UNIT 6 IT SECURITY MEASURES IN BUSINESS

Structure

6.0 Objectives
6.1 Introduction
6.2 Why Systems Are Not Secure?
6.3 Cyber Security
   6.3.1 Principles of Cyber Security
6.4 Identity Theft
6.5 Key Security Principles
   6.5.1 Identification
   6.5.2 Authentication
   6.5.3 Authorization
6.6 Six Essential Security Actions
6.7 Applying Principles to Information Security Policy
6.8 Security Self-Assessment
6.9 Digitization
   6.9.1 Impact of Digitization in Business World
6.10 CAPTCHA Code
   6.10.1 Purpose of CAPTCHA
   6.10.2 Types of CAPTCHA
6.11 One Time Password (OTP)
   6.11.1 How to Get a One Time Password
   6.11.2 How a One Time Password Works
   6.11.3 Benefits of a One Time Password
6.12 Let Us Sum Up
6.13 Key Words
6.14 Answers to Check Your Progress
6.15 Terminal Questions

6.0 OBJECTIVES

After studying this unit you should be able to:

- understand the meaning and importance of Cyber Security;
- understand the difference between Identification, Authentication and Authorization;
- understand what is Digital Signature and Digitization; and
- understand what is CAPTCHA Code and OTP.
6.1 INTRODUCTION

In the previous unit we have learned about securing business organizations from unauthorized users such as hackers. In this unit we will discuss the steps which are taken for securing the assets of business organizations. For small business organization checking the cyber-security may not be the top priority, because of its dimensions, but this aspect is important for their growth & survival. In the present scenario of digital era, organizations are migrating to online platforms to serve their customers better and their availability is enhanced by using internet. Because of migrating online the business organizations are vulnerable to a wide array of cyber attacks & threats. The organizations are being targeted constantly as well as security breaches are happening, but they hide it for the sake of their business.

Hackers are constantly looking to hack businesses organizations and many times they succeed in their efforts. The good cyber security system can protect the business organizations and hence, from the threats of these hackers. Cyber-security is the most important aspect of security for any organizations and hence should be taken seriously. Not only organizations are secure by adopting cyber security measures but their employees are also safe. All business organizations want to secure their assets and hence the role of cyber-security becomes extremely important. If a business organization has an effective security plan in place before any attack happens then only it can protect its assets from the hackers.

6.2 WHY SYSTEMS ARE NOT SECURE?

System security can be classified in two categories. First one is the physical machine security which is used to prevent theft of computer hardware. It is much more important now days to prevent theft or damage to the information system available in business data. Further, in today’s corporate world, data is money and value is greater than the value of hardware in terms of cost. We can access the data of any business organization just by using remote access technology and networking devices, and thus physical security has no sense & meaning in today’s digital world. We can only secure physical components of computer system by physical security. To secure the systems we have to define the policy on every system that what actions can be performed on a particular system and at what time. Thus we have to define the user category and the rights normal users and administrators well in advance. It may not be secure for beyond the specific policy and for advances in technology over the passage of time.

Although significant advances have been made in the state of the art of computer security in recent years, the information in computers is much more
vulnerable than ever because of online frauds. Every major technological advance in computing systems brings new security threats. The technology grows at a much faster rate than the rate at which solutions to curb the threats arising thereof can be developed. Further there is a need to cautiously deal with hackers, given their ability to acquire latest expertise in this regard. Therefore, we would be fighting a lost battle if the systems of a business organization are compromised. The system security is team work and it can’t be achieved in isolation. By following logical piece of well-defined security architecture in the business organization we can protect our system from external threats & hackers.

We don’t have any control on the way the world works and it is beyond our imagination and scope also, but just by understanding why it works & the way it functions, we can avoid the typical pitfalls and choose acceptable security for any organization. This unit contains some basic and fundamental reasons why the implementation of computer security is not an easy task for any business organization.

6.3 CYBER SECURITY

In present scenario, cybercrime is not only problem of a country but it’s a global problem. The boundaries of cybercrime are invisible & are spread world-wide. The cyber crime news is becoming headlines in recent times. Cyber crime is a threat to individual security and an even bigger threat to large international companies, banks, government organization and business organizations. The cyber crime is a type of organized crime and is committed by large organized & skilled cyber criminals online. The cyber criminals often employ highly-trained developers and these developers keep on updating their online attacks constantly. The cyber security has become essential now days for all the business organizations because no business organization wants can afford online attacks in present digital world. We can define cyber security in following words:

Cyber security is a pre-defined set of techniques used to protect the integrity of computer networks, programs, and data of business organizations from attack, damage or unauthorized access. The term security of business data has two important components, and these are namely cyber security and physical security. The enterprises have to protect their confidential data against unauthorized access from physical security as well as cyber threat. The term Information security, is designed to maintain the confidentiality, integrity, and availability of data, all the time and by all means. The use of cyber security can help prevent cyber attacks, data breaches, identity theft and can aid in risk management.
Cyber security involves protecting the system from un-authorized access, un-authorized deletion, & un-authorized modification from the hackers. Cyber security provides a protocol that protects against all cyber attacks and makes sure that business data is secure from the hackers.

Fig. 6.1: Cyber security threats posed by hackers

The present generation uses smart phones and is connected with the internet all the time, and has no idea, how information reaches securely to their computers from unsecured media. This provides golden opportunity to hackers to hack data of these youth. There are so many access points, public IP’s and constant traffic and tons of data to exploit by hackers. Furthermore, cyber attacks are evolving by the day. The hackers are becoming smarter and more creative now days with the state of art of training they receive from their trainers. It is a very tough task for the security administrator of big companies to outsmart the hackers and to protect their data from malwares & viruses which are tools used by hackers to bypass the firewalls of any organization.

