ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା

Odisha State Open University, Sambalpur, Odisha

Established by an Act of Government of Odisha.

Certificate in E-Commerce

CEC

CEC-1

Future Issues and Implications

Block

3

Unit-1 : Privacy & confidentially, Security, Redressal, Integration of the existing systems

Unit-2 : Human resource availability & development; Security of networks, Management of change

Unit -1 Privacy & confidentially, Security, Redressal, Integration of the existing systems

Learning objectives

After reading this unit you will

- Understand what is Security, types and threats to E-Commerce.
- To discuss the Precautionary Security Steps For E-Commerce.
- what are the concept of Confidentiality, Accuracy, Privacy And Availability

Structure

1.1 INTRODUCTION

Electronic Commerce is the most rapid growing sector in today’s time. It is used for Purchasing Order i.e. for buying and selling online goods and all other type of things. And there is need for development of a number of ecommerce protocols, which ensure integrity, confidentiality, atomicity and fair exchange.

Further, When doing business online is electronic commerce and there are four main areas in which companies conduct business online today: direct marketing, selling and service, online banking and billing, secure distribution of information and value chain trading and corporate purchasing

Privacy is a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for E-Commerce providers. E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business.

Transmission of data using network and communication link has necessitated the need to protect the data during transmission over the network. The term computer security to refer to both the computer security and network security.

- Computer security focuses on the security attacks, security mechanisms, and security services.
- Security attacks are the reasons for breach of security. It compromise of all actions that breaches the computer security.
- Security mechanisms are the tools that include the algorithms, protocols that are designed to detect, prevent or recover from a security attack.
- Security services are the services that are provided by a system for a specific kind of protection to the system resources.

1.2 MEANING OF SECURITY IN E-COMMERCE

Several security measures are available in recent times to protect confidential data and most useful data such as passwords, encryption, firewalls and virus protection. The two types of security system can be as follows:

(A) **Access Security-**It is the security to be provided to prevent an unauthorized user to access your computer or computing resources and ensuring that the computers are available to authorized users only;

(B) **Transaction Security-** It consists of services such as privacy, authenticity and message integrity in the transactions over the internet.

1.3 TYPES OF THREATS IN E-COMMERCE

Passive Threats: Such threats are in the nature of monitoring of the transmission of the organization. It includes:

(I) Release of message contents by way of telephonic conversation. E-mail that may contain sensitive information;

(II) Traffic analysis which means reading packet headers to determine the location and identity of communicating hosts.

Active Threats-It is the unauthorized use of device attached to a communication facility to alter transmitting data or control signals. It includes modification of the message stream, message service denial and masquerades. The various security threat problems are:

- Hacking
- Viruses
- Brand hijacking
- Spoofing
- Data alteration and unauthorized disclosure

Table : Cyber crimes in India during 2015

Sl.	**Types**	**Number**
1.	Phishing	534
2.	Network scanning / Probing	3673
3.	Virus / Malicious Code	9830
4.	Website Defacement	26244
5.	Website intrusion and Malware Propagation	961
6.	Others	8213
	Total	49455

Source: Ministry of Communication and IT

There are some common problems occur due to the virus attacks which are given bellow;

1. Computer speed or performance has slowed.

2. Computer system freezes and blue screens of death.

3. The computer keeps on rebooting again and again.

4. An entire disk or drive is erased.

5. Cause erratic screen behavior.

6. Unexplained messages appear on the screen.

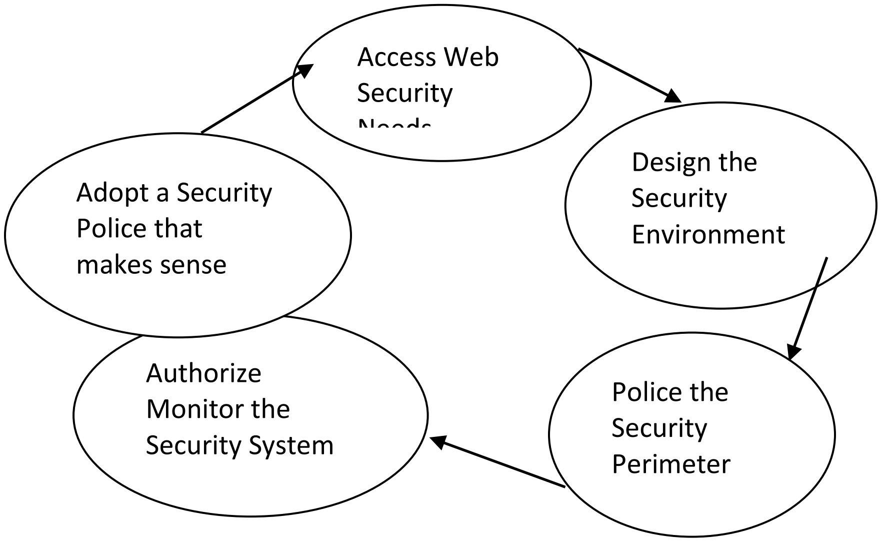
7. The browser home page changed itself.

8. Application software seems to be changed.

9. Operating system software appears to be modified.

10. Unexplained printing problems occur.

The Security System Design Process


Access Web Security Needs
Design the Security Environment
Police the Security Perimeter
Authorize Monitor the Security System
Adopt a Security Police that makes sense

A publication of the National Bureau of Standards identified some of the threats that have stimulated the upsurge of interest in security:

- Organised way and intentional attempts to obtain economic or market oriented information from competitive sector.
- Organised and intentional attempts to getting economic information from government organizations.
- Inadvertent acquisition of economic or market information.

