While these firms may not be conducting e-commerce per se (although in many instances, e-commerce in its traditional sense is in fact one of their sales channels), as a group they have perhaps profited the most from the development of e-commerce.

8.2 MAJOR B2C BUSINESS MODELS

Business-to-consumer (B2C) e-commerce, in which online businesses seek to reach individual consumers, is the most well-known and familiar type of e-commerce. **Table 8.5** illustrates the major business models utilized in the B2C arena.

Table 8.5 B2C business model

BUSINESS MODEL	VARIATIONS	EXAMPLES	DESCRIPTION	REVENUE MODELS
E-tailer	Virtual Merchant	Amazon Blue Nile Bluefly	Online version of retail store, where customers can shop at any hour of the day or night without leaving their home or office	Sales of goods
	Bricks-and-Clicks	Walmart Sears	Online distribution channel for a company that also has physical stores	Sales of goods
	Catalog Merchant	L.L.Bean LillianVernon	Online version of direct mail catalog	Sales of goods
	Manufacturer-Direct	Dell Mattel	Manufacturer uses online channel to sell direct to customer	Sales of goods
Community Provider		Facebook LinkedIn Twitter Pinterest	Sites where individuals with particular interests, hobbies, common experiences, or social networks can come together and "meet" online	Advertising, subscription, affiliate referral fees
Content Provider		Wall Street Journal CNN ESPN Netflix Apple Music	Offers customers newspapers, magazines, books, film, television, music, games, and other forms of online content	Advertising, subscription fees, sales of digital goods
Portal	Horizontal/General	Yahoo AOL MSN Facebook	Offers an integrated package of content, search, and social network services: news, e-mail, chat, music downloads, video streaming, calendars, etc. Seeks to be a user's home base	Advertising, subscription fees, transaction fees
	Vertical/Specialized (Vortal)	Sailnet	Offers services and products to specialized marketplace	Advertising, subscription fees, transaction fees
	Search	Google Bing Ask	Focuses primarily on offering search services	Advertising, affiliate referral
Transaction Broker		E*Trade Expedia Monster Travelocity Orbitz	Processors of online sales transactions, such as stockbrokers and travel agents, that increase customers' productivity by helping them get things done faster and more cheaply	Transaction fees
Market Creator		eBay Etsy Amazon Priceline	Businesses that use Internet technology to create markets that bring buyers and sellers together	Transaction fees
Service Provider		VisaNow Wave RocketLawyer	Companies that make money by selling users a service, rather than a product	Sales of services

E-TAILER

Online retail stores, often called **e-tailers**, come in all sizes, from giant Amazon to tiny local stores. E-tailers are similar to the typical bricks-and-mortar storefront, except that customers only have to connect to the Internet or use their smartphone to place an order. Some e-tailers, which are referred to as "bricks-and-clicks," are subsidiaries or divisions of existing physical stores and carry the same products. REI, JCPenney, Barnes & Noble, Walmart, and Staples are examples of companies with complementary

online stores. Others, however, operate only in the virtual world, without any ties to physical locations. Amazon, Blue Nile, and Bluefly are examples of this type of e-tailer.

Several other variations of e-tailers—such as online versions of direct mail catalogs, online malls, and manufacturer-direct online sales—also exist.

Given that the overall global retail market in 2016 is estimated to be around €20.9 trillion, the market opportunity for e-tailers is very large. Every Internet and smartphone user is a potential customer. Customers who feel time-starved are even better prospects, because they want shopping solutions that will eliminate the need to drive to the mall or store (Bellman, Lohse, and Johnson, 1999). The e-tail revenue model is product-based, with customers paying for the purchase of a particular item.

This sector, however, is extremely competitive. Because **barriers to entry** (the total cost of entering a new marketplace) into the e-tail market are low, tens of thousands of small e-tail shops have sprung up. Becoming profitable and surviving is very difficult, however, for e-tailers with no prior brand name or experience. The e-tailer's challenge is differentiating its business from existing competitors.

Companies that try to reach every online consumer are likely to deplete their resources quickly. Those that develop a niche strategy, clearly identifying their target market and its needs, are best prepared to make a profit. Keeping expenses low, selection broad, and inventory controlled is key to success in e-tailing, with inventory being the most difficult to gauge.

COMMUNITY PROVIDER

Although community providers are not a new phenomenon, the Internet has made such sites for like-minded individuals to meet and converse much easier, without the limitations of geography and time to hinder participation. **Community providers** create an online environment where people with similar interests can transact (buy and sell goods); share interests, photos, videos; communicate with like-minded people; receive interest-related information; and even play out fantasies by adopting online personalities called avatars. Facebook, LinkedIn, Twitter, and Pinterest, and hundreds of other smaller, niche social networks all offer users community-building tools and services.

The basic value proposition of community providers is to create a fast, convenient, one-stop site where users can focus on their most important concerns and interests, share the experience with

friends, and learn more about their own interests. Community providers typically rely on a hybrid revenue model that includes subscription fees, sales revenues, transaction fees, affiliate fees, and advertising fees from other firms that are attracted by a tightly focused audience.

Community providers make money from advertising and through affiliate relationships with retailers. Some of the oldest online communities are The Well, which provides a forum for technology and Internet-related discussions, and The Motley Fool, which provides financial advice, news, and opinions. The Well offers various membership plans ranging from $10 to $15 a month. Motley Fool supports itself through ads and selling products that start out "free" but turn into annual subscriptions.

Consumers' interest in communities is mushrooming. Community is, arguably, the fastest growing online activity. While many community providers have had a difficult time becoming profitable, many have succeeded over time, with advertising as their main source of revenue. Both the very large social networks such as Facebook, Twitter, and LinkedIn, as well as niche social networks with smaller dedicated audiences, are ideal marketing and advertising territories. Traditional online communities such as The Motley Fool and WebMD (which provides medical information to members) find that the breadth and depth of knowledge offered is an important factor. Community members frequently request knowledge, guidance, and advice. Lack of experienced personnel can severely hamper the growth of a community, which needs facilitators and managers to keep discussions on course and relevant. For the newer community social networks, the most important ingredients of success appear to be ease and flexibility of use, and a strong customer value proposition. For instance, Facebook leapfrogged over its rival MySpace by encouraging the development of third-party revenue-producing applications. Online communities benefit significantly from offline word-of-mouth, viral marketing. Online communities tend to reflect offline relationships. When your friends say they have a profile on Facebook and ask you to "friend" them, you are encouraged to build your own online profile.

CONTENT PROVIDER

Content providers distribute information content, such as digital video, music, photos, text, and artwork. Content providers can make money via a variety of different revenue models, including advertising, subscription fees, and sales of digital goods.

For instance, in the case of Spotify, a monthly subscription fee provides users with access to millions of music tracks. Other content providers, such as the *Financial Times* online newspaper, *Harvard Business Review*, and many others, charge customers for content downloads in addition to, or in place of, a subscription fee.

Of course, not all online content providers charge for their information: just look at the websites or mobile apps for the BBC, Football365, and Silicon.co.uk, and the online versions of many newspapers and magazines. Users can access news and information without paying a cent, although sometimes they may be required to register as a member. These popular online content providers make money in other ways, such as through advertising and partner promotions. Increasingly, however, "free content" may be limited to headlines and text, whereas premium content—in-depth articles or videos—is sold for a fee.

Generally, the key to becoming a successful content provider is owning the content. Traditional owners of copyrighted content—publishers of books and newspapers, broadcasters of radio and television content, music publishers, and movie studios—have powerful advantages over newcomers who simply offer distribution channels and must pay for content, often at very high prices.

Some content providers, however, do not own content, but syndicate (aggregate) and then distribute content produced by others. *Syndication* is a major variation of the standard content provider model. Aggregators, who collect information from a wide variety of sources and then add value to that information through post-aggregation services, are another variation. For instance, Shopzilla collects information on the prices of thousands of goods online, analyzes the information, and presents users with tables showing the range of prices and links to the sites where the products can be purchased. Shopzilla adds value to content it aggregates, and resells this value to advertisers.

Any e-commerce start-up that intends to make money by providing content is likely to face difficulties unless it has a unique information source that others cannot access. For the most part, this business category is dominated by traditional content providers. The *Insight on Technology* case, *Will the Connected Car Become the Next Hot Entertainment Vehicle?,* discusses how changes in Internet technology are driving the development of new business models in the online content market.

PORTAL

Portals such as Yahoo, MSN, and AOL offer users powerful search tools as well as an integrated package of content and services, such as news, e-mail, instant messaging, calendars, shopping, music downloads, video streaming, and more, all in one place. Initially, portals sought to be viewed as "gateways" to the Internet. Today, however, the portal business model is to be a destination. They are marketed as places where consumers will hopefully stay a long time to read news, find entertainment, and meet other people (think of destination resorts). Portals do not sell anything directly—or so it seems—and in that sense they can present themselves as unbiased. Portals generate revenue primarily by charging advertisers for ad placement, collecting referral fees for steering customers to other sites, and charging for premium services.

Although there are numerous portals/search engines, the top five (Google, Microsoft's Bing, Yahoo, Ask, and AOL) in the United States gather more than 95% of U.S. search engine traffic because of their superior brand recognition. Many of the top portal/search engines were among the first to appear on the Web and therefore had first-mover advantages. Being first confers an advantage because customers come to trust a reliable provider and experience switching costs if they change to late arrivals in the market. By garnering a large chunk of the marketplace, first movers—just like a single telephone network—can offer customers access to commonly shared ideas, standards, and experiences.

The traditional portals have company: Facebook and other social networks are now the initial start or home page (portal) for millions of Internet users. Yahoo, AOL, and others like them are considered to be horizontal portals because they define their marketspace to include all users of the Internet. Vertical portals (sometimes called vortals) attempt to provide similar services as horizontal portals, but are focused around a particular subject matter or market segment. For instance, Sailnet focuses on the world's sailing community, and provides sailing news, articles, discussion groups, free e-mail, and a retail store. Although the total number of vortal users may be much lower than the number of portal users, if the market segment is attractive enough, advertisers are willing to pay a premium in order to reach a targeted audience. Also, visitors to specialized niche vortals spend more money than the average Yahoo visitor. Google and Ask can also be considered portals of a sort, but focus primarily on offering search and advertising services.

They generate revenues primarily from search engine advertising sales and also from affiliate referral fees.

TRANSACTION BROKER

Companies that process transactions for consumers normally handled in person, by phone, or by mail are **transaction brokers**. The largest industries using this model are financial services, travel services, and job placement services. The online transaction broker's primary value propositions are savings of money and time. In addition, most transaction brokers provide timely information and opinions. Companies such as Monster offer job searchers a national marketplace for their talents and employers a national resource for that talent. Both employers and job seekers are attracted by the convenience and currency of information. Online stock brokers charge commissions that are considerably less than traditional brokers, with many offering substantial deals, such as cash and a certain number of free trades, to lure new customers.

Given rising consumer interest in financial planning and the stock market, the market opportunity for online transaction brokers appears to be large. However, while millions of customers have shifted to online brokers, some are still wary about switching from their traditional broker who provides personal advice and a brand name.

Fears of privacy invasion and the loss of control over personal financial information also contribute to market resistance. Consequently, the challenge for online brokers is to overcome consumer fears by emphasizing the security and privacy measures in place, and, like physical banks and brokerage firms, providing a broad range of financial services and not just stock trading.

Transaction brokers make money each time a transaction occurs. Each stock trade, for example, nets the company a fee, based on either a flat rate or a sliding scale related to the size of the transaction. Attracting new customers and encouraging them to trade frequently are the keys to generating more revenue for these companies.

Travel sites generate commissions from travel bookings and job sites generate listing fees from employers up front, rather than charging a fee when a position is filled.

MARKET CREATOR

Market creators build a digital environment in which buyers and sellers can meet, display and search for products and services, and establish prices. Prior to the Internet and the Web, market creators relied on physical places to establish a market. Beginning with the medieval marketplace

and extending to today's New York Stock Exchange, a market has meant a physical space for transacting business. There were few private digital network marketplaces prior to the Web. The Web changed this by making it possible to separate markets from physical space. Prime examples are Priceline, which allows consumers to set the price they are willing to pay for various travel accommodations and other products (sometimes referred to as a reverse auction), and eBay, the online auction site utilized by both businesses and consumers. Market creators make money by either charging a percentage of every transaction made, or charging merchants for access to the market.

For example, eBay's auction business model is to create a digital environment for buyers and sellers to meet, agree on a price, and transact. This is different from transaction brokers who actually carry out the transaction for their customers, acting as agents in larger markets. At eBay, the buyers and sellers are their own agents. Each sale on eBay nets the company a commission based on the percentage of the item's sales price, in addition to a listing fee. eBay is one of the few e-commerce companies that has been profitable virtually from the beginning. Why? One answer is that eBay has no inventory or production costs. It is simply a middleman.

The market opportunity for market creators is potentially vast, but only if the firm has the financial resources and marketing plan to attract sufficient sellers and buyers to the marketplace. As of June 30, 2016, eBay had more than 164 million active buyers, and this makes for an efficient market (eBay Inc., 2016). There are many sellers and buyers for each type of product, sometimes for the same product, for example, laptop computer models. Many other digital auctions have sprung up in smaller, more specialized vertical market segments such as jewelry and automobiles.

Uber, Airbnb, and Lyft are another example of the market creator business model (although they could also be categorized as service providers). On-demand service companies (also sometimes called sharing economy companies) are market creators that have developed online platforms that allow people to sell services, such as transportation or spare rooms, in a marketplace that operates in the cloud and relies on the Web or smartphone apps to conduct transactions. It is important to note that, although referred to as sharing economy or mesh economy companies, these companies do not in fact share resources. Users of these services are either selling something or buying something, and the companies produce revenue by extracting fees for each transaction. However, they do unlock the economic value in spare resources (personal cars and

rooms) that might otherwise have been lost. In the process they have created huge online markets. For instance, Uber (founded in 2009) currently operates in over 480 cities in 69 countries around the world. Airbnb, founded in 2008, operates in more than 190 countries and 34,000 cities, lists over 2 million rooms available for rent, and has had over 60 million people use its services to book a room. Airbnb has raised around $2.4 billion in funding thus far and is valued at $30 billion; Uber has raised over $12.5 billion and is valued at around $68 billion.

SERVICE PROVIDER

While e-tailers sell products online, **service providers** offer services online. There's been an explosion in online services that is often unrecognized. Photo sharing, video sharing, and user-generated content (in blogs and social networks) are all services provided to customers. Google has led the way in developing online applications such as Google Maps, Google Docs, and Gmail. Other personal services such as online medical bill management, financial and pension planning, and travel recommendation are showing strong growth.

Service providers use a variety of revenue models. Some charge a fee, or monthly subscriptions, while others generate revenue from other sources, such as through advertising and by collecting personal information that is useful in direct marketing.

Many service providers employ a freemium revenue model, in which some basic services are free, but others require the payment of additional charges. Much like retailers who trade products for cash, service providers trade knowledge, expertise, and capabilities for revenue. Obviously, some services cannot be provided online. For example, dentistry, plumbing, and car repair cannot be completed via the Internet. However, online arrangements can be made for these services. Online service providers may offer computer services, such as data storage (Dropbox and Carbonite), provide legal services (Rocket Lawyer), or accounting or bookkeeping services (Wave, Bench). Grocery shopping sites such as Fresh Direct and Peapod are also providing services. To complicate matters a bit, most financial transaction brokers (described previously) provide services such as college tuition and pension planning. Travel brokers also provide vacation-planning services, not just transactions with airlines and hotels. Indeed, mixing services with your products is a powerful business strategy pursued by many hard-goods companies (for example, warranties are services).

The basic value proposition of service providers is that they offer consumers valuable, convenient, time-saving, and low-cost alternatives to traditional service providers or provide services that are truly unique. Where else can you search billions of web pages, or share photos with as many people instantly? Research has found, for instance, that a major factor in predicting online buying behaviour is *time starvation*.

Time-starved people tend to be busy professionals who work long hours and simply do not have the time to pick up packages, buy groceries, send photos, or visit with financial planners. The market opportunity for service providers is as large as the variety of services that can be provided and potentially is much larger than the market opportunity for physical goods. We live in a service-based economy and society; witness the growth of fast-food restaurants, package delivery services, and wireless cellular phone services. Consumers' increasing demand for convenience products and services bodes well for current and future online service providers.

Marketing of service providers must allay consumer fears about hiring a vendor online, as well as build confidence and familiarity among current and potential customers. Building confidence and trust is critical for service providers just as it is for retail product merchants.

8.3 B2B BUSINESS MODELS

Earlier we noted that business-to-business (B2B) e-commerce, in which businesses sell to other businesses, is more than 10 times the size of B2C e-commerce, even though most of the public attention has focused on B2C. For instance, it is estimated that revenues for all types of B2B e-commerce worldwide will total around €19.8 trillion in 2016, compared to about €2.35 trillion for retail and travel-related B2C e-commerce. Clearly, most of the revenues in e-commerce involve B2B e-commerce. Much of this activity is unseen and unknown to the average consumer. **Table 8.1** lists the major business models utilized in the B2B arena.

Table 8.1 B2B business models

BUSINESS MODEL	EXAMPLES	DESCRIPTION	REVENUE MODEL
(1) NET MARKETPLACE			
E-distributor	Grainger Amazon Business	Single-firm online version of retail and wholesale store; supply maintenance, repair, operation goods; indirect inputs	Sales of goods
E-procurement	Ariba Supplier Network PerfectCommerce	Single firm creating digital markets where sellers and buyers transact for indirect inputs	Fees for market-making services, supply chain management, and fulfillment services
Exchange	Go2Paper	Independently owned vertical digital marketplace for direct inputs	Fees and commissions on transactions
Industry Consortium	TheSeam SupplyOn	Industry-owned vertical digital market open to select suppliers	Fees and commissions on transactions
(2) PRIVATE INDUSTRIAL NETWORK			
	Walmart Procter & Gamble	Company-owned network that coordinates supply chains with a limited set of partners	Cost absorbed by network owner and recovered through production and distribution efficiencies

E-DISTRIBUTOR

Companies that supply products and services directly to individual businesses are **e-distributors**. W.W. Grainger, for example, is the largest distributor of maintenance, repair, and operations (MRO) supplies. In the past, Grainger relied on catalog sales and physical distribution centers in metropolitan areas. Its catalog of equipment went online in 1995. In 2015, Grainger's e-commerce platform, which includes websites and mobile apps, produced $3.3 billion in sales (41% of its total revenue) for the company.

E-distributors are owned by one company seeking to serve many customers. However, as with exchanges (described on the next page), critical mass is a factor. With e-distributors, the more products and services a company makes available, the more attractive it is to potential customers. One-stop shopping is always preferable to having to visit numerous sites to locate a particular part or product.

E-PROCUREMENT

Just as e-distributors provide products to other companies, **e-procurement firms** create and sell access to digital markets. Firms such as Ariba, for instance, have created software that helps large firms organize their procurement process by creating minidigital markets for a single firm. Ariba creates custom-integrated online catalogs (where supplier firms can list their offerings) for purchasing firms. On the sell side, Ariba helps vendors sell to large purchasers by providing

software to handle catalog creation, shipping, insurance, and finance. Both the buy and sell side software is referred to generically as "value chain management" software.

B2B service providers make money through transaction fees, fees based on the number of workstations using the service, or annual licensing fees. They offer purchasing firms a sophisticated set of sourcing and supply chain management tools that permit firms to reduce supply chain costs. In the software world, firms such as Ariba are sometimes also called Software as a Service (SaaS) or Platform as a Service (PaaS) providers; they are able to offer firms much lower costs of software by achieving scale economies. **Scale economies** are efficiencies that result from increasing the size of a business, for instance, when large, fixed-cost production systems (such as factories or software systems) can be operated at full capacity with no idle time. In the case of software, the marginal cost of a digital copy of a software program is nearly zero, and finding additional buyers for an expensive software program is exceptionally profitable.

This is much more efficient than having every firm build its own supply chain management system, and it permits firms such as Ariba to specialize and offer their software to firms at a cost far less than the cost of developing it.

EXCHANGES

Exchanges have garnered most of the B2B attention and early funding because of their potential market size even though today they are a small part of the overall B2B picture. An **exchange** is an independent digital marketplace where hundreds of suppliers meet a smaller number of very large commercial purchasers. Exchanges are owned by independent, usually entrepreneurial startup firms whose business is making a market, and they generate revenue by charging a commission or fee based on the size of the transactions conducted among trading parties. They usually serve a single vertical industry such as steel, polymers, or aluminum, and focus on the exchange of direct inputs to production and short-term contracts or spot purchasing. For buyers, B2B exchanges make it possible to gather information, check out suppliers, collect prices, and keep up to date on the latest happenings all in one place. Sellers, on the other hand, benefit from expanded access to buyers. The greater the number of sellers and buyers, the lower the sales cost and the higher the chances of making a sale. The ease, speed, and volume of transactions are summarily referred to as *market liquidity*.

In theory, exchanges make it significantly less expensive and time-consuming to identify potential suppliers, customers, and partners, and to do business with each other. As a result, they can lower transaction costs—the cost of making a sale or purchase.

Exchanges can also lower product costs and inventory-carrying costs—the cost of keeping a product on hand in a warehouse. B2B exchanges have had a difficult time convincing thousands of suppliers to move into singular digital markets where they face powerful price competition, and an equally difficult time convincing businesses to change their purchasing behaviour away from trusted long-term trading partners. As a result, the number of exchanges has fallen significantly.

INDUSTRY CONSORTIA

Industry consortia are industry-owned vertical marketplaces that serve specific industries, such as the automobile, aerospace, chemical, floral, or logging industries. In contrast, horizontal marketplaces sell specific products and services to a wide range of companies. Vertical marketplaces supply a smaller number of companies with products and services of specific interest to their industry, while horizontal marketplaces supply companies in different industries with a particular type of product and service, such as marketing-related, financial, or computing services. For example, SupplyOn, founded in 2000 and owned by industrial giants Bosch (one of the world's largest suppliers of automotive components), Continental (a leading automotive manufacturing company), and Schaeffler (a global manufacturer of various types of bearings), among others, provides a shared supply chain collaboration platform for companies in various manufacturing industries. In 2016, in addition to its shareholders, its customers include Airbus, BMW, BorgWarner, Siemens, Thales, and many other major global manufacturing companies.

Industry consortia have tended to be more successful than independent exchanges in part because they are sponsored by powerful, deep-pocketed industry players, and also because they strengthen traditional purchasing behavior rather than seek to transform it.

PRIVATE INDUSTRIAL NETWORKS

A **private industrial network** (sometimes referred to as a private trading exchange or PTX) is a digital network designed to coordinate the flow of communications among firms engaged in business together. The network is owned by a single large purchasing firm. Participation is by invitation only to trusted long-term suppliers of direct inputs. These networks typically evolve

out of a firm's own enterprise resource planning (ERP) system, and are an effort to include key suppliers in the firm's own business decision making. For instance, Walmart operates one of the largest private industrial networks in the world for its suppliers, who on a daily basis use Walmart's network to monitor the sales of their goods, the status of shipments, and the actual inventory level of their goods.

8.4 CHECK YOUR PROGRESS

1. Identify the key components of e-commerce business models.
2. List the major B2C business models.
3. List the major B2B business models.
4. What is a freemium strategy?
5. What is seed capital?

Answers to Check Your Progress:

1. Value proposition, Revenue model, Market opportunity, Competitive environment, Competitive advantage, Market strategy, Organizational development, Management team
2. Portal, E-tailer, Content provider, Transaction broker, Market creator, Service provider, Community provider
3. E-distributor, E-procurement, Exchange, Industry consortium, Private industrial network
4. **freemium strategy -** companies give away a certain level of product or services for free, but then charge a subscription fee for premium levels of the product or service
5. **seed capital -** typically, an entrepreneur's personal funds derived from savings, credit card advances, home equity

8.5 SUMMARY

Thousands of firms have discovered that they can spend other people's invested capital much faster than they can get customers to pay for their products or services. In most instances of failure, the business model of the firm is faulty from the beginning. In contrast, successful e-commerce firms have business models that are able to leverage the unique qualities of the Internet, the Web, and the mobile platform, provide customers real value, develop highly effective and efficient operations, avoid legal and social entanglements that can harm the firm,

and produce profitable business results. In addition, successful business models must scale. The business must be able to achieve efficiencies as it grows in volume. But what is a business model, and how can you tell if a firm's business model is going to produce a profit? In this unit, we focused on business models and basic business concepts that you must be familiar with in order to understand e-commerce.

8.6 KEYWORDS

- **Business model -** a set of planned activities designed to result in a profit in a marketplace
- **Business plan -** a document that describes a firm's business model
- **E-commerce business model -** a business model that aims to use and leverage the unique qualities of the Internet, the Web, and the mobile platform
- **value proposition -** defines how a company's product or service fulfils the needs of customers
- **revenue model -** describes how the firm will earn revenue, produce profits, and produce a superior return on invested capital
- **advertising revenue model -** a company provides a forum for advertisements and receives fees from advertisers
- **subscription revenue model -** a company offers its users content or services and charges a subscription fee for access to some or all of its offerings
- **freemium strategy -** companies give away a certain level of product or services for free, but then charge a subscription fee for premium levels of the product or service
- **transaction fee revenue model -** a company receives a fee for enabling or executing a transaction

8.7 QUESTIONS FOR SELF-STUDY

1. Identify and describe the business model element that specifies how the company's product will fulfil the needs of its customers.
2. How can e-commerce technologies be used to improve a firm's value web?
3. What revenue models do content providers use, and what is the key to becoming a successful content provider?

4. What disadvantages are faced by "first-mover" companies entering a marketspace?

5. Define market opportunity and describe how you would determine a new company's realistic market opportunity.

8.8 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

2. http://williamstallings.com/Cryptography/

Karnataka State Open University
Mukthagangothri, Mysore – 570 006.
Dept. of Studies and Research in Management

MBA IT Specialization
III Semester

E-commerce

Block 3

Karnataka State Open University

Mukthagangothri, Mysore – 570 006.

Dept. of Studies and Research in Management

MBA. IT Specialization

III Semester

E-commerce

BLOCK 3

BLOCK 3 INTRODUCTION

E-commerce refers to aspects of online business involving exchanges among customers, business partners and vendors. E-commerce has increased the speed and ease with which business can be transacted today, resulting in intense competition between enterprises. Companies are at the crossroads, with just two vistas ahead of them—either go online or go out of business. Once the choice of online business is made, further roadblocks are encountered: which business model to adopt; which management strategies and tactics will make business successful? How to explore opportunities, understand limitations, and issues? The solution is to gain a deeper insight into the e-commerce strategies.

This block consists of 4 units and is organized as follows:

Unit 9 : Traditional Marketing, The Uniqueness of the Web, Maintaining a Website, Aggregate Metrics for E-business Sites, Online Marketing, How Should Buyers Pay Online?, Advantages of Online Marketing, Various Businesses that Can Flourish on the Internet, E-advertising, Various Means of Advertising, Personalized Online Communications, Measuring the Effectiveness of E-advertising

Unit 10: Information System Security, Security on the Internet, Security Incidents on the Internet, How Vulnerable are The Internet Sites?, Network and Website Security, Security Audits and Penetration Testing.

Unit 11: The Firewall Concept, Firewall Components, What Should a Firewall Contain?, Benefits of an Internet, Defining an Enterprise-wide Security Framework, Understanding the Security Framework, Secure Physical Infrastructure, Information Security Environment in India

Unit 12: E-payment systems, The Mobile Payments, Classification of New Payment Systems, Micropayment Systems, Properties of Electronic Cash (e-Cash), e-Cash in Action, Cheque Payment Systems on the Internet, Designing e-Payment Systems, Digital Signature

UNIT 9: E-CUSTOMER RELATIONSHIP MANAGEMENT

Structure

9.0 Objectives

9.1 Introduction

9.2 Traditional Marketing

9.3 The Uniqueness of the Web

9.4 Maintaining a Website

9.5 Aggregate Metrics for E-business Sites

9.6 Online Marketing

9.7 How Should Buyers Pay Online?

9.8 Advantages of Online Marketing

9.9 Various Businesses that Can Flourish on the Internet

9.10 E-advertising

9.11 Various Means of Advertising

9.12 Personalized Online Communications

9.13 Measuring the Effectiveness of E-advertising

9.14 Check Your Progress

9.15 Summary

9.16 Keywords

9.17 Questions for Self Study

9.18 References

9.0 OBJECTIVES

After studying this unit, you will be able to:

- Give an account on Traditional Marketing
- Analyze the Uniqueness of the Web
- Find Aggregate Metrics for E-business Sites
- Give an account on Online Marketing with its advantages
- Study steps how Buyers Pay Online
- Enumerate different Businesses that Can Flourish on the Internet

- Give an account on E-advertising and its various means
- Measuring the Effectiveness of E-advertising

9.1 INTRODUCTION

Nearly 2 billion people around the world are expected to tap into the Internet, by 2011. With the Internet growing at an astonishing pace in recent years, marketers around the world are racing to take advantage of its interactive nature, to communicate and foster exchanges and relationships with customers, suppliers, and the public. Also, the amount of transactions on the Internet are increasing exponentially.

The accelerating confluence of traditional print and broadcast media with new digital media like the Internet has created dynamic new channels for marketers. At the same time, advertisers have begun demanding greater economic efficiency in reaching target customers. The Internet is changing the design and implementation of marketing strategies. This dynamic technology provides marketers with efficient and powerful methods of designing, promoting, and distributing products, conducting research, and gathering market information.

E-marketing can include any Internet-based promotion, including websites, targeted e-mail, Internet bulletin boards, sites where customers can dial-in and download files, and so on.

9.2 TRADITIONAL MARKETING

If marketing is whatever you do to promote the sale of your products or services, then it should include:

1. Market research—from competitive information-gathering to industry awareness to soliciting customer opinions and preferences
2. Publicity from press releases to the positioning of your company and its offerings in the marketplace
3. Advertising that is text-based (classifieds) and graphic-based (display)
4. Sales, including distribution and merchandising
5. Customer service and customer support.

Traditional marketing seems to fall far short of three features. There are certain problems associated with it, which can be listed as follows:

1. Traditional marketing is often expensive. It can cost a lot of money to produce and print brochures, product sheets, and catalogues. It is also expensive to keep support personnel on hand to answer inquiries from customers, and it costs a lot of money in postage and shipping fees to send information to prospective customers.

2. Traditional marketing can be a very time-consuming process. Mistakes have to be corrected; you have to go back to the ad agency or printer to revise, add or delete, and you often have to wait for months for an ad that you have placed to appear in a publication.

3. Traditional marketing often has a "hit and miss" quality. Marketers often send out bulk of mails to customers and yet receive a tiny response. Moreover they feel that they do not cater to the taste of the consumers or rather that they do not come across the right consumer.

Businesses have always made their presence felt by establishing shops, factories, warehouses, and office buildings. An organization's presence is the public image it presents to its stakeholders. The stakeholders of a firm include its customers, suppliers, employees, stockholders, neighbours, and the general public. Companies tend not to worry much about the image they project until they make their mark. Initially, they focus only on their survival. On the Web, making one's presence felt is much more important. The only contact that customers and other stakeholders have with a firm on the Web might be its website or its Web pages. Therefore, creating an effective and appealing Web page is essential even for the smallest and the newest firm operating on the Web.

9.3 THE UNIQUENESS OF THE WEB

When firms first started creating websites in the mid 1990s, they often built simple sites that conveyed basic information about their businesses. Few firms conducted any market research to see what kinds of things potential visitors might want to obtain from these websites, and even fewer considered what business infrastructure improvement would be needed to keep the site alive. For example, few firms had e-mail address links on their sites. Those firms that did include an e-mail link, often understaffed the department responsible for answering visitors' e-mail messages. Thus, many of the visitors' e-mails remained unanswered. The failure to understand how the Web is different from other presence-building media is one reason why so many

businesses fail to achieve their Web objectives. The scenario has changed for the better in the recent times with the prominence of Internet technologies over others.

Now, most of the websites that are designed to create an organization's presence in the web medium include links to a fairly standard information set. The sites give visitors easy access to its history, statements about its objectives or mission, information about products or services offered, financial information, and means of communication with the organization. Such sites achieve varying levels of success, depending largely on how they convey these information. Presentation is important, so also is realizing the fact that the Web is an interactive medium.

9.4 MAINTAINING A WEBSITE

Creating a website that meets the needs of visitors with such a wide range of motivations can be challenging. Not only do website visitors arrive with different needs, but also they arrive with different experience and expectation levels. In addition to the problems posed by the diversity of visitor characteristics, technology issues can also arise. These website visitors will be connected to the Internet through a variety of communication channels that provide different bandwidths and data transmission speeds. They also will be using several different Web browsers. Even those who are using the same browser can have a variety of configurations. The wide array of browser add-in and plug-in softwares adds yet another dimension to visitor variability. Considering and addressing the implications of these many visitor characteristics when building a website can help convert those visitors into customers.

One of the best ways to accommodate a broad range of visitor needs is to build flexibility into the website's interface. Many sites offer separate versions with and without frames and give visitors the option of choosing either one. Some sites offer a text-only version. As researchers at the Trace Center (http://trace.wisc.edu/) note, this can be an especially important feature for visually impaired visitors who use special browser software, such as the IBM Home Page Reader, to access website content. The W3C Web Accessibility Initiative site includes a number of useful links to information regarding these issues.

If the site design uses graphics, the site can give the visitor the option to select smaller versions of the images so that the page will load on a low-bandwidth connection in a reasonable amount of time. If the site includes streaming audio or video clips, it can give the visitor the option to specify a connection type so that the streaming media adjusts itself to the bandwidth of that connection.