6.3.1 Principles of Cyber Security

In implementing cyber security, there are two specific goals to be attained: first, confidential information must be kept out of reach of potential cyber attackers and other unauthorized individuals. Second, cyber security measures must not hinder authorized users' access to the information. Three main principles of cyber security are follows:

1) **Confidentiality**: Cyber security should ensure that the information to be secured is only accessible to authorized users and prevents the disclosure of information to unauthorized parties. For example, to implement confidentiality of company information on a cloud-based Customer Relationship Management (CRM) system, access can be restricted to users with the right username-password combination. Most systems also
implement confidentiality through data encryption, which is an additional layer of security. Decryption of the data requires an individual or system to attempt access using the requisite key.

2) **Integrity**: Cyber security efforts should ensure information remains accurate, consistent and not subject to unauthorized modification. For example, from the CRM example provided, integrity is achieved when measures are put in place to ensure that email communication between a sales representative and a customer is not intercepted and modified by an intruder when it is still in transit.

3) **Availability**: Efforts to secure information in cyberspace should not hinder its access by an authorized party. Additionally, cyber security implementation has to provide for redundancy access in case of any outage. For example, the company using cloud-based CRM system can implement proxy servers and firewalls as a security measure against Denial of Service (DOS) attacks, which would create system unavailability if successful.

### 6.4 IDENTITY THEFT

The term identity theft means cyber criminals illegally acquire credentials of innocent users and use these credentials to do online cyber crime by hiding their actual identity and using the identity of other innocent users. It is the criminal act of illegally and deceptively assuming the identity of another individual without their expressed consent with the intent of committing a crime; it also includes fraudulent and illicit attainment of personal information through the usage of unsecured websites. Through the use of stolen documentation attained upon illicit means of electronic acquisition - individuals can fraudulently assume the identity of others in order to engage in fraudulent purchases and illicit economic gain by using internet. In other words, identity theft is also called as identity fraud and is the act of a person obtaining information illegally about someone else without consent. The Hackers try to find out information about users such as full name, maiden name, and address, date of birth, UID, passwords, phone number, e-mail, and credit card numbers & CVV No. etc. to harm the users.

---

**Fig. 6.2: Protecting the User Credential from Hackers**
The hackers then use this information to gain access to other details of users such as his bank accounts, e-mail, cell phones, etc. Doing such acts, of acquiring information about others illegally is a crime under IT Act 2008 and may attract strict punishment by the judiciary under IT Act and such persons can be send to imprison for entire life if found guilty.

**Methods to prevent identity theft:**

i) At the time of entering any personal information on the Internet, please make sure that connection is encrypted.

ii) Avoid storing credit card or personal information on any website if you do online shopping over the Internet.

iii) Do have an active and up-to-date spy ware protection software & antivirus software.

iv) Make yourself aware about fake e-mails and phishing e-mails that claim to be a company

v) Never use unknown & unsecured systems & smart phones.

vi) Always have strong password & keep answer of secret question unguessable.

**Check Your Progress A**

**Part A: Multiple Choice Questions**

1) What is need of a Proxy Server?
   a) It is used to create a stronger connection with the target.
   b) It is used to create a ghost server on the network.
   c) It is used to obtain a remote access connection.
   d) It is used to hide malicious activity on the network.

2) In securing the environment against an attack which of the following is not needed?
   a) Education level of the attacker
   b) Configuration of system
   c) Architecture of network
   d) Companies business strategy
   e) Employees level of access to website

3) Which technology is used to hide information inside a picture?
   a) The Root kits
   b) The Bitmapping
   c) The Steganography
   d) The Image processing

4) Why Denial of Service attack is used?
   a) To exploit a weakness in the TCP/IP stack
b) For executing Trojan on a system

c) Just to overload a particular system so that it is no longer operational

d) Shutting down the service by turning them off

Part B: Short Answer Type Questions

1) What do you mean by Cyber Security?

2) Explain the reasons why systems are not secure.

3) What is do you mean by Identity Theft? Explain with example.

6.5 KEY SECURITY PRINCIPLES

IT security has to respect three contradictory requests; protection of confidentiality, integrity and availability of information. The key IT security principles are identification, authentication and authorization. Defining the security policies and designing the security elements lead to a safe and secure environment for information systems as a main support for open and dynamic business systems. User identification is a procedure during which a potential user identifies him to the information system when logging in. Generally, it is a process during which one entity introduces itself and identifies to another entity.

Authentication is the authenticity check procedure, i.e. it checks the user’s identity, by comparing the data received from the entity with those stored in the base. It should be mentioned that the entity integrity is not necessary. For example, when logging on ISP it is possible to connect more people from the
same telephone line and the same computer, under the same user name and password.

![Fig. 6.3: Displaying the Steps of Information Security Policy](image-url)

Authorization is the procedure of a system user access rights definition and most often it is a part of authentication. We will discuss details of these three principles of IT security in this section.

### 6.5.1 Identification

The term Identification in computer science is used to define and manage the roles and access privileges of individual users on the network. It also deals with the circumstances in which users are granted (or denied) those privileges. The user may be either customers or employee of the company. Identification is used to give the digital identity per individual, &once that digital identity has been established, it must be updated, maintained, and monitored throughout each user’s “access lifecycle”.