- Inadvertent acquisition of information about individuals.
- International fraud through illegal access to computer data banks with emphasis, in decreasing order of importance, on acquisition of founding data, economic data, law enforcement data and data about individuals.
- Government intrusion on the rights of individuals.
- Invasion of individual rights by the intelligence community.

LIFE CYCLE OF COMPUTER VIRUS

Stage I **-** Creation – The Computer viruses are created by misguided individuals who wish to cause widespread, random damage to computers.

Stage II **-**Replication **-** Computer Viruses replicate by nature means it copies itself from one PC to anther PC.

Stage III **-**Activation **-** Viruses that have damage routines will activate when certain conditions are met. Viruses without damage routines don't activate, instead causing damage by stealing storage space.

Stage IV **-**Discovery **-** This phase doesn't always come after activation, but it usually does. Discovery normally takes place at least a year before the virus might have become a threat to the computing community.

Stages V **-**Assimilation **-** At this point, antivirus developers modify their software so that it can detect the new virus. This can take anywhere from one day to six months, depending on the developer and the virus type.

Stage VI **-**Eradication **-** If enough users install up-to-date virus protection software, any virus can be wiped out. So far no viruses have disappeared completely, but some have long ceased to be a major threat

1.4 THREATS TO E-COMMERCE TRANSACTIONS

E-commerce transactions face the following threats. E-commerce and mobile-app based service provides such as Amazon, Flipkart, Snapdeal, Paytm and Ola are increasingly roping in ethical hackers to lack for loop holes in their system by continuously trying to hack into them from outside.

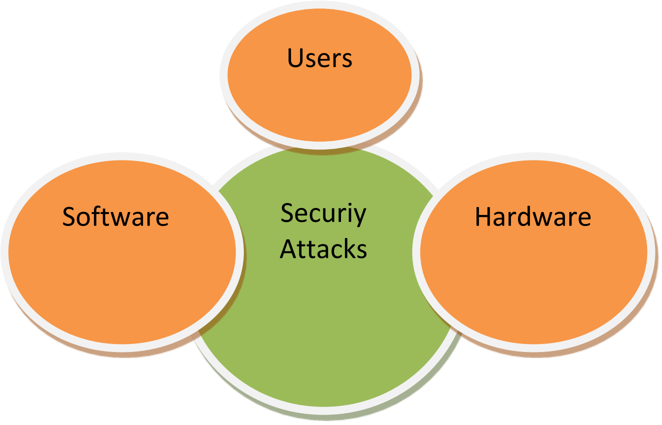
Hacking: Hacking refers to breaking security to gain access to a system. It also refers to unauthorized entry into a website. The confidential information and misuse such information to their use/advantage or modify and even destroy its contents to harm the parties. Hacking can be divided into different categories elaborated below:

1. Trojan programs that share files via instant messenger.

2. Phishing
3. Fake Websites.
4. Spoofing
5. Spyware
6. Electronic Bulletin Boards
7. Information Brokers
8. Internet Public Records
9. Trojan Horses
10. Wormhole Attack

- **Cyber Squatting**: In order to take advantage of some established brand name or trade mark, a firm might use the name/mark for its own website while getting the domain name (name of the website) registered. This is done so as to induce a customer to believe that there is a direct link between the website holder and the trade mark. Such a practice is known as cyber squatting.
- **Viruses**: Viruses causes harm to the efficient and smooth functioning of e-commerce. Some viruses are destroying all the information stored in a computer or system. It causes a huge loss of revenue and time. Viruses may enter a computer system through e-mail or disc drive floppies.
- **Typo piracy**: Some websites try to take advantage of common typographical errors that the users might make in typing a website address to direct users to a different website. Such people who try to take advantage of some popular websites to generate accidental traffic for their websites are called typo pirates and such a practice is referred to as typo piracy. For instance, if a user instead of typing rediff.com in the address bar of Internet Explorer, types by mistake ridif.com or redif.com, then he will find that a different webpage with altogether a different name might open. Impersonation: In e-commerce transactions, sometimes hackers may pretend to be consumers themselves. They, thus, make use of stolen credit card numbers of real customers.

- **Fraudulent Trading**: A business enterprise operating a website might indulge in fraudulent practices. It may operate a fake website, take away money from customers and not supply the good or service to the customer.



1.5 DISPUTES REGRADING E-COMMERCE TRANSACTIONS

Different kinds of disputes may arise regarding e-commerce transactions.

- The customer pays for the merchandise but the business fails to deliver.
- The customer pays in full, but receives a partial order or the wrong or damaged merchandise.
- The customer does not like the product but the business has no procedure for accepting returned merchandise.
- The business delivers but the customer does not admit that he ever received the merchandise.
- The customer receives the merchandise, but it arrives damaged. The carrier (Courier Company) denies responsibility and the business says it is carrier's responsibility. For example COD (Cash on Delivery) is a major pain point for online market place, as the percentage of return is higher. However, the newly launched Snapdeal Gold service is to bring down the Cash on Delivery component to 50 percent.