A good site design lets visitors choose among information attributes such as level of detail, forms of aggregation, viewing format and downloading format. Many e-commerce websites give visitors a selectable level of detail, presenting products information by product line. The site presents one page for each line of products. A product line page contains pictures of each item in that product line, accompanied by a brief description. Using hyperlinked graphics for the product pictures, the site offers visitors the option of clicking the product picture to get the page containing a detailed description of that product.

Websites can also offer visitors, multiple information formats by including links to files in those formats. For example, the page offering financial information could include links to an HTML file, an Adobe PDF file, and an Excel spreadsheet file. Each of these files could contain the same financial information, though in different formats, allowing visitors to choose the format that best suits their immediate needs. Visitors looking for a specific financial fact might choose the HTML file so that the information would appear in their Web browsers.

9.5 AGGREGATE METRICS FOR E-BUSINESS SITES

Many metrics have been used to assess the success of sites in terms of popularity and/ or revenue generated.

Hits/Second

This measures the number of requests for objects served in each second by a website. A page is usually composed of one HTML file and several other embedded image files that are automatically requested from the Web server when a user requests the HTML document. So, hits/second counts not just the HTML pages but all embedded objects in a page as separate requests, which does not give a precise idea of the number of times a specific page, with its advertisement banners, was viewed.

Page Views/Day

This reflects the number of individual pages served per day. A company paying for a banner ad to be posted on a page may be interested in the number of times its ad is being seen. Very popular sites can display a few hundred million page views per day.

Click-throughs

This measures the percentage of users who not only view an online ad but also click on it to get to the Web page behind it. This metric is oriented more towards assessing the impact of online

ads. However, this measure can be misleading. If the message in the banner ad is too general, it may draw a larger number of clicks than a more specific message. However, users who respond to the more specific messages are more likely to be interested in the product being advertised than those who react to the more general message.

Unique Visitors

This indicates how many different people visited a website during a certain period of time. Many times it is more important to know how many different people visited your site than the total number of visits received during a certain period.

Revenue Throughput

This is a business-oriented metric that measures the number of dollars/sec derived from sales from an e-commerce site. This measure implicitly represents customer and site behaviour. A customer who is happy with the quality of service (e.g. response time) of an e-business site will shop at the Web store, and the revenue throughput will increase.

Potential Loss Throughput

This is another business-oriented metric that measures the amount of money in customers' shopping carts that is not converted into sales because the customer leaves the site due to poor performance or other reasons.

9.6 ONLINE MARKETING

Online marketing means using the power of online networks, computer communications and digital interactive media to reach your marketing objectives. Online marketing will not replace traditional forms of marketing anyway. Instead, it will both add to and subtract from today's marketing mix. It will add more interactivity. But it will subtract costs. It will add more customer choices. But it will remove marketing's dependence on paper. It will add "information value" to products and services. But it will take away barriers to starting a business or extending a business into international markets. And most importantly, it will turn upside down some old notions we have held of what marketing is all about. There are three new market segments which are as follows:

Cyber buyers

These are professionals who spend a good deal of time online, mainly at their places of business. These professionals often have to make complex purchasing decisions that require reams of data

and difficult to locate sources of supply, all within a tight time frame. That is a perfect fit with the capabilities of online technology.

Cyber consumers

These are the home computer users wired up to commercial online services and the Internet. This group represents the pot of gold, and marketers simply need to find ways to make it more attractive to shop and buy online than to go to the local store

Cyber surfers

They use online technology to expand their horizons, challenge their abilities, and for fun. This segment is typically younger, and possesses shorter attention spans. Some of the important aspects of marketing are advertising, sales, security of the transactions and the mode of payment used for payments. And all of these have had to adapt and change themselves according to the demands of the Internet.

9.7 HOW SHOULD BUYERS PAY ONLINE?

The marketplace, as usual, is responding quickly to this concern. A few basic models or approaches to net-based sales transactions are beginning to come into focus. They are:

1. The consumer, responding to net-based marketing presentation, sends in a cheque, or calls and verbally transmits a credit card number, over the merchant's telephone. This is a fairly traditional approach, and no financial transaction takes place on the Internet.

2. The consumer (i) sets up an account with a merchant or a third party organization, (ii) leaves his or her credit card number by means other than the Internet, and (iii) gives the merchant the authorisation to bill the account, whenever the consumer chooses to buy something.

3. The consumer leaves his or her credit card number on an unsecure online order form. With this approach, the consumer is put at some risk that the credit card number will be compromised, but the risk is perhaps not much greater than giving it out over the phone.

4. The consumer uses a secure (encrypting) client software program to transfer his or her encrypted credit card number to a secure (decrypting) merchant server.

5. The consumer exchanges traditional currency (cash, cheque, credit card authorization) for some form of digital currency, and then spends units of that currency whenever and wherever he or she likes. This requires some form of "electronic wallet" to hold the

currency and an account set up between the currency provider and the participating merchants.

9.8 ADVANTAGES OF ONLINE MARKETING

Some of the advantages of online marketing can be listed in the following manner:

1. Online marketing offers bottom-line benefits that tie in directly to the demands placed on the organization trying to make a transition into the new economy.

2. Online marketing can save money and help you stretch your marketing budget. Electronic versions of catalogues, brochures, and specification sheets do not have to be printed, packaged, stored, or shipped. These can be updated online, and hence, you need not have to send them back to the printer for changes. This saves a lot of money.

3. Online marketing can save time and cut steps from the marketing process. Marketers no longer have to wait for one of their sales representatives to give them the desired information. They can get it online on their own. E-mail allows you to exchange information with potential buyers quickly. It helps you get your message out to the market sooner, with online brochures, catalogues and so on.

4. Online marketing gives customers another way to buy, while enabling them to take control of the purchasing process. Today, customers want more. They want more information about the products they buy, more input into the product itself, and support after the sale. Smart marketers can leverage the inherent interactivity of online communications by encouraging the customer to get engaged in making decisions about the product. They can choose the colour, select the shipping method, and place the purchase order themselves. The more you can get the customer involved in the process of customizing the product and the selling process to meet their particular needs, the more likely it is that you will get the sale.

5. Online marketing can be information-rich and interactive. It appeals to information hungry buyers and analytical buyers. It allows buyers and current customers to search and locate the information they need quickly.

6. Online marketing can offer you instant international reach and indeed, online networks have created an instant global community. Online marketing erases the time and distance barriers that get in the way of conducting business transactions with customers in other countries.

7. Online marketing can lower barriers to entry and offer equal opportunity for access. When you are doing business online, distinctions related to the ethnic background or gender or even the size of business do not seem to matter as much. The online world is a great leveller. And online marketing helps to lower many of the marketplace barriers that have held some would be entrepreneurs from full participation in the free market system.

8. Online marketing can be continuously available. One of the best attributes of an online information server is that it is always on the job, twenty four hours a day, 365 days a year

9.9 VARIOUS BUSINESSES THAT CAN FLOURISH ON THE INTERNET

Banking

The advent of Automated Teller Machines has long extended banking into the realm of computer-network-enabled services. Now, online banks are being set up exclusively to serve clients through the Internet, with the full range of banking services—deposits, withdrawals, funds transfer, loans and other forms of transactions. Simultaneously, online financial services are being offered by other companies, bringing investment opportunities to customers. And several companies are offering e-cash services.

Databanks

In the information economy, pure data is emerging as a hot commodity. With the ease and low cost of delivering information over the Internet pushing down prices, data-vendors are building profitable businesses in the market space. Convenient mechanisms for searching databases are making information services user-friendly as well. And importantly, businesses are also springing up to enable data-shoppers to hunt for the information they need, in the form of search engines which search millions of documents on the Internet to track down information.

Music

Since it is recorded and stored digitally, music as well as the other audio products are the perfect products for distribution over the Internet. Instead of buying cassettes or CDs, customers can simply download the recordings from the site. The world's top music labels are setting up websites from which Internet shoppers can buy their favourite pieces. They are also creating customer involvement by setting up virtual communities of music aficionados who can access sample, trivia, and other value-added information, such as lyrics and scores, directly through the Internet.

Retailing

Two genres of online shopping malls are being set up by digital entrepreneurs. The first consists of multimedia catalogues which shoppers can download through the Internet without taking physical delivery. The second variety is a supermarket service that offers gateways to the websites of scores of other shops, acting as a single window for virtual shoppers. With electronic payment systems becoming secure, customers will soon complete entire retailing transactions on the Internet

9.10 E-ADVERTISING

Advertising is a $500 billion worldwide industry that, until now, has been mainly a one-way street, with consumers passively absorbing advertising messages. Advertisers hoped that potential buyers would remember their slogan or jingle long enough to make a trip to the store and purchase the product.

This has changed with the advent of interactivity. The new concept of 'interactivity' has overpowered the traditional concept of advertising, by putting the buyer in the driver's seat. Interactivity allows consumers to increase their control over the buying process. We are all deluged with an overflow of data. We long for a sense of mastery over the information that washes over us. Given the opportunity, we will be more selective about the kind of information we choose to receive. Interactivity gives us that option. Thus, the audience is not captive any more, and the marketers would have to work harder than before to entice them. The marketing efforts will have to be information-rich and user-friendly.

Web-based advertising has become an important part of a company's media mix. Numerous companies are committing large advertising budgets to the Internet. Following are the reasons for the growing importance of e-advertisements:

1. People increasingly prefer to surf the Internet rather than watch TV.
2. The target audience goes to the advertisement, rather than the other way around
3. Development of business search engines by companies such as C2B Technologies, which aim to link buyers with online bargain sites for over a million products for comparison-shopping purposes.
4. Yahoo! has a business unit which offers contests and prizes to online participants, which drive players to the websites of different clients. To play, participants must provide

certain data, including their preference of advertisements and tastes, which presents a valuable database as to customer preferences.

5. The growth of e-business. Dell Computers, for example, estimates that by 2005, 85 per cent of its sales will be through the Internet.

6. The Internet is not geographically restricted. Amazon.com sells 20 per cent of its books to foreign destinations, whereas a physical book store serves an area of only a few square miles

9.11 VARIOUS MEANS OF ADVERTISING

E-mail

The advantages of e-mail are its low cost and its ability to reach a wide variety of targeted audiences. Most companies develop a customer database, to whom they send e-mails. E-mail is emerging as a marketing channel that affords cost-effective implementation and better, quicker response rates than other advertising channels. Marketers should be racing to embrace the medium. Sometimes, it may also happen that when every marketer starts inundating prospects and customers with e-mail, the consumers may react negatively.

Banners

They make up 50 per cent of online ad revenues, but their effectiveness may be waning. When IBM kicked off banner ads in 1994 on tech site Hotwire, 30 per cent of the people who saw the ads clicked on them. Now the overall click-through rate for banner ads has dropped to a measly 0.3 per cent.

But it is the most commonly used form of advertising on the Internet. As you surf your way through the information superhighway, banners are everywhere. The smaller the file size, the quicker it gets loaded. Typically, a banner contains a short text or a graphical message to promote a product. A major advantage of using banners is the ability to customize them to the target audience. One can decide which market segment to focus on.

Skyscrapers

These are the extra-long skinny ads running down the right or left side of a website.

Banner Swapping

Banner swapping is nothing but a direct exchange of links between websites. To be precise, company A may agree to display a banner (in the form of a link) of company B in exchange for company B displaying company A's banner.

Streaming Video and Audio

Companies and content networks including RealNetworks, NetRadio, and MusicVision, insert ads for marketers into music and video clips, as consumers listen to them. It is much more like the TV that marketing advertisers know and trust. You can get click-through rates of about 3.5 per cent, according to RealNetworks. Its widespread use will depend on high-speed Internet connections.

Effectiveness Tracking

This is an upstart DynamicLogic designed by a pioneering service to help traditional advertisers gauge the impact of their marketing by placing tiny files, called cookies, on viewers' computers. This helps them track where people go after seeing their ads.

Mini-sites, Pop-ups

These ads burst upon the screens, allowing companies such as Volvo and SmithKline Beecham's Oxy acne medicine to dish up games and product information. Mini-sites allow advertisers to market without sending people away from the site they are visiting. This type of advertising also gets higher click rates. Sometimes, these can be intrusive and annoying.

Interstitials

Visit the railway site (www.indianrail.gov.in). When the site uploads, a new window will open in your browser from Citibank, asking you to apply for a loan. These windows are called interstitials, and they demand your attention because you must click on them, even if only to close the window. It is estimated that the click-through rates are as high as 5 per cent.

Sponsorships

Sponsorships can vary from a simple sponsorship of an e-mail list to much more sophisticated site sponsorship deals. For example, the e-retailer 800.com (www.800.com) sponsored a list of the top 10 videos which appeared alongside the 800.com logo on the Hollywood stock exchange (www.hsx.com). By clicking on one of the video titles, visitors were transported to the 800.com site, where they could purchase the video. The advantage of sponsorships is that they can help to build a sponsor's brand by presenting it within the context of the sponsored site and by creating value for visitors to that site.

Coupons

Companies such as cool savings (www.coolsavings.com) offer their members discount coupons which they can print out and then use for both online and offline retailers. Coupons can be an

attractive marketing mechanism because they encourage product trial, and they are a way of selectively discounting prices to the most price sensitive customers (those are willing to go to website and print out a coupon).

Pay Per Advertising View

Companies such as Cyber Gold "pay" customers to view advertisements. The approach uses the accountability of the Web to reward consumers for processing the "right" kind of information.

Loyalty Programs

Companies such as click rewards (www.clickwards.com) offer their members the chance to earn a currency, such as airline miles, by shopping at their network of partner sites. The economics of customer retention are well known. An existing, loyal customer is much more profitable than a new one, so rewarding existing customers to encourage them to remain loyal can be a good tactic.

Partnerships

While many offline companies arrange partnerships, the use of partnerships is more pervasive in the New Economy. Similar to the manner in which complementary companies often collaborate to push a new technology, Web companies often partner with complementary sites to quickly provide a more value-enhanced service to site visitors. One prevailing strategy is to select a customer niche and provide services that encompass the customer's entire needs in that area.

Innovative Customer Acquisition

As the Internet market becomes more competitive, competitive advantage will be derived from innovative marketing. One form of innovative marketing is to ally with groups (or associations) and provide a complementary service that benefits the group's membership. By creating such an alliance, a new site can launch with a large customer base without incurring expensive and risky marketing fees. In such an arrangement, a site generally pays the group a fee for access to its membership.

Providing Information

The Web allows sites to instantly offer information that is relevant to their customer base. Many sites provide instantly accessible information to their customers as a form of marketing and product differentiation. The e-commerce market for travel (airlines, hotels, etc.) is very competitive, with many well-funded players. Sites try to differentiate themselves by offering vast amounts of information to their customers. Travel information can range from top restaurant and

hotel information targeted toward expense account business travellers, to time-sensitive travel information to budget-minded leisure travellers. Customers evaluate the information they receive and establish a relationship with the site that best meets their needs. Sites try to capitalize on this relationship by offering e-commerce opportunities like travel reservation services

Leverage the Customer Base

A primary goal of e-commerce businesses today is to invest heavily in creating a large customer base and establishing a relationship of trust with their customers. Many firms are trying to establish a reputation that conveys to its customer base that they are a solid company that is good at fulfilling e-commerce orders. Eventually, as a company establishes a large and loyal customer base, the goal is to leverage this relationship by offering an expanded product/ service selection to its customers. Amazon has successfully leveraged its customer base. Within four months of offering CDs and six weeks of offering videos, Amazon was the topselling site for both products.

9.12 PERSONALIZED ONLINE COMMUNICATIONS

Online companies have the opportunity to reduce mass-marketing expenses and increase response rates by developing marketing strategies that centre around each individual customer. The manner in which transactions occur on the Internet provides e-commerce companies with detailed information on their customers. Information derived from customers registering preferences and demographic information, as well as firms analyzing past purchases and Web-surfing habits, provides e-commerce companies the opportunity to create a one-to-one marketing relationship with each of their customers. In addition to this information, many e-commerce companies use their sites to establish a two-way dialogue with their customers. This dialogue provides additional information regarding product desires and better avenues to market them. We categorize personalized marketing into five primary forms: (1) permission marketing, (2) personalized recommendations, (3) personalized advertisements, (4) personalized web pages, and (5) personalized e-commerce stores.

1. **Permission marketing**.

   Seth Godin coined the term permission marketing to describe how successful e-mail campaigns can result from creating relationships with customers. Permission marketing has become the current rage of online marketers and has led to increases in marketing response rates. Permission marketing presumes that successful marketing campaigns can be created by establishing a mutually beneficial and trusting relationship between the

14

firm and its customers. In exchange for some offered benefit, customers volunteer information about themselves and, in essence, ask to be marketing targets. Once customers initiate this relationship, they anticipate e-mail messages because they know that these messages will be on relevant topics. By using the permission marketing philosophy, online firms create a valuable database of customers who have given the firm the permission to market to them and are receptive to marketing messages. Permission marketing e-mails must be relevant to the consumer. Relevance can range from general interest to very specific interest. Response rates and trust can increase by sending permission marketing e-mails that are highly specific to customers' interests. Many online firms ask their permission marketing customers for detailed personal information when they sign up for e-mails. This information allows them to send more targeted e-mails to specific segments of the firm's customer base. Customers appreciate these targeted e-mails, and this increases their relationship level with the firm. The associated increased trust level may also induce customers to reveal additional information about themselves

2. **Personalized recommendations**.

Many e-commerce sites have personalized services that make specific merchandise recommendations for each user based on past purchases, web pages viewed, and survey information that the user has provided.

3. **Personalized advertisements**.

Websites increasingly are using personalized technology software to determine dynamically, in real time, which Web advertisements should be exposed to viewers. ZDNET uses personalization technology that is based on an analysis of five user profile and impression environment variables. Variables used include the user's past click behaviour, time of day, the page, recency/frequency of visits, and search keywords. Based on these variables, users are given a relevancy score (i.e. indicator of the probability of a click), and ads that are most likely to be of interest to the viewer are displayed.

4. **Personalized Web pages.**

Many portals and e-commerce sites allow users to create their own personalized Web page. This allows users to create a Web page that caters exactly to their interests.

Personalization encourages users to return more often and increases the user's familiarity and trust with the Web page. This leads to users spending more time on the website, thereby increasing advertising exposure time. Since a creator/user of a personalized Web page reveals detailed personal information, the site sponsoring the personalized Web page can deliver more targeted consumers to advertisers. This results in an opportunity to charge increased ad rates to reach specific customer groups. At portal site Excite, users can create a personalized portal page using Excite's 'My Excite' service. Excite found that users who create a 'My Excite' personal page come back five times as often as others, and view twice the number of pages compared to Excite users who do not have a personal page. This has allowed Excite to reap higher advertising revenues. In addition, personalization increases users' switching costs.

5. **Personalized e-commerce stores**.

One of the goals of online merchants is to use Internet technology and their knowledge about individual consumers to tailor their products and services for each of their customers. Jeff Bezos, Amazon's chairman, has stated that one of his goals is to have his "store redecorated for each and every customer." However, he cautions that it could take up to 10 years to achieve such individual customization. Office Depot offers its small-business customers personalized catalogues, allowing businesses to create real-time unique catalogues for their employees, based on their buying authority. In addition to making their customers' shopping experience more pleasant, personalization is a key tool for increasing switching costs. If a customer is satisfied and becomes dependent on a site that offers personalized services, it will be more costly to switch sites. Even if a competing site offers superior services, there is a certain inertia that often slows users from switching sites.

9.13 MEASURING THE EFFECTIVENESS OF E-ADVERTISING

As more companies rely on their websites to make a favourable impression on potential customers, the issue of measuring website effectiveness has become important. Mass media efforts are measured by estimates of audience size, circulation, or number of addressees. When a company purchases mass-media advertising, it pays a dollar amount for each thousand persons in

the estimated audience. This pricing metric is called cost per thousand or cost per metric, and is often abbreviated as CPM in short for cost per thousand impressions.

In reality, measuring Web audiences is more complicated because of the Web's interactivity and also because the value of a visitor to an advertiser depends on how much information the site gathers from the visitor (for example, name, address, e-mail address, telephone number, and other demographic data). Since each visitor voluntarily provides or refuses to provide these bits of information, all visitors are not of equal value. Internet advertisers have developed some web-specific metrics, described in this section, for site activity, but these are not generally accepted and are currently the subject of debate.

One of the most difficult things for companies to do as they move on to the Web is to determine the costs and benefits of advertising on the Web. Many companies are experimenting with new metrics they have created that consider the number of desired outcomes that their advertising yields. For example, instead of comparing the number of click-throughs that companies obtain per dollar of advertising, they measure the number of new visitors to their site that buy for the first time after arriving at the site via a click-through. They can then calculate the advertising cost of acquiring one customer on the Web and compare it to the cost of acquiring one customer through traditional channels.

9.14 CHECK YOUR PROGRESS

1. The _____is changing the design and implementation of marketing strategies.
2. Write significance of websites.
3. What is online marketing?
4. The advent of Automated Teller Machines has long extended banking into the realm of computer-network-enabled services.(True/False)
5. Mention five categories of personalized marketing.

   Answers to Check your progress

1. Internet
2. Websites can also offer visitors, multiple information formats by including links to files in those formats. For example, the page offering financial information could include links to an HTML file, an Adobe PDF file, and an Excel spreadsheet file.
3. Online marketing means using the power of online networks, computer communications and digital interactive media to reach your marketing objectives.

17

4. True

5. (1) permission marketing, (2) personalized recommendations, (3) personalized advertisements, (4) personalized web pages, and (5) personalized e-commerce stores.

9.15 SUMMARY

This unit introduces about the problems associated with traditional marketing. Few strategies to maintain a website is discussed. Also, various metrics to access the performance of E-business sites are detailed. A brief note on online marketing is given. The procedure how online payment is made by buyers is elaborated. Few advantages of Online Marketing is detailed. Along with significance of *Electronic advertising*, its various means are described. Also five categories of personalized marketing is highlighted and described briefly.

9.16 KEYWORDS

- **Traditional marketing**: refers to any type of marketing that isn't online. This means print, broadcast, direct mail, phone, and outdoor advertising like billboards.

- **Website**: A website (also written as web site) is a collection of web pages and related content that is identified by a common domain name and published on at least one web server. Examples of notable websites are Google, Facebook, Amazon, and Wikipedia.

- **E-business websites** can be online storefronts or online marketplaces. An online marketplace will make it easier to buy or sell goods and services between merchants and customers.

- *Electronic advertising* is advertising that uses the Internet and other forms of digital media to help a business promote and sell goods and services.

- **Personalized marketing**, also known as one-to-one marketing or individual marketing, is a marketing strategy by which companies leverage data analysis and digital technology to deliver individualized messages and product offerings to current or prospective customers.

9.17 QUESTIONS FOR SELF STUDY

1. Narrate the problems associated with traditional marketing.
2. How to maintain a website? Explain.

3. Explain various metrics to access the performance of E-business sites.

4. Write a note on online marketing.

5. Explain the procedure how online payment is made by buyers.

6. Mention advantages of Online Marketing.

7. Write significance of *Electronic advertising*.

8. Explain various means of advertising.

9. Discuss five categories of personalized marketing.

9.18 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

2. Joseph, P. T. (2019). *E-commerce: An Indian perspective*. PHI Learning Pvt. Ltd..

Structure

10.0 OBJECTIVES

After studying this unit, you will be able to:

- Steps to analyze Information System Security goals

- Status of Security on the Internet

- Analyze various Security Incidents on the Internet

- Discuss how vulnerable are the Internet Sites.

- Narrate Network and Website Security

- Give an account on Security Audits and Penetration Testing

10.1 INTRODUCTION

Any business, whether it is a traditional brick-and-mortar business, a brick-and-click e-business, or a pure-play e-business, needs to be concerned about network security. The Internet is a public network consisting of thousands of private computer networks connected together. This means that a private computer network system is exposed to potential threats from anywhere on the

public network. Protection against these threats requires businesses to have stringent security measures in place. In the physical world, crimes often leave evidence— finger prints, footprints, witnesses, video on security cameras and so on. Online, a cyber-crime also leaves physical, electronic evidence, but unless good security measures are taken, it may be difficult to trace the source of a cyber-crime.

10.2 INFORMATION SYSTEM SECURITY

As seen in Figure 10.1, the goals of security are:

1. Integrity of the data sent and received.

2. Confidentiality of the data so that it is not accessible to others.

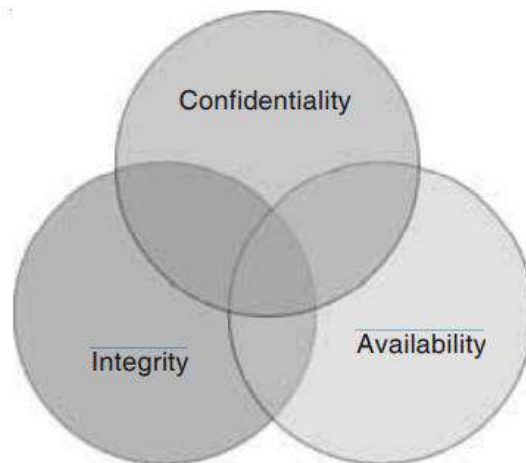3. The data ought to be available to the people for whom it is meant

Fig 10.1 Security Goals

As shown in Figure 10.2, the data sent from the source ought to reach in destination without any tampering as shown in Figure 10.2(a). But the above criteria shown in Figure 10.2(a) may be violated by the following:

1. Interrupt the data and cut it off as shown in Figure 10.2(b).
2. Intercept the data with the intent of spying on it as shown in Figure 10.2 (c)

3. Interrupt the data and modify it and send a different data to the receiver as shown in Figure 10.2(d).

4. Obstruct the data and fabricate new data and send it to the receiver as shown in Figure 10.2(e).

- Encryption
- Software Controls (access limitations in a data base, in operating system protect each user from other users)
- Hardware Controls (smartcard)
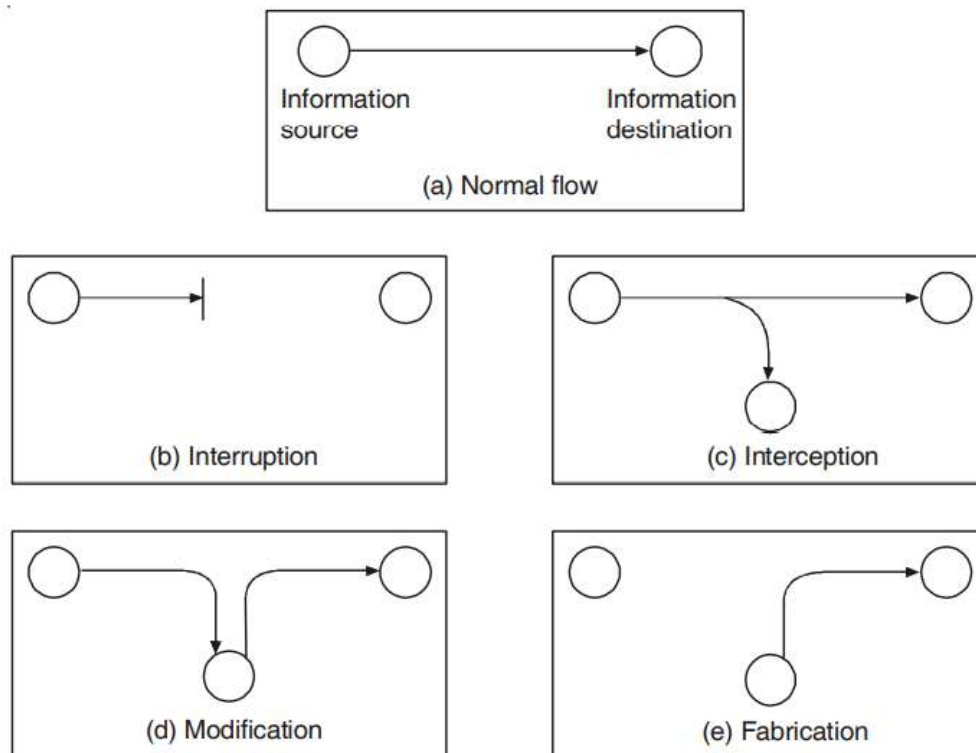- Policies (frequent changes of passwords)
- Physical Controls

Fig 10.2 Methods of defence

Additionally, e-businesses must protect against the unknown. New methods of attacking networks and websites and new network security holes are being discovered with disturbing frequency. By carefully planning its network and website security system, an e-business can

protect itself against many known and as yet unknown threats. An e-business must always be prepared for network and website attacks, or risk the loss of assets.

Another very important reason to protect an e-business's network and website is to protect the e-business's relationships with its customers. Many Internet users perceive that there is a large risk to their privacy and security when they buy products and services or submit personal information online. Although the perception of risk may be greater than the actual risk, it is still a cause for concern.

An e-business must address customers' perceived risks just as much as any actual risks. An e-business cannot expect to achieve perfect security for its network and website. The important issue for an e-business is to have adequate security to protect its assets, revenue stream, customer privacy, and its own reputation. Determining adequate security depends on an individual e-business's situation. For example, a website providing information on flavors of dog food may not require the same level of security as an online banking website. An e-business must determine its security needs according to the risks involved, the value of the assets at risk, and the cost of implementing a security system.

How does an e-business identify the security issues to be addressed?

First, the e-business must thoroughly understand its business and how all its systems, not just its web servers, are used. Several aspects of e-business computer systems security need to be addressed.

Security has become one of the primary concerns when an organization connects its private network to the Internet. Regardless of the business, an increasing number of users on private networks are demanding access to Internet services such as the world wide web (WWW), Internet mail, Telnet, and File Transfer Protocol (FTP). In addition, corporations want to offer web home pages and FTP servers for public access on the Internet.

10.3 SECURITY ON THE INTERNET

Network administrators have increasing concerns about the security of their networks when they expose their organization's private data and networking infrastructure to Internet crackers. To provide the required level of protection, an organization needs a security policy to prevent unauthorized users from accessing resources on the private network and to protect against the unauthorized export of private information. Even if an organization is not connected to the

Internet, it may still want to establish an internal security policy to manage user access to certain portions of the network and protect sensitive or secret information.

The fundamental problem may be that the Internet was not designed to be very secure, i.e. open access for the purposes of research was the prime consideration at the time the Internet was implemented. However, the phenomenal success of the Internet, combined with the introduction of different types of users, including unethical users, has aggravated existing security deficiencies to the extent that wide-open Internet sites risk inevitable break-ins and resultant damages. Other factors include the following:

1. **Vulnerable TCP/IP services**. A number of the TCP/IP services are not secure and can be compromised by knowledgeable intruders; services used in the local area networking environment for improving network management are especially vulnerable.

2. **Ease of spying and spoofing**. A majority of Internet traffic is unencrypted; e-mail, passwords, and file transfers can be monitored and captured using readily-available software. Intruders can then reuse passwords to break into systems.

3. **Lack of policy**. Many sites are configured unintentionally for wide-open Internet access, without regard for the potential for abuse from the Internet; many sites permit more TCP/IP services than they require for their operations, and do not attempt to limit access to information about their computers that could prove valuable to intruders.

4. **Complexity of configuration**. Host security access controls are often complex to configure and monitor; controls that are accidentally misconfigured often result in unauthorized access.

Sites that ignore these problems face some significant risk that they will be attacked by intruders and that they may provide intruders with a staging ground for attacks on other networks. Even sites that do observe good security practices, face problems with new vulnerabilities in networking software and the persistence of some intruders.

Some of the problems with Internet security are the result of inherent vulnerabilities in the services (and the protocols that the services implement), while others are a result of host configuration and access controls that are poorly implemented or overly complex to administer.

This is further aggravated by the tremendous growth of the Internet and the way it is used. Businesses and agencies now depend on the Internet for communications and research, and thus have much more to lose if their sites are attacked. The following sections describe the problems on the Internet and the factors that contribute to these problems:

1. **How secure is the server software?** Security should be in place to prevent any unauthorized remote logon to the system. It should be extremely difficult to make changes to the server software. The servers themselves should be physically located in a secure environment.

2. **How secure are communications?** Customer credit card information and other sensitive data that is being transmitted across the Internet must be protected.

3. **How is the data protected once it is delivered to the e-business?** Is it stored in unencrypted text files at the website? Is it moved to offline storage?

4. **How are credit card transactions authenticated and authorized?** Credit card transactions must be authenticated and authorized, so as to make it more secure for the users.

10.4 SECURITY INCIDENTS ON THE INTERNET

As an evidence of the above, three problems have occurred within a short period of time. In the first, persistent vulnerabilities in the UNIX sendmail program were discovered. Sites which had not corrected their sendmail programs, were forced to scramble to correct the programs before their vulnerabilities were attacked. However, due to the complexity of the sendmail program and networking software in general, three subsequent versions of sendmail were found to still contain significant vulnerabilities. The sendmail program is used widely, and sites without firewalls to limit access to sendmail are forced to react quickly whenever problems are found and vulnerabilities revealed.

In the second, a version of a popular and a free FTP server was found to contain a Trojan horse that permitted privileged access to the server. Sites using this FTP server, but not necessarily the contaminated version, were again forced to react very carefully and quickly to this situation. Many sites rely on the wealth of free software available on the Internet, especially security-related software that adds capability for logging, access control, and integrity checking that

vendors often do not provide as part of the operating system. While the software is often of high quality, sites may have little recourse other than to rely on the authors of the software if it is found to have vulnerabilities and other problems.

The third problem has the strongest implications: intruders had broken into potentially thousands of systems throughout the Internet, including gateways between major networks, and installed sniffer programs to monitor network traffic for usernames and static passwords typed in by users to connect to networked systems. The intruders had used various known techniques for breaking into systems, as well as using passwords that had been "sniffed". One of the implications of this incident is that static or reusable passwords are obsolete for protecting access to user accounts. In fact, a user connecting to a remote system across the Internet may be unintentionally placing that system at the risk of attack by intruders who could be monitoring the network traffic to the remote system.