In other words: identification in computer science is an organizational process for identifying, authenticating & authorizing users to get access to applications, systems or networks by associating each user unique rights and restrictions with established identities. The identities are also referred as software processes that need access to organizational systems. Identification is used to uniquely identify user of a system as well as application that is running in the system.

In most information systems a username and a password are used as for checking the identity of a valid user. Anyone who enters the correct username and password is a valid user for information system. Therefore, to protect the system we should always keep secret the user name and password; otherwise the information stored in the system will not be secure. As long as the combination of username and password is secret the information stored in the database is secure.
6.5.2 Authentication

Authentication is the process to check the credentials of users before they are given access to use the resources of the system. It is the ability to prove that a user or application is genuine & on this basis it can use the resources of the organization or network. Authentication Identification is done on the basis of the identity of the user. Authorization process involves by giving username, a process ID, a smart card, or anything else that can uniquely identify that object at the time of authentication. If a user wants to access the information system which is available on a server then it must show its identity. In authentication, the user has to prove its identity to the server or client before it is allowed to use resources.

When a user provides appropriate credentials to prove its identity then only it is allowed to use the resources and this process is known as authorization. For example, when a user enters the correct username & right password then it proves that the user is the lawful owner of the username. In short, the authentication gives proof of a claimed identity& is allowed to access the resources. Server uses authentication process to know exactly who is accessing their information or site. Authentication is used by a client to establish connection with the server. There are several definitions of authentication; some of them are given below:

i) Server identifies a user by its username & password. Other ways to authenticate in a system are through cards, retina scans, voice recognition, and fingerprints.

ii) The third trusted party such as VeriSign is used to check the validity of each user certificate before it could be allowed by user to login.

iii) In bank websites username, password & CAPTCHA is used for authentication purpose.

iv) Authentication only identifies and verifies who the person or system is.

v) In bank ATM’s password or PIN is used for authentication purpose.

vi) Smart cards and biometric credentials are used by employees to prove their identity. In the organization.

6.5.3 Authorization

The name authorization is methodology adopted by software companies to allow lawful users to system resources including files, services, computer programs, data and application programs. It is the process to grant or deny access to a network resource based on the user's identity. The authorization can also be defined in following words:

i) It is a process by which a server determines if the client has permission to use a resource which is available on the network.
ii) Authorization is followed by authentication by the server & it determines who the client is & what he is requesting for over the network.

iii) There are several types of authorizations and requirements for each of them may vary;

iv) There is no authorization required in some cases and in other authorization is required.

Some web security systems are based on a two-step authorization process, in which first step is authentication process, and the second stage is authorization process. The present operating systems work on effectively designed authorization processes to facilitate application deployment and management of resources. The main factors on which the modern operating systems work are: number of users and their credentials to login the system. The moment a user is identified and authenticated, it can be granted authorization based on its profile.

In other words, if all the users logs on by using same account, then they will be allowed to access the resources. In such situations it is very difficult to differentiate between the users of the system. Further, if users have been authenticated by different user accounts, they can be granted access to different resources based on their identity & profile.

Check Your Progress B

Part A: Multiple Choice Questions

1) Aim of Authentication is to:
   a) Restrict what operations/data the user can access
   b) Determine if the user is an attacker
   c) Flag the user if he/she misbehaves
   d) Determine who the user is
   e) None of the above

2) Cyber Attack is:
   a) DOS Attack
   b) Phishing attach
   c) Sending malware
   d) All the above

3) Authentication method is:
   a) Secret question
   b) Biometric
   c) Password
   d) SMS code
   e) All of the above
4) In role-based access control, each user is assigned one or more roles, and the roles determine which parts of the system the user is allowed to access.
   a) True
   b) False

**Part B: Short Answer Type Questions**

1) What are the key security principles of IT security for business organization? Explain with example.

2) Explain the need for user identification in online banking system.

3) What do you mean Authentication? Explain with example.

4) What is the difference between Authentication and Authorization? Explain with example.

---

**6.6 SIX ESSENTIAL SECURITY ACTIONS**

All the business organisations have to protect their IT security from unauthorized users and need to take steps to protect them from illegal users. The number of cyber attacks is increasing day by day and are affecting
Data Handling

businesses of all sizes. In such situations, it is necessary for every company to be aware of the dangers posed by cyber criminals and be ready to safeguards their data from such criminals and having in place proper security mechanisms. There are several approaches for securing the systems in the market and installation cost and time of use is also involved in their selection.

But which is the best security tool can be used in an organization depends upon various parameters. If the parameters of a security tool are best fit for any organization then it has to be purchased and installed. Further, the heads of organizations and heads of Security Company can discuss and negotiate to finalize the software which is best for any company. We have to also keep in mind that the software which is most advanced and which provides long-term protection can be given priority over the short protection time.

Almost all small businesses organizations use web-based technology tools to carry out transaction. For example, conducting long-distance conferences, giving advertisement, marketing products, doing research, identifying new markets, and communicating with customers and suppliers, have become integral part to the smooth functioning of small businesses organizations.