1.6 SECURITY MECHANISMS ON THE INTERNET

It deals with prevention, detection and recovery from a security attack. Prevention involves mechanisms to prevent the computer from being damaged. Detection requires mechanisms that allow detection of when, how and by whom an attacked occurred. Recovery involves mechanism to stop the attack, assess the damage done and then repair the damage. Moreover, E-commerce server also needs protection through security of transaction information, correctness and completeness, confidentiality and availability of the database. Controls can be set upon to protect e-commerce channels by way of privacy and integrity of the transaction information by using techniques such as digital signatures, encryption, cryptography, firewall, user identification and authentication etc.

i. **Digital Signature**

Digital signature means the authentication of any electronics record by a subscriber by means of an electronic method. It is an electronic signature that can be used to:

- Authenticate the identity of the sender of a message or the signature of a document.
- To ensure for the original content of the message or document/data that has been sent is unchanged or unaltered..
- To ensure non-denial by the sender. Which becomes committed to the contents of the document and the intentions expressed therein.

ii. **Cryptography**

Cryptography is an art of protecting information by transforming it into an unreadable format, called cipher text. Only those who possess a secret key can decrypt the message into plain text. The types are as follows:

- **Secret Key (Symmetric) -** With secret key, the same key is used to encrypt information and decrypt information.
- **Public/Private Key (Asymmetric) -** Private key means the key of a key pair used to create a digital signature. Public key means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

iii. **Security Protocols**

- ❖ **Secure Socket Layer (SSL) -** It is a key protocol for securing web transactions, data packets in the internet. It provides server and client authentication and an encrypted SSL connection. It uses public key cryptography and system for validating public key and digital certificate of the server.
- ❖ **Secure Hyper Text Transfer Protocol (S-HTTP) -** S-HTTP secures web transaction. It is secure http. It secures transaction confidentiality, integrity and non-repudiation of the information

on the internet. S-http can be used along with SSL to increase protection.

- **Secure Electronic Transaction (SET)** - This protocol provides confidentiality through encryption, authentication of consumer and merchant identities and message integrity. The main features of this protocol are as follows:
  - ✓ Customer credit card not revealed to a merchant
  - ✓ Only credit card number and total amount revealed to the acquirer and not purchase invoice details.
  - ✓ Digitally signed purchase invoice coupled with the credit card number.

The basic goals of SET transaction are as follows:

- Confidentiality
- Integrity
- Secrecy
- Public Key Cryptography
- Merchant authentication
- Validating Digital signatures
- Interoperability

(IV) Firewalls

Firewalls are hardware and software combinations that are built using routers, servers and a variety of software. Firewalls regulate the activities between networks within the same organization. The benefits of firewall are:

- Strictly controlled access to host.
- Protection from services which are more prone to attacks.
- Maintain the statistics of network use and misuse.
- Preventing unsecured access to an internal network.

It must ensure

- **Data Integrity:** That no one can change data from outside.
- **Authentication:** which guarantees that senders are who they claim to be and
- **Confidentiality:** the sensitive data or messages are masked from intruding eyes.

Functions of Firewall- The main purpose of firewall is to protect computers of an organization from unauthorized access. Some of the basic functions of firewall are:

- Firewalls provide security by examining the incoming data packets and allowing them to enter the local network.
- Firewalls provide user authentication by verifying the username and password. This ensures the only authorized users have access to the local network.
- Firewalls can be used for hiding the structure and contents of a local network from external users.

Working of Firewall- The working of firewall is based on a filtering mechanism. The filtering mechanism keeps track of source address of data, destination address of data and contents of data. Firewall related terminology:

- **Gateway:** The computer that helps to establish a connection between two networks is called gateway. A firewall gateway is used for exchanging information between a local network and the internet.
- **Proxy Server:** A proxy server masks the local networks IP address with the proxy server IP address. Web proxy and application level gateway are some examples of proxy servers.
- **Screening Routers**: They are special type of router with filters, which are used along with the various firewalls. Screening routers check the incoming and outgoing traffic based on the IP address and ports.

Types of Firewall

The type of firewall used varies from network to network. The following are the various types of firewalls generally used:

- Packet filter Firewall
- Circuit filter Firewall
- Proxy server or Application-level gateway

Packet Filter Firewall-It is usually deployed on the routers. It is the simplest kind of mechanism used in firewall protection.

- It is implemented at the network level to check incoming and outgoing packets.
- Packet filter firewall does not provide a complete solution.
- It is fast, easy to use, simple and cost effective.

Circuit Filter Firewall- Circuit filter firewall provide more protection than packet filter firewalls. Circuit filter firewall is also known as a “stateful inspection” firewall.

- It protect transfer of suspected packets by checking them at the network layer.
- It checks for all the connections made to the local network.
- It takes its decision by checking all the packets that are passed through the network layer.

Application-Level Gateway- An application-level gateway protects all the client applications running on a local network from the internet by using the firewall itself as the gateway.

- A proxy server creates a virtual connection between the source and the destination hosts.
- A proxy server is easy to implement on a local network.
- It operates on the application layer.
- It tends to be more secure than packet filters.

Firewall Protects against the Following Situations

- E-mail services that are known to be problems.
- Unlimited interactive log-ins from the outside world.
- Undesirable material such as pornographic images, movies or literature.
- Unauthorized sensitive information leaving the company.

(V) Users Identification and Authentication

Identification is the process whereby a system recognizes a valid user’s identity. Authentication is the process of verifying the claimed identity of a user. For example, a system uses user –password for identification. The user enters his password for identification and authentication is the system which verifies that the password is correct, and the user is a valid user. Authentication mechanisms are described below:

- User name and password
- Smart card
- Biometrics-Fingerprints, retina scan

User name and Password

It is the most common method for user. Some actions that can be taken to make the passwords safer are as follows:

- It is good to change passwords periodically.
- Make a password complex like mix numbers, special characters.
- Use longer passwords, making them difficult to break.
- Be cautious not to leave passwords lying around and don’t share them with friends.
- Do not use your or your family’s name, address, age, city etc. as part of the passwords.