Weak Authentication

Security handling teams estimate that many incidents stem from the use of weak, static passwords. Passwords on the Internet can be "cracked" in a number of different ways. However, the two most common methods are by cracking the encrypted form of the password and by monitoring communications channels for password packets. The UNIX operating system usually stores an encrypted form of passwords in a file that can be read by normal users. The password file can be obtained by simply copying it. It can also be obtained by a number of other intruder methods. Once the file is on hand, an intruder can run readily-available password cracking programs against the passwords. If the passwords are weak, e.g. less than 8 characters, and so on, they could be cracked and used to gain access into the system.

Ease of Spying

It is important to note that when a user connects to her account on a remote host using Telnet or FTP, the user's password travels across the Internet unencrypted or in plain text. Thus, another method for breaking into systems is to monitor connections for IP packets bearing a username and a password, and then using them on the system for normal login. If the captured password is to an administrator's account, then the job of obtaining privileged access is made much easier. As noted previously, hundreds and possibly thousands of systems across the Internet have been penetrated as a result of monitoring for usernames and passwords. E-mail, as well as the contents of Telnet and FTP sessions, can be monitored and used to learn information about a site and its

business transactions. Most users do not encrypt e-mail, since they assume that e-mail is secure and thus safe for transmitting sensitive information.

Ease of Spoofing

The IP address of a host is presumed to be valid and is therefore trusted by TCP and UDP services. A problem is that, using IP source routing, an attacker's host can masquerade as a trusted host or a client. Briefly, IP source routing is an option that can be used to specify a direct route to a destination and return path back to the origin. The route can involve the use of other routers or hosts that normally would not be used to forward packets to the destination. An example of how this can be used such that an attacker's system could masquerade as the trusted client of a particular server is as follows:

1. The attacker would change her host's IP address to match that of the trusted client.
2. The attacker would then construct a source route to the server, that specifies the direct path the IP packets should take to the server and should take from the server back to the attacker's host, using the trusted client as the last hop in the route to the server.
3. The attacker sends a client request to the server using the source route.
4. The server accepts the client's request as if it came directly from the trusted client, and returns a reply to the trusted client.
5. The trusted client, using the source route, forwards the packet on to the attacker's host.

Many UNIX hosts accept source routed packets and will pass them on as the source route indicates. Many routers will accept source routed packets as well, whereas some routers can be configured to block source routed packets.

E-mail on the Internet is particularly easy to spoof and, without enhancements such as digital signatures, generally cannot be trusted. As a brief example, consider the exchange that takes place when Internet hosts exchange mail. The exchange takes place using a simple protocol consisting of ASCII-character commands. An intruder could easily enter these commands on Telnet to connect directly to a system's Simple Mail Transfer Protocol (SMTP) port. The receiving host trusts this sending host, and thus the origin of the mail is spoofed easily by entering a sender address that is different from the true address. As a result, any user, without privileges, can falsify or spoof e-mail.

Other services, such as Domain Name Service (DNS), can be spoofed, but with more difficulty than e-mail. These services still represent a threat that needs to be considered when using them.

10.5 HOW VULNERABLE ARE THE INTERNET SITES?

The Internet, while being a useful and a vital network, is at the same time vulnerable to attacks. Sites that are connected to the Internet face significant risk in some form by intruders. The following factors would influence the level of risk:

- Number of systems connected to the site
- Services utilized by the sites.
- Interconnectivity of the site to the internet
- Site's profile or how well known the site is.
- Site's readiness to handle computer security incidents.

The more the number of systems that are connected, obviously the harder it is to control their security. Equally, if a site is connected to the Internet at several points, it is likely to be more vulnerable to attacks than a site with a single gateway. At the same time, though, how well prepared a site is, and the degree to which the site relies on the Internet, can increase or decrease the risk. A site's high profile could attract more potential intruders who wish to do some harm to the site's image. It should be mentioned though, that "quiet", less-frequently used sites are also attractive to intruders since they can more easily hide their activity.

Sites that use recommended procedures and controls for increasing computer security have significantly lower risks of attack. Firewalls, combined with one-time passwords that are immune from monitoring or guessing, can increase greatly a site's overall level of security and make using the Internet quite safe.

The more the number of systems that are connected, obviously the harder it is to control their security. Equally, if a site is connected to the Internet at several points, it is likely to be more vulnerable to attacks than a site with a single gateway. At the same time, though, how well prepared a site is, and the degree to which the site relies on the Internet, can increase or decrease the risk. A site's high profile could attract more potential intruders who wish to do some harm to the site's image. It should be mentioned though, that "quiet", less-frequently used sites are also

attractive to intruders since they can more easily hide their activity. Sites that use recommended procedures and controls for increasing computer security have significantly lower risks of attack. Firewalls, combined with one-time passwords that are immune from monitoring or guessing, can increase greatly a site's overall level of security and make using the Internet quite safe.

Electronic Industrial Espionage

It is a major risk and a big dollar issue that most companies are reluctant to discuss openly—electronic industrial espionage. Often, e-businesses that have been hacked and had business secrets stolen are too embarrassed to admit the break-in. However, in late October 2000, one very high-profile company, Microsoft, found itself scrambling to deal with first rumours and then published reports of a serious hacking incident with industrial espionage overtones. The apparent culprit was a Trojan horse virus named QAZ Trojan that was first identified in mid-July in China. The QAZ Trojan virus infects a computer system when a user opens an e-mail attachment containing the virus. Then the virus replaces the system's Notepad text editor with its own code, searches for other shared hard drives to infect, and sends the IP addresses of infected computers to an outside e-mail address. This creates a "back door" a hacker can use to enter a system, search for passwords, and install software programs to allow remote control of the computer. Although by August 2000, all major antivirus software makers had included the QAZ Trojan information in their downloadable virus updates, somehow the QAZ Trojan virus was used to create a "back door" in Microsoft.

Credit Card Fraud and Theft of Customer Data

Almost all B2C purchase transactions involve credit cards. An e-business that accepts credit cards in payment for goods and services, must secure the credit card information in transit to its website, and it must secure stored credit card information. Also, systems must be in place for credit card transaction authentication (verifying that the person placing the order really is the holder of the credit card used in the transaction), and credit card authorization (verifying that the charge can be made to the card number).

A hacker can break into a database server and steal thousands of credit card numbers and other information in a matter of moments, and an e-business might not even recognize that the hacker

was there. For example, one of the largest reported cases of stolen credit card information took place in January 1999 (but was not reported until much later) when information on 485,000 credit cards, including card numbers, expiration dates, names, and addresses, was stolen from an e-business website and stored at a US government agency's website, where the agency's website administrator discovered the data. There was no reported evidence of fraudulent use, and some of the accounts were not active. But this event highlights the risk to a vulnerable e-business of the theft of sensitive information.

Security and E-mail

E-mail users who desire confidentiality and sender authentication use encryption. Encryption is simply intended to keep personal thoughts personal. There are two good programs to encrypt e-mails and they are: Pretty Good Privacy (PGP), and Privacy Enhanced Mail (PEM).

E-mail is typically encrypted for the reason that all network correspondence is open for eavesdropping. Internet e-mail is obviously far less secure than the postal system, where envelopes protect correspondence from casual snooping. In contrast, the header area of any e-mail message will show that it has passed through a number of nodes on its way to you. Each of these nodes presents the opportunity for snooping.

Privacy Enhanced Mail Standard

PEM is the Internet Privacy Enhanced Mail standard, designed, proposed, but not yet officially adopted by the Internet Activities Board, to provide secure electronic mail over the Internet. Designed to work with current Internet e-mail formats, PEM includes encryption, authentication, and key management, and allows use of both public-key and secret-key crypto-systems. The system supports multiple cryptographic tools: for each mail message, the specific encryption algorithm, digital signature algorithm, hash function and so on, are specified in the header. PEM explicitly supports only a few cryptographic algorithms; others may be added later. It uses the DES algorithm for encryption and the RSA algorithm for sender authentication and key management. PEM also provides support for non-repudiation, which allows the thirdparty recipient of a forwarded message to verify the identity of the message originator (not just the message forwarder) and to verify whether any of the original text has been altered.

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is the implementation of public-key cryptography based on RSA. It is a free software package developed by Phillip Zimmerman, that encrypts e-mail. Since being published in US as freeware in June 1991, PGP has spread rapidly and has since become the de facto worldwide standard for encryption of e-mail. It is freely available for DOS, Macintosh, UNIX, Amiga, VMS, Atari, and OS/2 systems. PGP provides secure encryption of documents and data files that even advanced supercomputers are hard pressed to "crack". The process is so simple that anyone with a PC can do it with almost no effort. For authentication, PGP employs the RSA public-key encryption scheme and the MD5 (Message Digest version 5) developed by Rivest, a one-way hash function to form a digital signature that assures the receiver that an incoming message is authentic (that it comes from the alleged sender and that it has not been altered).

10.6 NETWORK AND WEBSITE SECURITY

The best way to recognize when a hacker is attempting unauthorized network access is to monitor network performance. Setting up, logging, and monitoring established network reference points, called benchmarks, can alert an e-business to security problems. A skilled system administrator and other well-trained technicians, who use these benchmarks to monitor and manage the network and servers, are critical. Other tools such as passwords, firewalls, intrusion detection systems, and virus scanning software should be used to protect an e-business' network and website.

A password is a code, or more often a common word, used to gain access to a computer network. Passwords are only effective when used properly. Often a computer user chooses a bad password, such as a short, common word—a name, or birthday—so that the user can remember the password easily. One way hackers penetrate network security is by using software that "guesses" a password by trying millions of common words until one of the words is accepted. Passwords that require a minimum length of six characters in a mix of letters and numbers increase the number of potential passwords into billions and make it more difficult for a hacker to guess them. A computer user should also change passwords regularly. If a user has access to multiple systems, it is a good idea to have different passwords on each system.

A firewall is a software or a hardware used to isolate and protect a private system or a network from the public network. A firewall provides an easy-to-manage entry point to multiple systems behind it. Firewalls can control the type of information that is allowed to pass from the public network to the private network, as well as what services inside the firewall are accessible from the outside. Firewalls can also log activity, to provide an audit trail in case the network is penetrated. Intrusion detection is the ability to analyze real-time data to detect, log, and stop unauthorized network access as it happens. Businesses can install intrusion detection systems that monitor the network for real-time intrusions and respond to intrusions in a variety of user-detected ways.

An intrusion detection system can defend a website against DoS attacks by adding more servers to increase the traffic the website can handle, by using filters and routers to manage traffic, and by having a backup plan to reroute legitimate traffic during an attack. Cisco's Secure Intrusion Detection System, and Network ICE's ICEpac Security Suite are two examples of intrusion detection systems.

Virus scanning software, including e-mail virus scanning, should be installed on all network computers. Antivirus software should be kept updated. Communication ports should be used to allow data to enter and exit the network. The system administrator should close all unused communication ports. Up-to-date security patches for operating systems should be installed as soon as the patches are available, to prevent hackers from exploiting built-in system weaknesses.

10.7 SECURITY AUDITS AND PENETRATION TESTING

Security audits can provide an overall assessment of an e-business' systems and security issues by checking for vulnerabilities in those systems and providing recommendations for fixing those vulnerabilities. Security consultants such as DefendNet Solutions Inc., Internet Security Systems, and Pinkerton Systems Integration offer security auditing services.

Accounting firms, such as Ernest & Young, also offer security auditing services. Some of the Big Five international accounting firms use the American Institute of Certified Public Accountants (AICPA) WebTrust seal and audit criteria. The WebTrust seal indicates to customers that the website is verified as being safe and secure by the AICPA. The AICPA audit criteria cover best

business practices, site security, and customer information privacy. Some accounting firms use their own audit seal instead of, or in addition to, the AICPA WebTrust seal.

When evaluating security consultants who will perform the penetration testing, there are several factors to consider. They can be listed as follows:

1. Get evidence that the security consultants have insurance to protect against accidental system damage or down time.
2. Have everyone on the consultant's penetration team sign a non-disclosure agreement.
3. Consider requiring a third-party background check on each member of the consultant's penetration team.
4. Decide whether it makes sense to use a security consultant who employs former hackers.
5. Determine if the consultant's team is going to use packaged security scanning software that could be employed by the in-house staff, or if they are using custom tools.
6. Develop a clear scope for the penetration test and a workable time frame.
7. Determine whether to have a DoS attack done, and if so, when to schedule it to least disrupt customer access.
8. Make sure the final report from the consultant includes an accounting of all attacks attempted and whether or not they were successful, a return of all the paper or electronic information gathered by the consultant, and recommendations on how to fix up any problems discovered during the tests.

Individual PC Security Risks Often managers in an e-business use stand-alone personal computer during the start up phase, until funds are available to build and operate a network or until the e-business can outsource its IT operations. Additionally, some e-businesses offer their employees the opportunity to telecommute—allowing an employee to use his or her home computer, or installing a business owned personal computer in the employee's home. Certainly, business employees often work on business files at home. Due to these factors, it is important for an e-business to understand that individual PCs are also at risk from hackers.

10.8 CHECK YOUR PROGRESS

6. Mention services provided by internet.
7. What is FTP server?
8. Define Pretty Good Privacy (PGP)
9. What is a password?

10. What is a firewall?

Answers to Check your progress

1. Internet services are world wide web (WWW), Internet mail, Telnet, and File Transfer Protocol (FTP).

2. An FTP server is a computer that offers files available for download via an FTP protocol, and it is a common solution used to facilitate remote data sharing between computers. An FTP server is an important component in FTP architecture and helps in exchanging files over the internet.

3. Pretty Good Privacy (PGP) is the implementation of public-key cryptography based on RSA. It is a free software package developed by Phillip Zimmerman, that encrypts e-mail.

4. A password is a code, or more often a common word, used to gain access to a computer network.

5. A firewall is a software or a hardware used to isolate and protect a private system or a network from the public network.

10.9 SUMMARY

This unit introduces the goals of information security. Security issues to be addressed by an e-business is narrated. The risk factors involved in the usage of internet is addressed. Also, the problems faced in internet are highlighted. The concept of spying and spoofing are detailed. The usage of firewall in security management and maintenance is detailed. The security provisions made to protect websites and users data are discussed. Also, significance of security audit is detailed.

10.10 KEYWORDS

- **Information security** protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

- **Security audit** is the high-level description of the many ways organizations can test and assess their overall security posture, including cybersecurity. You might employ more

than one type of security audit to achieve your desired results and meet your business objectives.

- **Firewall** is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

- **Password Authentication**: Standard password authentication involves a user entering their username, accompanied by a secret code or passphrase that allows them to gain access to a network, account, or application. In theory, if a password is kept private and secure, unauthorized access will be prevented.

- **Intrusion Detection System (IDS)** is a monitoring system that detects suspicious activities and generates alerts when they are detected.

10.11 QUESTIONS FOR SELF STUDY

10. Narrate the goals of information security.

11. How does an e-business identify the security issues to be addressed?

12. Explain risk factors of internet.

13. Discuss the problems faced in internet.

14. What is spying and spoofing? Explain.

15. Write a note on firewall.

16. How a website can be secured? Explain.

17. Write a note on security audit.

10.12 REFERENCES

3. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

4. Joseph, P. T. (2019). *E-commerce: An Indian perspective*. PHI Learning Pvt. Ltd..

Unit 11: E-BUSINESS RISK MANAGEMENT ISSUES

Structure

11.0 Objectives

11.1 Introduction

11.2 The Firewall Concept

11.3 Firewall Components

11.4 What Should a Firewall Contain?

11.5 Benefits of an Internet

11.6 Defining an Enterprise-wide Security Framework

11.7 Understanding the Security Framework

11.8 Secure Physical Infrastructure

> 11.8.1 Security of the Premises
>
> 11.8.2 Security of the Equipment
>
> 11.8.3 Secure Behaviour

11.9 Information Security Environment in India

11.10 Check Your Progress

11.11 Summary

11.12 Keywords

11.13 Questions for Self Study

11.14 References

11.0 OBJECTIVES

After studying this unit, you will be able to:
- Analyze the Firewall Concept and its components.
- Signify the Benefits of an Internet
- Defining an Enterprise-wide Security Framework
- Understanding the Security Framework
- Describe Secure Physical Infrastructure
- Discuss Security of the Equipment
- Analyze Secure Behaviour
- Discuss Information Security Environment in India

11.1 INTRODUCTION

An e-business should manage its e-business risks as a business issue, not just as a technology issue. An e-business must consider the direct financial impact of immediate loss of revenue, compensatory payments, and future revenue loss from e-business risks such as:

1. Business interruptions caused by website defacement or denial-of-service attacks;
2. Litigation and settlement costs over employees' inappropriate use of e-mail and the Internet;
3. Product or service claims against items advertised and sold via a website;
4. Web-related copyright, trademark, and patent infringement lawsuits; and
5. Natural or weather-related disasters.

An e-business should put in place an effective risk management program that includes the following:

- Network and website security and intruder detection programs
- Antivirus protection
- Firewalls
- Sound security policies and procedures
- Employee education

Another important component of a risk management program is the transfer of risk via insurance. Table 11.1 illustrates some of the different kinds of insurance coverage an e-business should consider when developing an effective risk management program. It is a good idea for an e-business's management to consult with a commercial insurance broker that offers e-risk management services, to help develop a risk management plan including insurance coverage.

Table 11.1 E-Risk Insurance

E-risk insurance	Coverage
Computer Virus Transmission	Protects against losses that occur when employees open infected e-mail attachments or download virus-laden software.
Extortion and Reward	Responds to Internet extortion demands and/or pays rewards to help capture saboteurs.
Unauthorized Access/ Unauthorized Use	Covers failure to protect against third-party access to data and transactions.
Specialized Network Security	Responds to breach of network security and resulting losses.
Media Liability	Protects against intellectual property infringement losses.
Patent Infringement	Covers defensive and offensive costs when battling over patent infringement issues.
Computer Server and Services Errors & Omissions	Protects e-businesses against liability for errors and omissions when their professional advice causes a client's financial loss.

11.2 THE FIREWALL CONCEPT

An Internet firewall is a system or group of systems that enforces a security policy between an organization's network and the Internet. The firewall determines which inside services may be accessed from the outside, which outsiders are permitted access to the permitted inside services, and which outside services may be accessed by insiders. For a firewall to be effective, all traffic to and from the Internet must pass through the firewall, where it can be inspected. The firewall must permit only authorized traffic to pass, and the firewall itself must be immune to penetration. Unfortunately, a firewall system cannot offer any protection once an attacker has got through or around the firewall.

It is important to note that an Internet firewall is not just a router, a bastion host, or a combination of devices that provides security for a network. The firewall is part of an overall security policy that creates a perimeter defence designed to protect the information resources of the organization. This security policy must include published security guidelines to inform users of their responsibilities; corporate policies defining network access, service access, local and remote user authentication, dial-in and dial-out, disk and data encryption, and virus protection measures and employee training. All potential points of network attack must be protected with the same level of network security. Setting up an Internet firewall without a comprehensive security policy is like placing a steel door on a tent.

A firewall is an approach to security. It helps implement a larger security policy that defines the services and access to be permitted, and it is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to control access to or from a protected network, i.e. a site. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

A firewall system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or a subnet from protocols and services that can be abused from hosts outside the subnet. A firewall system is usually located at a higher-level gateway, such as a site's connection to the Internet. However, firewall systems can be located at lowerlevel gateways to provide protection for some smaller collection of hosts or subnets.

Why Firewalls?

The general reasoning behind firewall usage is that without a firewall, a subnet's systems expose themselves to inherently insecure services, and to probes and attacks from hosts elsewhere on the network. In a firewall-less environment, network security relies totally on host security and all hosts must, in a sense, cooperate to achieve a uniformly higher level of security. The larger the subnet, the less manageable it is to maintain all hosts at the same level of security. As mistakes and lapses in security become more common, break-ins occur not as the result of complex attacks, but because of simple errors in configuration and inadequate passwords.

A firewall approach provides numerous advantages to sites by helping to increase overall host security. The following sections summarize the primary benefits of using a firewall.

Protection of Vulnerable Services

A firewall can greatly improve network security and reduce risks to hosts on the subnet by filtering inherently insecure services. As a result, the subnet network environment is exposed to fewer risks, since only selected protocols will be able to pass through the firewall.

For example, a firewall could prohibit certain vulnerable services such as Network File System (NFS) from entering or leaving a protected subnet. This provides the benefit of preventing the services from being exploited by outside attackers, but at the same time permits the use of these services with greatly reduced risk of exploitation.

Firewalls can also provide protection from routing-based attacks, such as source routing, and attempts to redirect routing paths to compromised sites via Internet Control Message Protocol or ICMP redirects. A firewall could reject all source-routed packets and ICMP redirects and then inform administrators of the incidents.

Controlled Access to Site Systems A firewall also provides the ability to control access to site systems. For example, some hosts can be made reachable from outside networks, whereas others can be effectively sealed off from unwanted access. A site could prevent outside access to its hosts except for special cases such as mail servers or information servers.

 This brings to the fore an access policy that firewalls are particularly adept at enforcing: do not provide access to hosts or services that do not require access. If, for example, a user requires little or no network access to her desktop workstation, then a firewall can enforce this policy.

Concentrated Security

A firewall can actually be less expensive for an organization in that all or most modified software and additional security software could be located on the firewall systems as opposed to being distributed on many hosts. In particular, one-time password systems and other addon authentication software could be located at the firewall as opposed to each system that needed to be accessed from the Internet.

Enhanced Privacy

Privacy is of great concern to certain sites, since what would normally be considered innocuous information, might actually contain clues that would be useful to an attacker. Using a firewall, some sites wish to block services such as finger and Domain Name Service. Finger displays information about users, such as their last login time, whether they have read mail, and other items. But, finger could leak information to attackers about how often a system is used, whether the system has active users connected, and whether the system could be attacked without drawing attention.

Firewalls can also be used to block DNS information about site systems; thus, the names and IP addresses of site systems would not be available to Internet hosts. Some sites feel that by blocking this information, they are hiding information that would otherwise be useful to attackers.

Need for Usage Statistics on Network

If all access to and from the Internet passes through a firewall, the firewall can log accesses and provide valuable statistics about network usage. A firewall, with appropriate alarms that sound when suspicious activity occurs, can also provide details on whether the firewall and network are being probed or attacked.

It is important to collect statistics about network usage and evidence of probing for a number of reasons. Of primary importance is, knowing whether the firewall is withstanding probes and attacks, and determining whether the controls on the firewall are adequate. Network usage statistics are also important as input into network requirements studies and risk analysis activities.

Policy Enforcement

Lastly, but perhaps most importantly, a firewall provides the means for implementing and enforcing a network access policy. In effect, a firewall provides access control to users and services. Thus, a network access policy can be enforced by a firewall, whereas without a firewall, such a policy depends entirely on the cooperation of the users. A site may be able to depend on its own users for their cooperation. However, it cannot or it should not depend on the Internet users in general.

11.3 FIREWALL COMPONENTS

The primary components (or aspects) of a firewall are:

1. Network policy
2. Advanced authentication mechanisms
3. Packet filtering
4. Application gateways.

The following sections describe each of these components in detail.

Network Policy

There are two levels of network policy that directly influence the design, installation and use of a firewall system. The higher-level policy is an issue-specific network access policy that defines those services which will be allowed or explicitly denied from the restricted network, how these services will be used, and the conditions for exceptions to this policy. The lower-level policy describes how the firewall will actually go about restricting the access and filtering the services

that were defined in the higher level policy. The following sections describe these policies in brief.

Service access policy.

The service access policy should focus on Internet-specific use issues as defined above, and perhaps all outside network access (i.e., dial-in policy, and SLIP and PPP connections) as well. This policy should be an extension of an overall organizational policy regarding the protection of information resources in the organization. For a firewall to be successful, the service access policy must be realistic and sound, and should be drafted before implementing a firewall. A realistic policy is one that provides a balance between protecting the network from known risks, while still providing users access to network resources. If a firewall system denies or restricts services, it usually requires the strength of the service access policy to prevent the firewall's access controls from being modified on an ad hoc basis. Only a management-backed sound policy can provide this.

A firewall can implement a number of service access policies. However, a typical policy may be to allow no access to a site from the Internet, but allow access from the site to the Internet. Another typical policy would be to allow some access from the Internet, but perhaps only to selected systems such as information servers and e-mail servers. Firewalls often implement service access policies that allow some user access from the Internet to selected internal hosts, but this access would be granted only if necessary and only if it could be combined with advanced authentication.

Firewall design policy.

The firewall design policy is specific to the firewall. It defines the rules used to implement the service access policy. One cannot design this policy in a vacuum isolated from understanding issues such as firewall capabilities and limitations, and threats and vulnerabilities associated with TCP/IP. Firewalls generally implement one of the following two basic design policies:

1. Permit any service unless it is expressly denied
2. Deny any service unless it is expressly permitted.

A firewall that implements the first policy allows all services to pass into the site by default, with the exception of those services that the service access policy has identified as disallowed. A firewall that implements the second policy denies all services by default, but passes those

services that have been identified as allowed. This second policy follows the classic access model used in all areas of information security.

The first policy is less desirable, since it offers more avenues for getting around the firewall, i.e. users could access new services currently not denied by the policy (or even addressed by the policy) or run denied services at non-standard TCP/UDP ports that are not denied by the policy. Certain services such as X Windows, FTP, Archie, and RPC cannot be filtered easily and are better accommodated by a firewall that implements the first policy. The second policy is stronger and safer, but is more difficult to implement and may impact users in that certain services such as those just mentioned may have to be blocked or restricted.

The relationship between the high-level service access policy and its lower level counterpart is reflected in the discussion above. This relationship exists because the implementation of the service access policy is heavily dependent upon the capabilities and limitations of the firewall system, as well as upon the inherent security problems associated with the wanted Internet services. For example, wanted services defined in the service access policy may have to be denied if the inherent security problems in these services cannot be effectively controlled by the lower level policy and if the security of the network takes precedence over other factors. On the other hand, an organization that is heavily dependent on these services to meet its mission may have to accept higher risk and allow access to these services. This relationship between the service access policy and its lower-level counterpart allows for an iterative process in defining both, thus producing the realistic and sound policy initially described.

The service access policy is the most significant component of the four described here. The other three components are used to implement and enforce the policy. (And as noted above, the service access policy should be a reflection of a strong overall organization security policy.) The effectiveness of the firewall system in protecting the network depends on the type of firewall implementation used, the use of proper firewall procedures, and the service access policy.

Advanced Authentication

Security lapses on the identity of Internet users have occurred in part due to the weaknesses associated with traditional passwords. For years, users have been advised to choose passwords that would be difficult to guess, or not to reveal their passwords. However, even if users follow this advice (and many do not), the fact that intruders can and do monitor the Internet for passwords that are transmitted in the clear has rendered traditional passwords obsolete.

Advanced authentication measures such as smartcards, authentication tokens, biometrics, and software-based mechanisms are designed to counter the weaknesses of traditional passwords. While the authentication techniques vary, they are indeed similar in one aspect. The passwords generated by advanced authentication devices cannot be reused by an attacker who has monitored a connection. Given the inherent problems with passwords on the Internet, an Internet-accessible firewall that does not use or does not contain the hooks to use advanced authentication makes little sense.

Some of the more popular advanced authentication devices in use today are called onetime password systems. A smartcard or authentication token, for example, generates a response that the host system can use in place of a traditional password. The token or card works in conjunction with software or hardware on the host, and therefore, the generated response is unique for every login. The result is a one-time password which, if monitored, cannot be reused by an intruder to gain access to an account.

Since firewalls can centralize and control site access, the firewall is the logical place for the advanced authentication software or hardware to be located. Although advanced authentication measures could be used at each host, it is more practical and manageable to centralize the measures at the firewall. Figure 11.1 illustrates that a site without a firewall using advanced authentication permits unauthenticated application traffic, such as Telnet or FTP, directly to site systems. If the hosts do not use advanced authentication, then intruders could attempt to crack passwords or could monitor the network for login sessions that would include the passwords. The figure also shows a site with a firewall using advanced authentication, such that Telnet or FTP sessions originating from the Internet to site systems must pass the advanced authentication before being permitted to the site systems. The site systems may still require static passwords before permitting access. However, these passwords would be protected against exploitation, even if the passwords are monitored, as long as the advanced authentication measures and other firewall components prevent intruders from penetrating or bypassing the firewall.
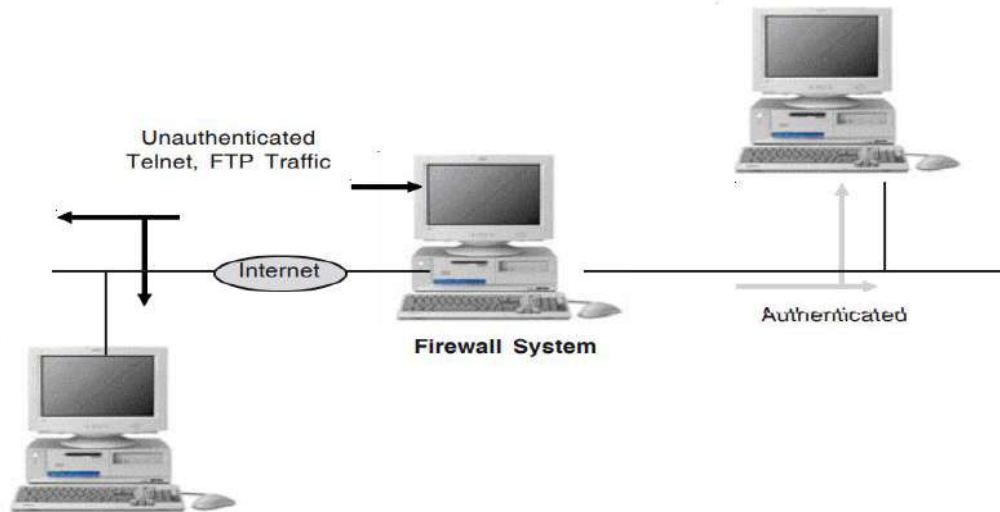
Fig. 11.1 Advanced authentication on a firewall to pre-authenticate Telnet, FTP traffic.

Packet Filtering IP packet filtering is done, usually, using a packet filtering router designed for filtering packets, as they pass between the router's interfaces. A packet filtering router usually can filter IP packets based on some or all of the following fields:

1. Source IP address
2. Destination IP address
3. TCP/UDP source port
4. TCP/UDP destination port.

Not all packet filtering routers currently filter the source TCP/UDP port, though vendors have now started incorporating this capability. Some routers examine the router's network interfaces in which a packet arrives, and then use this as an additional filtering criterion. Some UNIX hosts provide packet filtering capability, although most do not.

Filtering can be used in a variety of ways to block connections from or to specific hosts or networks, and to block connections to specific ports. A site might wish to block connections from certain addresses, such as from hosts or sites that it considers to be hostile or untrustworthy. Alternatively, a site may wish to block connections from all addresses external to the site (with certain exceptions, such as SMTP for receiving e-mail) (see Figure 11.2).
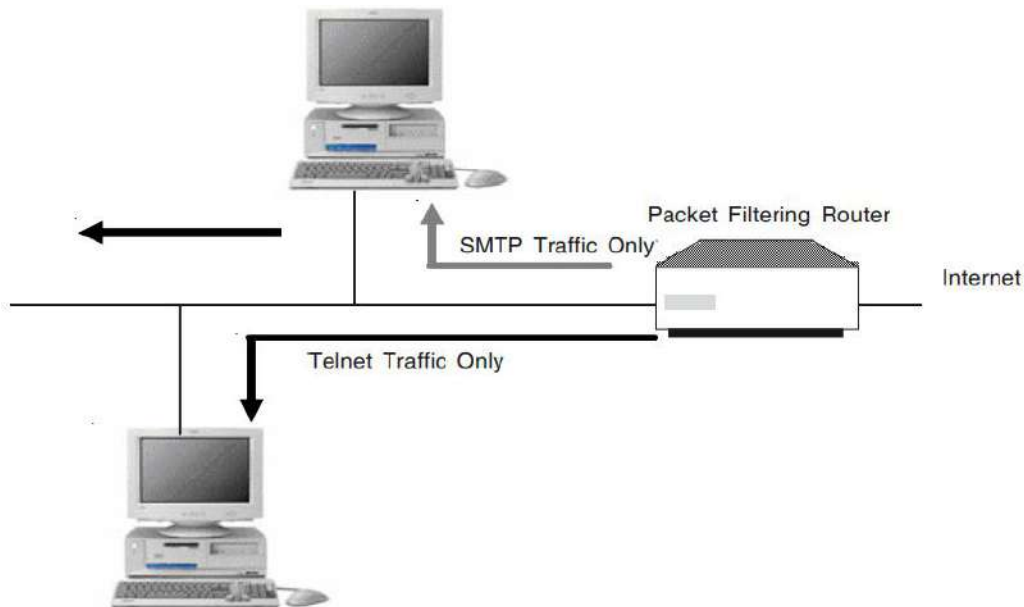
Fig. 11.2 Representation of packet filtering on Telnet and SMTP

Application Gateways To counter some of the weaknesses associated with packet filtering routers, firewalls need to use software applications to forward and filter connections for services such as Telnet and FTP. Such an application is referred to as a proxy service, while the host running the proxy service is referred to as an application gateway. Application gateways and packet filtering routers can be combined to provide higher levels of security and flexibility than if either were used alone.

11.4 WHAT SHOULD A FIREWALL CONTAIN?

Once the decision is made to use firewall technology to implement an organization's security policy, the next step is to procure a firewall that provides the appropriate level of protection and is cost-effective. However, what features should a firewall have, at a minimum, to provide effective protection? One cannot answer this question entirely with specifics, but it is possible to recommend that, in general, a firewall should have the following significant features or attributes.