![Image of a secure office setup with a safe and computer equipment]

**Fig. 6.4: Securing the Hardware from theft in Business Organization**

We can install cameras to protect systems from physical theft now days. The advancement of technological aids and state-of-art security cameras, have made physical theft negligible. But protection from virtual world in current digital era is not easy and it needs technical skill set to protect data from outside world. The modern organisations are connected worldwide by internet and latest networking devices, which a boon and makes communication easy, but at the same time vulnerable to online theft. Along with several benefits of internet, there are many risks involved in digital era and is only growing every day. The small businesses organizations have many loopholes due to that they are prone to cyber-attackers. To protect the organization from cyber attacks following six measures are necessary to be adopted by them.
1) **Firewall:** Firewall is a type of virtual protection wall which helps to protect network traffic inbound and outbound to any organization. It stops unauthorized hackers from attacking the network by blocking them from the systems of organizations. Firewalls are programmed in such a way that they restrict the network from sending out proprietary data and confidential emails. The present era hackers have become more sophisticated with the state of art hacking technologies due to this reason firewall have become obsolete to stop them from the network of organizations.

The firewalls are the most core of security tool of any organization, and will continue to remains for times to come. The firewalls are useful for the security of business organizations, but they have limitations too. The trained & skilled hackers have learned how to create data and programs that trick firewalls into believing that they are trusted one. This makes them to go through the firewall without facing any difficulty. Despite above limitations, firewalls are still very effective in detecting the unauthorized and less sophisticated malicious attacks on the data of business organizations.

2) **Antivirus Software:** The Antivirus program is used to remove the virus from system and network of business organizations. It is basic software and should be the part of any cyber security system. In addition to this use of anti-malware software is also essential now days. The antivirus works as the final frontier in securing and defending unwanted attacks from intruding the network of business organizations. The antivirus works by detecting and removing virus and malware, adware and spyware from the network. It also scans & filter out potentially harmful downloads and emails of systems of all the organizations. Install antivirus and anti-spyware software - any computer or network used by an organization should be secured with a good firewall that takes Wi-Fi into consideration. The latest versions of anti-spyware and antivirus software should be installed. Vendors provide security patches and updates for software, so be sure to update to the latest version regularly. Configure all software to install updates automatically.

3) **Use Complex Passwords:** The user-id and password is essential to access the resources of business organization over the network. We should always have strong password and keep it confidential from the hackers. The passwords should be changed periodically. Strong password is difficult for users to crack it and thus makes the data secure. We should confidential and complex answers to secret questions, so as to make it difficult for hackers to crack it. We should have strong password on social media sites so that our data on these sites is safe and its security is not compromised. We should use space before or after passwords to
throw the hacker off from the hacking the system. Keeping space makes password difficult to guess by unknown persons. If some has access to your password but is unaware that password has space then he or she can’t access to your data. We should also use combination of upper and lower characters and special characters to make it complex for users to guess or crack. A combination of alphanumerical characters and symbols could also be used to make the password strong.

4) **Regular Backup**: The process of saving data regularly and taking backup saves organizations from the risks of data loss. In case of data loss backup is very useful and could be used to restore the data in business organisation. With advancements in hacking technology no network is safe & perfect now days. In present time data hacking and money hacking from banks become headlines in newspapers in which hackers try to bypass the bank network security and steal money illegally. In case of hardware failure backup data is very important to run the business smooth and business interest can be safegaurds with regular backup.

To reduce the risk, regular back of data is very much essential. We should set automatic backup option on in the servers of modern business organization. If the backup is regularly taken then it provides piece of mind to the management and helps to protect the interest of the business in the market. We should have multiple physical copies of our important documents in present digital age so that we can get back it in case of loss of data from physical or software failures, and in case of our systems are compromised by the hackers.

5) **Penetration Testing and Limit Access to Critical Data**: Testing is used to test the software with the objective of finding faults in it. There are several types of testing in software engineering and penetration testing is one of them. The penetration testing is used to test the security of business organizations by calling security professionals to test the network security of business data. The security professionals; use the same technique which the hackers use to find the potential weakness and vulnerability in the security systems. We should follow the advice of security professionals and add more security tools as per the suggestions to further enhance the security of servers.

Penetration testing is one method to secure and enhance the security of data in business organizations. In addition to this we should have restriction on the access of critical business data from its employees. The critical data should be accessed by authorized users only and by means of authentication and authorization. Unauthorized and outsiders should not be allowed to access the critical data and should use mechanism to do
the needful this regard. We should keep the number of people with access to critical data to a minimum such as the company’s CEO, CIO, and a handful of trusted staff only and should have a clear plan that mentions which individual has access to which sensitive information for increased accountability.

6) **Employee Training:** All the employees of business organizations handling critical data must be trained before they are given responsibility to secure the data. There are several types of attacks and phishing is one of them. To protect the business organizations from phishing attacks the employees must be trained how to handle keep secure data from such attacks.

If the employee is trained enough for phishing attacks then only he can protect the critical data from loss. The phishing attack is making similar websites like original one and targeting customers and stealing their user id and password illegally. Once user’s credentials are collected over phishing websites and then this credential could be used later on to withdraw money and the original users illegally. Thus training of employee’s makes organization secure from online attacks and thus the data is made secure from unauthorized access.

The employee who is handling the security tools must be trained to handle it properly before they are given responsibility to secure the organization. The first step in securing the organization from online threats is to recognize threat. Second step is to track the threat. The third step is to find the tools and antivirus to resolve the threat. The employees or the users who are accessing the network must be trained about the risk and precautions to which they have applied in case of cyber attack in business organization so that the risk is minimized. Further, in case of online usage, usage policy, usage rights, and usage profiles must be monitored to know the behaviour of employees and safeguard the business data from illegal access.