Smart Card

A smart card is in a pocket-sized card with embedded integrated circuits which can process data. It is made of plastic, generally PVC. The card may embed a hologram. Smart cards are used in secure identity applications like employee-ID badges, electronic passports, driving license and online authentication devices.

Biometric Techniques

Biometrics is the science and technology of measuring and statistically analyzing biological data. It can include finger prints, eye retinas and irises, voice patterns, fascial patterns and hand measurements. It is very costly and is used in environments requiring high level security.

1.7 PRECAUTIONARY SECURITY STEPS FOR E-COMMERCE

(a) To install proper firewalls for protection of data.
(b) To ensure that network is configured properly.
(c) To protect most sensitive data through encryption.
(d) To maintain and update all antivirus programs on different Terminal.
(e) To restrict access the files by “Need to Know”.
(f) To assign unique IDs to authorized personnel.
(g) To evaluate and track all IDs on a daily basis.
(h) To ensure that system administrator has contemporary security skills.
(i) To enforce and update company information and security policy.

1.8 SECURITY SERVICES

The security services provide specific kind of protection to system resources. Security services ensure Confidentiality, Integrity, Privacy and Non-Repudiation of data stored on the computer. It provides assurance for access control and availability of resources to its authorized users.

- **Confidentiality**: The confidentiality aspect specifies availability of information to only authorized users. It ensures that private and confidential information is not accessible to unauthorized persons. Information which is sensitive or confidential must remain so and is shared only with appropriate users. It requires ensuring the privacy of data stored on a server. Data encryption is used for ensuring confidentiality.
- **Privacy**: It ensures the information which have been collected and saved by people is accessible by them and who this information can be revealed to.
- **Integrity**: Information must retain its integrity and not be altered from its original state. It assures that the received data is exactly as sent by the sender, i.e. the data has not been modified, duplicated, reordered, inserted or deleted before reaching the intended recipient.
- **Availability**: It ensures that the system works quickly and does not exclude authorized users. Information and systems must be available to those who need it.
- **Non-repudiation**: Prevention against any one party from reneging on an agreement after the fact. It prevents either sender or receiver from denying a transmitted message. For example, if a sender places an order for a certain product to be purchased in a particular quantity, the receiver knows that it came from a specified sender. Non-repudiation deals with signatures.
- **Access Control-**It is the prevention of unauthorized use of a resource. This specifies the users who can have access to the resource, and what are the users permitted to do once access is allowed.

1.9 LET US SUM UP

Online Computer security threats are Virus Threats, Spyware Threats, Hackers, Phishing Threats, Adware and Trojans. The major attacks to network security are passive attack, active attack, distributed attack, insider attack, Phishing Attack, Hijack attack, Password attack etc. Privacy and data theft will be the top security issues that organizations need to focus. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting

Internet users) has become integral to the development of new services as well as governmental policy

1.10 KEY TERMS

- ✓ **Monitoring:** It means capturing processing details, verifying that e-commerce is operating within the security policy and verifying that attacks have been unsuccessful.
- ✓ **Denial of Service (DoS):** It is attack by a third party that prevents authorized users from accessing the infrastructure.
- ✓ **Virus:** It is a malicious code that replicates itself and disrupts the information infrastructure.
- ✓ **Spyware:** It is software that the user unknowingly installs through an e-mail attachment or downloading an infected file that could be used for illicit reasons.
- ✓ **Adware:** Software that sneaks into a user's hard disk installed by Internet Advertising Companies to promote Pop-up ads and release information for advertisers on the outside.
- ✓ **Encryption:** It is the coding of messages in traffic between computers.
- ✓ **Cyberwalls:** It is all-in-one software package to improve security for the entire private network of an organization.
- ✓ **Server:** It is the destination point on internet.
- ✓ **Browser:** It is a software program loaded on a PC that allows you to access or read information stored on the internet.
- ✓ **Malware:** It is a software code included into the system with a purpose to harm the system.
- ✓ **Integrity:** It assures that the received data is exactly as sent by the sender.
- ✓ **Key:** It is a secret parameter for a specific message exchange context.
- ✓ **Encryption:** It is the process of converting plain text to cipher text.
- ✓ **Security attacks:** The intruder comes to know of the open lock and gets inside the house known as security attack.
- ✓ **Firewall:** A firewall protects a local network from the threats.
- ✓ **Smart card:** A smart card is a pocket sized card with strong security authentication for single sign-on.

1.11 SELF ASSESSMENT QUESTIONS

1. Define Passive attack and active attack.
2. Define cryptography?
3. List the Functions of firewall.

1.12 FURHER READINGS

I. Kalakota, Ravi. & Whinston, Andrew B. (2011) Frontiers of Electronic Commerce,Pearson Education, 12th Edition.

II. Pradhan, Bubhuti B. & Dash, Manoranjan.(2010)E-Commerce for the Digital age, Virnda Publications, New Delhi, First Edition.

III. Westland, Christopher J. & Clark, Theodre H K.(2001) Global Economic Commerce: Theory and case studies, Orient Longman.

IV. Jaiswal, S. (2006) E-commerce, Galgotia Publishers, New Delhi.

V. Laudon, C. Kenneth and Traver, Guercio Carol.(2003) E-commerce, Pearson Education, First Indian Reprint.

VI. Chabra, T.N., Suri, R.K and Etal. (2004) E-Commerce: New Vistas for Business, Dhanpat Rai and Co.

VII. Murty, C.s.V. (2011) E-commerce: concepts, Models and strategic, Himalaya Publishing company, New Delhi.

VIII. Chan, Henry, Lee, Raymond, Dillon, Tharam, Chang, Elizabeth.(2004) E-commerce: fundamentals and applications, John Wiley sons Edition.