1. Be able to support a "deny all services except those specifically permitted" design policy, even if that is not the policy used;

2. Support your security policy, not impose one;

3. Be flexible and able to accommodate new services and needs if the security policy of the organization changes;

4. Contain advanced authentication measures, or should contain the hooks for installing advanced authentication measures;

5. Employ filtering techniques to permit or deny services to specified host systems, as needed;

6. Use proxy services for services such as FTP and Telnet, so that advanced authentication measures can be employed and centralized at the firewall. If services such as NNTP, http, or gopher are required, the firewall should contain the corresponding proxy services;

7. Contain the ability to centralize SMTP access, to reduce direct SMTP connections between site and remote systems. This results in centralized handling of site e-mail;

8. Accommodate public access to the site, such that public information servers can be protected by the firewall but can be segregated from site systems that do not require the public access;

9. Contain the ability to concentrate and filter dial-in access;

10. Contain mechanisms for logging traffic and suspicious activity, and also mechanisms for log reduction so that logs are readable and understandable;

11. Be developed in a manner that its strength and correctness is verifiable. It should be simple in design so that it can be understood and maintained;

12. Be updated with patches and other bug fixes, at regular time intervals.

If the firewall requires an operating system such as UNIX, a secured version of the operating system should be a part of the firewall, with other security tools as necessary to ensure firewall host integrity. The operating system should have all patches installed.

The IP filtering language should be flexible, user-friendly to program, and should filter on as many attributes as possible, including source and destination IP address, protocol type, source and destination TCP/UDP port, and inbound and outbound interface.

There are undoubtedly more issues and requirements, however many of them will be specific to each site's own needs. A thorough requirements definition and high-level risk assessment will identify most issues and requirements; however it should be emphasized that the Internet is a constantly changing network. New vulnerabilities can arise, and new services and enhancements to other services may represent potential difficulties for any firewall installation. Therefore, flexibility to adapt to changing needs is an important consideration.

11.5 BENEFITS OF AN INTERNET

Firewall Internet firewalls manage access between the Internet and an organization's private network. Without a firewall, each host system on the private network is exposed to attacks from other hosts on the Internet. This means that the security of the private network would depend on the "hardness" of each host's security features and would be only as secure as the weakest system.

Internet firewalls allow the network administrator to define a centralized "choke point" that keeps unauthorized users such as hackers, crackers, vandals, and spies, out of the protected network, prohibits potentially vulnerable services from entering or leaving the protected network, and provides protection from various types of routing attacks. An Internet firewall simplifies security management, since network security is consolidated on the firewall systems rather than being distributed to every host in the entire private network.

Firewalls offer a convenient point where Internet security can be monitored and alarms generated. It should be noted that for organizations that have connections to the Internet, the question is not whether attacks will occur but, when do they occur? Network administrators must audit and log all significant traffic through the firewall. If the network administrator does not take the time to respond to each alarm and examine logs on a regular basis, there is no need for the firewall, since the network administrator will never know if the firewall has been successfully attacked!

For the past few years, the Internet has been experiencing an address space crisis that has made registered IP addresses a scarce resource. This means that organizations wanting to connect to the Internet may not be able to obtain enough registered IP addresses to meet the demands of their user population. An Internet firewall is a logical place to deploy a Network Address Translator (NAT) that can help alleviate the address space shortage and eliminate the need to renumber when an organization changes its ISPs. An Internet firewall is the perfect point to audit or log Internet usage. This permits the network administrator to justify the expense of the Internet connection to management, pinpoint potential bandwidth bottlenecks, and provide a method for departmental charge-backs if this fits the organization's financial model.

An Internet firewall can also offer a central point of contact for information delivery service to customers. The Internet firewall is the ideal location for deploying World Wide Web and FTP

servers. The firewall can be configured to allow Internet access to these services, while prohibiting external access to other systems on the protected network.

Finally, some might argue that the deployment of an Internet firewall creates a single point of failure. It should be emphasized that if the connection to the Internet fails, the organization's private network will still continue to operate though the Internet access is lost. If there are multiple points of access, each one becomes a potential point of attack that the network administrator must firewall and monitor regularly.

By adequately securing little corners of cyberspace, you can instil and maintain the right levels of trustworthiness that your customers both demand and deserve. We have seen that e-security requires a holistic approach. It is as much a set of behaviours as it is a bundle of software tools and network sniffers which, by themselves, might leave us with a false sense of security. Analogies abound in our everyday lives. We buy expensive alarm systems for our homes, move around elite communities, opt for a German Shepherd or a Doberman Pinscher, and yet we know that these are only partial solutions.

True security requires that you educate your staff, develop manageable security policies and procedures, and create a secure organization (whether it be one or many employees) that enforces those policies. It requires that you properly configure your network for your organization, without assuming that off-the-shelf configurations are right for you. It also means investing in the tools and expertise that you deem necessary to evaluate and monitor your network in order to detect intrusions before they actually happen, as well as develop a clear strategy for dealing with an intrusion when it inevitably happens. Finally, a secure network calls for constant vigilance. This means keeping up with the technological changes around you by reading trade journals and periodicals, joining user groups that discuss security issues and disseminate the latest security information, and attending conferences, seminars, and any relevant training that will keep you abreast of evolving security needs.

11.6 DEFINING AN ENTERPRISE-WIDE SECURITY FRAMEWORK

Traditionally, organizations have relied on policies to communicate high-level directives from the management. These documents, once issued, provide a top-down influence for everyone in the company—from business units to departments to individual employees. Furthermore, these policies typically were developed at one time in the organization's evolution to capture the current environment. One of the major challenges for an organization in this area is the continued

growth and adaptation of the policies to mirror the transformation within the organization. The fastest area of growth and change within an organization is Information Systems. With the rapid development and push towards new technologies, organizations find themselves striving to maintain current technical environments with outdated policies. Secondly, with the emergence of new technology strategies such as Intranets and Extranets, security and protection of informational assets has become paramount.

The first step is an enterprise-wide Information Systems security policy that is consistently enforced even as business needs change. Unfortunately, most companies have only bits and pieces of security scattered throughout the organization. These may make some departments or individuals feel safe, but they do little to protect the enterprise as a whole. A security policy should include People, Policy, and Technology. The security process is a mixture of these three elements. Each element depends in some manner on the other elements. Also, issues receive greater coverage when the elements are combined. The controls environment is greatly enhanced when these three elements work in concert. A simple diagram will suffice to illustrate this (see Figure 11.3). This diagram shows the basic elements and also the coverage areas.

As you move towards the union of these elements, the controls environment increases— there is greater coverage. Let us understand these three elements individually.

People. This core element is the most important. The people element comprises the people and various roles and responsibilities within the organization. These are the people that are put in place to execute and support the process. A few key roles include senior management, security administrators, system and IT administrators, end users, and auditors.

Policy. This element comprises the security vision statement, security policy and standards, and the control documentation. This is basically the written security environment—the bible that the security process will refer to for direction and guidance.
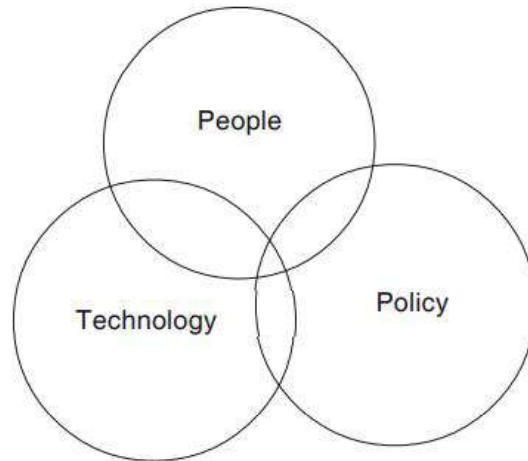
Fig. 11.3 People, policy and technology model.

Technology.

This element includes tools, methods, and mechanisms in place to support the process. These are core technologies—the operating systems, the databases, the applications, the security tools—embraced by the organization. The technology then is the enforcement, monitoring, and operational tools that will facilitate the process.

The concept is that each core element could be measured for effectiveness and coverage. Also, issues can be measured against the model to determine what controls coverage for that issue. The objective then is to move issues into the intersecting areas of the elements—with the final objective of moving the issue into the middle area of greatest coverage. As risk issues are identified, each step to manage the risk will fall into one of the core elements of people, policy, or technology. If the issue is resolved with one of the elements, addressing one of the other elements can enhance this resolution. As the core elements are added to the controls environment and utilized in concert, the issue is then resolved on several fronts— the controls coverage is greater.

The People, Policy, Technology (PPT) Model

The PPT model can be illustrated with a few simple examples. Figure 11.4 shows the PPT model with regards to Internet usage and misuse. Users are educated on the proper usage of the Internet. The controls environment relies solely on the user. An Internet usage policy is written to document proper use of the Internet and the consequences of misuse. The controls environment now is supported by two of the three core elements.

51

The PPT model is simply the analysis of a risk issue. If the issue is broken down into the three core elements, action items can be determined for each core element. In this manner, control coverage can be moved from one element to two, and ultimately to coverage by all of the elements.
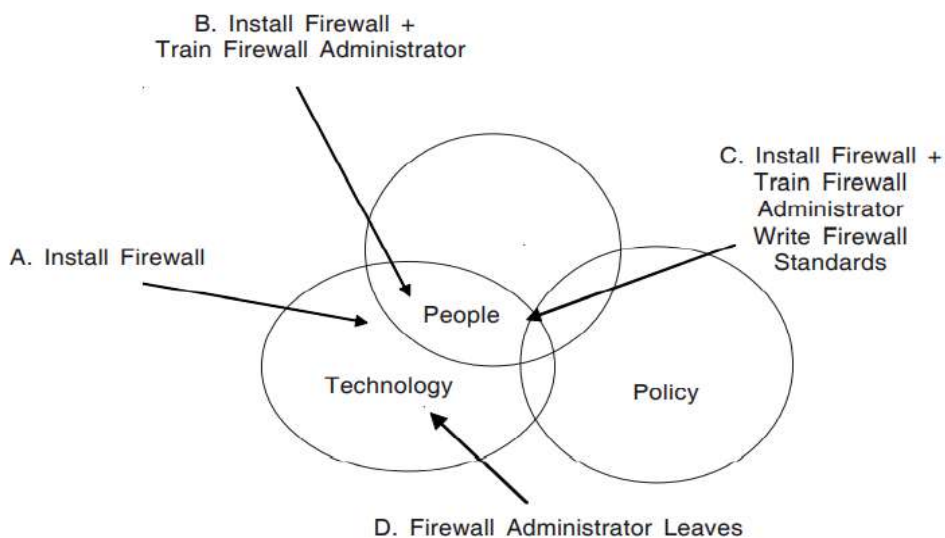

Fig. 11.4 Internet connection: coverage by three elements.

11.7 UNDERSTANDING THE SECURITY FRAMEWORK

Key elements, also referred to as the "Four Pillars" to Information Security, include:

- Solid Senior Management Commitment
- An overall Security Vision and Strategy
- A comprehensive Training and Awareness Program
- A solid Information Security Management Structure including key skill sets and documented responsibilities as depicted in Figure 11.5.

Within the four "pillars" of the program, several phases are included.

The first is the Decision Driver Phase, which contains factors determining the business drivers of security. These include Technology Strategy and Usage, Business Initiatives and Processes, and Threats, Vulnerabilities and Risk. All these combine to form a unique "Security Profile" of the organization. The "profile" needs to be reflected in the Security Policies and Technical Controls. The next facet of the Information Security Framework includes the design of the security environment, also called the Design Phase. This is the stage where the organization documents its security policy, the control environment and deals with controls on the technology level. A

key element in this process is not only the clear definition of security policy and technical control information, but also the "Security Model" of the enterprise. Information Classifications and Risk Assessment methods fall under this component. These processes allow the organization to manage risk appropriately and identify the risks and value of information assets.

The final facet of the Information Security Framework is the Implementation Phase. This begins by documenting the Administrative and End-User guidelines and procedures.
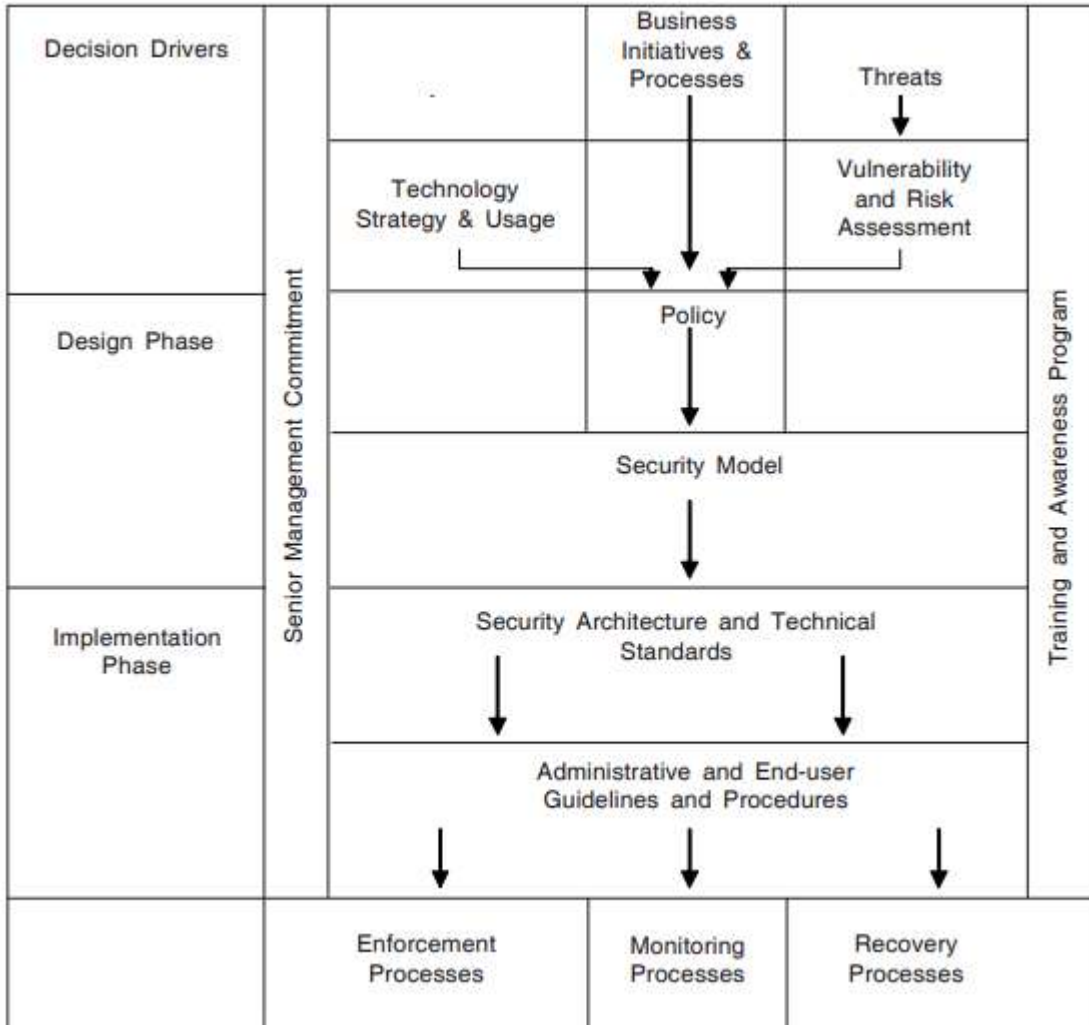

Fig. 11.5 Information security management structure.

These guidelines must be succinct and flexible for the changing environment. Enforcement, Monitoring, and Recovery processes are then layered on for the operational support of the security program. These processes are "where the rubber hits the road". All the benefits of the Security Program design and documentation are diminished if it is not put into effect on an operational day-to-day basis.

11.8 SECURE PHYSICAL INFRASTRUCTURE

All of us are concerned about physical and environmental security. We may not always do a formal risk assessment exercise, but intuitively, we try to ensure that we are secure.

BS 7799 is very explicit about the requirements of this domain, which is applicable to the business premises and business information processing facilities. Design, implementation and monitoring of many controls for this domain will have to be jointly done with the physical security department.

Security can be best achieved by ensuring multiple layers of security and not depending on a single measure. This principle is very evident here. The controls for physical and environmental security are defined in three areas:

- Security of the premises
- Security of the equipment
- Secure behaviour

11.8.1 Security of the Premises

Physical security perimeter. We begin by defining the boundary of the premises and examining the security requirement, based on the risk assessment. The best way to do this will be to walk around the premises and 'case the joint.' Evaluate all the entry points through which an intruder could come in. Take help of a security agency to do this. Do not depend on your skills as an armchair detective. The classical approach to securing the premises is to create multiple barriers. Start with the outermost perimeter. How much resistance this perimeter is expected to provide? Based on risk assessment, you need to decide all the physical specifications like height, width for the protective wall. Next, consider all the entry points. Are the doors strong enough? Are the door frames strong enough? Are the windows, ventilators, air-conditioning firmly secured with grills? Do the physical barriers extend from real floor to real ceiling, or is there a gap between false ceiling and real ceiling through which somebody could crawl in? We need to detect the weakest link while assessing the perimeter defence. How are the access points guarded? Are they controlled through card-controlled entry gates? Are watchmen, guards or receptionist monitoring the entry points?

Physical entry controls. Only the authorized persons should be allowed access to the secure areas. This objective could be achieved by having a clear access control policy defining the

access rights. Based on this policy, appropriate measures should be in place. These measures may take the form of access control devices like swipe card controlled doors, logging information about visitors and visible identification badges.

Securing offices, rooms and facilities. Location of the secure office within the physically secure perimeter should be chosen with care. All the risks pertaining to fire, flood, explosion, civil unrest and other forms of natural or man-made disaster should be considered. There could also be threat from neighbouring premises, caused by leakage of water, spreading of fire, or storage of toxic/inflammable/explosive material. Even bulk supplies like stationery should not be stored within the secure premises.

The secure location should not be publicized in any manner. No display board, banners, signs to indicate the presence of any important information processing activity. Even the internal telephone directories should not be readily accessible to outsiders.

Support facilities like photocopier, fax machines, which are constantly accessed by everyone, should be located away from the secure area. Suitable intrusion detection systems like CCTV, motion sensors etc. should be installed and regularly tested.

Working in secure areas. Security equipment like CCTV and swipe-card controlled gates are of no use if the persons working in these locations are not trustworthy, or are incompetent, or simply lack awareness of their responsibility. They should be hand-picked and trained for these operations. They should not brag about their nature of work or location. Also, information should be provided on need-to-know basis. Segregation of duties should be scrupulously followed with strict supervision. Third-party personnel should be granted restricted access. No photographic, video, audio or other recording equipment must be allowed inside the premises, unless authorized.

Isolated delivery and loading areas. We have taken care of every aspect of physical security in the above paragraphs, but do we know how canteen facilities get into secured premises? How the trash is taken out? How the courier delivers the parcels? In industrial premises, there could be constant movement of incoming and outgoing material. All this traffic needs to be isolated from the secure office area, so that it does not pose a threat.

11.8.2 Security of the Equipment

Equipment setting and protection. Our next concern is the appropriate security of the equipment. Information processing equipment needs to be handled carefully. The first level of

equipment protection depends on physical location. The location should minimize the need for unnecessary access, as well as prevent snooping. It should be such as to minimize the risk of theft as well as the risk from natural disasters like fire, flood, chemicals etc. Also, consider risks like electrical and electromagnetic interference, humidity etc.

Power supplies. Information processing will come to halt in the absence of a suitable power supply. This could be the worst type of a denial-of-service attack. A thorough business risks assessment is necessary to understand the impact on non-availability of power for certain durations. Based on the evaluation, appropriate measures need to be taken. These could be:

1. Taking power from multiple feeds of electric supply.
2. In case all the electric supplies fail simultaneously, you need to have an uninterruptible power supply (UPS) with adequate battery capacity capable of sustaining the initial load.
3. The UPS could in-turn be supported by backup generator sets.
4. The backup generator would require adequate supply of fuel, which also needs to be stored with replenishment, assured by the suppliers.
5. Proper installation of emergency lights should also be planned; lightning protection should be provided to the power installation and the communication lines.

Cabling security. We really need to remember every detail, including the proverbial last nail. Do we know the physical layout of power cables and communication cables in our premises? The first step will be to obtain wiring diagrams and update them. Then, do a physical inspection and assess the protection needs against damage, interference or interception. Establish the best practices for laying the network cables as well as power cables, and ensure that these are actually implemented. The next step is to decide on additional security protection required for the network. This could be expensive for an old installation. Safety measures like use of armoured conduit cables, underground ducts, or fibre optic cabling will require huge investment and need to be justified based on risk assessment. But simple measures like providing locks to the communication cable patch board, which are often over-looked, should be immediately implemented.

Equipment maintenance. It is normally expected that due care is taken for equipment maintenance, and proper records are maintained. From a security angle, two more measures are required. One is to maintain record of faults that were noticed, and the second step is to maintain records of all equipment sent off the premises for maintenance.

Security of equipment off premises. Shrinking size of computers and expanding wide area networks have made the computer equipment extremely mobile. Processing as well as storage capacity of mobile devices has been following Moore's law of doubling every 18 months. Securing these devices is as important as securing the data centre. Various controls that should be considered are: administrative controls like permissions and corporate policy on use of mobile computers in places like airplanes, physical controls like securing the devices with security chains, alarms, and storing them at non-obvious places, using access control devices like USB tokens, and finally taking adequate insurance cover.

Secure disposal or reuse of equipment. Storage devices have long memory, unless specifically destroyed. Mere deletion is not enough. This becomes important when an old computer equipment is disposed off or transferred to another location. Equipment sent for repair are equally susceptible to reading of data from the 'deleted' storage devices. Every such device should be subjected to a thorough erasing and overwriting to destroy the data. Since some reports claim that the data could be recovered even after multiple overwriting and formatting, it may be desirable to physically destroy the media containing top secret information.

11.8.3 Secure Behaviour

Clear desk and clear screen policy.

Our concern for information security should not stop at securing the premises and equipment. Sensitive information could be accessible in many forms, and it is necessary to identify and protect the information in all its incarnations. Classification of information will help to identify the sensitivity, but having an organizational "clear desk and clear screen policy" could ensure actual protection. In brief, it means keep everything under lock and key and do not allow anybody to snoop. The following guidelines should be issued:

- Lock up all documents and media when not being used.
- Protect the computers and terminals through use of key locks, passwords, and screen savers.
- Fax and telex machines used for confidential information should not be left unattended.
- Access to photocopiers and scanners is restricted after office hours.
- Printing of classified information should be supervised and all printouts must be removed immediately.

Removal of property. Any movement of equipment, information or software should be only with proper authorization. All these movements should be logged and records maintained for all outgoing and incoming items. In these days of storage media capable of containing gigabytes of information, this procedure becomes very important. Employees should be made aware that spot checks would be carried out to ensure full compliance. Security is being paranoid about threats. Physical security is very demonstrative about this paranoia. But, it also sets the tone about the organization's concern about information security.

11.9 Information Security Environment in India

Most Indian companies that are aiming to go global will require certifying their ability to maintain proper security levels when scouting for international clients. Information security is no more a mere legal requirement but it is fast becoming a factor for companies to compete on and grow businesses. A "secure and reliable" environment—defined by strong copyright, IT and cyber laws—is an imperative for the growth and future success of the ITES–BPO industries. NASSCOM has been proactive in pushing this cause and ensuring that the Indian Information Security environment benchmarks with the best across the globe. Indian ITES– BPO companies today adhere to international best practices—they are regularly audited by independent certified auditors, comply with international standards at the highest levels, update procedures and practices regularly and meet, if not exceed the worldwide information security standards to ensure that data and personal information of international customers is adequately protected.

Security Environment in India

Indian companies are known for their quality deliverables. International certifications like ISO 9000 went a long way in establishing this reputation. Likewise following international standards in information security is also helping Indian companies build credibility among customers. While most Indian BPO firms are recognized for high quality processes and services, information security practices need to be constantly reviewed and updated according to the rapidly changing environment. Customer data demands special focus.

Indian companies have robust security practices comparable to those followed by western companies. Indian companies primarily comply with BS 7799—a global standard that covers all domains of security. Companies sign Service Level Agreements (SLA), which have very strict confidentiality and security clauses built into them at the network and data level. Such SLAs also

cover all relevant laws that the companies want its offshore providers to comply with and actions that can be taken in case of breaches.

Laws such as the IT Act, 2000, Indian Copyright Act, Indian Penal Code Act and the Indian Contract Act, 1972 provide adequate safeguards to companies offshoring work to US and UK. Most of the BPO companies providing services to UK clients ensure compliance with UK Data Protection Act, 1998 (DPA) through contractual agreements.

Companies dealing with US clients require compliance depending upon the industry served, e.g. Healthcare requires compliance with HIPAA, Financial services require compliance with GLBA. To ensure compliance with such laws, Indian vendors follow security practices as specified by clients such as security awareness, protection of information, non-disclosure agreements, screening of employees, etc. Further, clients conduct periodic audits to ensure compliance. Many companies in India are undergoing/have undergone SAS-70 Audit. SAS-70 assignments helps service companies operating from India to implement and improve internal controls, ensure minimal disruptions to business from clients' auditors, and is potent marketing tool in the face of increasing competition.

NASSCOM's Security Initiative

NASSCOM has taken a holistic view of Information Security through its 'Trusted Sourcing'5 Initiative to strengthen the regulatory framework and further improve India's attractiveness as an outsourcing destination. This multi-pronged initiative is targeted at employees, organizations, enforcement agencies and policy amendment, through a '4E Framework'—Engagement, Education, Enactment and Enforcement.

NASSCOM has been working closely with the ITES–BPO industry in India, to create a robust and secure Information Security culture, and in association with other stakeholders like the Indian Government on the issue of creating a relevant regulatory environment. All these initiatives aim to further strengthen information security environment, together with initiatives being rolled out by NASSCOM and the ITES–BPO industry.

NASSCOM, with the Indian government has also laid the foundation for the required legal framework through the proposed Amendments to the Indian IT Act of 2000 which includes laws and policies concerning data security and cyber crimes and the Indian Copyright Act of 1972 which deals with copyright issues in computer programs.

11.10 CHECK YOUR PROGRESS

11. "A firewall is an approach to security" Justify.

12. What is Domain Name System?

13. Mention components of a firewall.

14. What is TCP/UDP Port?

15. What is NASSCOM?

Answers to Check your progress

1. It helps implement a larger security policy that defines the services and access to be permitted, and it is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to control access to or from a protected network, i.e. a site. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

2. *DNS*, or the *domain name system*, is the phonebook of the Internet, connecting web browsers with websites.

3. The primary components (or aspects) of a firewall are:

   - Network policy
   - Advanced authentication mechanisms
   - Packet filtering
   - Application gateways.

4. TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol. A key difference between TCP and UDP is speed, as TCP is comparatively slower than UDP. Overall, UDP is a much faster, simpler, and efficient protocol, however, retransmission of lost data packets is only possible with TCP.

5. The National Association of Software and Services Companies (NASSCOM) is a not-for-profit Indian consortium created to promote the development of the country's IT (information technology) and business process outsourcing (BPO) industries.

11.11 SUMMARY

This unit introduces the need for firewall. The benefits of using the firewall is narrated. The physical components of a firewall is described. Significant features of a firewall is highlighted. The benefits of using internet is described. The People, Policy, Technology (PPT) Model with a diagram is narrated. Information security management structure is detailed. Also, a brief note is given on Information Security Environment in India.

11.12 KEYWORDS

- **Information security management** is a way of protecting an organisation's sensitive data from threats and vulnerabilities. The process is typically embedded via an ISMS (information security management system), which provides the framework for managing information security.

- *ISO 9000* **family** is the world's most best-known quality management standard for companies and organizations of any size.

- A **service-level agreement** (SLA) sets the expectations between the service provider and the customer and describes the products or services to be delivered, the single point of contact for end-user problems, and the metrics by which the effectiveness of the process is monitored and approved.

- **Data Protection Act** gives individuals the right of access to information about themselves which is held by an organisation, and sets out how personal information should be collected, stored and processed.

- A **Network Address Translation** (NAT) is the process of mapping an internet protocol (IP) address to another by changing the header of IP packets while in transit via a router. This helps to improve security and decrease the number of IP addresses an organization needs.

11.13 QUESTIONS FOR SELF STUDY

18. Explain the need for firewall.
19. Narrate the benefits of using the firewall.
20. Explain physical components of a firewall.
21. Mention the significant features of a firewall.
22. Discuss the benefits of using internet.

23. Describe "The People, Policy, Technology (PPT) Model" with a diagram.

24. Explain Information security management structure.

25. Write a note on Information Security Environment in India.

11.14 REFERENCES

5. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

6. Joseph, P. T. (2019). *E-commerce: An Indian perspective*. PHI Learning Pvt. Ltd..

Unit 12: e-PAYMENT SYSTEM

Structure

12.0 OBJECTIVES

After studying this unit, you will be able to:

- Analyze e-payment systems

- Signify the Mobile Payments

- Classification of New Payment Systems

- Discuss Micropayment Systems

- Discuss Properties of Electronic Cash (e-Cash)

- Give an account on e-Cash in Action

- Cheque Payment Systems on the Internet

- Designing e-Payment Systems

- Give an account on Digital Signature

12.1 INTRODUCTION

Main Concerns in Internet Banking

In a survey conducted by the Online Banking Association, member institutions rated security as the most important issue of online banking. There is a dual requirement to protect customers' privacy and protect against fraud. Banking Securely: Online Banking via the World Wide Web provides an overview of Internet commerce and how one company handles secure banking for its financial institution clients and their customers. Some basic information on the transmission of confidential data is presented in Security and Encryption on the Web. A multi-layered security architecture comprising firewalls, filtering routers, encryption and digital certification ensures that your account information is protected from unauthorized access:

- Firewalls and filtering routers ensure that only the legitimate Internet users are allowed to access the system.

- Encryption techniques used by the bank (including the sophisticated public key encryption) would ensure that privacy of data flowing between the browser and the Infinity system is protected.

- Digital certification procedures provide the assurance that the data you receive is from the Infinity system.

The growth of e-commerce is dependent, among other factors, on the existence of secure, user-friendly and cost-effective payment systems. Handling payments is a costly process that has been a central part of bank business for the past century. However, it is now being transformed by technological developments, and in particular, the Internet. The importance of the payment function lies in the fact that it could encourage convergence between sectors with disparate objectives, since payment systems are the common denominator of all e-commerce transactions. Conceptually, the alternative means of payment available for e-commerce may be classified as either electronic money (e-money), or electronic access products. The difference between them is that whereas electronic access products basically provide Internet access to traditional products (credit card payments, bank transfers, and the like), e-money is a new concept, and in particular is considered to be "private money not depending on central bank reserves."

Consolidated methods of payment used for distance selling mostly at national level, such as cheque, cash-on-delivery and credit-transfer mechanisms, have proven easy to adapt to electronic

transactions. The credit card system has to date been the usual payments instrument for goods ordered over the Internet. This is despite security concerns and relatively higher transaction cost. Nevertheless, the lack of a widely accepted e-payment system is not considered to be a major barrier for the gearing up of e-commerce. The most important factors are undoubtedly user trust and user confidence.

12.2 E-PAYMENT SYSTEMS

E-payment systems are becoming central to e-commerce as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities. The current state of online electronic payments is in many ways reminiscent of the medieval ages. The merchants of Asia and Europe faced a similar problem while trying to unlock the commercial potential of the expanding marketplace. Those ancient traders faced a number of obstacles, such as conflicting local laws and customs regarding commercial practices, and incompatible and nonconvertible currencies that restricted trade. To circumvent some of these problems, traders invented various forms of payment instruments, such as promissory notes, bills of exchange, gold coins, and barter. The merchants also developed commercial law surrounding the use of these instruments, that proved to be one of the turning points in the history of trade and commerce. We are on the verge of a similar sort of development today with regard to e-payment systems.

Everyone agrees that the payment and settlement process is a potential bottleneck in the fast-moving electronic commerce environment, if we rely on conventional payment methods such as cash, cheques, bank drafts, or bills of exchange. Electronic replicas of these conventional instruments are not well-suited for the speed required in e-commerce purchase processing. For instance, payments of small denominations (micropayments) for bits and pieces of information must be accepted by vendors in real time. Conventional instruments are too slow for micropayments, and the high transaction costs involved in processing them add greatly to the overhead. Therefore, new methods of payment are needed to meet the emerging demands of e-commerce. These new payment instruments must be secure, have a low processing cost, and be accepted widely as global currency tender.

Digital Payment Requirements

For any digital payment system to succeed, the criteria given in Table 12.1 ought to be satisfied.

Table 12.1 Digital payment requirements

Criteria	Need for the criteria
Acceptability	Payment infrastructure needs to be widely accepted.
Anonymity	Identity of the customers should be protected.
Convertibility	Digital money should be convertible to any type of fund.
Efficiency	Cost per transaction should be near zero.
Integration	Interfaces should be created to support the existing system.
Scalability	Infrastructure should not breakdown if new customers and merchants join.
Security	Should allow financial transactions over open networks.
Reliability	Should avoid single points of failure.
Usability	Payment should be as easy as in the real world.

Online Payment Categories

Online payments can be broadly divided into three categories as shown in Table 12.2.

Table 12.2 Online Payment Categories

Category	Description
Micropayment	Transaction value less than 5 euros or dollars. Transaction costs are nearly zero.
Consumer payments	Transaction value between 5 and 500 euros or dollars. Payments are executed by credit card transactions.
Business payments	Transaction value more than 500 euros or dollars. Debit cards or invoices are appropriate solutions in this system.