### 6.7 APPLYING PRINCIPLES TO INFORMATION SECURITY POLICY

The information security for all the organizations must be framed keeping in mind the level of its security required as per the suggestions and recommendations of cyber security experts. Important information security practices should be enforced and must not be overlooked by the security team at any cost. As we know that prevention is better than cure and if we have all the security measures in place then we can save the business data from wrong hands. The businesses must adhere to strict policies for information security inside their organizations.
It has been observed that preventive steps are only taken after the cyber attacks happen inside the business data. We should not wait for attacks to happen but take steps to secure the data from the very first day of organization commencing its business. There are several steps to protect business data of any business organization. In addition to cyber attacks there are self propagating malwares which are risks for business organizations. All business organization wants their online presence to boost their business due to this reason their security becomes prime factor and utmost important for the management.

In view of above, business needs to look into tightening their security policies before it is too late for them to act. In this section we shall mention some steps which must be adopted to secure the business data in current digital age. These are:

1) **Access control policy**: The term access control management plays very important role in securing the critical data from outsiders. Every business organization should implement access control policies strictly to protect it data. The social websites now days have become threat for the business organizations. These websites and Internet itself poses a lot of hidden threat for the data and we should deal these threats effectively by applying access control policy.

The better password management techniques also helps to reduce the online risks involve in present digital era. The system admin should monitor the online threats regularly and advise all the users of business organization to adhere the security policy used in the organization. The system admin should advise all the users to change their passwords periodically and frequently to safeguard their system from hackers. Only authorized users should be allowed to use the resources of the system and unauthorized users must be stopped to access the system.

2) **Two-factor authentication policy**: The one time password technique is also known as two factor authentication policy and can be implemented to mitigate the illegal use of accounts. In this mechanism one time
password is send to the registered mobile number of the user. The user is then asked to enter the onetime password received through SMS. If user enters right one time password then his authentication is authorized and he is allowed to use the resources online.

The one time password technique has some limitations also and is not the best technique for two factor authentication policy. The alternate email authentication process is another method for double authentication of the users in the business organizations. We should use any of the double authentication policy to make secure the critical data of business organization.

3) **Encrypt your interactions:** The term encryption means hiding the plain text data and converting it to some code which is difficult for outsider to crack. To protect confidential data from outsiders it is encrypted before it is send from source computer to destination computer by using insecure network. Once the encrypted data reaches to the destination computer it is once again converted to actual form by using decryption techniques.

This way of sending encrypted data over insecure network is known as encryption and decryption. The term encryption is used to convert plain text into coded form, and decryption is used to convert coded form into plain text at destination server. By using encryption and decryption techniques we can protect the critical business data from the hands of hackers.

4) **Safeguard your keys:** It is very much important to keep the login credentials secret to protect the data from unwanted hands, and access to the keys gives access to the information. Further, in case of physical lockers one should always have second set of keys which can be used in case first set is lost or stolen. Furthermore in case of loss of keys the second set of keys must be used to open the locker and may be at later time can be changed to avoid data or information loss from the business organization. Thus by safeguarding the keys we can stop business organizations data and information from unauthorized users and hackers.

5) **Backup your information:** One has to always make them sure about the backup and make it safe and protected. The term backup means making copies of business data and storing it at safe place at regular period to avoid loss of data in case of hardware failure or software failure. Business data &information should be accessible and must be encrypted and stored in a secure place. Sometimes business contracts have confidential information clause(s), which should not be disclosed to any organization which can misuse that information for its advantage. Such confidential data should always be maintained confidential and should not be disclosed to competing organization.
The business organizations do sign memorandum of understanding (MOU) for various types’ partnership and exchange of goods from each other for the purpose of running their business in the market. Such MOU’s should always be kept confidential and should not be disclosed any third party which has potential to misuse the data and information of MOU’s between two business organizations. In case of any misuse of private and confidential data and information of a business organization by other competing organization can be challenged in court of law and quantum of punishment and penalty is given by the courts for compensation the loss of any business organization.

The breach of confidentiality may occur without signing MOU agreement between cooperating organizations also. In India, employees of a business organization are required to keep confidential any secret information disclosed to them by the other party during their service time. Further, if employee does breaches of confidentiality then it may be challenged in the courts to get justice. The courts may hear the argument of both the parties and give justice to decide the case as per the proceedings and evidence produced in the court. The following types of questions may be asked by the court during hearing:

i) Information about confidentiality of facts
ii) Is discloser has any link in circumstances of case
iii) Is the party who received the information had misused it or not

Further, this is to be mentioned that although the law implies a duty of confidentiality – its scope, nature, and obligations are indeterminate and subject to judicial determination. The Frequency of leakage of confidential data and its nature should be dealt with utmost confidentially during the arguments in the courts. Some examples of such cases is given below to understand the confidentiality of data and information

i) Stealing of (laptop, computer, paper, MOU’s etc. – physical security)
ii) Improper disposal of confidential information
iii) Unauthorized access type and its nature (access controls, authentication, lack of understanding of confidentiality agreements, negligence, etc.)
iv) Quantum of Loss of confidential data (negligence, etc.)
v) Hacking incident logs etc. (most often Internet security )
vi) The way of leakage of confidential data is measured by cyber security experts.
The ever-changing IT environment within organizations has evolving technology platforms, adoption of new devices, subscriptions and solutions. It is for this reason that enterprises must continually keep up with the reality of everyday routines that ultimately drive business (or slow it down). Practices that may have been efficient a year ago can rapidly diminish and become limiting today. Routine security risk assessments can help organizations stay proactive. With the right cloud tools and controls, enterprises can quickly adapt to the present changes.