IX. Laudon, Kenneth C. & Laudon, Jane P., International Edition, Management Information Systems, Organization and Technology in the Networked Enterprise, Prentice Hall, 2000, ISBN: 0-13-015682-5, page 25.

X. Mahapatra,D.M. and Mohanty,A.K. and etal.(2015)" Digital India: A study of New-Age E-Entrepreneurship in India", Siddhant, Vol.15,No.2,April-June issue,pp.110-116.

1.13 MODEL QUESTIONS

1. What are the basics concepts of network security? What are some common network security vulnerabilities and threats?
2. What is the use of digital signature?
3. What are the precautionary security steps for e-commerce?
4. How does the different type of firewall work?

5. What are security attacks?

1.14 SELF ASSESSMENT QUESTIONS AND ANSWERS

1. **Define Passive attack and active attack.**

Ans: Computer security threats are Virus Threats, Spyware Threats, Hackers, Phishing Threats, Adware and Trojans. The major attacks to network security are passive attack, active attack, distributed attack, insider attack, Phishing Attack, Hijack attack, Password attack etc.

Passive attacks: Such threats are in the nature of monitoring of the transmission of the organization. It includes: (a) Release of message contents by way of telephonic conversation. E-mail that may contain sensitive information; and Traffic analysis which means reading packet headers to determine the location and identity of communicating hosts.

Active attacks-It is the unauthorized use of device attached to a communication facility to alter transmitting data or control signals. It includes modification of the message stream, message service denial and masquerades. The various security threat problems are: (a)Hacking (b)Viruses (c) Brand hijacking (d) Spoofing and Data alteration and unauthorized disclosure.

2. **Define cryptography?**

Ans: Cryptography is an art of protecting information by transforming it into an unreadable format, called cipher text. Only those who possess a secret key can decrypt the message into plain text. The types are as follows:

- **Secret Key (Symmetric) -** With secret key, the same key is used to encrypt information and decrypt information.
- **Public/Private Key (Asymmetric) -** Private key means the key of a key pair used to create a digital signature. Public key means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

3. **List the Functions of firewall?**

Ans: Functions of Firewall are as follows:

Firewalls are hardware and software combinations that are built using routers, servers and a variety of software. Firewalls regulate the activities between networks within the same organization. The type of firewall used varies from network to network. The following are the various types of firewalls generally used:

- Packet filter Firewall
- Circuit filter Firewall
- Proxy server or Application-level gateway

The main purpose of firewall is to protect computers of an organization from unauthorized access. Some of the basic functions of firewall are:

- Firewalls provide security by examining the incoming data packets and allowing them to enter the local network.
- Firewalls provide user authentication by verifying the username and password. This ensures the only authorized users have access to the local network.
- Firewalls can be used for hiding the structure and contents of a local network from external users.

Unit -2: Human resource availability & development; Security of networks, Management of change

Learning objectives

After reading this unit you will

1. To understand the development of human resource availability.
2. To Know the Human traits for E-commerce.
3. To discuss the strategy and barriers of management of change.

Structure

2.1 INTRODUCTION

Security, Privacy and trust are the components of electronic technologies. Ecommerce security is applied i.e. computer security, data security, integrity, availability and other wider realms of the framework of Information Security. Human resources are one of the most vital assets of an organization. It is the people who make other resources moving. The placement of right kind of people in right numbers, at the right place and right time is the basic function of Human Resources management. Human Resource Planning is to get the right number of employees with the right skills, experience, and competencies in the right jobs at the right time and at the minimum cost.

This Human Resource is a predominately part of an organization, which ensures for business production requirements with an efficient and effective manner. Too much employees are challenging due to the risk of high labour cost, downsizing, or layoffs. Further, if it is few employees is also difficult due to high overtime costs, the risk of unmet production requirements. Moreover, Technology can be used to support HR activity across the entire employment cycle from talent acquiring human resources [recruitment], to rewarding [performance management, pay and benefits], developing [training and development, career management], protecting [health and safety, employee relations], and to retaining human resources [retention strategies, work-life balance].

2.2 MEANING OF HUMAN RESOURCE(HR)

The role of HR has changed with the new of tools like LinkedIn, Facebook and Twitter leave aside the influence of globalisation, technology, and change in demography and human values. Thus, the human capital resources are managed is crucial to organization performance.

2.3 DEVELOPMENT OF HUMAN RESOURCE AVAILABILITY

1. Staffing: It enables companies to know current employees strength in order to predict for the future. The recruiting aspect there are number of websites for recruiting of employees in companies some of the popular and important web sites in India are listed below they are as follows:

- naukri.com
- jobsahead.com

- monsterindia.com
- careerindia.com
- placementindia.com
- jobsearch.rediff.com
- bestjobsindia.in
- jobzing.com
- cybermediadice.com
- Careerjet.co.in

But the main job titles in E-Commerce category are Project Manager, Team Leader, E-Commerce Development Manager, Systems Architect, ECommerce Specialist, Systems Administrator, System Analyst, Database Analyst, Database Developer, Database Administrator, System Engineer, Network Administrator, Security & Risk Consultant, E-Commerce Architect, Technical Support Manager.