E-payment systems are proliferating in banking, retail, healthcare, online markets, and even in government—in fact, anywhere money needs to change hands. Organizations are motivated by the need to deliver products and services more cost-effectively and to provide a higher quality of service to customers. Research into e-payment systems for consumers can be traced back to the 1940s, and the first applications, the credit cards, appeared soon after.

Digital Token-based e-Payment Systems

The introduction of charge cards in the early 1900s, beginning with western union in 1914, represented a breakthrough in payments. But while these cards enhanced customer loyalty and stimulated repeat behaviour, they were generally limited to the local market, or in store use. In 1958, Bank of America took a major step forward, introducing what eventually became the modern credit card. Based on extensive test marketing in Fresno, California, it became clear there was a large market for a general purpose bank card featuring a revolving credit facility and

wide acceptance. With the launch of Bank of America's card, the consumer was not tied to one merchant or product, but was now free to make credit purchases at a wide range of outlets. As the adoption of the bank card grew, the potential size of the market for transactions expanded geometrically. It was a profound turning point in the history of money.

The development of the modern electronic payment network took an important step forward in the mid-1970s, with the creation of a global joint venture that would eventually be known as visa. Through shared investments, the visa association created a global system to authorize transactions, clear and settle electronic payments, codify operating regulations to protect consumers and merchants alike, and set interoperability standards to ensure that, unlike cash and cheques, a visa card could be used anywhere in the world.

Two developments in the 1990s further broadened the utility of electronic payments.

Debit cards, a popular "pay now" product, allowed consumers to access funds in a demand deposit account to conduct transaction at the point of sale; and e-commerce emerged as mainstream business channel, both relying on and stimulating electronic payments.

The rapid adoption of these relatively recent developments demonstrate the speed at which the payments landscape is changing. Looking forward, there is broad experimentation in ways to migrate electronic payment functions into consumer devices such as mobile phones, PDAs, and other popular electronic products. This process is well underway in some European and Asian markets where mobile phones are nearly as ubiquitous as payment cards. Visa describes this new range of payment choices as "u-commerce," or universal commerce— the ability to conduct commerce anywhere, anytime, or any way.

This shift in consumer preference is driving major changes in personal consumer expenditures (PCE). The growth in card usage as a share of PCE continues to expand relative to cash and cheques.

Also, in most markets around the world, the use of cash and cheques is declining—a trend that is likely to continue. The trend away from cash and cheques is driven by well established benefits of electronic payments to all parties.

Credit Cards as e-Payment Systems

Without doubt, the basic means of payment used and initiated via the Internet for consumer transactions till date is the credit card. Credit cards have proved popular for a number of reasons as the following:

1. The system is familiar to users and was widely used before the advent of e-commerce, thus bolstering the users' confidence.
2. Transaction costs are hidden from users (i.e. basically met by sellers, and passed on to all customers, not just credit card users).
3. Payment is simple anywhere and in any currency, thus matching the global reach of the Internet.
4. The credit-issuing company shares the transaction risk; helping overcome consumers' fear and reluctance to buy goods they have not actually seen, from sellers they do not know (in the physical world this function was important because it enabled sellers to take payment from buyers they do not know; online this trust relationship is needed in both directions).

The disadvantages of credit cards for e-commerce include the fact that they cannot be used directly for small value payments or peer-to-peer transactions.

Disadvantages of Credit Cards

Credit cards have their own disadvantages. First, the relatively high transaction cost makes them impractical for small-value payments. Second, they cannot be used directly by individuals to make payments to other individuals (peer-to-peer transactions). Third, protecting the security of transactions is vital, especially in the virtual world where there is no payment guarantee to the merchant by a bank. Users' fears about security issues seem to be a consequence of the newness and relative unfamiliarity of the medium, rather than the real risks involved in the system

Debit Cards as e-Payment Systems

Nowadays, as the online banking system continues to gain acceptance and much improvement, many consumers are taking advantage of the system and are shifting from the use of cash and cheques to debit cards. Basically, a debit card is a plastic card issued to customers by banks and debit card companies. It allows the cardholder to purchase products or services directly from their savings account that come from checking machines. Funds used are prepaid and exists in the bank account prior to any transaction made using the card. Debit cards, which are also known as bank card or check card, are significant when making purchases or while travelling. Having debit cards on hand means that buyers do not have to bring huge amounts of cash in their pockets since numerous establishments accept these cards as mode of payment. Almost all stores like shopping centres, restaurants, hotels, airlines, and malls have made their Point-of-Sale terminals

capable of receiving payment from prepaid cards. For a customer, it is easier to swipe than to count cash and coins. Also, internet shoppers who buy goods online use debit cards too. Usually, businesses who sell through the internet and deliver by mail only accept debit or credit cards for fees.

Further, for people who pay their bills through an automated teller machine (ATM), a debit card is vital. By just inserting the card in the machine and pressing the amount to be paid, the payee saves time and effort compared to falling in line to pay to the teller. The remaining amount of money can be checked online or mobile phone. Another importance of debit cards is that they are used to withdraw cash from ATMs. Consumers who use debits cards can easily track their expenses since these are listed in their bank statements. The number of debit cards issued by banks grew around 34 per cent from FY 2008 levels in FY 2009, and is estimated to touch around 182 million cards by the end of FY 2010.

Disadvantages of Debit Cards Debit cards offer lower levels of security protection than credit cards. Theft of the users' PIN using skimming devices can be accomplished much easily with a PIN input than with a signature-based credit transaction. Unlike a credit card, debit card transactions give you no grace period. They are a quick, pay-now deal. They can make balancing your account tricky if you are not fastidious about keeping receipts and recording transactions in a timely fashion. It is easy to forget, for example, when you pay at the gas pump with a debit card and drive off without your receipt. Some ATM machines charge a fee for their use and then your bank adds another foreign ATM charge (if the machine is not from your bank). Know ahead of time what the fees are and where you can access your money for free if possible.

12.3 THE MOBILE PAYMENTS

The biggest wildcard in the e-commerce and e-payment field at the moment is the way mobile Internet access develops. Already schemes such as Internet access via SMS (short message service), and pre-paid re-loadable cards are in place, allowing payment to be made via a mobile phone. The use of the SIM card in the user's mobile phone as part of a payment system implies a shift in the roles of both banks and telephone operators. Mobile payments system is likely to become a popular mode of fund transfer in the coming months as banks have issued nearly 8.5 million Mobile Money Identifier (MMID) to customers. National Payment Corporation of India (NPCI) said, "Eighteen major banks who have already joined our Interbank Mobile Payment Service (IMPS) have started issuing MMID to the registered mobile banking customers."

The MMID, in combination with the mobile number, acts as a proxy for the account number. MMID is a seven-digit number issued by your bank for transactions through mobile banking. There will be different MMIDs for different savings accounts, but all these can be linked to one mobile number. Axis Bank, Federal Bank and Kotak Mahindra Bank, recently launched Interbank Mobile Payment Service (IMPS) or mobile banking. "The idea is to enable quick transfer of funds through mobile phones. Many customers who would like to receive money electronically and have hesitation in revealing their bank branch and account number, would have a solution. They can now share their mobile number and MMID with the remitter without the fear of providing personal banking details. Mobile banking is available free of cost for the consumer, a transaction cost for availing IMPS is levied by National Payments Corporation on the bank from which the money is transferred.

Money can be transferred across banks, provided the beneficiary bank is registered for mobile banking. As per the Reserve Bank of India norms, an individual can transfer amount but you can receive an unlimited amount. Transfer of funds can be done by anyone who has an MMID but he needs to be a registered net banking user. Net banking users automatically get registered for mobile banking. Apart from fund transfer, mobile banking can also be used for purchase of goods and services, making bill payments, investments in mutual funds or creating fixed deposits.

12.4 CLASSIFICATION OF NEW PAYMENT SYSTEMS

For the time being, the New Payment Systems can be roughly divided into 2 groups: one, using smart cards, and the other using the Internet. Traditional payment instruments such as cash, cheques, credit cards, EFT/POS, and account transfer have strong points—convenience and ease of circulation—but they are weak due to their high handling costs. The New Payment Systems are an experiment to augment payment instruments with the use of networks and electronics, while maintaining the strength of the older systems.

Smart Card Cash Payment System

We will first look at the smart card-based cash payment system. In the early 1990s, a payment system for low value amounts using smart cards was first introduced in Europe. Most of these methods are known as stored value cards or electronic purse system. Units of prepayment or currency value are electronically stored on an IC chip imbedded in these cards. When purchases are made, the payment is effected through these units of electronic value.

Smart cards are credit and debit cards and other card products enhanced with microprocessors, capable of holding more information than the traditional magnetic stripe. The chip, at its current state of development, can store significantly greater amounts of data, estimated to be 80 times more than a magnetic stripe.

The smart card technology is widely used in countries such as France, Germany, Japan and Singapore to pay for public phone calls, transportation, and shopper loyalty programmes. The idea has taken longer to catch on in the United States, since a highly reliable and fairly inexpensive telecommunications system has favoured the use of credit and debit cards.

Smart cards are basically of two types: relationship-based smart credit cards and electronic purses. Electronic purses, which replace money, are also known as debit cards and electronic money.

The benefits of smart cards will rely on the ubiquity of devices called smart card readers that can communicate with the chip in a smart card. In addition to reading from and writing to smart cards, these devices can also support a variety of key management methods. Some smart-card readers combine elements of a personal computer, a point-of-sale terminal, and a phone to allow consumers to quickly conduct financial transactions without leaving their homes.

In the simplest form, the card reader features a two-line with a 16-character display that can show both the prompt and the response entered by the user. Efficiency is further enhanced by colour-coded function keys, which can be programmed to perform the most frequently used operations in a single key stroke. It can communicate via an RS-232 serial interface with the full range of transaction automation systems, including PCs and Electronic Cash Registers (ECRs).

Card readers in the form of screen phones are becoming more prominent. Proponents of screen phone applications have long stated that consumers, familiarity with phones gives screen phones an entry that computers cannot match. Some screen-based phones feature a four-line screen, a magnetic stripe card reader, and a phone keypad that folds away to reveal a keyboard for use in complex transactions. The phone prompts the users for transactions, using menus patterned on those found on automated teller machines.

Smart card readers can be customized for specific environments. The operating environment allows programmers to use the C programming language to create and modify applications without compromising the device's security functions. The development system for most card readers even comes with pre-coded modules for accelerated application development. To

promote smart card usage, the Smart Card Forum—a group of about 130 businesses and government agencies—is drawing up common specifications to promote the use of multiple application smart cards useable for every kind of payments.

12.5 MICROPAYMENT SYSTEMS

VISA Cash of Visa International

Visa International, the world's largest credit card company, introduced their own stored value card (VISA Cash) in 1995 under license from and incorporation of the technology developed by Danmont in Denmark.

In the system of VISA Cash, the transaction is made on an existing financial network of Visa, where large value payments are also transacted. The level of security is quite high. However, as all transaction data go through the data centres of Visa International, anonymity could be jeopardized. The transactions handled here are different from transactions by credit card. The user's identification and authentication are not required at the time of payment. Each bank does clearing of units of prepayment and deposit; thus the person concerned cannot be identified. In this manner, it provides anonymity. The operational cost is relatively high, since all transactions pass through the network for settlement at banks.

12.6 PROPERTIES OF ELECTRONIC CASH (E-CASH)

There are many ways of implementing an e-cash system. Specifically, e-cash must have the following four properties: monetary value, interoperability, retrievability, and security.

E-cash must have a monetary value; it must be backed by either cash (currency), a bankauthorized credit, or a bank-certified cashier's cheque. 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, electronic benefits transfers, and the like. Most e-cash proposals use a single bank. In practice, multiple banks are required with an international clearing house that handles the exchange ability issues because all customers are not going to use 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 a 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 travelling. The cash could be stored on a remote computer's memory, in smart cards, or in other easily transported standard or special-purpose devices. Since it is easy to create counterfeit cash that is stored in a computer, it is preferable that cash is stored 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 view the 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 or not. 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 postfact detection and punishment.

12.7 e-CASH IN ACTION

E-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 none 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.

Purchasing e-Cash from Currency Servers

The purchase of e-cash from an online currency server (or bank) involves two steps: (i) establishment of an account, and (ii) 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 do not have a bank account.

Currently, in most e-cash trials, all customers must have an account with a central online bank. This is too restrictive for international use and multicurrency 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 clearing house for many credit card issuing banks.

12.8 CHEQUE PAYMENT SYSTEMS ON THE INTERNET

Magnetic Ink Character Recognition (MICR)

In this system, data are printed at the bottom of cheques in magnetic ink, for an electronic read is a typical use of electronics for cheque processing.

Check Free Payment Services of CheckFree

In September 1995, CheckFree offered the electronic cheque service CheckFree Payment Services on the Internet. Upon customer request, this service issues an electronic cheque and executes settlement between customer and retailer. If needed, a paper cheque can also be issued to the retailer. This system implements not only cheque processing but also electronic cheque issuance.

Electronic Cheque (e-Cheque)

FSTC is a consortium of 60 organizations in the US including financial institutions, clearing houses, universities, and companies. It was founded in 1993 for the development of payment systems for E-commerce (EC). Bank of America, Citibank, and Chemical Bank are a few of the well-known participants.

In September 1995, FSTC commenced an electronic cheque system on the Internet called electronic cheque. This is one of FSTC's five major development projects, the others being:

1. Cheque truncation
2. Electronic commerce
3. Security measures
4. Smart card system.

In this electronic cheque system, a consumer possesses an electronic chequebook on a Personal Computer Memory Card International Association (PCMCIA) card. As needed, cheques are written electronically from the e-chequebook on the card. They are then sent over the Internet to the retailer, who in turn sends the e-cheques to the customer's bank. Settlement is made through a financial network such as an ACH. In addition to payment data, commercial data such as invoice number and date of receipt can be enumerated, thereby achieving a higher degree of efficiency by eliminating duplication. With a view to increasing the practicality of the system, FSTC is experimenting with the adoption of a smart card as an electronic chequebook. An electronic signature with public key encryption has been adopted by FSTC for ensuring data security over the Internet.

12.9 DESIGNING E-PAYMENT SYSTEMS

Despite cost and efficiency gains, many hurdles need to be overcome for the spread of e-payment systems. These include several factors, mostly non-technical in nature, that must be addressed before any new payment method is made successful. They are as follows:

1. Privacy. A user expects trustworthiness of a secure system; just as the telephone is a safe and a private medium, free of wiretaps and hackers, electronic communication must merit equal trust.

2. Security. A secure system verifies the identity of two-party transactions through "user authentication", and reserves flexibility to restrict information/services through access control. Tomorrow's bank robbers will need no getaway cars—just a computer terminal, the price of a telephone call, and a little ingenuity. Millions of dollars have been embezzled by computer fraud. No systems are yet foolproof, although designers are concentrating closely on security.

3. Intuitive interfaces. The payment interface must be as easy to use as a telephone. Generally speaking, users value convenience more than anything.

4. Database integration. With home banking, for example, a customer wants to play with all his accounts. Separate accounts are stored on separate databases. The challenge before

banks is to tie these databases together and allow customers access to any of them while keeping the data up-to-date and error-free.

5. Brokers. A "network banker"—someone to broker goods and services, settle conflicts, and facilitate financial transactions electronically—must be in place.

6. Pricing. One fundamental issue is how to price payment system services. For example, should subsidies be used to encourage users to shift from one form of payment to another—from cash to bank payments, from papers based to e-cash? The problem with subsidies is the potential waste of resources, as money may be invested in systems that will not be used. Thus, investment in systems not only might not be recovered, but also substantial ongoing operational subsidies will be necessary. On the other hand, it must be recorded that, without subsidies, it is difficult to fix up an affordable price to all services.

7. Standards. Without standards, the welding of different payment users into different networks and different systems is impossible. Standards enable interoperability, giving users the ability to buy and receive information, regardless of which bank is managing their money.

None of the above hurdles are insurmountable. Most of these will be overcome within the next few years. These technical problems, experts hope, will be solved as technology is improved and experience is gained. The biggest question concerns how customers will take to a paperless and (if not cashless) a less-cash world.

12.10 DIGITAL SIGNATURE

Digital signatures provide information regarding the sender of an electronic document. The technology has assumed huge importance recently, with the realization that it may be the remedy to one of the major barriers to growth of electronic commerce: fear of lack of security. Digital signatures provide data integrity, thereby allowing the data to remain in the same state in which it was transmitted. The identity of the sender can also be authenticated by third parties.

The most widely used type of cryptography is public key cryptography, where the sender is assigned two keys—one public, one private. The original message is encrypted using the public key while the recipient of the message requires the private key to decrypt the message. The recipient can then determine whether the data has been altered. However, although this system guarantees the integrity of the message, it does not guarantee the identity of the sender (public key owner). In order to remedy this, a Certificate Authority is required.

In Figure 12.1, Ravi (the sender) uses his private key to compute the digital signature. In order to compute the digital signature, a one-way hashing algorithm may be used to first calculate a message digest, as is done by RSA. The message digest is an efficient way to represent the message, as well as being a unique number that can only be calculated from the contents of the message. The sender's private key is used at this point to encrypt the message digest. The encrypted message digest is what is commonly called a digital signature.
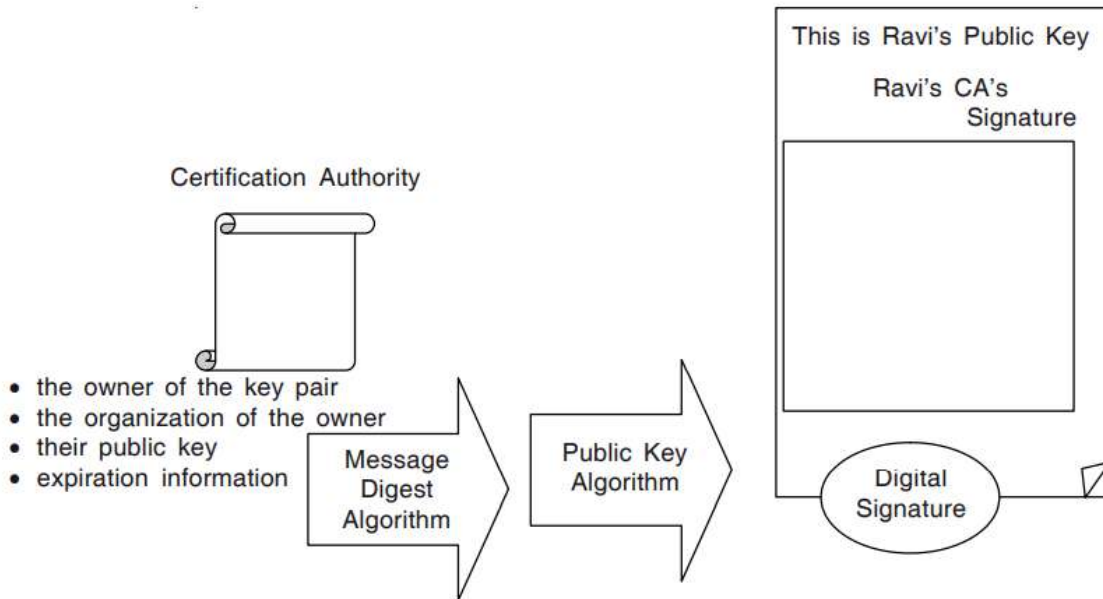
Figure 12.1 Digital Signature Process

A certification authority (CA) performs the task of managing key pairs, while the verification of the person or entity bound to that key pair is initially ascertained at the time of application by the registration authority. A certificate is issued by a CA and links an individual or entity to its public key, and in some cases to its private key. Certification authorities can offer different grades of certificates, depending upon the type of initial identification provided by the individual. From an information security viewpoint, these simple "electronic signatures" are distinct from the "digital signatures" and in the technical literature, although "digital signature" is sometimes used to mean any form of computer-based signature. These guidelines use "digital signature" only as it is used in information security terminology, as to mean the result of applying the technical processes.

Legal Position of Digital Signatures

Although the digital signature technology has been available for some time, it has only recently become feasible to use digital signatures to authenticate a document. This breakthrough has made digital signatures one of the most important areas of development within electronic commerce. It is important because the technology and the law governing it must develop in a way that promotes—or at the very least does not inhibit—the growth of electronic commerce.

A substantial amount of legislation regulating the use of digital signatures and their legal status has been enacted. So far, this has been enacted on a state by state basis, resulting in those countries taking contrasting legal positions. International law on digital signatures has yet to be formulated.

Developments are also taking place at a global level. Bodies such as the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), and W3C are currently working on standardization of digital signatures. The OECD has issued 'Guidelines for Cryptology Policy', which includes a guide for states on the creation of legislation governing the use of digital signatures. UNCITRAL has also released draft legislation on electronic commerce, including guidelines for digital signatures.

Signatures and the Law

A signature is not a part of the substance of a transaction, but rather its representation or form. Signing writings serve the following general purposes:

Evidence

A signature authenticates the writing by identifying the signee with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.

Legality

The act of signing a document calls to the signer's attention, the legal significance of the signer's act, and thereby helps prevent "inconsiderate" engagements.

Approval

In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's claim that it has legal validity.

Efficiency and Logistics

A signature on a written document often imparts a sense of clarity and finality to the transaction, and may lessen the subsequent need to inquire beyond the face of a document. Negotiable

instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

Authenticity

The formal requirements for legal transactions, including the need for signatures, vary in different legal systems, and also vary with the passage of time. There is also variance in the legal consequences of failure to cast the transaction in a required form. The statute of frauds of the common law tradition, for example, does not render a transaction invalid for lack of a "writing signed by the party to be charged", but rather makes it unenforceable in the court, a distinction which has caused the practical application of the statute to be greatly limited in case law.

12.11 CHECK YOUR PROGRESS

16. What is multi-layered security architecture?

17. List online payment categories.

18. E-payment systems are proliferating in banking, retail, healthcare, online markets, and even in government—in fact, anywhere money needs to change hands. (True/False)

19. What is visa card?

20. Write significance of MMID.

21. What are smart cards?

Answers to Check your progress

1. A multi-layered security architecture comprising firewalls, filtering routers, encryption and digital certification ensures that your account information is protected from unauthorized access.

2. Online payment categories are micropayments, consumer payments and business payments.

3. True

4. Visa describes new range of payment choices as "u-commerce," or universal commerce— the ability to conduct commerce anywhere, anytime, or any way.

5. The MMID, in combination with the mobile number, acts as a proxy for the account number. MMID is a seven-digit number issued by your bank for transactions through mobile banking. There will be different MMIDs for different savings accounts, but all these can be linked to one mobile number.

6. Smart cards are credit and debit cards and other card products enhanced with

microprocessors, capable of holding more information than the traditional magnetic stripe. The chip, at its current state of development, can store significantly greater amounts of data, estimated to be 80 times more than a magnetic stripe.

12.12 SUMMARY

This unit introduces the internet banking concepts and the requirements of digital payment systems. Various e-Payment Systems such as Credit cards and Debit cards along with its pros and cons are detailed. Significance on mobile payments is highlighted. Details about smart card technology is elaborated. Narration is made on micropayment system. E-cash and e-Cheque is described. Various factors that has to be addressed before making e-payments are detailed. Digital signature process in detail is described.

12.13 KEYWORDS

- **Encryption** is an important way for individuals and companies to protect sensitive information from hacking. For example, websites that transmit credit card and bank account numbers should always encrypt this information to prevent identity theft and fraud.

- **Visa Cash** is a smart card electronic cash system, implemented as a stored-value card owned by Visa.

- **Currency Server** was designed to be the most advanced currency-enabling component on the market. It provides exchange rate information and currency internationalization, conversion and rounding services via COM, . NET and SOAP Web services, and Ajax-style scripting.

- **e-Cheque** is an electronic counterpart of paper cheque. It turns the cheque writing and deposit processes totally online. Paying with e-Cheques will be an entirely paperless experience.

- **Digital signature** is an electronic, encrypted, stamp of authentication on digital information such as email messages, macros, or electronic documents. A signature confirms that the information originated from the signer and has not been altered.

12.14 QUESTIONS FOR SELF STUDY

26. Write the significance of internet banking.

27. Narrate the requirements for digital payment systems.

28. Discuss Credit cards and Debit cards as e-Payment Systems.

29. Mention the advantages and disadvantages of credit cards and debit cards.

30. Write a note on mobile payments.

31. Explain briefly about smart card technology.

32. Narrate about micropayment system.

33. What is e-cash? Explain its properties.

34. Write a note on e-Cheque.

35. Mention various factors that has to be addressed before making e-payments.

36. Explain digital signature process in detail.

12.15 REFERENCES

7. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

8. Joseph, P. T. (2019). *E-commerce: An Indian perspective*. PHI Learning Pvt. Ltd..

Karnataka State Open University
Mukthagangothri, Mysore – 570 006.
Dept. of Studies and Research in Management

MBA IT Specialization
III Semester

E-commerce

Block 4

Karnataka State Open University

Mukthagangothri, Mysore – 570 006.

Dept. of Studies and Research in Management

MBA. IT Specialization

III Semester

E-commerce

BLOCK 4

BLOCK 4 INTRODUCTION

E-commerce refers to aspects of online business involving exchanges among customers, business partners and vendors. E-commerce has increased the speed and ease with which business can be transacted today, resulting in intense competition between enterprises. Companies are at the crossroads, with just two vistas ahead of them—either go online or go out of business. Once the choice of online business is made, further roadblocks are encountered: which business model to adopt; which management strategies and tactics will make business successful? How to explore opportunities, understand limitations, and issues? The solution is to gain a deeper insight into the e-commerce strategies.

This block consists of 4 units and is organized as follows:

Unit 13 : Customer Relationship Management, E-CRM Solutions, How Technology Can Help? E-CRM Toolkit, Typical Business Touch-points, Managing Customer Value Orientation and Life Cycle, Privacy Issues and CRM, Customer Relationship Management System for a Bank

Unit 14: What is Mobile Commerce? Components of Mobile commerce, Ideal m-Commerce Market Characteristics, Content Drives Usage, Mobile Music and Entertainment, Wireless Applications, Cellular Network, Cellular Telephony,

Unit 15: Portal Benefits, Portal Features, Requirements of Intelligent Websites, Setting Website Goals and Objectives, Considering the Website's Target Audience, Selecting a Hosting Service

Unit 1**6**: Computers as Targets for Crime, Computers as Storage Devices, Computers as Communications Tools, Privacy is at Risk in the Internet Age, Cookies and Privacy, Internet threats, The Special Nature of Computer Ethics

Unit 13: e-CUSTOMER RELATIONSHIP MANAGEMENT

Structure

13.0 Objectives

13.1 Introduction

13.2 Customer Relationship Management

13.3 E-CRM Solutions

13.4 How Technology Can Help?

13.5 E-CRM Toolkit

13.6 Typical Business Touch-points

13.7 Managing Customer Value Orientation and Life Cycle

13.8 Privacy Issues and CRM

13.9 Customer Relationship Management System for a Bank

13.10 Check Your Progress

13.11 Summary

13.12 Keywords

13.13 Questions for Self Study

13.14 References

13.0 OBJECTIVES

After studying this unit, you will be able to:

- Awareness about Customer Relationship Management
- Analyze E-CRM Solutions
- Study how Technology can help in CRM.
- Explore E-CRM Toolkit
- Discuss Typical Business Touch-points
- Describe Managing Customer Value Orientation and Life Cycle
- Signify Privacy Issues and CRM
- Case study- Customer Relationship Management System for a Bank

13.1 INTRODUCTION

Customer Relationship Management (CRM) is defined as the aligning of business strategy with the corporate culture of the organization, along with customer information and a supporting

information technology of the customer interactions that promote a mutually beneficial relationship between the customer and the enterprise. Primarily, customer relationship management is a business strategy, but it is a business strategy enabled by the advances in technology. Widespread implementation of customer information, Enterprise Resource Planning (ERP) systems, sales force automation, and integrated point-of-sale systems have made customer information readily available in large volumes. Reduced costs and higher levels of performance for database management platforms allow us to gain access to this customer information and gain new insights into our customers and their behaviour through a variety of analysis methods.

13.2 CUSTOMER RELATIONSHIP MANAGEMENT

Advances in contact management technology and supporting infrastructure allow us to take advantage of this information in increasingly cost-effective and innovative ways. Perhaps most significantly, the Internet provides a completely new way for an enterprise to interact with its customer— the electronic channel, or the e-channel. With consumers buying everything—from groceries to automobiles—on the Internet and the businesses beginning to shift their purchasing activities to industry-oriented virtual marketplaces, the characteristics of customer interaction are constantly changing. In the business environment, the focus is being shifted to customer retention.

The link between customer satisfaction and the return on investment is the profit for a company, as shown in Figure 13.1.

Figure 13.1 Customer satisfaction and profit

Beyond the glamour of developing the e-channel, business is investing heavily to deploy customer relationship management in traditional channels. In most cases, these capabilities are developed independently, requiring expensive integration later on to achieve the vision of true customer relationship management on an enterprise-wide scale. Integration of these resources is one of the key challenges of successful deployment of CRM across the enterprise. This is because it has a direct impact on the consistency of the customer experience with the enterprise. So how does the enterprise integrate systems across functions and channels? It does not happen by accident, but through foresight and planning. All the functions and the channels must come

together to develop an enterprise-wide strategy for CRM. Only then can the enabling information technology be fully integrated with maximum efficiency and effectiveness. This technology spreads customer information throughout the enterprise and it must be based on a unified information architecture.

Independently developed CRM capabilities within the various parts of the enterprise usually begin based on function-specific short-term needs. Marketing begins to implement CRM with a variety of products, often combined with integrated suites to plan, execute, and monitor marketing campaigns and perform database marketing. Lead management and sales force automation capabilities are deployed to support the field sales force. Systems that manage the supply chain and product delivery are deployed to support mass customization and to provide up-to-the minute information about the goods in transit, to the customer. Field service representatives and contact centres deploy sophisticated telephony and information systems to provide ongoing customer service and cross-selling.

These separate capabilities do provide a means to support function-specific and channelspecific CRM strategies. Business culture can shift from product-focus to customer-focus. Sales and marketing can focus on retention and increase of share of customers instead of acquisition and market share. Customer service can identify and take advantage of cross-sell and up-sell opportunities. However, customer information does not freely flow across the enterprise. To obtain the vision of customer relationship management, information must move about freely. This requires integration.

Only through the integration of marketing, sales, fulfilment and service across business partnerships, the direct sales force, the telechannel and the e-channel, is the vision of customer relationship management realized. Customer information must flow like water within, around, and through these functions and channels to ensure that the enterprises can build mutually beneficial relationship with the customers, and even amongst their customers. Everyone in the enterprise participating in the conversation with the customer needs access to the latest information on the customer's profile, behaviour, and expressed needs. Marketing provides the latest promotions and offers for individual customers, based on their interactions on the website. Products are customized to meet specific customer needs and customer service is fully done, resulting in increased levels of customer satisfaction and loyalty. With an enterprisewide view of each customer, the value of each relationship is measurable, and each relationship is managed

based on this value. Every customer touch becomes an opportunity to modify customer behaviour in a beneficial way based on the totality of information at the disposal of the enterprise. Achieving this vision results in unprecedented competitive advantage in some industries . . . or mere survival in other industries.

13.3 E-CRM SOLUTIONS

E-Customer Relationship Management or E-CRM solutions are especially valuable to companies that face the following circumstances:

1. Business is driven by mission-critical customer service requirements
2. Current costs for CRM run high
3. Large volumes of information is distributed
4. A complete customer care solution is needed.

E-CRM solutions can be deployed and managed to provide increased revenues and decreased costs for companies while improving customer service. E-CRM goals can be achieved with Internet business strategies, web-based CRM specification development, web systems design and project management, interactive interface design and electronic publishing. The strategy for e-CRM can be visualized in three stages, as given in Figure 13.2.
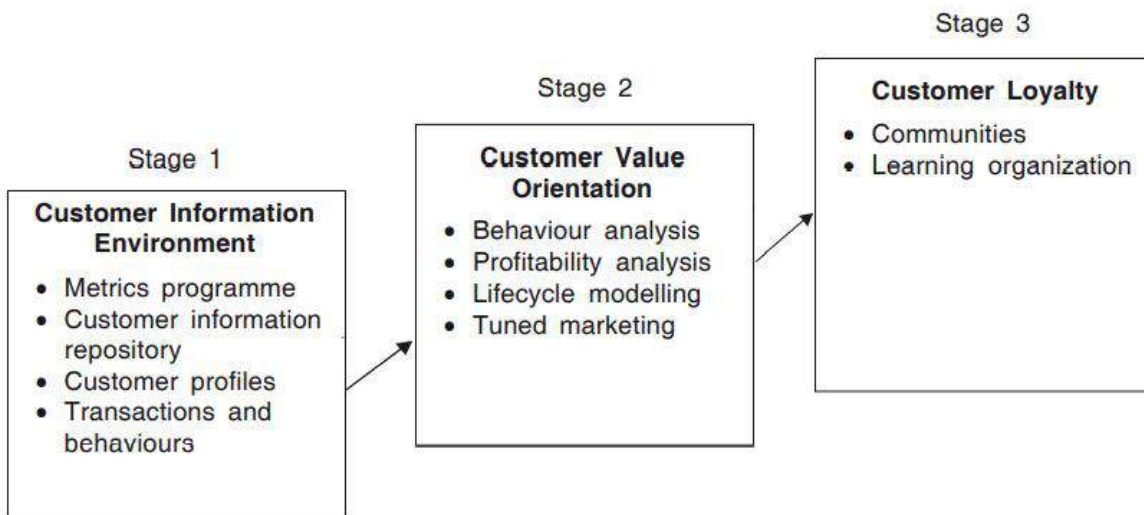

Figure 13.2 strategy for e-CRM

Customer Information Environment

In the first stage, building up of a customer information environment and acting on it forms the starting point. It consists of Metrics programmes, Customer information repository, and monitoring customer behaviours.