It's important to ensure that physical devices are secured well in the business organization from physical theft. The cameras must be installed at strategic locations to deter & prevent physical theft in the business organization. The attackers try to gain the access of servers of business organizations through internet-enabled devices and un-patched exploits. The physical networking devices such as wireless printers, Wi-Fi routers, Hubs, UTP cables and moveable devices may be exploited by the hackers to get access of entire network of business organization. There are different levels of risk assessment and cyber security experts may be used by business organizations to check for loopholes in the security of computer network and suggest the measures to resolve it. The security analysis of business organization can be done by expert network administrator of business organization also. The cyber security companies specialized in vulnerability and risk assessment testing for clients may be roped in to suggest the means and ways to secure the network. The services of cyber security experts have some cost involved, and this cost may not be feasible for small business organizations.

The employees of business organization should do risk assessment and must make it a routine process, irrespective of size and scale of businesses industry. The security breaches may happen to any business organization, especially small businesses, either because hackers believe that they are easy target while trying to breach a larger company by chance. The self-assessment and monitoring should be made a compulsory and continuous process for securing the business assets. Further, a comprehensive security risk assessment should be conducted at least once or twice in a year, which has been suggested by Information Systems Audit and Control Association.

The self assessment method is very effective in finding vulnerabilities in any business organization. It is the responsibility of IT staff to present self assessment plan to management and implement it in association with management to find the vulnerability in the network. The creator of a network understands the network structure well and his services may be utilized for assessing the vulnerability in the network. Since he is the network creator he would be able to assess the security issues, more quickly than
Data Handling

others. To protect the business we should secure the network first and do the needful assessment periodically.

Further, if online transaction is accepted by any business organization then it is much essential to call the cyber security experts for assessing the vulnerability in the network and to fix the vulnerability by initiating steps to secure the network as per the suggestions received by the cyber security experts. If any business organization has not done security assessment then it is prone to cyber theft and it must take steps for security assessment as soon as possible. In today’s digital world cyber-attacks on businesses organizations are increasing everyday and it is a reality. In past year several cyber attacks were reported by print and electronic media such as phishing scams, ransom etc. In future several cyber attacks shall be carried out by cyber attackers to steal the data and information of business organization. It is the duty of all the internet governing agencies of the world to sit together to plan the strategy to check the cyber attacks and frame the policies to punish the hackers worldwide to protest the interest of business community world wide to secure business organizations.

Basic Steps of Risk Assessment

The basic steps of security assessment could be as follows:

1) **Identify:** Characterize the system (process, function, or application)
2) **Protect:** Identify Threats
3) **Detect:** Determine inherent risk & impact
4) **Respond:** Analyse the control environment
5) **Recover:** restoration of systems and improvements

Empowering Users: In most cases, the biggest threat to an organization is the people who work there. Employees within an organization are the main threat to cyber security. Those without knowledge have the most opportunity to expose your data, second to vendors with access to your systems. Recognizing phishing mail and proper management of user access and authentication, to recognizing phishing emails, users can make or break your security. Keeping employees educated is the key to preventing attacks and responding to them accurately.

Creating a Risk Assessment: In today’s digital world, 85% of business assets are in digital format. Therefore, it is critical that organizations take precautions before it’s too late. Risk assessments of any business organization should be assessed by cyber experts including application program, functional part, or the processes followed in by that organization. First of all we have to understand the size, scope and complexity of the business organization to go for security assessment. Once it is estimated then the time, cost, and manpower needed for security assessment should also be
estimated. In risk estimation process we have to identify internal and external systems of business organization which critical for running the organization. In this process we have to take the backup of sensitive business data including operations, process, legal MOU’s, credit card information and many more, before we start security assessment.

Risk assessment can be done on the basis criticality and sensitivity of information. The assessment results gives us idea how to secure the business data, how much time is needed and what methodology to be followed and how much man power is required to secure the data in given time period. All these help us to recognize the missing piece of business data.

In recent years several automated tools and application have been developed by software developers for assessing the network security of any business organization. Some of the tools are open source and you can directly download them from internet. Some tools are paid and you can download them just by paying nominal charges online and can use them to secure your business organization. The Microsoft Windows-0 is equipped with security assessment tool and same can be used to protect the data of business organization.

**Check Your Progress C**

**Part A: Multiple Choice Questions**

1) The Network Layer Firewall works as per the following
   a) The Frame filter
   b) The Packet filter
   c) Both Frame as well as Packet filter
   d) None of the mentioned

2) What is Firewall
   a) A hardware
   b) A software
   c) A hardware as well as software
   d) Neither hardware nor software

3) The full form of DPI is
   a) Dots processing Inch
   b) Dots per Inch
   c) Diagram per Inch
   d) Diagram processing Inch
Part B: Short Answer Type Questions

1) Explain six security essentials for action with example.

2) Explain principles of IT security with example.

3) What do you mean Security Self-Assessment? How it is implemented?

4) What do you mean by Empowering Users? Explain with example.

6.9 DIGITIZATION

The term digitization is used to convert paper based data and information into electronic way of saving, so that it can be retrieved, processed and updated by using computer system. The integration of digital technologies into computer readable format is known as digitization. The everyday routine things can be digitized by using electronic devices such as computer system and mobile phones. The digitization is a process of converting information into a digital format. In digital format, information and data is organized & stored on storage devices such as hard-disk, into discrete units of data, which could be separately recognized & addressed. In digitization data is stored in computer
hard disk in the form of binary number, which can be processed by using computer systems.