2. **Training and Development**: Usually done to beef up employees capabilities to meet current business trends. This HR activity is enforced often after conducting performance appraisal. By this means, training and development might assist management to identify labor deficiencies, if any, in the company. India's online recruitment industry took shape in 1997. The growth of the services sector, following the launch of economic reforms in 1991, resulted in the creation of additional jobs. In this background, internet proved to be an efficient medium that allowed employers and job seekers to connect.
3. **Career Development**: Career development appears to be a crucial HR exercise which project into the future. This practice seems to endorse succession planning principles to guarantee the enterprises continual existence. Career development gives employees the chance to upgrade themselves for mutual benefit. This HR activity creates the platform to either add to the number of employees or lessen the size.
4. **Downsizings**: Management decision with respect to upcoming downsizing should be reported to officers to prevent any operations interruption.

2.4 HUMAN RESOURCE TRAITS FOR E-COMMERCE

1. The culture of E-commerce has been changed through transparent work..
2. Ability of Team player is to create the feeling of 'one team, one goal, one achievement'.
3. Understanding different companies and their talent landscapes.
4. Ability and experience and expertise for active participation in business decisions.
5. Ability to do the right communication with the right people at the right time in the right manner.
6. Continual improvement and optimization at recent times in all processes in the organization.
7. Adaptability and ability to mold as per evolving business situations.
8. Looking for talent hunt and it's ability.

2.5 MEANING OF MANAGEMENT OF CHANGE

E-business erais now predominately and strategically change traditional business models. Electronic Business, e-business is the execution by electronic means of interactive, inter-organizational processes. E-business represents a shift in business doctrine that is changing traditional organizational models, business processes, relationships and operational models that have been dominant for the past 20 years. E-business infrastructure includes hardware, software, telecommunication network, support services and human capital used in electronic business and commerce. Major features and value drivers of e-business infrastructure are: cost leadership, total customer service and emerging new business models. E-business models offered major organizational changes, from internal modes of process-based structures to external modes of partnership-alliance based organization structures.

2.6 NATURE OF MANAGEMENT OF CHANGE

Management of change the new sunrise induction of e-commerce systems. But the targeted levels of performance, productivity, profitability and efficiency in an organization. With the availability of human resource , flexibility, or productivity, but also improving their knowledge, managing their natural resistance to change, and helping to convert that resistance into commitment. Employees should be educated to use new information technology. Progressive organizations should be built on the potential of their skilled employees.

- With careful strategy as the part of management which is faced with the challenge of managing complex and dynamic process of change.
- Individuals in organizations resist change because of perceived loss of power, threat to skills, end of monopoly of knowledge or power, loss of opportunity, loss of security, status loss, etc. This can be traced to a mental model which has not changed with time.
- The change strategy has to focus on altering the mind model which has become frozen because of lack of insight.
- With change of behavioral science that issues at world relate to human psychology.

2.7 STRATEGY OF MANAGEMENT CHANGE

Technological, economic, and societal factors have contributed to create the modern net centric organization. The technical capabilities of the Internet, combined with intranets and extranets, enable new ways to communicate and exchange information at any time, in any place, in a variety of ways.

Some of the change management strategies are as follows:

1. **Education, skill and Communication-** This method which is time consuming is often used when lack of information is the perceived cause of resistance.
2. **Participation, Involvement and Enrichment-** The entire department or unit of an organization is enrolled. More empowerment to the people. It is however time consuming and risky.
3. **Facilitation and Support services -** This approach is recommended when an organization suffers from morale decline. It deals with adjustment problems and is expensive.
4. **Manipulation and reaction-** This method is used to manage when time is of the essence. It can, however, result in staff reaction.
5. **Explicit Coercion-** If the change agent has the power, and time is of the essence, this method works. But one has to be wary of long term consequences.

2.8 BARRIERS TO MANAGEMENT OF CHANGE

Change methods may be crafted around ‘indirection’ and change packaged as natural evolution rather than revolution. Crisis can elevate change acceptance from a state of extreme doubt and resistance to a state of new beliefs. A state of belief in the new order is the prerequisite for change. Change Management has to overcome the following three classes of barriers:

1. **General-** related to organization's history, culture, style etc.
2. **Role-** specific incumbent positions create trouble.
3. **Individual-** specific individual objections.

The change management is a result of induction of IT tools and BPR, the compounded barrier compromises of both these:

- Technology revolution is obsolescing the competencies of it staff. They resist new technologies.
- Embedded behavioral system in an organization. They resist change in status quo.

2.9 CHANGE MANAGEMENT IN GOVERNMENT

Change management strategy for re-engineered processes in government has to keep in view the following characteristics of public administration.

- Bureaucratic structure level with over commitment to rules, regulations and precedents. Monopoly service provided by bureaucratic setup.
- Budget allocations and disbursement are not based on results and performance of department. Hence, pressure to perform does not work
- Salaries and incentives of employees not related to their performance. Seniority, and no merit, which determines promotion and recognition. Effective reward and punishment system absent in all times.
- Political interference in working of departments. Top officials are not free to effect change. Hence, no motivation to change.
- The changes also called for company/organizations and human resource arrangements is to bring about radical change/improvements in recent time, customer satisfaction, service quality are extremely difficult.
- The re-planning, concurrent re-design and implementation of administrative processes and organizational structure are essential to improve.

2.10 METHODS OF IMPLEMENTATION PLAN OF MANAGEMNT OF CHANGE

Some of the methods are as follows:

- Top level management should be fully committed to change.
- Create a technical plan for e-commerce for the organization.

- Small segment of work, such as invoices dealing with a specific product related to a particular group, for a pilot project.
- Identify key players in the organization.
- Develop the software and workflow based on their perception.
- Identify customers/users for this pilot who would use the e-commerce/EDI technology to interact with the organization.
- Implement the pilot.
- Feedback is essential and take it seriously to modify procedures.
- Induct people who are neutral to change. Thus, build their confidence level.
- Provide instant help to employees as in case of need.
- Expand the pilot by including another large group of products or services.