Customer Value Orientation

In the second stage, operational effectiveness is the focus. Customers want value for their money. They believe that they have got value, when the perceived benefits they receive from something exceed the costs of owning it. These components are represented in Figure 13.3.
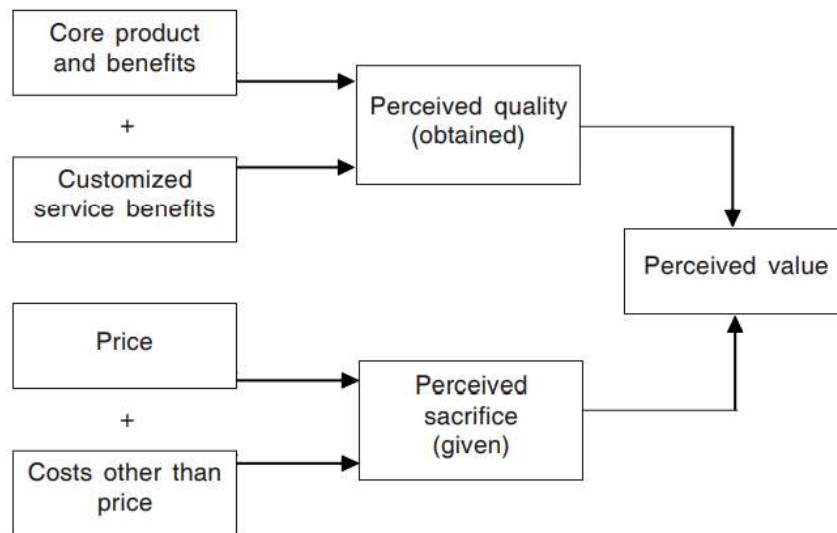

Figure 13.3 Perceived Value

Customer Loyalty

In the third stage, the focus is on the integration of internal process of the organization with the customer in creating a community.

Moving costly customer services to the Internet is critical to staying competitive. Providing customer services on the Internet means a lot more than just having a website. With the users demanding more services via the Internet, leading companies have realized the importance of their e-services strategies on the Web.

Most companies are focussed on today's most critical business challenge—attracting and retaining customers. These companies require customer-directed e-business solutions and E-CRM to meet those requirements. Companies benefit from huge cost savings and increased revenues. Customers benefit from on-demand access to information, less hassles with better support, and less expensive services.

The strategy of the portals is to become global supermarkets providing everything for individuals, families and organizations. Their customer base is what stock market considers to be the most important asset of these companies.

13.4 HOW TECHNOLOGY CAN HELP?

Interactive computer and communications technology can assist in the sales and support process in several ways. Telephone, live chat and e-mail can enhance the effectiveness of customer service representatives. Computer-mediated e-mail, chat and animated chat can take over when a human representative is exhausted. They can serve as a filter, answering all but the most difficult questions for the representatives.

Web technology can also help offload the support issue to customers who enjoy helping each other on the Web. For example, Lands' End (www.LandsEnd.com) adds to the fun of shopping with its Shop With a FriendTM option. Two shoppers can browse together and add items to the same shopping cart. For example, two friends working in different companies can go shopping during their lunch break, just as though they had met and gone shopping in the same brick-and-mortar retail outlet. There is no elaborate data warehousing or cluster analysis involved, just a two-way Web chat connection and a slight modification in their shopping cart model. The customers take care of navigating the Web and helping each other with product selection.

In a similar vein, several vendors, including Cahoots, Hypernix, ICQ, MyESPcom, Third Voice, and WebSideStory, offer live-chat technology to make online shopping less sterile and more emotionally engaging. Their idea is to create a sense of community for a particular website by allowing prospective customers to communicate with each other at any time, even without knowing each other's name.

For example, customers shopping for widgets on a particular website could ask if other customers had a good or bad experience with the widgets purchased there. Anyone visiting that website could respond to the query and discuss the merits and demerits of those widgets. The goal is to improve upon the Web's record of two-thirds cart abandonment. That is, about two-thirds of all shopping carts are abandoned at some point before final checkout. From the perspective of a website owner and the one paying for the live-chat capabilities, the danger is that the discussions may become derogatory and out of control.

Human-mediated personal contact, phone contact, live Web chat, e-mail, and animated Web chat are representatives of the range of possibilities currently available, where animated Web chat

represents the greatest level of technological involvement. There are also several technologies on the horizon, such as two-way Web-based video links, but the realities of current bandwidth limitations of the Internet are holding these technologies at bay. Also, the value for each characteristic attributed to a touch point represents a typical case. As with any measurement or estimate, there is variability in the actual value shown.

13.5 E-CRM TOOLKIT

An E-CRM 'toolkit' covers a wide diversity of channels (see Figure 13.4). In order to bring true customer management across online business, one needs the E-CRM products to fulfil the following criteria:

Content

Is the system delivering the contents a customer wants to see? How is it being managed on the IT platform?

Storefront and Merchandising Services

With large numbers of visitors failing to complete transaction at the checkout, it is needed to ensure that your storefront services propel your customers to the cash point.

E-mail Management

Are e-mail campaigns focussed to provide an offer that customer cannot refuse? How are these tied in with websites so that customers enjoy a seamless experience?

Customer Management

Is the company managing data across all the sales and marketing functions to its best?

E-marketing

How well are e-marketing efforts targeted? How well do they combine with online selling operation?

Assisted Selling

One needs only to look at the Dell business model to see how assisted selling can enhance the shopping experience and achieve business success. But what assisted selling approach will work best for any company?
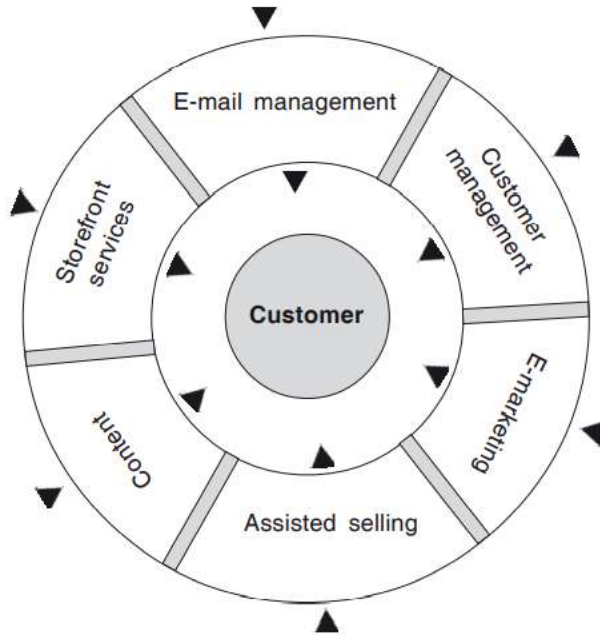
Figure 13.4 E-CRM Toolkit

13.6 TYPICAL BUSINESS TOUCH-POINTS

Typical business touch-points from a consumer perspective include: Media—TV, radio, newspaper and flyers; Physical—the physical plant, such as a showroom or retail outlet; Personal—direct people contact, including salespeople and customer representatives; Mail—correspondence, bills, and payments through postal service; Phone—telephone communications with sales, marketing, and customer service representatives; Fax–facsimile communications, including quotes and invoices; E-mail—communications via computer regarding orders and services; and Web—information and ordering through the Web. Figure 13.5 illustrates the state where every touch-point is significant. The arrows therein indicate the relative significance of each touch-point.
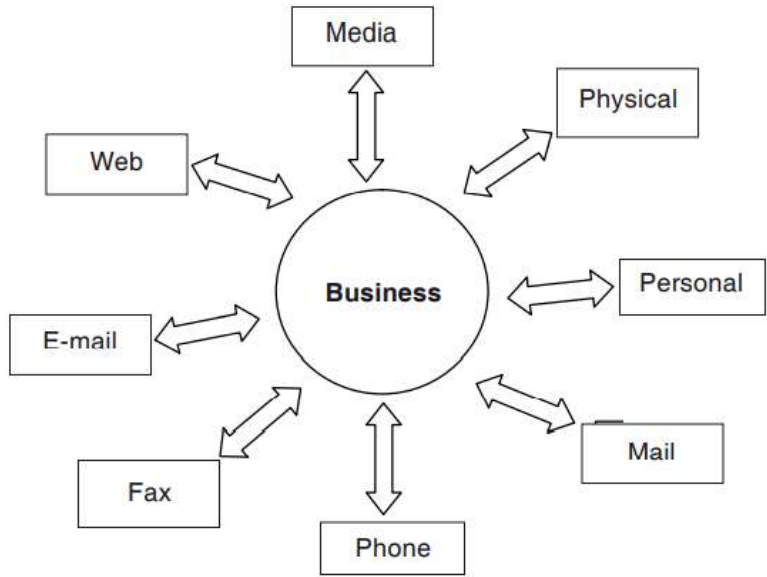
Figure 13.5 Touch points to normal CRM

For any company, it simply is not enough to know "who buys what?" in order to build a successful, profitable marketing campaign. It needs to know who its customers are, and how much it should invest on them. This necessitates the maintenance of a consolidated database. The components of the data warehouse can be found in Figure 13.6.
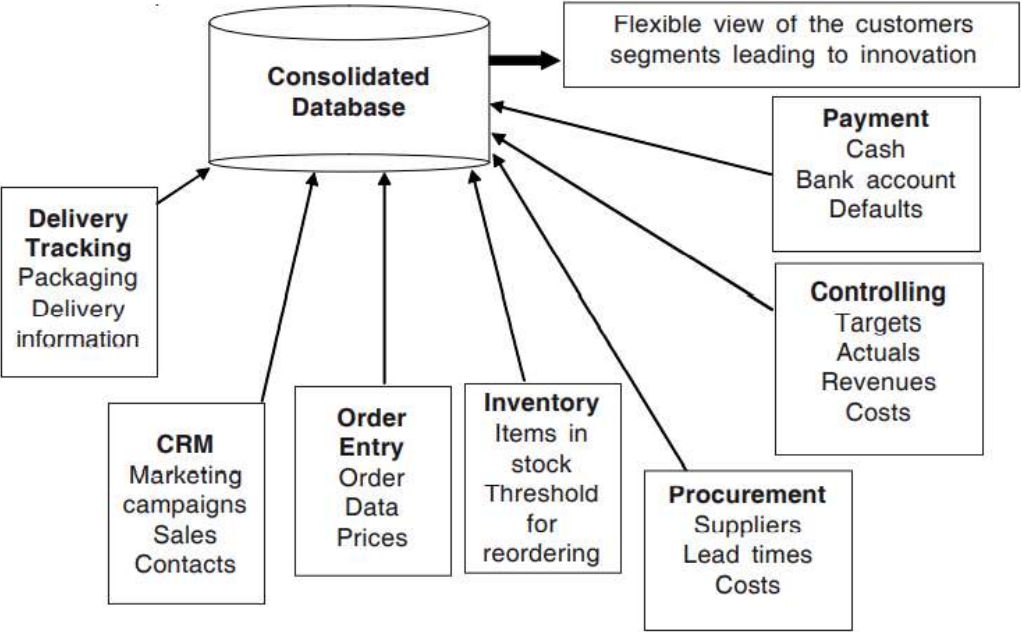

Figure 13.6 Data Warehouse Architecture

13.7 MANAGING CUSTOMER VALUE ORIENTATION AND LIFE CYCLE

The CRM industry has matured rapidly over the past few years. Contact managers have evolved into full-function sales force automation systems. CRM front-office suites now support marketing, sales and service. Integration between CRM systems and enterprise resource planning (ERP) systems is becoming more common, if not commonplace.

The E-CRM market is new and rapidly evolving. Implementing CRM for traditional front-office marketing, sales and service operations is becoming the top priority for most companies. That prospect has been challenging enough, being formidable to the new touchpoints such as the Web. Integration is still the key. Online or offline, client/server technology is still a major factor. Anyone who has implemented client/server applications between the various contact centres and touch points within an enterprise can afford the complexity and the cost involved in them. In short, CRM is a square peg and e-business is a round hole. However, everything is changing with the introduction of new, Web-based CRM solutions.

To help organize the chaos, E-CRM solutions can be grouped into two categories— Web-based solutions and Web-extended solutions.

The Web-based CRM solutions are designed from the bottom up, exclusively for the Internet. These are very innovative products, initially focussed on the sales (e-commerce) function. More marketing and service capabilities will be soon added.

Web-extended CRM solutions are established (primarily client/server-based) CRM suites, originally designed for enterprise users with extensions, to include web-interface functions. There are three phases of CRM:

1. Acquisition
2. Enhancement
3. Retention.

Each has a different impact on the customer relationship, and each can more closely tie a company with its customer's life.

Acquisition

You acquire new customers by promoting product/service leadership that pushes performance boundaries with respect to convenience and innovation. The value proposition to the customer is the offer of a superior product backed by excellent service.

Enhancement

You enhance the relationship by encouraging excellence in cross-selling and up-selling. This deepens the relationship. The value proposition to the customer is an advantage with greater convenience at low cost (one-stop shopping).

Retention

Retaining profitable customers for life should be the aim. Retention focusses on service adaptability, i.e. it delivers not what the market wants, but what the customers want. The value proposition to the customer enhances a proactive relationship that works well with the best interest of the customers. Today, leading companies focus on retention of existing customers much more than on attracting new customers. The reason behind this strategy is simple: If you want to make money hold on to your good customers. But do not be fooled; it is not as easy as it seems.

All the phases of CRM are interrelated as shown in Figure 7.7. However, performing the tasks well in all the three phases is a difficult proposition, even for the best of companies. Companies often have to choose which one of these dimensions will be their primary focus.

13.8 PRIVACY ISSUES AND CRM

The most sensitive aspect of customer relations is privacy. All of us have boundaries, and don't trust people who become too familiar too soon.

From the business perspective, ubiquitous data and information that flow seamlessly from one touch point to another represents a kind of selflessness, regardless of the business model. The goal of every service-conscious business is to understand not only all customers, but their circumstances as well, and this requires information. In addition to the obvious business opportunities, there are numerous consumer benefits for ready access to personal information, no matter where the location is.

Paradoxically, Internet initially gave the illusion of privacy and anonymity. People could voice their opinions on any subject, view pornography, and read any topic they wanted, without disclosing their identity. However, it was a very short, temporary illusion. In the workplace, e-mails as well as the employees' activities on the Web are often monitored.

There is currently a hot debate over the rights of companies to create dossiers on consumers without their knowledge and then sell the information to third parties. While companies like DoubleClick (www.DoubleClick.com) received a lot of media attention for the intentional use of consumer data, other companies such as America Online, which have much more consumer

information at their fingertips, have maintained a low profile. America Online, for example, maintains information on 21 million subscribers, including demographics, credit card numbers, and their whereabouts. Although America Online is not currently in the business of selling consumer data, it sells names and addresses to bulk mailers, and buys information about subscribers for targeted advertisements. Some service providers intentionally track subscriber movements with subscribers' knowledge, and sell the information to third parties. Subscribers are given free Internet access and extensive personal profiles.

Tracking consumer-purchasing patterns is not always used with the consumer's best interest in mind. For example, personal tracking data are often used in yield management, a technique designed to maximize revenue and profitability. The idea is that some customers are more profitable than others, especially those placing orders with short lead times. Since suppliers can charge higher prices for orders with short lead times, they reserve capacity for such orders and turn down less profitable, long-range orders. As customers are ranked in terms of profitability and system compatibility, less-profitable customers are deleted from the list and their orders declined. For example, a company may not be able to purchase hotel rooms in bulk for conferences, unless its conferences are to a certain minimum size. This mechanism is great for businesses, but may not be appreciated by some customers.

It is now clear that customer relations are based on a timeless, technology-independent, triad—service, trust, and loyalty. Customers have to trust that a business is working with their best interests in mind. Without trust, which is a major contributor to the emotional bond between a business and its customers, there can be no relationship. Furthermore, even the best intentions are worthless without action. A business must repeatedly provide a valuable, consistent service to prove its customers that the company stands behind its marketing rhetoric. If a business provides its customers with a valuable service and develops a trusting relationship, the business can do all it can to galvanize a loyal customer following.

13.9 CUSTOMER RELATIONSHIP MANAGEMENT SYSTEM FOR A BANK

The scope of Customer Relationship Management System (CRMS) is:

1. Creation of a Web intranet site to manage content and provide a platform for sharing information.
2. Creation of a self-managed cross-functional team.
3. High employee satisfaction.

4. Higher productivity.

CRMS is a tool to help grow the bank's Wealth Management business, better manage the enterprise around customer behaviours and develop products and services to attract, satisfy and retain current and potential customers (See figure 13.7).
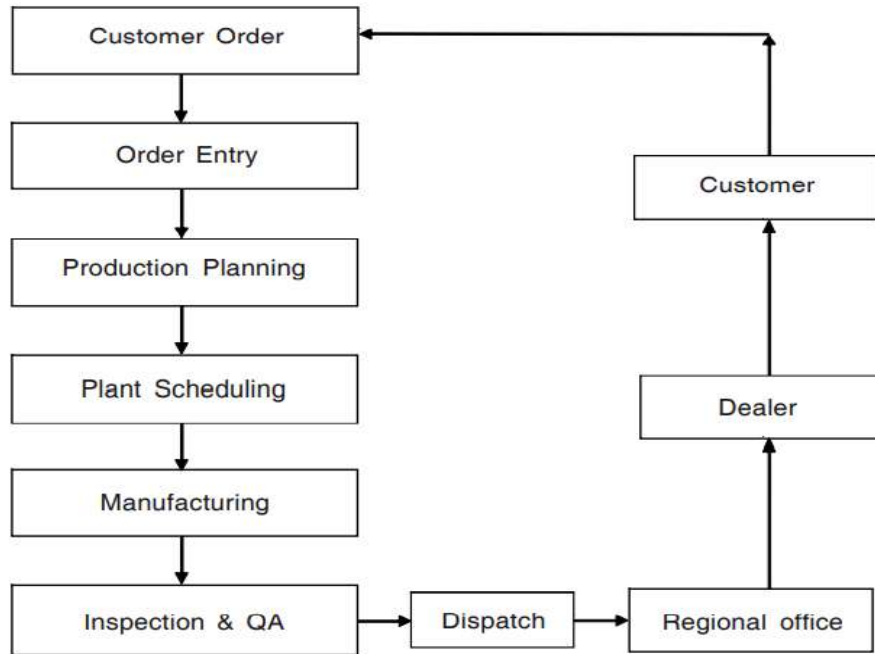

Figure 13.7 Workflow for order fulfillment

Sources of Data for a CRMS

Almost all facilities are granted to customers based on a detailed understanding of their current circumstances.

- Applications forms are the primary source of generating information
- Call centre is another important source of data, especially during marketing campaigns
- Sales force is yet another critical form of generating data
- Group offices also refer data, when requested
- Existing customer database is yet another reliable source
- Market research is performed from time to time
- Tools like CRMS help in analysing customer data.

What is Customer Relationship Management in a Bank?

It is a business strategy that aims to understand, anticipate and manage the needs of an organization's current and potential customers.

It is a strategic, process, organizational and technical change, whereby a company seeks to better manage its own enterprise around customer behaviours.

- Simply put, it involves four major drivers:
- Prospecting by identifying the 'best' prospective customers
- Acquisition by attracting them to become customers
- Cross-Sell/Up-Sell and build Loyalty by doing more and the right kind of business with them
- Retention by keeping them as long as possible, that is, win back and save your customers

Customer Relationship Management is known by different names like 'Total Customer Care', 'Customer Value Management', although globally it is better known by its acronym 'CRM'.

What is Customer Relationship Management System (CRMS)?

The Customer Relationship Management System (CRMS) is a sales support system, developed to further the Bank's personal banking wealth management initiatives. This system is a tool for Customer Service Representatives (CSRs) and Relationship Managers (RMs) aid in the sales process. CRMS drives a more 'customer centric' behaviour, thus helping us deepen relationships with our customers.

CRMS provides:

- Consolidated 'Overview' screen
- Customer 'Demographic' screen
- 'Contact History' screen
- Product 'Cross Sell Opportunities'
- A 'sales referral system' to grow our business with group offices
- Transaction and account details
- Online tracking of sales activity Sales/leads reports
- An intranet site (CNS) to view product information
- Update details of customer interactions.

When to Use CRMS?

CRMS is used as a principal tool for servicing customers such as:

- Account-related enquiries
- Transaction history enquiries
- Product campaign enquiries

This in turn can lead to:

- Discussion of customer's needs
- Cross-sell other products and services

The basic objective of CRMS was to manage the sales automation and provide elementary relationship management tools. The system provided functionalities which included an overview of the customer's current relationship, cross-sell opportunities based on a product gap analysis, creating leads and closing sales, scheduling tasks, contact management, notes and sharing of information, referring business to other departments or entities, receiving referrals from the call centre and other businesses.

The problems associated with implementing a CRM are:

- Lack of understanding of CRM—the bank's mission and objectives
- Lack of customer management (customer-centric)
- Variances in application of business processes
- Lack of data integrity and completeness
- Lack of the sales process and how CRMS helps deliver this
- Lack of complete knowledge the functionalities available on the system
- Lack of support infrastructure

The demands of the system to achieve effectiveness are:

- Redesign processes and communicate this efficiently
- Create awareness about CRM practices and its effective usage
- Encourage users to effectively record all contacts and sales
- Provide a recognition platform for the high performers
- Provide clearer communication regarding support
- Address standard questions/problems faced by users

The content information of the CRMS comprises:

- Mission Statement
- Meet the Team (message from senior management)
- What is Customer Relationship Management?
- What is CRMS and how does it fit into the Group's Sales process?
- Business Process Guides Roles and Responsibilities Guide for Users
- Problem Reporting Procedures
- CRMS High Fliers
- FAQ Glossary

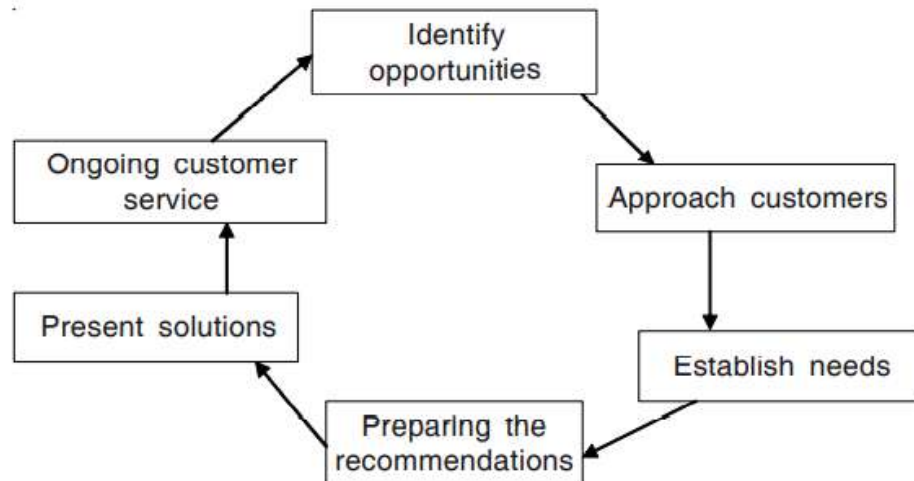Figure 13.8 shows the workflow in a banking CRM situation.

Fig. 13.8 Workflow in a banking CRM situation.

13.10 CHECK YOUR PROGRESS

1. What is Customer Relationship Management (CRM) ?
2. How E-CRM goals can be achieved?
3. With the users demanding more services via the Internet, leading companies have realized the importance of their e-services strategies on the Web. (True/False)
4. What are typical Business Touch-Points?
5. List the categories of E-CRM solutions.

   Answers to Check your progress

1. Customer Relationship Management (CRM) is defined as the aligning of business strategy with the corporate culture of the organization, along with customer information

and a supporting information technology of the customer interactions that promote a mutually beneficial relationship between the customer and the enterprise.

2. E-CRM goals can be achieved with Internet business strategies, web-based CRM specification development, web systems design and project management, interactive interface design and electronic publishing.

3. True

4. Typical business touch-points from a consumer perspective include: Media—TV, radio, newspaper and flyers; Physical—the physical plant, such as a showroom or retail outlet; Personal—direct people contact, including salespeople and customer representatives; Mail—correspondence, bills, and payments through postal service; Phone—telephone communications with sales, marketing, and customer service representatives; Fax–facsimile communications, including quotes and invoices; E-mail—communications via computer regarding orders and services; and Web—information and ordering through the Web.

5. E-CRM solutions can be grouped into two categories— Web-based solutions and Web-extended solutions.

13.11 SUMMARY

This unit introduces Customer Relationship Management. A brief discussion is made on E-CRM solutions related to deployment and management. Also, different strategies of E-CRM is detailed with a diagram. Description is given on how technology can assist in Customer Relationship Management. Significance on E-CRM tool kit is provided. Various business touchpoints in relation with CRM is analyzed. Further privacy issues related to CRM is detailed. Finally a case study on Customer Relationship Management System in a Bank is made.

13.12 KEYWORDS

- **Customer relationship management** (CRM) is a technology for managing all your company's relationships and interactions with customers and potential customers. The goal is simple: Improve business relationships. A CRM system helps companies stay connected to customers, streamline processes, and improve profitability.

- **Electronic customer relationship management** (e-CRM) involves the integration of Web channels into the overall enterprise CRM strategy with the goal of driving

consistency within all channels relative to sales, customer service and support (CSS) and marketing initiatives.

- **Customer orientation** is a business approach that puts the needs of the customer over the needs of the business.

- **Customer loyalty** describes an ongoing emotional relationship between you and your customer, manifesting itself by how willing a customer is to engage with and repeatedly purchase from you versus your competitors.

- **Merchandising service** is the solutions that is being provided by a firm to a company's advertisers about how to manage their space allocation or have a proper layout design for placement of different products.

13.13 QUESTIONS FOR SELF STUDY

1. Describe Customer Relationship Management.
2. How E-CRM solutions can be deployed and managed?
3. Explain different strategies of E-CRM.
4. How technology can assist in Customer Relationship Management? Explain.
5. Write a note on E-CRM tool kit.
6. Explain business touchpoints in relation with CRM.
7. Discuss privacy issues related to CRM.
8. Discuss Customer Relationship Management System in a Bank.

13.14 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.
2. Joseph, P. T. (2019). *E-commerce: An Indian perspective*. PHI Learning Pvt. Ltd..

UNIT 14: INFORMATION SYSTEMS FOR MOBILE COMMERCE

Structure

14.0 Objectives

14.1 Introduction

14.2 What is Mobile Commerce?

14.3 Components of Mobile commerce

14.4 Ideal m-Commerce Market Characteristics

14.5 Content Drives Usage

14.6 Mobile Music and Entertainment

14.7 Wireless Applications

14.8 Cellular Network

14.9 Cellular Telephony

14.10 Check Your Progress

14.11 Summary

14.12 Keywords

14.13 Questions for Self Study

14.14 References

14.0 OBJECTIVES

After studying this unit, you will be able to:

- Give an account on Mobile Commerce.

- Discuss components of Mobile commerce

- Analyze Ideal m-Commerce Market Characteristics

- Describe Content Drives Usage

- Signify Mobile Music and Entertainment

- Give an account on Wireless Applications

- Analyze Cellular Network and Cellular Telephony

14.1 INTRODUCTION

Mobility is one of the key factors which help business thrive. Businesses that embrace the idea of Mobile Information Society will reinvent themselves as real-time organizations, where access and interaction can be instant. New brands, partnerships and customer loyalties are on the raise, thanks to the growing number of mobile terminals. Three major segments that can substantially benefit from anywhere and have anytime access to information and services from the use of mobile phones are, financial service providers, health care industry and corporations with a mobile workforce.

14.2 WHAT IS MOBILE COMMERCE?

Mobile Commerce, or m-Commerce, is about the explosion of applications and services that are becoming accessible from Internet-enabled mobile devices. It involves new technologies, services and business models. It is quite different from traditional e-Commerce. Mobile phones or PDAs impose very different constraints than desktop computers. But they also open the door to a slew of new applications and services. They follow you wherever you go, making it possible to access the Internet while walking down the street with friends and family or while driving, looking for a nearby restaurant or gas station.

As the Internet finds its way into our purses or shirt pockets, the devices we use to access it are becoming more personal too. Already today, mobile phones and PDAs know the phone numbers of our friends and colleagues. They are starting to track our location. Tomorrow, they will replace our wallets and credit cards. One day, they may very well turn into intelligent assistants capable of anticipating many of our wishes and needs, such as automatically arranging for taxis to come and pick us up after business meetings or providing us with summaries of relevant news and messages left by colleagues. But, for all these changes to happen, key issues of interoperability, usability, security, and privacy still need to be addressed. Banks and other financial institutions are exploring the use of m-Commerce to broaden/ retain their business by allowing their customers to not only access account information, e.g. bank balances, stock quotes and financial advice, from anywhere, but also the possibility to make transactions, e.g. purchasing stocks, remitting money, via mobile phones. This service is often referred to as Mobile Banking or M-Banking. The stock market services offered via mobile devices have also

become more popular and are known as Mobile Brokerage, as they allow the subscriber to react to market developments in a timely fashion and irrespective of their physical location.

For financial services providers, the mobile phone has introduced a new channel to reach customers—one that is personal, easy-to-use, secure, location and time independent. Bank branches are increasingly expensive to operate, and the established self-service solutions, such as ATMs and Internet banking, cannot provide competitive efficiency or satisfy the needs of the new generation of customers who want to do business when it is most convenient for them.

14.3 COMPONENTS OF MOBILE COMMERCE

Mobile commerce (M-commerce) can be broadly divided into three categories as shown in Figure 14.1:

1. **Mobile banking**: It is the state-of-the-art process that has been introduced in the banks to make sure that the customers are better equipped with all the systems and process. This helps to carry out the transaction quickly and the account holders can check their account balance and the newly available schemes from the mobile web itself. Mobile banking can be accessed through mobile and people can use it for their benefit and they do not have to be physically present at the banks for checking the account balance. Mobile banking has made life a lot easier and this is a programme that is being used by the younger generation a lot more, but if you are a middle-aged or senior person, you can certainly avail it because it is genuinely user friendly.

2. **M-payment (mobile payment):** It is a point-of-sale payment made through a mobile device, such as a cellular telephone, a smartphone, or a personal digital assistant (PDA). Using m-payment, a person with a wireless device could pay for items in a store or settle a restaurant bill without interacting with any staff member.

3. **Mobile money:** A facility that allows people to use their cell phones and other hand-held devices to handle financial transactions.
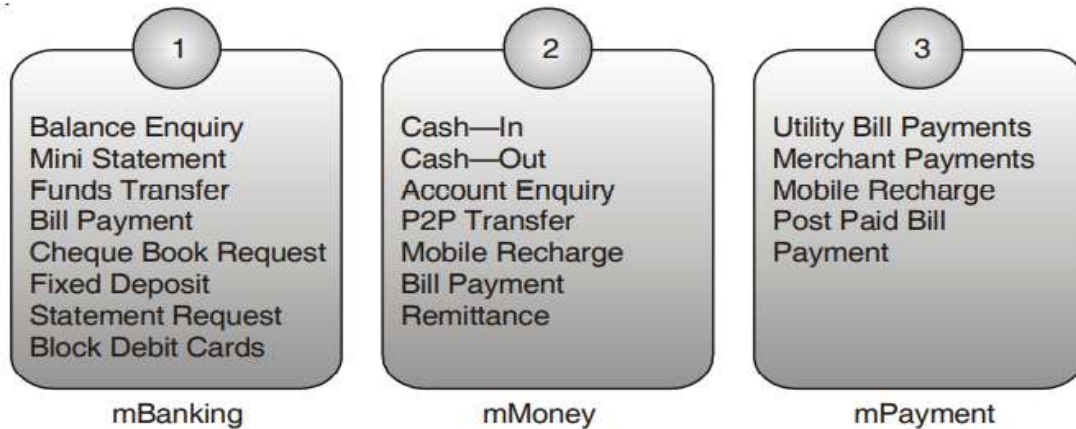
Fig. 14.1 Components of M-commerce.

PDA's and cellular phones have become so popular that many businesses are beginning to use mobile-commerce (m-commerce) as a more efficient method of reaching the demands of their customers. Banks and other financial institutions are exploring the use of m-Commerce to broaden/retain their business by allowing their customers to not only access account information, e.g. bank balances, stock quotes and financial advice, from anywhere, but also the possibility to make transactions, e.g. purchasing stocks, remitting money, via mobile phones. This service is often referred to as Mobile Banking or M-Banking. The stock market services offered via mobile devices have also become more popular and are known as Mobile Brokerage, as they allow the subscriber to react to market developments in a timely fashion and irrespective of their physical location.

News information is also becoming more popular with subscriptions to daily headlines from anywhere in the world being transmitted to mobile devices. Sports and entertainment are areas that have also grown with the demand for mobile related services. Shopping and reservation services are now more accessible when using mobile devices. Corporations are now using m-commerce to expand everything from services to marketing and advertisement. Although there are currently very few regulations on the use and abuses of mobile commerce, this will change in the next few years. With the increased use of m-commerce comes increased security. Cell phone companies are now spending more money to protect their customers and their information from online intrusions and hackers.