The text, audio, images and video data can be digitized by using scanners, cameras and apps. The scanners are used to scan the images and save them in the form of jpg or bitmap images which can be stored in the computer memory for future use. An Optical Character Recognition (OCR) technology is used to analyse and identify the digits and data written on bank cheques and to convert each character into an ASCII code.

The audio and video digitization is used to convert analog-to-digital & vice versa by using computer system. In this process analog signals are converted into digital signals and their quality is enhanced by using the tools and apps, without compromising the actual basic content of picture data. In this process analog signal strength is also enhanced and its resolution can be enhanced by using computer software. Thus the digitization process is very much helpful in storing and keeping the paper format for longer time and for future reference purpose for the knowledge society. For example all the court paper based judgments are now being digitized in India and stored in binary format in computer which can be easily referred in another case by Judge in the courts.

The digitized information makes it easier to preserve, access, and share by using Internet and computer network. For example, an original historical document may only be accessible to people who visit its physical location, but if the document is digitized, it can be made available to the people of entire country and even for whole world. In today’s digital world there is a growing trend towards digitization of historically and culturally data in our country.

6.9.1 Impact of Digitization in Business World

Digitization is very vital in business world in the present digital era. It requires constant change and development in the business organization. With the advancement in hardware and software technology, digitization is now very easy task in compared to times decades ago. Digitization has made life simple and with the help of digitization digital data is 24×7 available to intended user with latest state of art internet technologies. In present digital era digitization is rapidly changing the business world and all the business houses must adapt to digitization to survive in the present digital age to reach to their customers.

1) Artificial Intelligence (AI): Artificial intelligence is the design and development of artificially intelligent machines which can do the work the way human do AI has already changed the business world to such an extent, that all the business organizations are using AI in their products.
For example AC, Refrigerators and all electronic household devices are not IOT based and these can communicate for better utilization and their use can be optimized. AI is now days being used for performing data analysis, creating algorithms, and even improving the communication between the company and clients worldwide including India.

2) **Flexible Work:** Digitization has given choice to IT employees to work from home rather than from office, thus saving in terms of travelling time, cost and office expenses. All the data and information is now days is stored on digital media and can be accessed just by sitting at home. Many IT companies are now offering at home jobs to their employees to decrease company cost and to increase the productivity. The technological progress and digitization in today’s digital age has made it possible to adjust work schedule as per our personal needs and lifestyle. Because of flexibility and better productivity more and more IT companies are relying on freelancers and remote workers to work for them by using internet and state of art network technologies.

3) **Innovation:** The digitization is now days being used to convert paper data into binary form to be stored in computer systems. These digital contents are now days being used widely for doing research by many research scholars in Universities and Colleges throughout India and rest part of the world. Digitization has made availability of digital data 24×7 for the researchers due to that many researchers are developing new and innovative products in the market. Because of digitization many new, innovative solutions have come into the market and thus are making the life simple of all types of people. The can be applied to almost any aspect of the business world, including traffic management, workforce management, production management and many more. The latest Innovations in technology have generated new ideas in business world to reach to a wider internet savvy customer to sell their product online thus making customers happy, satisfied, and product is available to the customer 24×7 by means of internet and network.

4) **New Business Models:** The digitization in today’s digital world has made it possible to create many new business models to deal and offer to customers. We can buy products online instead of physically visiting the shops and incurring travel and time cost. In today’s digital age all the information and tools are available online and business organizations can create and propagate their business models to their customers freely and easily. The companies can apply new ideas to reach to the customers to sell and market their products and just making their business flourishing day by day.
5) **Communication:** Business organizations have to communicate with their counterparts and customers in their business process. The Internet and social media such as Facebook, WhatsApp, and Instagram has made the communication very simple in today’s digital age. Further, communication plays very vital role in life as well as in business. The proper communication makes business thrive and develop and present the right product to the customer. The lack of right information transfer leads to misunderstandings and conflicts. There are many tools, channels and apps via which a business can communicate, both with the employees and with its clients. The Internet has provided various platforms for smooth exchange of information, and even files, documents, data etc between company and its users. In today’s digital age one can use, Skype, Slack, Blogs, videos, Facebook and other “tools” to communicate and exchange their thoughts, with their customers and cooperating organizations.

### 6.10 CAPTCHA CODE

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a method used to protect websites against spam. The goal is to stop interactive websites from being spammed by filtering out automatically generated input. The full form of CAPTCHA is to differentiate between humans and computers. CAPTCHA was invented by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford in the year 2003. As early on as the year 1950, the computer scientist ‘**Alan Turing**’ suggested a method for testing the intellectual capacity of artificial intelligence. According to the computer pioneer, a machine is able to mimic the human mind when it manages to converse with people in a chat without then realizing it is a computer. To stop spam IT companies use CAPTCHA codes to differentiate between users and computers as users. The CAPTCHA is used in the login process by secure websites. The CAPTCHA letters are a way to check if the person registering in website is a real live human being or a computer program attempting to spam the into the website.

![CAPTCHA Image]

*Source: CAPTCHA*

**Fig. 6.6: System generated CAPTCHA Code**
The use of CAPTCHA makes websites secure from hackers but at the same time it irritates genuine users. By using CAPTCHA, we can be secure from getting spam emails from unauthorized users, thus it makes websites secure and safe for the users.

### 6.10.1 Purpose of CAPTCHA

CAPTCHA are usually used when web applications require user input. Imagine you are running an online store and want to give your customers the opportunity to write product reviews in a comments section. In this case, you want to ensure that the entries are actually from your customers or at least from human site visitors.