2.11 MEANING OF NETWORK SECURITY

A network security can be defined as the protection of network resources against:

- Unauthorized disclosure.
- Modification.
- Utilization.
- Restriction or Destruction.

SECURITY ASPECTS:

- ✓ **Confidentiality**: An attack causes a confidentiality breach if it allows unauthorized access to data.
- ✓ **Integrity**: An attack causes an integrity breach if it allows unauthorized modification to the system state or data.
- ✓ **Availability**: An attack causes an availability breach if it keeps authorized users from accessing a particular system resource when they need it.
- ✓ **Control**: An attack grants an attacker privilege to interfere with system operation in violation of the access control policy of the system. This can lead to subsequent confidentiality integrity, availability breach.

2.12 CHARACTERISTICS OF NETWORK SECURITY

Allowing access to your hosts only for the users that you intended is the goal of security in a TCP/IP network. Network must be secured from:

- Tampering with physical media.
- Inoperability of network devices.
- Disturbing routing protocol information.
- Cracking passwords.
- Changing or modifying information.

2.13 TYPES OF NETWORK SECURITY

There are two types of network security which is described as below:

- **Client Server Network Security**
  It includes all methods and authorization to make sure that only valid user can access the information. It is related with the physical and software security problems.
- **Data and Transmission Security-** It means the security of the data and security during transmission of data. It is needed to prevent changes in messages while transmission. On internet it is provided by the firewall.

E-Commerce Security Tools

- Firewalls :both Software and Hardware
- Public Key infrastructure
- Encryption software
- Digital certificates
- Digital Signatures
- Biometrics such as retinal scan, fingerprints, voice etc
- Passwords
- Locks and bars such as network operations centers

2.14 NETWORK SECURITY MEASURES

Several security techniques are used for security purposes. Some of these are listed below:

- **Intrusion Detection Systems-**A network based intrusion detection monitors real time network traffic for malicious activity and sends alarms for network traffic that meets certain attack patterns or signatures.

- **Virus Protection Software-** It should be installed on all network servers. These screen in all software coming into network system preventing a virus from entering into the system.
- **Data and Information Backups-**It is required for disaster recovery and business continuity. Further, the back-ups should be taken daily and periodically.
- **IP Security Protocol-** The IP Security protocol suite is used to provide privacy and authentication services at the internet layer. It can be used to protect any application traffic across the internet.

A network security problem can be divided into four areas:

- Secrecy (to prevent information from unauthorized users)
- Authentication
- Non-repudiation

Integrity control

2.15 NETWORK SECURITY POLICY

- A security policy is a formal statement that embodies the organizations overall security expectations, goals and objectives with regard to the organizations technology, system and information.
- It is practical and implementable; policies must be defined by standards, guidelines and procedures.
- A security policy must be comprehensive, up-to-date, complete, delivered effectively, and available to all staff.
- It must also enforceable.
- Security policies are included within a security plan and procedure.
- It also includes the physical security of the computers.

Formulating a Security Policy

Security policies are defined based on an organizations needs. It includes approaches and techniques that an organization is going to apply in order to secure its resources. The steps followed while formulating the security policy are:

- Analyzing current security policies.
- Identifying Information technology assets that need to be secure with (a) Physical resources and (b) Information resources.

- Identifying security threats and likely security attacks.
- Defining the proactive and reactive security strategies. M-wallet (mobile based card less mode of payments) have emerged a one of the biggest beneficiaries of a digital payment industry in the country.

The M-wallet players such as Paytm, Citrus Pay, Mobikwik, Oxigen, Airtel Money, M-Pesa and M-rupee among others are moving aggressively to scale up. M-wallet players will have to advantage in e-commerce cab service, online recharge, bus ticket bookings and online food payments etc. The Global Mobile Banking Report 2015 claims that adoption of mobile technologies for banking has reached 60-70% of the total banking population in India and China, which is higher than that of US and Europe. Globally, the e-commerce market is worth around $22.1 trillion, according to latest UNCTAD estimates.

Different wallets introduced by different companies

1	Bank Sponsored Wallets	ICICI Pockets, Axis Live, HDFC PayZapp, SBI Buddy, Kotak Bank’s Kay Pay
2	Third-Party Wallets	PayTM, PayVMoney, Oxigen, Citrus Pay
3	E-Commerce Wallets	Flipkart Wallet, OLA Money
4	Mobile Operators Wallets	Airtel Money, Vodafone Mpesa, Idea Money

- **(Source: Business Standard, 30th November 2015, p.2)**

CASE STUDY OF COMPUTER VIRUS

A computer virus is a malicious software program loaded onto a user's computer or system without the user's knowledge and it can performs malicious actions are taken.
The term 'computer virus' was first formally defined by Fred Cohen in 1983. Computer viruses never occur naturally. They are always induced by people. Once it is created and released, however, their diffusion is not directly under human control. After entering a computer, a virus attaches itself to another program in such a way that execution of the host program triggers the action of the virus simultaneously. It can self-replicate, inserting itself onto other programs or files, infecting them in the process.

Brain: The Brain boot sector virus also known as Pakistani Brain, and Pakistani flu was created in 1986 in Lahore, Pakistan by 19-year-old programmer Basit Farooq Alvi, and his brother, Amjad Farooq Alvi. It was the first IBM PC compatible virus, and the program responsible for the first IBM PC compatible virus epidemic. Brain affects the IBM PC computer by replacing the boot sector of a floppy disk with a copy of the virus.