- Relatively high penetration of mobile users

- High Internet awareness

- Relatively high e-commerce maturity

- General consumer demand for new services

- A high proportion of early adopters, with a willingness to pay

14.4 IDEAL M-COMMERCE MARKET CHARACTERISTICS

Financial Institutions such as Banks see mobile commerce as offering new channels of service to customers as well as offering them new and innovative products. These financial institutions are working to design and implement new applications that will offer mobile payment (i.e. being able to pay for groceries) and mobile brokering. The travel industry, in realizing the possible benefits of m-commerce, is working on technologies that will take care of travel arrangements, update customers on flight status, notify them when this information changes and will offer to make new arrangements based on preset user preferences requiring no input from the user. Therefore, a customer's entire trip can be scheduled and maintained using only their mobile device. The retail sector is also looking into the possibility of using mobile commerce for making the purchase of merchandize easier. Customers will be able to browse and order products while using a cheaper more secure payment method. An example of this is; instead of using paper catalogues, retailers can send customers a list of products that the customer would be interested in, directly to their mobile device. Additionally, retailers will also be able to track customers at all times and notify them of discounts at local stores in which that customer would be interested in. Shopping will also be easier. Soon, phones will be equipped with "bar-code scanners" and shoppers could scan an item and find out its pricing and availability. In the entertainment industry, m-commerce could be used for the purchasing of movie tickets, verify someone's ID or authorize their reservation information. This industry will also be able to promote wireless gaming and music.

14.5 CONTENT DRIVES USAGE

In terms of economics, entertainment and information services are driving m-commerce forward, just as they did in the early days of radio and television.

Low-priced, relatively simple and straightforward content—such as ringtones and wallpaper—continue to be the revenue drivers in terms of product consumption. However, that is changing as network providers build out broadband wireless cellular and Internet connectivity, technology providers forge standards for streaming audio and video content, and manufacturers ship greater numbers of portable multimedia devices.

As more phones and other small-form handheld devices get "smarter", so does the potential for people to use them more often, and for many varied and different purposes. The number of mobile cell phone subscribers worldwide surpassed 1 billion in 2006, and technological innovation continues apace as time to market for new products continues to shrink. Telecom providers continue looking for ways to add premium data and value-added products and services to their networks.

As with light and heat, they are attracting a bigger and broader cross-section of media, Internet technology and telecoms companies to the space—increasingly powerful mobile handsets and devices come equipped with Internet access, GPS, digital cameras, streaming audio and video, and other capabilities.

The mobile entertainment market is opening wide while, at the same time, it offers artists more avenues to reach their audiences directly.

14.6 MOBILE MUSIC AND ENTERTAINMENT

In this increasingly competitive environment, mobile telecom providers must change the way they do business and cast a wider net in their search for value-added data and multimedia products and services. Entertainment was the content of choice in the early days of television, and so it is today in the mobile telecoms and mobile, or m-commerce, space.

While mobile music and infotainment—mostly ringtones and wallpapers—account for the largest portion of the mobile entertainment market today.

14.7 WIRELESS APPLICATIONS

A wireless application is a software that runs on a wireless device that exchanges content over a wireless network. The actual wireless applications are distinguished from one another based on the wireless devices, networks and application families, which can be summarized as:

- **Web phones.** The most common device is the Internet-ready cellular phone, which we call a web phone. There are three major Web phones: the US HDML & WAP phone, the European WAP phone, and the Japanese I-mode phone. With them, you can exchange short messages, access the web with a microbrowser, and run personal service applications such as locating nearby items of interest. Most web phones work only when they have a network connection. Newer advanced web phones can run applications.

- **Wireless handhelds**. Another common device, the wireless handheld, such as a Palm, can also message and use a microbrowser. The industrial handhelds, such as Symbol or Psion, can perform very complex operations such as completing orders and taking customer signatures. They have the advantage of working offline.

- **Two-way pagers**. A device used often in business is the pager. The most popular is the two-way pager because it lets you receive and send a message as well as use a microbrowser.

- **Voice portals**. A recent innovation is the voice portal, which lets you have a conversation with an information service by using a kind of telephone or mobile phone.

- **Communicating appliances**. Such electronic devices are outfitted with wireless technology that can participate in the Internet. Examples include, wireless cameras, watches, radios, pens, and many other devices.

- **Web PCs.** The standard Internet-connected personal computer is still used as an access method to mobile accounts, wirelessly or not.

14.8 CELLULAR NETWORK

A cellular network is a radio network made up of a number of radio cells (or just cells) each served by a fixed transmitter, known as a cell site or base station. These cells are used to cover different areas in order to provide radio coverage over a wider area than the area of one cell. Cellular networks are inherently asymmetric with a set of fixed main transceivers each serving a cell and a set of distributed (generally, but not always, mobile) transceivers which provide services to the network's users.

Cellular networks offer a number of advantages over alternative solutions:

- increased capacity

- reduced power usage

- better coverage

The primary requirement for a network to be succeed as a cellular network is for it to have developed a standardised method for each distributed station to distinguish the signal emanating from its own transmitter from the signals received from other transmitters. Presently, there are two standardised solutions to this issue: frequency division multiple access (FDMA) and; code division multiple access (CDMA).

FDMA works by using varying frequencies for each neighbouring cell. By tuning to the frequency of a chosen cell the distributed stations can avoid the signal from other cells. The principle of CDMA is more complex, but achieves the same result; the distributed transceivers can select one cell and listen to it. Other available methods of multiplexing such as polarization division multiple access (PDMA) and time division multiple access (TDMA) cannot be used to separate signals from one cell to the next since the effects of both vary with position and this would make signal separation practically impossible. Time division multiple access, however, is used in combination with either FDMA or CDMA in a number of systems to give multiple channels within the coverage area of a single cell.

Broadcast Messages and Paging

Practically every cellular system has some kind of broadcast mechanism. This can be used directly for distributing information to multiple mobiles, commonly, for example in mobile telephony systems, the most important use of broadcast information is to set up channels for one to one communication between the mobile transreceiver and the base station. This is called paging.

The details of the process of paging vary somewhat from network to network, but normally we know a limited number of cells where the phone is located (this group of cells is called a Location Area in the GSM or UMTS system, or Routing Area if a data packet session is involved). Paging takes place by sending the broadcast message to all of those cells. Paging messages can be used for information transfer. This happens in pagers, in CDMA systems for sending SMS messages, and in the UMTS system where it allows for low downlink latency in packet-based connections.

Movement from Cell to Cell and Handover

The use of multiple cells means that, if the distributed transceivers are mobile and moving from place to place, they also have to change from cell to cell. The mechanism for this differs depending on the type of network and the circumstances of the change. For example, if there is an ongoing continuous communication and we don't want to interrupt it, then great care must be taken to avoid interruption. In this case there must be clear coordination between the base station and the mobile station. Typically such systems use some kind of multiple access independently in each cell, so an early stage of such a handover (handoff) is to reserve a new channel for the mobile station on the new base station which will serve it. The mobile then moves from the channel on its current base station to the new channel and from that point on communication takes place. The exact details of the mobile system's move from one base station to the other varies considerably from system to system. For example, in all GSM handovers and W-CDMA inter-frequency handovers the mobile station will measure the channel it is meant to start using before moving over. Once the channel is confirmed okay, the network will command the mobile station to move to the new channel and at the same time start bi-directional communication there, meaning there is no break in communication. In CDMA 2000 and W-CDMA same-frequency

handovers, both channels will actually be in use at the same time (this is called a soft handover or soft handoff). In IS-95 inter-frequency handovers and older analog systems such as NMT it will typically be impossible to measure the target channel directly whilst communicating. In this case other techniques have to be used such as pilot beacons in IS-95. This means that there is almost always a brief break in the communication whilst searching for the new channel followed by the risk of an unexpected return to the old channel.

14.9 CELLULAR TELEPHONY

The most common example of a cellular network is a mobile phone (cell phone) network. A mobile phone is a portable telephone which receives or makes calls through a cell site (base station), or transmitting tower. Radio waves are used to transfer signals to and from the cell phone. Large geographic areas (representing the coverage range of a service provider) are split up into smaller cells to deal with line-of-sight signal loss and the large number of active phones in an area. In cities, each cell site has a range of up to approximately 1/2 mile, while in rural areas, the range is approximately 5 miles. Many times in clear open areas, a user may receive signal from a cell 25 miles away. Each cell overlaps other cell sites. All of the cell sites are connected to cellular telephone exchanges "switches", which in turn connect to the public telephone network or another switch of the cellular company(see figure 14.2).

Figure 14.2 Cell site

As the phone user moves from one cell area to another, the switch automatically commands the handset and a cell site with a stronger signal (reported by the handset) to go to a new radio channel (frequency). When the handset responds through the new cell site, the exchange switches the connection to the new cell site.

With CDMA, multiple CDMA handsets share a specific radio channel; the signals are separated by using a pseudonoise code (PN code) specific to each phone. As the user moves from one cell to another, the handset sets up radio links with multiple cell sites (or sectors of the same site) simultaneously. This is known as "soft handoff" because, unlike with traditional cellular technology, there is no one defined point where the phone switches to the new cell.

Modern mobile phones use cells because radio frequencies are a limited, shared resource. Cell sites and handsets change frequency under computer control and use low power transmitters so that a limited number of radio frequencies can be reused by many callers with less interference. CDMA handsets, in particular, must have strict power controls to avoid interference with each other. An incidental benefit is that the batteries in the handsets need less power.

Since almost all mobile phones use cellular technology, including GSM, CDMA, and AMPS (analog), the term "cell phone" is used interchangeably with "mobile phone"; however, an exception of mobile phones not using cellular technology is satellite phones.

Wireless Spectrum

The electromagnetic spectrum, or simply spectrum, is the entire range of energy waves over which communicating devices transmit. The electromagnetic spectrum is assigned common groupings of energy waves, commonly called airwaves, that make bands of the spectrum. Over the airwaves, TV, radio, cell phones, or any wireless Internet devices communicate with a transceiver. Each kind of transceiver uses dedicated frequency ranges that are measured in Hertz (Hz); 1 Hz is one cycle per second. An interesting property of the spectrum is that higher frequencies travel shorter distances. They take more power to transmit. With enough power, they can be life-threatening. Higher frequencies can be modulated to carry more bits per second than longer waves, but they are subject to atmospheric interference. Broadcasters generally prefer owning a lower frequency because it costs less to transmit a signal, it carries farther, and it is

generally "safer". The US Federal Communications Commission (FCC) and similar agencies around the world break up the spectrum and assign bands for specific purposes. Bands are ranges of frequency with common names. World wide bodies such as the International Telecommunications Union (ITU) also make frequency agreements, so that devices will operate clearly worldwide. Regulating radio interference is necessary so that wireless devices do not interfere with one another. To prohibit interference from a neighbouring transmitter, the FCC restricts bands of coverage.

GSM-900 and GSM-1800

GSM-900 and GSM–1800 are used in most parts of the world: Europe, Middle East, Africa and most of Asia.

GSM-900 uses 890–915 MHz to send information from the Mobile Station to the Base Transceiver Station (uplink) and 935–960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz.

Most of the GSM operators in India use the 900 MHz band. Operators like, Airtel, Idea, and some others, use 900 MHz in rural areas as well as in urban areas whereas hutch uses 1800 MHz everywhere except in its bpl network

GSM-850

GSM-850 and GSM-1900 are used in the United States, Canada, and many other countries in the Americas. GSM-850 is also sometimes erroneously called GSM-800.

In Australia, GSM-850 is the frequency allocated to Telstra's NextG Network which was switched on in October 2006. The NextG Network is a step up from the 3G Network and is available at faster speeds Australia wide compared to the 3G Network which is limited to only major population centres.

GSM-850 uses 824–849 MHz to send information from the Mobile Station to the Base Transceiver Station (uplink) and 869–894 MHz for the other direction (downlink). Channel numbers 128 to 251.

Multi-band and Multi-mode Phones

Today, most telephones support multiple frequencies used in different countries. These are typically referred to as multi-band phones. Dual-band phones can cover GSM networks in pairs such as 900 and 1800 MHz frequencies (Europe, Asia, Australia and Brazil) or 850 and 1900 (North America). European tri-band phones typically cover the 900, 1800 and 1900 bands giving good coverage in Europe and allowing limited use in North America, while North American tri-band phones utilize 850, 1800 and 1900 for widespread North American service but limited worldwide use. A new addition has been the quad band phone, supporting all four major GSM frequency groups, allowing for widespread usage globally, including in North America.

There are also multi-mode phones which can operate on GSM systems as well as on mobile-phone systems using other technical standards. Often these phones use multiple frequency bands as well. For example, one version of the Nokia 6340i GAIT phone sold in North America can operate on GSM-1900, GSM-850 and legacy TDMA-1900, TDMA-800, and AMPS-800, making it both multi-mode and multi-band.

14.10 CHECK YOUR PROGRESS

6. What Mobile commerce ?

7. What is meant by mobile banking?
8. A _____is a software that runs on a wireless device that exchanges content over a wireless network.
9. What does cellular network comprises of?
10. Acronym for FDMA and CDMA.

    Answers to Check your progress
1. M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as smartphones and tablets. As a form of e-commerce, m-commerce enables users to access online shopping platforms without needing to use a desktop computer.
2. Mobile banking is the act of making financial transactions on a mobile device (cell phone, tablet, etc.). This activity can be as simple as a bank sending fraud or usage

activity to a client's cell phone or as complex as a client paying bills or sending money abroad.

3. wireless application

4. A cellular network is a radio network made up of a number of radio cells (or just cells) each served by a fixed transmitter, known as a cell site or base station.

5. Frequency Division Multiple Access (FDMA) and Code Division Multiple Access (CDMA).

14.11 SUMMARY

This unit introduces about Mobile commerce and its applications. Above all mobile payments are given more importance at a global range. Various payment procedures and methodologies are highlighted. Also the components of Mobile commerce are elaborated with a schematic diagram. Wireless application software is highlighted with its diverse applications. The advantages of wireless network are detailed. Structural study of cellular telephony is mentioned with recent technologies.

14.12 KEYWORDS

- **Mobility** is defined as the potential for movement and the ability to get from one place to another using one or more modes of transport to meet daily needs.

- **Mobile payment** (m-payment) is a point-of-sale (PoS) transaction made or received with a mobile device.

- W*eb phone*, also known as a web dialer, is a web application that enables two-way international phone calls from a web browser.

- C**ellular network** or mobile network is a communication network where the link to and from end nodes is wireless. The network is distributed over land areas called "cells", each served by at least one fixed-location transceiver (typically three cell sites or base transceiver stations).

- T**ransceive**r is a combination transmitter/receiver in a single package. While the term typically applies to wireless communications devices, it can also be used for transmitter/receiver devices in cable or optical fiber systems.

- **GSM 850** is simply GSM technology operating in the Cellular (850 MHz or "800") frequency band. Both the technology and frequency band have been around for many years, but not until 2002 were they combined. In the U.S. prior to 2002, GSM technology only operated in the PCS (1900 MHz) frequency band.

14.13 QUESTIONS FOR SELF STUDY

9. Write a brief note on Mobile commerce.

10. Describe the components of Mobile commerce.

11. Discuss about wireless applications.

12. Explain the advantages of wireless network.

13. Write a note on cellular telephony.

14.14 REFERENCES

3. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

4. Joseph, P. T. (2019). *E-commerce: An Indian perspective*. PHI Learning Pvt. Ltd..

UNIT 15: PORTALS OF E-BUSINESS

Structure

15.0 OBJECTIVES

After studying this unit, you will be able to:

- Discuss Benefits Portal

- Brief out on Portal Features

- Requirements of Intelligent Websites

- Setting Website Goals and Objectives

- Considering the Website's Target Audience

- Selecting a Hosting Service

15.1 INTRODUCTION

Portals

The term "Portal" means different things to different people. To many, a simple website aimed at employees is a portal. A portal may be defined as a point of access to and interaction with relevant information, applications and business processes, by select targeted audiences, in a highly personalized manner.

Different types of Portals Portals can be broadly classified into different categories as shown in Figure 15.1.
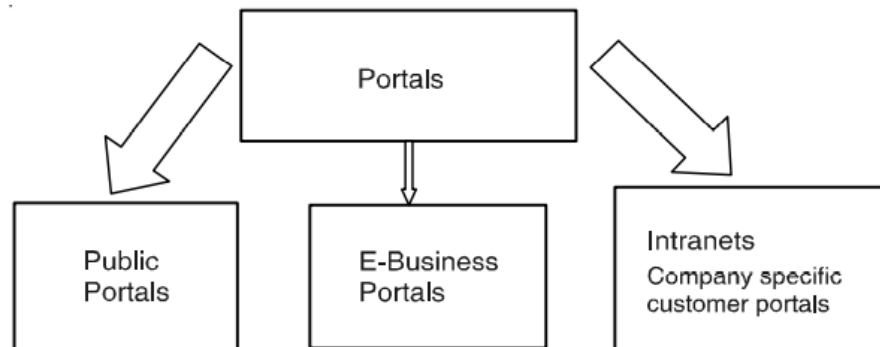

Fig. 15.1 Types of portals.

1. **Public portals.** Most internet users are aware of portals like Yahoo or Google. Indian Railways is another example.

2. **e-Business portals**. These portals support business transactions (i.e. buying, selling, order booking, payments, etc.) online.

   These can be classified into three categories:

   2(a) B2C portals. These portals extend the reach of the business to its customers for the purpose of ordering, billing, customer service, self-service, etc. Some of the successful B2C portals are: Amazon, eBay, Dell, etc. where people browse products, buy, order and pay online. Indian Rail site (IRCTC) is one of the successful B2C sites in India where thousands of people book train tickets and pay online daily.

   2(b) B2C. Those portals are quite popular for airline ticket booking, hotel booking, etc. The basic idea of such portals is to attract and keep the attention of buyers as well as to collect information about buyers that can be used to enhance and personalize the customer relationship and thus, drive future sales. More personalized relationships can result in increased customer loyalty.

   2(c) B2B portals. This extends the enterprise to its suppliers and partners. This helps to build better relationships between the company and its suppliers, customers and partners (via extranets) and this improved relationship can lead to increased trading partner loyalty. Generally, these portals are made by individual companies for their own suppliers and customers.

3. **Intranets.** These are normally portals aimed at customers of an organization. Employee portals, University portals, etc. are some of the examples.

15.2 PORTAL BENEFITS

Portals can bring benefits in a number of areas:

- Unify the enterprise.
- Give visibility for the enterprise all over the world.
- Reduce cost.
- Improve productivity.
- Reduce administration overhead.
- Increase revenue.
- Improve customer support and customer loyalty.
- Improve support for sales and marketing.

15.3 PORTAL FEATURES

Surveys have shown that four factors constituting the elements of a good website encourage viewers to return to the site. These are:

- High quality content.
- Having the right information at the right place and right time.
- Ease of use. The structure of the side should not be overcomplicated or too big. You never get lost in a good site, since it is always clearly signposted.
- Quick to download. Good sites also download quickly. Bad sites are cumbersome and slow. Visitors would not wait.
- Frequently updated. Good sites put up new information which is useful, relevant and timely for their audience, which takes money, time and energy to maintain.

Figure 15.2 shows the customer interface elements that are needed in a website. The Web gives the customer unlimited choice, with millions of sites to select from. In order to make the customer visit, stay and revisit your site, the site must have a unique proposition for the visitor. This is called an Internet Value Proposition (IVP)
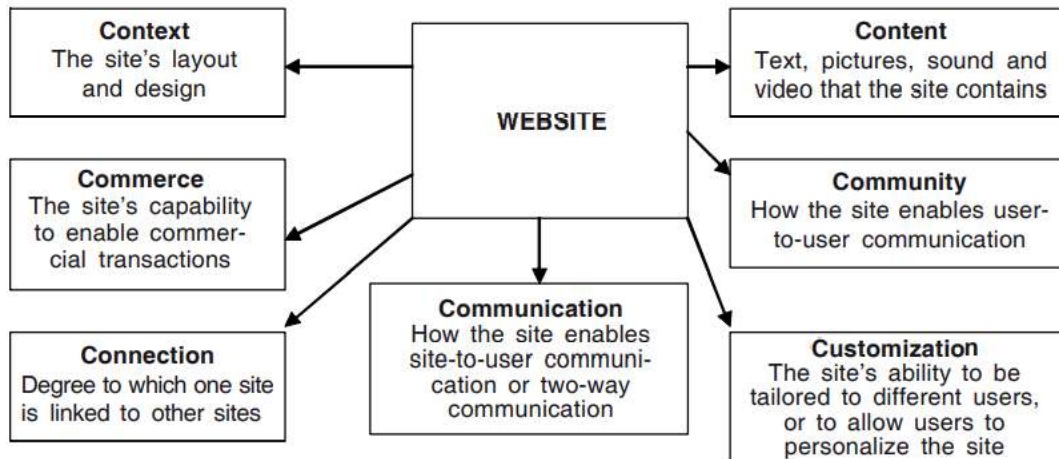
Fig. 15.2 Interface elements in a website

Ideally, a good website needs to find a proposition that explains how and what their organization is offering. For example:

- Is different from its competitors
- Is not available in the real world
- Makes a difference to the customer's life

At the very least the proposition should clearly show the offered services and the credibility to deliver. Once a proposition has been finalized, the following steps need to be taken:

1. First we need to leverage the proposition in traffic-building by combining it with the URL or Web address and advertising it.
2. We need to clearly state the proposition on-site.
3. We need to deliver on the proposition through all interactions a customer has, including online and offline fulfilment and service.

The two basic aspects of site context are function and aesthetics.

Function. The vast amount of information displayed on a website must be presented to the customer in a coherent manner, and the customer must be able to move freely throughout the website. Three factors are critical in the layout of the site:

1. Section breakdown. This describes the way that the site is organized into subcomponents. For example, www.chennaibazaar.com is an online retail store whose site structure includes search, different kinds of merchandise, gift ideas, and help. There are also categories of goods—men's, women's, kid's clothes.

37

2. Linking structure. Linking structure describes the way in which alternative sections of the site are linked. Clicking on sarees on the homepage of www.chennaibazaar.com takes you to the sarees section, with lots of choices. This linking structure enables the users to easily move back and forward between the sections of the site

3. Navigation tools. Navigation tools refer to the site tools that facilitate the movement of the user throughout the site. Navigation tools for www.chennaibazaar.com include sarees search for all occasions. Aesthetics.

Aesthetics = Multimedia + Colour + Style + Layout and Typography

The aesthetic nature of the site is largely captured by visual characteristics such as colours, graphics, photographs, font choices, and other visually-oriented features. Two aesthetic features are described below:

- Colour scheme. The colour scheme refers to the colour choices throughout the site. As one might guess, www.chennaibazaar.com has emphasized a colourful screen, with different colours splashed for different items.

- Visual themes. Visual themes capture the story or stories portrayed across the site. Women clad in sarees catch the attention of the audience easily.

There are basically four dimensions of website content. These are examined below and then applied to the now familiar example of Gear.com.

Offering mix. The content of the site can include product information and/or services. Frequently, sites include a mixture of these three elements. www.chennaibazaar.com focuses almost exclusively on product content, with significantly less emphasis on information or services.

Appeal mix. This refers to the promotional and communications messaging projected by the company. Academic literature has identified two broad types of appeal: cognitive and emotional. Cognitive appeals focus on the functional aspects of the offering, like low price, reliability, availability, customer support, and degree of personalization. Emotional appeals focus on emotionally resonant ties to the brand or product—humour, novelty, warmth, or stories.

Multimedia mix. This term refers to the variety of media—text, audio, image, video, and graphics—incorporated into the site. There is very limited use of product photographs.

Content type. Current content on a website is highly time-sensitive, whereas reference content is less time-sensitive and has a longer shelf life. www.timesofindia.com, the online version of The Times of India, offers an archive of articles published in the past.

Personalization plays an important role in making a website customer-effective. Internetbased personalization delivers customized content and services for the individual, either through Web pages, e-mail, or through push-technology. Personalization contributes to a website in the four following ways:

- **Sell.** Personalization can make it easier for customers to select their products. Customers of an online supermarket do not want to select a new shopping basket of goods each time they shop.

- **Serve.** Customers who uses an online travel booking service do not want to have to key in the same journey details if it is a common itinerary. Instead, personalization helps them to save their itinerary.

- **Speak.** Through personalization, customers can select the type of communication they want to receive from a company as part of permission marketing.

- **Sizzle.** All the above can help add value, strengthen the brand, and develop the relationship.

To attract users and make them return, some sites provide a variety of features. Some of them are described below:

- Login registration. Having previously registered on a site, the user returns and enters the requisite information through the site interface. The site recognizes the returning user, and configures itself to the user's preset preferences.

- Cookies. Most sites, to identify visitors, attempt to track and gather data on returning user's behaviour by quietly saving, identifying and tracking information on the user's local disk storage in temporary files called cookies.

- Personalized e-mail accounts. Many sites provide free e-mail accounts to send and receive e-mails from the site, using a unique e-mail address.

- Content and layout configuration. Users can select screen layouts and content sources based on their interests.

15.4 REQUIREMENTS OF INTELLIGENT WEBSITES

Building an intelligent website that optimally leverages all sources of information for an online company does not happen overnight. It takes several iterations, a significant investment in technology, and an accumulation of knowledge that comes only with experimentation, trial and error. Companies that are new to the online game usually are at stage zero and use almost no data at all, whereas companies more advanced in e-business intelligence are able to integrate data coming from transactions, clickstream, and other sources to build powerful consumer relationships and market leadership.

There are four primary types of customer information that are leveraged through e-business intelligence:

1. **Demographics**. This describes the basic attributes of the customers—who they are, what neighbourhood they live in, what their income bracket is, their marital status, and so on.

2. **Expressed preferences**. This describes what topics customers have expressed an interest in (e.g. types of books or music they like, stocks they track, sports teams they follow). The preferences are usually captured through form-based questionnaires when the consumer registers for a site or service.

3. **Past transactions**. These are the records of past transactions that the consumers have had with the company (e.g. what books they have purchased, what auctions they have conducted). These are recorded when the consumer actually conducts his or her purchases.

4. **Observed behaviours**. This information is derived from observing the navigation the customer follows in using the website, as well as where he came from and where he went afterwards. This data, called clickstream information, comes from every single click throughout the consumer online experience, and it is collected in large log files.

As the e-commerce company gets more and more sophisticated in building an intelligent e-business, it should progressively leverage these different types of information in an efficient way. Let us now look at the steps e-commerce companies typically follow in leveraging their information, in the order in which they typically evolve as they get more and more skilled in exploiting the power of e-business intelligence.

Step 1: Basic Web traffic analysis. The very first type of analysis of any Web activity is the measure of Web traffic. In the early days of the Web, hit counters were the rage. Hits and page

views are the lowest level of clickstream data—the sequential record of pages visited. This data provides a record of entry and exit points into a website, pages that were visited, links that were followed, the duration for which a person viewed a particular page, the precise day and time, the browser type, the visitor's IP address, and other information. This type of information is often used to help secure advertising dollars. It can also point to problems in a site—a problematic page, for example, where people drop off because response time is too slow. It can help a website establish its quality and systems maintenance practice to ensure that the site is able to absorb high traffic times

Step 2: Customer interaction analysis. The next step is to go into more details about customer interactions with the website. The first type of measure is the conversion rate from a browser to a customer. Conversion rates have been viewed as a key indicator of a website's effectiveness.

Registered users are the people who have had to register for site usage, often by filling out a survey form. The New York Times, for instance, is a free site, but requires the user to fill in a registration form. Depending on the questions asked, this data could allow a website to size up its visitors and customers by profession, education, age, gender, race, leisure activities, merchandise purchasing, and so forth. Through the registration process, the site is able to get the demographic as well as the preference information. Recorded e-mail addresses provide a way for the site to communicate with these registered visitors.

This data may then be used to help inform personalization engines to serve the contents according to the visitor's interests. It enables the site to display the person's name when he visits, in a bid to build intimacy. A visitor with an expressed affinity for golf or gardening, may then be served advertisements or contents, specific to those interests. Combined with clickstream data on the visitor's site usage, the website is able to develop a fuller picture of both individual visitors and its visitors population as a whole. Once users have become customers, the site is able to analyze the historical transactions to identify their most loyal customers and their purchasing patterns, as well as the segments they fall into with respect to interests, frequency, or profitability.

Step 3: Real-time personalization. Personalization is the ultimate realization of the one-to-one marketing dream. Customers are recognized when they come in, can tailor the way they interact with the merchant, and receive promotions and marketing programs that perfectly fit their personal requirements and preferences.

The four primary ways of performing personalization are greetings, customization, narrowcasting, and recommendation.

- **Greetings** are the most basic form of personalization. The customer is greeted by name and welcomed back when he or she comes on the site. Personalization engines recognize a visitor's Internet protocol address or cookies stored on his personal computer, and correlate that information with past visits in order to recognize the visitor.

- **Customization** allows a customer to tailor the service he is receiving from an e-commerce site, or to configure the products he wants to buy. As an example, any Yahoo! user can customize his use of the popular search by creating a 'MyYahoo!' environment which is more adapted to his needs. The 'MyYahoo!' page will, for instance, show only stock quotes for your portfolio, and the particular news subjects you are interested in.

- One great example of customization is the American Airlines website. Once logged into the site, customers are welcomed by name, and they are shown the number of frequent flyer miles they have on their account, as well as customized information and special offers based on their profile and previous choice of preferences, including home airport, preferred destination, hotel and car rental companies, and preferred seating choices.

- **Narrowcasting i**s the delivery of time-sensitive information, personalized to each consumer. Instead of sending messages to a large numbers of customers, they can be intimated about particular events they want to be alerted about. These kinds of personalized messages can be sent through e-mail, phone, or pagers which enable the customer to be informed without having to connect to the site. Yahoo!Finance, for example, enables a customer to define an alert that will be delivered if a stock price fluctuates more than a certain percentage. United Airlines also provides flight-paging services via various wireless devices. Flight paging provides customers automatic notification of flight delays or cancellations so that they can remain informed of any changes in the status of United Airlines flights.

- **Recommendation** enables a site to propose products that are tailored to the customers' requirements, whether they have been explicitly expressed by the consumer or implicitly calculated by the e-commerce engine. Recommendation technology has evolved dramatically in the past few years. It used to be based only on the preferences that a customer would have explicitly expressed at registration time. Now it can be done in real

time and predicted automatically by the personalization engine using different types of information such as observed real-time behaviour, purchase histories, and expressed preferences. Finally, it can match that data with information regarding other consumers who share similar interests, using a technique known as collaborative filtering. The system is then able to make recommendations that are quite accurate.

Step 4: Getting to fine-grained segmentation. Personalization technologies are not very adaptive to drive a massive marketing campaign, nor are they particularly suitable for many types of purchasing decisions with complex sales cycles and multiple decision-makers. The next step, therefore, is to enhance the site's marketing power by using an e-business intelligence system performing customer segmentation. We start with products that are at a hand's reach through coarse segmentation, and we continue on to fine-grained segmentation.

The harvesting of Web generates large, complex data volumes. Companies are gathering data that is more finely grained than in the past. By integrating data from various systems, they are able to go beyond the basic profile of a customer who is a 35 year old male who buys a piece of electronics equipment on the average of once a year. Website activity, information on cookies, household and demographic information, online surveys, customer support calls, consumer credit reports and other sources enable the company to collect additional details. The number of attributes associated with one single piece of data can grow by several factors.

The mounting quantity and complexity of this data often beg for data mining. Data mining goes beyond reporting, query, and multidimensional analysis to automatically sift through large data sets to discern patterns that might otherwise be difficult to detect. It uses artificial intelligence technologies to conduct knowledge discovery—that is, it can look for patterns in large data sets and identify common elements.

Step 5: Going through the streams of clicks. Every move on a website, every ad banner clicked through, every page request from every visitor is recorded by the website owners into massive log files; this is the clickstream information.

The clickstream data contains details on customer behaviour that are richer than what can be achieved in traditional channels. It moves a step beyond the department store practice of using video surveillance cameras to track customer movement throughout the store to improve merchandising.

Step 6: Enrich content with external data. Once a customer has made several purchases, the website is able to further enhance the customer profile. Demographic data from thirdparty providers may be appended to the profile to provide a richer view of the customer base. Analyzing that enriched data might show, for instance, that a customer who buys history books falls into a demographic segment inclined to also buy classical music. Marketing pitches in the form of e-mails and personalized content may then be delivered to cross-sell classical music CDs.

This data is critical in building profitable repeat business. It enables refinements in oneto-one marketing in the form of e-mails, snail mail, and personalized content served during site visits. The overall customer base may be segmented by a host of characteristics to better understand who is buying what. The data may be analyzed to determine an overall customer score that provides the website with a roadmap on which customers are their best bets for marketing efforts.

The simple fact to be realized is, the more data you have about your customers, the more sophisticated data mining and segmentation models you will be able to build. Using thirdparty data to enrich your database will help you find segments that were otherwise undetectable. Sometimes this data must be purchased. Sometimes, you can devise business arrangements or partnerships that provide it. American Airlines and United Airlines, for example, have recognized that a great source of information that helps in their marketing efforts is the data coming from the affinity credit card businesses they have associated with their name, and their frequent flying programs.

Step 7: Reaching optimal intelligence. A company can reach optimal intelligence once it is able to combine historical transaction records, observed behaviour via clickstream data, and preferences expressed in online surveys.

15.5 SETTING WEBSITE GOALS AND OBJECTIVES

The first thing that an e-business entrepreneur should do before any Web page is created, is to determine the goals, objectives, and overall purpose of the e-business website. Without these the website may not have the focus it needs to be successful. To help determine the goals and objectives, you should ask and answer questions such as the following. Will the website:

1. Allow customers to order products and services online?
2. Provide technical support for products and services?

3. Advertise products and services?

4. Build the e-business's image and brand?

5. Collect information about current and potential customers?

6. Provide links to related web pages?

7. Provide general or industry information? and 8. Recruit employees?

A quick look at this list of sample questions clearly indicates that most e-business websites have multiple goals and objectives. The answers to these and similar questions are used to determine the website's overall purpose.