I Love You :It is also known as Love Letter, or VBS, or Love Bug worm, it it infected millions of Windows computers worldwide within a few hours of its release on May 5, 2000. Created by a Filipino computer science student, the ILOVEYOU is considered to be one of the most damaging worms ever.

Flame : I is known as Flamer, sKyWIper and Skywiper this modular computer malware was discovered in 2012. It is being used for targeted cyber espionage in Middle Eastern countries.

CryptoLocker: This CryptoLocker is aTrojan Horse, discovered on September 2013 encrypts the files on a user's hard drive, then prompts them to pay a ransom to the developer in order to receive the decryption key, making it the first true ransomware.

Regin :This Regin is a Trojan Horse named after the Norse Mythology character Regin, first came to prominence in November 2014 when it primarily spread via spoofed Web pages.

Conficker: It is a worm are known and have been dubbed Conficker A, B, C, D and E, which were discovered 21 November 2008, 29 December 2008, 20 February 2009, 4 March 2009 and 7 April 2009, respectively. Microsoft released the KB958644 on December 16, 2008, patching the server service vulnerability responsible for the spread of Conficker.

Ransomware : It is an unprecedented global wave of cyber attacks, which have affected over 45,000 computers in at least 74 countries on 13th May 2017 have also spread to India. The Ransomware virus infects computer files and then demands anywhere between $300- $600 Bitcoins to unblock them. It has struck targets from Russia's banks to British hospitals and French carmaker Renault's factories, **Portugal** Telecom, the **US** delivery company FedEx and a local authority in **Sweden,** local railway ticket machine in **Germany** and a university computer lab in **Italy** were also affected.

2.16 LET US SUM UP

Change management is the process, tools and techniques to manage the people side of change to achieve the required business outcome. Change management incorporates the organizational tools that can be utilized to help individuals make successful personal transitions resulting in the adoption and realization of change. Security policies are defined based on an organizations needs.

2.17 KEY TERMS

- ✓ **Firewall** is defined as a hardware or software that filters communication packets and prevents some malicious packets from entering the network, based on a security policy.
- ✓ **SSL (Secure Sockets Layer)** protocol provides a security “handshake” in which the client and server computers can exchange a brief burst of messages. It can be used to encrypt messages that are sent between client browsers and web browsers.
- ✓ **Encryption** is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the reliever. The science that studies encryption is called cryptography. The combination of two Greeks words “Krupto” and “Grafh” that mean “secret” and “writing” respectively.
- ✓ **Security plan** specifies how the rules put forward by security policy will be implemented.
- ✓ **Security Policy** states the managements overall security expectations, goals and objectives with regard to the organizations technology, system and information.
- ✓ **Manipulatio**n is used to manage when time is of the essence.
- ✓ **Biometrics** measures and analyzes human traits like fingerprints, retinas, voice patterns, facial patterns for authentication.

2.18 SELF-ASSESSMENT QUESTIONS

1. What is Management change?
2. What is a security policy? List the steps followed in formulating security policy.
3. Explain in details about network security.

2.19 FURTHER READINGS.

1. Joseph, P.T and S.J (2009) E-Commerce an Indian Perspective", PHI, New Delhi, 3rd edition.
2. Bhaskar, Bharat (2007) "Electronic Commerce: Framework, Technologies and Applications, Tata McGraw-Hill, New Delhi, 2nd edition.
3. Mishra, Jibitesh (2011) "E-commerce", Macmillan Publishers, New Delhi.
4. Jaiswal, S. (2003) E-Commerce, Galgotia Publication, 1st Edition.

2.20 MODEL QUESTIONS

1. What are the human resource traits for e-commerce?
2. How does change management work in government?
3. Explain development of human resource availability.
4. Explain in detail the method of implementation of management of change.

2.21. SELF-ASSESSMENT QUESTIONS AND ANSWERS

1. **What is Management of change?**

Ans: Management of change the new sunrise induction of e-commerce systems. But the targeted levels of performance, productivity, profitability and efficiency in an organization. With the availability of human resource , flexibility, or productivity, but also improving their knowledge, managing their natural resistance to change, and helping to convert that resistance into commitment. Employees should be educated to use new information technology. Progressive organizations should be built on the potential of their skilled employees.

2. **What is a security policy? List the steps followed in formulating security policy.**

Ans: A security policy is a formal statement that embodies the organizations overall security expectations, goals and objectives with regard to the organizations technology, system and information.(a)It is practical and implementable; policies must be defined by standards, guidelines and procedures;(b)A security policy must be comprehensive, up-to-date, complete, delivered effectively, and available to all staff;(c)It must also enforceable;(d)Security policies are included within a security plan and procedure;(e)It also includes the physical security of the computers. The steps are as follows:

Formulating a Security Policy

Security policies are defined based on an organizations needs. It includes approaches and techniques that an organization is going to apply in order to secure its resources. The steps followed while formulating the security policy are:

a) Analyzing current security policies.
b) Identifying Information technology assets that need to be secure with (a) Physical resources and (b) Information resources.
c) Identifying security threats and likely security attacks.
d) Defining the proactive and reactive security strategies

3. Explain in details about Network Security

Ans: A network security can be defined as the protection of network resources against(a)Unauthorized disclosure;(b)Modification;(c)Utilization;(d)Restriction or Destruction. There are two types of network security which is described as below:

- **Client Server Network Security:** It includes all methods and authorization to make sure that only valid user can access the information. It is related with the physical and software security problems.
- **Data and Transmission Security-** It means the security of the data and security during transmission of data. It is needed to prevent changes in messages while transmission. On internet it is provided by the firewall.