15.6 CONSIDERING THE WEBSITE'S TARGET AUDIENCE

After you establish the website's goals, objectives, and overall purpose, the next step is to consider the website's target audience. In too many instances, e-businesses design websites around the needs of the e-business rather than the needs of the target audience. It is critical to consider both the information the target audience wants and the tools it uses to access the Web. Again, a series of questions such as the following, should be asked and answered:

1. Is the audience composed of experienced internet users, novice users, or a mix of both? Experienced internet users are likely to be able to handle a more sophisticated level of website complexity than novice users.

2. What type of browser will the audience be using—Netscape, Internet Explorer, WebTV, or other specialized browsers? Some design techniques that are supported by later Web browser versions, such as animations and frames, may not be supported by earlier versions of the same browser or by other browsers.

3. At what speed does the audience connect to the internet—at 56 Kbps over a modem or over a high-speed dedicated connection? A website designed to be viewed successfully over a high-speed dedicated connection may be problematic for viewers using a slow modem connection.

4. At what screen resolution does the target audience view Web pages—640 ———————————— 480, 800 ———————————— 600, or higher? Websites designed to be viewed at 800 ———————————— 600 resolution without horizontal scrolling will greatly annoy those who view the site using a monitor with 640 ———————————— 480 resolution.

Answers to each of these questions will determine how the Web page design can enhance or detract from a visitor's viewing experience and, ultimately, the ability or failure of the website to meet its goals.

15.7 SELECTING A HOSTING SERVICE

For larger website implementations, the team will want to obtain the advice of consultants or other firms that rate ISPs and CSPS, such as Keynote Systems and the Directory of Internet Service Providers published by Boardwatch Magazine. The most important factors to evaluate when selecting a hosting service include:

- Functionality

- Reliability, bandwidth and server scalability

- Security

- Back-up and disaster recovery

- Cost

Companies that sell hosting services provide different features and different levels of service. The functionality offered by a service provider can include credit card processing and the ability to link to existing databases that store customer and product information. Some tracking software provides much more detailed information and easy-to-use report generators than other tracking software. You should determine the functionality offered by a hosting service and carefully evaluate whether that functionality will be sufficient to meet the needs of your website.

The service should offer a guarantee that limits possible down time. E-commerce buyers expect hosting services to be up and running 24 hours a day, every day. Of course, no hosting service can promise never-to-fail service, but some can provide staffing and back-up hardware that minimizes reliability problems. Coordination of this function with the service provider can be very important. Usually, a business must have some round-the-clock staff available or on-call to work with the service provider when an interruption occurs.

The bandwidth of the service's connection to the Internet must be sufficient to handle the peak transaction loads that its customers require. Sometimes a service provider will sign up new accounts faster than it can expand the bandwidth of its connections, resulting in access bottlenecks. A guarantee that specifies bandwidth availability or server response times is worth negotiating into a service provider contract. If you expect your site's traffic to increase rapidly, it

is important that your service provider increases rapidly the server capacity and the bandwidth provided. In general, larger hosting services can scale up more easily than smaller hosting services. Again, it is worth negotiating some scalability into the service provider contract in such situations.

Since the company's information on customers, products, pricing, and other data will be placed in the hands of the service provider, the vendor's security policies and practices are very important. The service provider should specify the types of security it provides and how it implements security. No matter what security guarantees the service provider offers, the company should monitor the security of the e-commerce operation through its own personnel or by hiring a security consulting firm. Security consultants can periodically test the system and launch attacks on the security features used by the service provider to determine whether they are easily breached.

The hosting service should be able to guarantee close to 100 per cent reliability by having a workable disaster recovery plan in place. In addition to having off-site data backup or mirroring, the hosting service should have a way to restore your site very quickly in the case of a natural disaster. Service providers offer many different pricing plans for different levels of service. Knowing what types of server hardware and software your site will require, and having a good estimate of the range of transaction loads the site is likely to generate, can help in negotiating a price for the hosting service.

15.8 CHECK YOUR PROGRESS

11. Define portal.
12. List different types of portals.
13. What is URL?
14. Need of website creation.
15. What is bandwidth?

Answers to Check your progress

1. A portal may be defined as a point of access to and interaction with relevant information, applications and business processes, by select targeted audiences, in a highly personalized manner.

2. The types of portals are : Public portals, e-Business portals and intranet.

3. Just as buildings and houses have a street address, webpages also have unique addresses

to help people locate them. On the Internet, these addresses are called URLs (Uniform Resource Locators).

4. Web page is created to determine the goals, objectives, and overall purpose of the e-business website

5. Bandwidth specifically refers to the capacity at which a network can transmit data. For example, if the bandwidth of a network is 40 Mbps, it implies that the network cannot transmit data faster than 40 Mbps in any given case.

15.9 SUMMARY

This unit elaborates on creation of website portals. Various types of portals are discussed considering varied applications. The benefits of creating the portals to various customers is highlighted. The steps how the customer uses the interfacing elements in a website are detailed. Different dimensions of website content are described. Various steps involved in e-business intelligence are highlighted. Also the important factors are discussed to evaluate when selecting a website hosting service.

15.10 KEYWORDS

- **Portals** are online platforms that allow businesses to conduct interactions and transactions with customers and suppliers instantly, facilitating a more intuitive and connected operation.

- I**ntrane**t is a private network contained within an enterprise that is used to securely share company information and computing resources among employees. An intranet can also be used for working in groups and teleconferences. Intranets encourage communication within an organization.

- **Web address** contains information about the location of the webpage. It is also known as the URL (uniform resource locator). Like the address for your home, a web address organizes information about a webpage's location in a predictable way.

- **Navigation tools** on the web are the links used to navigate from one web page to another. Navigation tools vary considerably from one website to the next. Well-organized websites include a variety of navigation tools ensuring you can easily understand the structure of the website, and find you way from page to another.

- **Narrowcasting** is the dissemination of information (usually via Internet, radio, newspaper, or television) to a narrow audience, rather than to the broader public at-large.

15.11 QUESTIONS FOR SELF STUDY

14. Write the significance of portals.

15. Discuss different types of portals.

16. List the benefits of creating the portals.

17. Discuss interfacing elements in a website.

18. Describe four dimensions of website content.

19. Discuss the steps involved in e-business intelligence.

20. Explain important factors to evaluate when selecting a website hosting service.

15.12 REFERENCES

5. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.

6. Joseph, P. T. (2019). *E-commerce: An Indian perspective*. PHI Learning Pvt. Ltd..

UNIT 16: LEGAL AND ETHICAL ISSUES

Structure

16.0 OBJECTIVES

After studying this unit, you will be able to:

- Signify Computers as Targets for Crime

- Give an account on Computers as Storage Devices

- Analyze Computers as Communications Tools

- Discuss about Privacy is at Risk in the Internet Age

- Give an account on Cookies and Privacy

- Elaborate Internet threats

- Analyze special nature of Computer Ethics

16.1 INTRODUCTION

Ethical Issues in the Digital Economy

Technology can be a double-edged sword. It can be the source of many benefits. One great achievement of contemporary computer system is the ease with which digital information can be transmitted and shared among many people. But at the same time, this powerful capability

creates new opportunities for breaking the law or taking benefits away from others. Balancing the convenience and privacy implications of providing personal data on-line is one of the compelling ethical issues raised by contemporary information systems.

Ethics refers to the principles of right and wrong that can be used by individuals acting as free moral agents to make choices to guide their behaviour. Information technology and information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights and obligations.

Five moral dimensions of the information age are:

1. **Information rights and obligations**. What information rights do individuals and organization possess with res pect to information about themselves? What can they protect?

2. **Property rights**. How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership is difficult, and ignoring such property rights is so easy?

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

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

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

The Internet is rapidly transforming the way we communicate, educate, and buy and sell goods and services. As the Internet's potential to provide unparalleled benefits to society continues to expand, however, there has been an increasing recognition that the Internet can also serve as a powerful new medium for those who wish to commit unlawful and criminal acts.

Unlawful conduct involving the use of the Internet is just as intolerable as any other type of illegal activity. Ensuring the safety and security of those who use the Internet is thus a critical element of the Administration's overall policy regarding the Internet and electronic commerce—a policy that seeks to promote private sector leadership, technology-neutral laws and regulation, and an appreciation of the Internet as an important medium for commerce and communication,

both domestically and internationally. Indeed, the continued growth and maturation of this new medium depends on our taking a balanced approach in order to ensure that the Internet does not become a haven for unlawful activity.

16.2 COMPUTERS AS TARGETS FOR CRIME

One obvious way in which a computer can be involved in unlawful conduct is when the confidentiality, integrity, or availability of a computer's information or services is attacked. This form of crime targets a computer system, generally to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server. Many of these violations involve gaining unauthorized access to the target system (hacking).

Offences involving theft of information may take a variety of forms, depending on the nature of the system attacked. Sensitive information stored on law enforcement and military computers offers a tempting target to many parties, including subjects of criminal investigations, terrorist organizations, and foreign intelligence operatives. Hackers also target non-governmental systems to obtain proprietary or other valuable information. For example, a hacker might gain access to a hotel reservation system to steal credit card numbers. Other cases may fall into the broad category of intellectual property theft. This includes not only the theft of trade secrets, but also much more common offences involving the unauthorized duplication of copyrighted materials, especially software programs. Other cases may involve a perpetrator who seeks private information about another individual, whether as a means to an end (e.g. to extort money or to embarrass the victim through public disclosure), to obtain a commercial advantage, or simply to satisfy personal curiosity.

Targets in this category include systems containing medical records, telephone customer records (such as call records or unlisted directory information), or consumer credit report information. Computers can also be the target of an offence in cases where an offender gains unauthorized access to a system. For instance, an offender may use his computer to break into a telephone switching system (including a private system, such as a PBX) to steal long-distance calling services. (This type of telephone equipment manipulation is often referred to as "phone phreaking" or simply "phreaking".) In some cases, hackers have used the resources of compromised systems to perform intensive computational tasks such as cracking encrypted passwords stolen from other sites. The theft-of-service offences are often associated with the

practice of "weaving", in which a hacker traverses multiple systems (and possibly multiple telecommunications networks, such as the Internet or cellular and landline telephone networks) to conceal his true identity and location. In this scenario, the sole reason for breaking into a given computer may be to use it as a stepping stone for attacks on other systems.

A more insidious type of damage takes place in cases where the attacker compromises a system in furtherance of a larger scheme. The most well-known examples of this type of attack have involved telephone network computers. In one case, a hacker manipulated telephone switching equipment to guarantee that he would be the winning caller in several call-in contests held by local radio stations. The fruits of his scheme included two sports cars and $30,000 in cash. Internet-connected computers are subject to similar types of attacks. Routers are analogous to telephone switches and thus are tempting targets for skilled hackers who are interested in disrupting, or even re-routing, communications traffic on the network.

In the category of attacks known collectively as "denial of service", the objective is to disable the target system without necessarily gaining access to it. One technically straightforward method of accomplishing this objective is "mailbombing", the practice of sending large volumes of e-mail to a single site (or user account) to clog the mail server or even to cause the target host to crash. Other methods—ranging from simply tying up incoming phone lines to more sophisticated attacks using low-level data transmission protocols—may also be used to achieve the same end of rendering the target system unavailable for normal use.

16.3 COMPUTERS AS STORAGE DEVICES

A second way in which computers can be used to further unlawful activity involves the use of a computer or a computer device as a passive storage medium. Drug dealers might use computers to store information regarding their sales and customers. Another example is a hacker who uses a computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software). Indeed, computers have made it possible for law enforcement agencies to gather some information that may not have been previously even maintained in the physical world.

For example, an unsophisticated offender, even after "deleting" computer files (as opposed to destroying paper records), might leave evidence of unlawful activity that a trained computer forensic expert could recover. In addition, because an average computer with several gigabytes of memory can contain millions of pages of information, a law enforcement agent might,

pursuant to lawful authority (such as a warrant), find volumes of information in one place. Of course, that information is useful only if there are trained computer experts on hand in a timely fashion, familiar with the relevant computer hardware or software configuration, to search the computer for specific information and to retrieve it in readable form.

16.4 COMPUTERS AS COMMUNICATIONS TOOLS

Another way in which a computer can be used in a cyber crime is as a communications tool. Many of the crimes falling within this category are simply traditional crimes that are committed online. The unlawful conduct that exists in the physical, "offline" world also exists in the online world, such as the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography. These examples are, of course, only illustrative; online facilities may be used in the furtherance of a broad range of traditional unlawful activity. E-mail and chat sessions, for example, can be used to plan or coordinate almost any type of unlawful act, or even to communicate threats or extortion demands to victims.

Just as the legitimate use of the Internet is growing, so too is the Internet increasingly being used to facilitate traditional offences. For example, because e-mail allows private communications between parties, individuals have used the Internet to send threatening e-mails (including threats to the President). The Internet's one-to-many broadcast capability has also allowed individuals to falsely advertise goods on the Internet or on a website.

The Internet's file transfer capability also enables the Internet to be used as a product delivery system. Because large files can be copied and transmitted reliably, quickly, and cheaply, software companies are now selling software over the Internet; the buyer simply provides a credit card number and downloads the software from the Internet to his or her personal computer. This same capability unfortunately allows for the unauthorized reproduction and distribution of copyrighted software.

Some criminal activities employ both the product delivery and communications features of the Internet. For example, paedophiles may use the Internet's file transfer utilities to distribute and receive child pornography, and use its communications features to make contact with children. Because users need not transmit their voice or appearance, it is easy for an adult to pose as a child and to gain the confidence of children online.

As noted above, this report's primary focus is on this third way in which computers can be used to commit unlawful acts–the use of computers and modern telecommunications facilities as tools

to commit an offence. Many of the enforcement and investigative challenges associated with unlawful conduct on the Internet, however, extend to all three ways in which computers can be used for unlawful activity. Consequently, the recommendations contained in this report, if acted upon, could assist law enforcement agencies in combating all types of unlawful conduct involving the use of the Internet.

Cyberstalking

Cyberstalking is a prime example of the use of computers and the Internet to facilitate a traditional, offline crime. Cyberstalking generally refers to the use of the Internet, e-mail, or other electronic communications devices to "stalk" another person—where "stalking" in the traditional sense means to engage in repeated harassing or threatening behaviour (such as following a person, appearing at a person's home or workplace, making harassing telephone calls, or leaving written messages or objects) that places the victim in reasonable fear of death or bodily injury. The Internet provides new avenues for would-be stalkers to pursue their victims.

16.5 PRIVACY IS AT RISK IN THE INTERNET AGE

Privacy is not just about hiding things; it is about self-possession, autonomy, and integrity. But this right of privacy does not mean that it is the right of people to close their doors and pull down their window shades, perhaps because they want to engage in some sort of illicit or illegal activity. It is the right of people to control what details about their lives stay inside their own houses and what leaks to the outside.

To understand privacy, we need to rethink what privacy really means today:

It is not about the man who wants to watch pornography in complete anonymity over the Internet. It is about the NGO who is afraid to use the Internet to organize their community against a proposed toxic dump—afraid because the dump's investors are sure to dig through their past if they becomes too much of a nuisance.

- It is not about people speeding on the nation's highways who get automatically generated tickets mailed to them thanks to a computerized speed trap. It is about lovers who will take less joy in walking around city streets or visiting stores because they know they are being photographed by surveillance cameras everywhere they step.

- It is not about the searches, metal detectors, and inquisitions that have become a routine part of our daily lives at airports. It is about a society that views law-abiding citizens as

potential terrorists, yet does little to effectively protect its citizens from the real threats to their safety.

Today, more than ever before, we are witnessing the daily erosion of personal privacy and freedom. We are victims of a war on privacy that is being waged by government eavesdroppers, business marketers, and nosy neighbours.

Today's war on privacy is intimately related to the dramatic advances in technology that we've seen in recent years. Video cameras observe personal moments. Computers store personal facts. Communications networks make personal information widely available throughout the world. Although some special technology may be used to protect personal information and autonomy, the overwhelming tendency of advanced technology is to do the reverse.

Privacy is fundamentally about the power of the individual. In many ways, the story of technology's attack on privacy is really the story of how institutions and the people who run them use technology to gain control over the human spirit, for good and ill. That is because technology by itself does not violate our privacy or anything else, it is the people using this technology and the policies they carry out that create violations.

Many people today say that in order to enjoy the benefits of modern society, we must necessarily relinquish some degree of privacy. If we want the convenience of paying for a meal by credit card, then we must accept the routine collection of our purchases in a large database over which we have no control.

Privacy-invasive technology does not exist in a vacuum. That is because technology itself exists at a junction between science, the market, and society. People create technology to fill specific needs, real or otherwise. And technology is regulated, as people and society deem fit.

Few engineers set out to build systems designed to crush privacy and autonomy, and few businesses or consumers would willingly use or purchase these systems if they understood the consequences. What happens more often is that the privacy implications of a new technology go unnoticed. Or if the privacy implications are considered, they are misunderstood. Or if they are understood correctly, errors are made in implementation. In practice, just a few mistakes can turn a system designed to protect personal information into one that destroys our secrets.

16.6 COOKIES AND PRIVACY

The Word Wide Web is built on a very simple but powerful premise. All material on the Web is formatted in a general, uniform format called HTML (Hypertext Markup Language), and all

information requests and responses conform to a similar standard protocol. When someone accesses a server on the Web, such as the Railway Reservation System, the user's Web browser will send an information request to the Railway Reservation System computer. The Web server will respond to the request by transmitting the desired information to the user's computer. There, the user's browser will display the received information on the user's screen.

Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information. For example, cookies are used to personalize Web search engines, to allow users to participate in WWW-wide contests, and to store shopping lists of items a user has selected while browsing through a virtual shopping mall.

Essentially, cookies make use of user-specific information transmitted by the Web server onto the user's computer so that the information might be available for later access by itself or other servers. In most cases, not only does the storage of personal information into a cookie goes unnoticed, so does access to it. Web servers automatically gain access to relevant cookies whenever the user establishes a connection to them, usually in the form of Web requests.

Cookies are based on a two-stage process. First the cookie is stored in the user's computer without their consent or knowledge. For example, with customizable Web search engines like My Yahoo!, a user selects categories of interest from the Web page. The Web server then creates a specific cookie, which is essentially a tagged string of text containing the user's preferences, and it transmits this cookie to the user's computer. The user's Web browser, if cookie-savvy, receives the cookie and stores it in a special file called a cookie list. This happens without any notification or user consent. As a result, personal information (in this case the user's category preferences) is formatted by the Web server, transmitted, and saved by the user's computer.

During the second stage, the cookie is clandestinely and automatically transferred from the user's machine to a Web server. Whenever a user directs her Web browser to display a certain Web page from the server, the browser will, without the user's knowledge, transmit the cookie containing personal information to the Web server.

Internet cookies are incredibly simple, but they are one of those things that have taken on a life of their own. Cookies started receiving tremendous media attention starting in February 2000 because of Internet privacy concerns, and the debate still rages.

On the other hand, cookies provide capabilities that make the Web much easier to navigate. The designers of almost every major site use them because they provide a better user experience and make it much easier to gather accurate information about the site's visitors.

A cookie is a piece of text that a Web server can store on a user's hard disk. Cookies allow a website to store information on a user's machine and later retrieve it. The pieces of information are stored as name-value pairs. For example, a website might generate a unique ID number for each visitor, and store the ID number on each user's machine using a cookie file.

If you use Microsoft's Internet Explorer to browse the Web, you can see all of the cookies that are stored on your machine. The most common place for them to reside is in a directory called c:\windows\cookies. When I look in that directory on my machine, I find 82 files. Each file is a text file that contains name-value pairs, and there is one file for each website that has placed cookies on my machine.

Amazon.com stores a bit more information on my machine. When I look at the cookie file Amazon has created on my machine, it contains the following:

- session-id-time 921242000 amazon.com/
- session-id 002-4135256-7625823 amazon.com/
- x-main eKQIfwnxuF7qtmX52x6VWAXh@Ih6Uo5H amazon.com/
- ubid-main 077-9263437-9645312 amazon.com/

It appears that Amazon stores a main user ID, an ID for each session, and the time the session started on my machine (as well as an x-main value, which could be anything).

The vast majority of sites store just one piece of information—a user ID—on your machine. But there really is no limit—a site can store as many name-value pairs as it likes.

A name-value pair is simply a named piece of data. It is not a program, and it cannot "do" anything. A website can retrieve only the information that it has placed on your machine. It cannot retrieve information from other cookie files, nor any other information from your machine.

16.7 Internet Threats

Phishng

Computer criminals used a relatively new method—phishing, which is becoming more and more popular amongst hackers. Recently many banks all over the world encountered a variety of frauds and scams committed by hackers, swindlers, and inside bank officials. But the most widespread crime against banks and especially accounts' owners is a so-called 'phishing scam'. This scam is always entailed by usual spam. Swindlers try to trick consumers into giving up credit card information by posing as mail from regulations.gov, the government website where citizens comment on federal rule-making.

The phishing e-mails typically have subject headings of 'Official information' or 'Urgent information to all credit card holders!' and claim that recent changes in the law require that Internet users identify themselves to the federal government to create a secure and safer Internet community.'

Like other phishing scams, the e-mail includes a link to a bogus website, which in this case closely resembles regulations.gov. Once there, users are asked to enter private and personal financial information, including credit card numbers.

Phishing expeditions can be a financial windfall for attackers, since some analysts' estimates put the success rate of such bogus e-mails at about 1 in every 20 recipients.

The most recent major outbreak of phishing attacks was between the summer of 2003 and January 2004, when Mimail and a host of copycats tried to trick users into giving up credit card information by masquerading as messages from PayPal, eBay, and other major companies and banks.

Application Fraud

Application fraud is one specific version of what is broadly referred to as "identity theft." As the name implies, it essentially involves a criminal using someone else's name and credentials to fill out a credit card application without their permission. Often, the thief sets the stage for application fraud by stealing supporting documents from the victim, such as utility bills or bank statements, which are then used to substantiate the thief's fraudulent credit card application. If and when they are approved for a card in the victim's name, thieves face few restraints in the damage they are capable of inflicting. FICO scores and payment histories can be ruined in a heartbeat by determined thieves in possession of a fraudulently granted credit card.

Skimming

An electronic method of capturing a victim's personal information used by identity thieves. The skimmer is a small device that scans a credit card and stores the information contained in the magnetic strip. Skimming can take place during a legitimate transaction at a business.

Skimming can occur easily in a restaurant because your card is taken away when the bill is being settled. If your server is a skimming identity thief, he or she will, before giving the card back to you, scan the credit card with a hand-held electronic device, which takes only seconds. The electronically captured information is then used by the thief or sold to other criminals.

ATM skimming is the practice of adding concealed technology to ATMs to capture bank account numbers, usernames and passwords. The point is to hijack bank accounts and clean them out before the customer is even aware of a problem.

ATM skimming has existed for years on a small scale. Skimmers attack both retail points-of-sale (POS) and ATMs, both bank-owned and non-bank. As the graphic below shows, the focus of these criminals has shifted recently. Notice that in the beginning in 2004, these criminals were working hard on POS fraud. Late in 2009, however, their focus began to shift to ATM machines and specifically bank-owned ATMs. According to Wall Street Journal, 80% of the credit card fraud during the first half of 2010 occurred on bank-owned ATMs.

Copyright

In general terms, copyright provides an author with a tool to protect a work from being taken, used, and exploited by others without permission. The owner of a copyrighted work has the exclusive right to reproduce it, prepare derivative works based upon it, distribute copies by sale or other transfer of ownership, to perform and display it publicly, and to authorize others to do so.

For a company that depends upon intellectual property for its livelihood, such as a software company or an Internet-based publisher, copyright law provides a framework that ensures that the company can compete in the marketplace. The importance of copyright is illustrated by comparing what happens to an appliance company when a refrigerator is stolen with what happens to a software company when its source code is stolen. The refrigerator company will simply have one less item of merchandise to sell and a loss reflected by the refrigerator's price. The software company, however, will suddenly be faced with the prospect of a market flooded with exact copies of its product—sold or given away by another. Without the ability to prevent

unauthorized copying, sale, and distribution of its product, the software company will not be able to survive.

Copyright law protects "original works of authorship". Sheer hard work alone will not suffice—a modicum of creativity is required. The work does not have to be the first of its kind, or novel—it just has to be the independent product of the author, not copied from another source. Copyright, in fact, does not protect against independent creation of similar or identical works.

Certain items are excluded from copyright protection. Registering a work with the Copyright Office is a critical step to be taken in protecting a work under copyright law. While time and money costs are involved, significant benefits are gained by completing the registration process in a timely manner. To protect a work from the date of first publication, it must be registered within three months of that time. The work may be registered by the owner or an exclusive licensee. There is a "mandatory" deposit requirement, but it is not a condition of copyright protection.

A copyright is infringed when one of the exclusive rights of the copyright holder is violated. These include the right to reproduce a copyrighted work, prepare derivative works based upon it, distribute copies by sale or other transfer of ownership, to perform and display it publicly, and to authorize others to do so.

Internet Gambling

The Internet and other emerging technologies, such as interactive television, have made possible certain types of gambling that were not feasible a few years ago. For example, an Indian citizen can now, from his home at any hour of the day or night, participate in an interactive Internet poker game operated by a computer located in the Caribbean. Indeed, a tech-savvy gambler can route his bets through computers located in other countries throughout the world, thereby obscuring the fact that he is placing his bet from India.

Online gambling also makes it far more difficult to prevent minors from gambling. Gambling websites cannot look at their customers to assess their age and request photo identification as is possible in traditional physical casinos and off-track-betting parlours. Currently, Internet gambling businesses have no reliable way of confirming that the gamblers are not minors who have gained access to a credit card and are gambling on their website. Although some companies are developing software to try to detect whether a player is old enough to gamble or whether that

player is from a legal jurisdiction, such software has not been perfected and would, of course, be subject to the same types of flaws and vulnerabilities that could be exploited by hackers.

Threats to Children

With the growing number of classrooms connected to the Internet and the rising number of personal computers used in the home, more and more children are now able to access the Internet. One of the greatest benefits of the Internet is that it provides children with access to such things as educational materials, subject matter experts, online friendships, and penpals. Nevertheless, like many other pursuits that children engage in without adequate parental supervision, the Internet should also be approached with careful consideration of risks and benefits. One concern of course is that the Internet may allow children unrestricted access to inappropriate materials. Such materials may contain sexually explicit images or descriptions, advocate hate or bigotry, contain graphic violence, or promote drug use or other illegal activities. In the worst instances, children have become victims of physical molestation and harassment by providing personal information about themselves over the Internet and making contact with strangers.

To protect children from such risks, parents and teachers therefore need to empower themselves with the tools, knowledge, and resources to supervise and guide children's online experience and to teach children how to use the Internet responsibly.

Technology provides tools that may assist in preventing children from accessing inappropriate materials on the Internet or divulging personal information about themselves or their families online. The most common technological tools are "blocking" and "filtering" software, as described in more detail below.

"Blocking" software uses a "bad site" list and prevents access to those sites. The vendor of the software identifies specified categories of words or phrases that are deemed inappropriate and configures the blocking software to block sites on which the prohibited language appears. Although some vendors allow parents to customize the "bad site" list by allowing them to add or remove sites, others keep the list secret and do not permit parents to modify it.

"Filtering" software blocks sites containing keywords, alone or in context with other keywords. For example, if parents wanted to restrict their child's access to sites related to drug use, the software would be configured to deny access to sites containing such words as "marijuana",

"cocaine", "heroin", etc. Filtering software is available both directly and through some Internet Service Providers (ISPs) such as Lycos or FamilyNet

16.8 THE SPECIAL NATURE OF COMPUTER ETHICS

Computer ethics is a special field of ethical research and application. Computer ethics has two parts:

    (i)   the analysis of the nature and social impact of computer technology and

    (ii)   the corresponding formulation and justification of policies for the ethical use of such technology.

We know that computing technology is being employed in a given situation, but we are puzzled how it should be used. There is a policy vacuum. For example, should a supervisor be allowed to read a subordinate's e-mail? Or should the government be allowed to censor information on the Internet? Initially, there may be no clear policies on such matters. They never arose before. There are policy vacuums in such situations. Sometimes it may be simply a matter of establishing some policy, but often one must analyze the situation further. Is e-mail in the workplace more like correspondence on company stationary in company files or more like private and personal phone conversations? Is the Internet more like a passive magazine or more like an active television? One often finds oneself in a conceptual muddle. The issues are not trivial matters of semantics. If someone's health status is discovered through e-mail or an impressionable child is exposed to distressing material on the Internet, the consequences may be very damaging. Obtaining a clear conception of the situation from which to formulate ethical policies is the logical first step in analysis, although chronologically one's uncertainty about the appropriate policy may precede and motivate the search for conceptual clarification. Given a tentative understanding of the situation, one can propose and evaluate possible policies for proper conduct. The evaluation of a policy will usually require a close examination and perhaps refinement of one's values. Such policy evaluation may lead one back for further conceptual clarification and then further policy formulation and evaluation. Eventually, some clear understanding and justifiable policy should emerge. Of course, with the discovery of new consequences and the application of new technology to the situation, the cycle of conceptual clarification and policy formulation and evaluation may have to be repeated on an ongoing basis.

Because computers are logically malleable, they will continue to be applied in unpredictable and novel ways, generating numerous policy vacuums for the foreseeable future. Moreover, because

computerized situations often become informationally enriched, we will continue to find ourselves in conceptual muddles about how precisely to understand these situations. This is not to say that we cannot achieve conceptual clarity and that we can't formulate to justify reasonable policies. Rather, it is to point out that the task of computer ethics is, if not Sisyphean, at least ongoing and formidable. No other field of ethics has these features to the degree that computer ethics does. Computer ethics is not simply ethics rotely applied to computing. Typically, problems in computer ethics require more than straightforward application of ethical principles to situations. Considerable interpretation is required before appropriate policies can be formulated and justified. Of course, to say that computer ethics is a special field of ethics does not mean that every ethical problem involving computers is unique or difficult to understand. Stealing a computer may be a simple case of theft. A straightforward application of an ethical principle is appropriate. In such a situation, there are no policy vacuums and no conceptual muddles. What is special about computer ethics is that it has a continually large number of evolving situations which are difficult to conceptualize clearly and for which it is hard to find justified ethical policies. Doing computer ethics is not impossible, but doing it typically involves much more than rote application of existing norms.

The Three Ethically Significant Characteristics of the Internet

Internet is a medium of communication and as such it has three special features:

1. Many-to-many communication on a global scale
2. It facilitates a certain kind of anonymity
3. Certain programs on the internet have the ability to replicate themselves.

The many-to-many communication on a global scale can be mis-used as a source of diabolic power to disrupt computer functioning by unleashing a computer virus. And as in the case of Melissa virus, it can cause huge losses for many organizations. The Internet has created a new kind of environment in which individuals who want to wreak havoc can do so with relatively little effort.

The widespread desire to be wired should make us reflect on what awaits us as the computer revolution explodes around the world. The digital genie is out of the bottle on worldwide scale. The prospect of a global village in which everyone on the planet is connected to everyone else with regard to computing power and communication, is breathtaking. What is difficult to comprehend is what impact this will have on human life. Surely some of the effects will be quite

positive and others quite negative. The question is to what extent can we bring ethics to bear on the computer revolution in order to guide us to a better world or at least prevent us from falling into a worse world. Although almost everyone would agree that computing is having a significant impact on the world, and that ethical issues about applications of this surging technology should be raised, there is disagreement about the nature of computer ethics.

16.9 CHECK YOUR PROGRESS

16. Define Ethics.

17. What is hacking?

18. Define cyberstalking.

19. What are cookies?

20. What is ATM skimming?

Answers to Check your progress

1. Ethics refers to the principles of right and wrong that can be used by individuals acting as free moral agents to make choices to guide their behaviour.

2. A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals.

3. Cyberstalking generally refers to the use of the Internet, e-mail, or other electronic communications devices to "stalk" another person—where "stalking" in the traditional sense means to engage in repeated harassing or threatening behaviour (such as following a person, appearing at a person's home or workplace, making harassing telephone calls, or leaving written messages or objects) that places the victim in reasonable fear of death or bodily injury.

4. Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information.

5. ATM skimming is the practice of adding concealed technology to ATMs to capture bank account numbers, usernames and passwords. The point is to hijack bank accounts and clean them out before the customer is even aware of a problem.

16.10 SUMMARY

This unit elaborates on ethical issues in the Digital Economy. Five moral dimensions of the information age are discussed. How computers are utilized for performing a crime are highlighted. Awareness is given on cyber stalking and internet cookies. Also major internet threats are discussed in detail.

16.11 KEYWORDS

- **Digital economy** is the economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes.
- **Cybercrime** is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them.
- **Privacy-invasive software** is a computer software that ignores users' privacy and is distributed with a specific intent, often of a commercial nature. Three typical examples of privacy-invasive software are adware, spyware and browser hijacking programs.
- **Web-based threats**, or *online threats*, are a category of cybersecurity risks that may cause an undesirable event or action via the internet.

16.12 QUESTIONS FOR SELF STUDY

1. Discuss about ethical issues in the Digital Economy.
2. Elaborate on five moral dimensions of the information age.
3. How computers are utilized for performing a crime? Explain.
4. Write a note on cyber stalking.
5. What are internet cookies? Explain.
6. Explain major internet threats in detail.

16.13 REFERENCES

1. Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2017 Business*. Pearson, 2020.
2. Joseph, P. T. (2019). *E-commerce: An Indian perspective*. PHI Learning Pvt. Ltd..