You can reduce the risk of this happening by protecting online forms with a CAPTCHA, by making users verify that they are human before they can submit their comment. CAPTCHA are now found in almost all sectors where human users need to be distinguished from bots. For example, this includes registration forms for e-mail services, newsletters, communities and social networks, as well as online surveys or web services, such as search engine services.

### 6.10.2 Types of CAPTCHA

CAPTCHA-based methods for human verification can be roughly divided into text and image-based CAPTCHA, audio CAPTCHA, mathematical CAPTCHA, logic CAPTCHA, and gamification CAPTCHA.

1) **Text-based CAPTCHA**: The oldest form of human verification is the text-based CAPTCHA. Known words or random combinations of letters and digits are alienated. In order to continue, a user has to decipher the code represented in the CAPTCHA box and enter the solution into the text box. Classic techniques used to create text-based CAPTCHA are Gimpy, ez-Gimpy, Gimpy-r, and Simard’s HIP.

![Text based CAPTCHA](image1)

**Fig. 6.7: Text based CAPTCHA**

Text distortion and background noise should make it difficult for recognition systems to read. Text CAPTCHA only provide reliable protection against spam when the solution can’t be cracked by programs with automatic text recognition.

2) **Image-based CAPTCHA**: An alternative to text CAPTCHA is the image-based method. Instead of presenting users with an alienated solution comprising of numerals and letters, image-based CAPTCHA are based on quickly recognizable graphical elements. As a rule, several
photos of everyday objects are displayed side by side. The user has to click on the images that are similar to the original image, or to show which ones represent a semantic content. This next example shows a cat as the main image. The user then has to decide which of the other 9 photos depict cats, and then click on them in order to complete the CAPTCHA.

3) **Audio CAPTCHA:** Text and image CAPTCHA can be assigned to the graphical Human Verification process. Whether a human user can easily pass this step depends on how good their ability is to recognize the displayed text or image information. How will a visually impaired person be able to read a CAPTCHA? Website operators should ensure that their selected CAPTCHA method has several solutions to increase their website’s usability. So that visually impaired people can also successfully solve CAPTCHA codes, text-based or image-based test methods are usually combined with so-called audio CAPTCHA. There’s often an extra button that the user can press in order to hear an audio recording, e.g. a short sequence of numbers, which is then entered into the input field.

4) **Mathematical tasks and logic CAPTCHA:** A CAPTCHA alternative, which also takes into account the needs of the visually impaired, relies on mathematical tasks or puzzles to filter out spam bots. A task like the following can be read out with a screen reader, if required, meaning that it can also be used by users with non-visual output devices. To verify themselves as human beings, users have to solve a mathematical problem. These mathematical equations are simple to solve, but the problem is that they aren’t much of a hindrance to computers since
computer people are good at dealing with numbers. This type of CAPTCHA is therefore often combined with various kinds of text alienation so that it’s impossible for screen readers to make sense of it. For example, calculate 7x7 and only enter the first digit of the result in the box. The result would be 49, so the CAPTCHA solution would be 4.

### 6.11 ONE TIME PASSWORD (OTP)

The full form of OTP is one-time password. It is also known as one-time pin. OTP is a password which can be used only once to login into the computer system and also to make secure online transactions. The OTP is numeric or alphanumeric automatic generated string which is used as one-time password for a single transaction or login session. The OTP is more secure than a static password, and is sent to the registered mobile number of the user. Since OTP is received on registered mobile number of the user due to this reason it has less chances of misuse by cyber hackers. The OTP is an additional authentication process used by website to double authenticate the real user before he is allowed to access the resources of the computer system or any server. OTP security tokens are microprocessor-based smart cards or pocket-size key fobs that produce a numeric or alphanumeric code to authenticate access to the system or transaction.

![Fig. 6.9: Two Factor SMS Authentication (2F OTP SMS)](image)

Source: smslane.com

This secret code changes every 30 or 60 seconds, depending on how the token is configured. Mobile device apps, such as Google Authenticator, rely on the token device and PIN to generate the one-time password for two-step verification. OTP security tokens can be implemented using hardware, software or on demand. Unlike traditional passwords that remain static or expire every 30 to 60 days, the one-time password is used for one transaction or login session.
6.11.1 How to Get a One-time Password

When an unauthenticated user attempts to access a system or perform a transaction on a device, an authentication manager on the network server generates a number or shared secret, using one-time password algorithms. The same number and algorithm are used by the security token on the smart card or device to match and validate the one-time password and user. Many companies use Short Message Service (SMS) to provide a temporary pass-code via text for a second authentication factor. The temporary pass code is obtained out of band through cell phone communications after the user enters his username and password on networked information systems and transaction-oriented web applications. For two-factor authentication (2FA), the user enters his user ID, traditional password and temporary pass-code to access the account or system.

6.11.2 How a One-time Password Works

The encryption and decryption techniques of cyber security are used to generate OTP. We use mathematical Hashed Message Authentication Code (HMAC) algorithm of cyber security to generate OTP-based authentication message. This OTP message is then sent to the user’s registered mobile number. For security reasons OTP values are valid for few seconds of their generations and users should enter them during that specified time to do login to access the resources of the computer system or server. The one-time password is delivered to a user through several channels, such as SMS-based text message, an email or a dedicated application on the endpoint.

6.11.3 Benefits of a One-time Password

The OTP is used to verify and validate the genuine users to allow them to login secure website by using their credentials as well as securely received OTP text message received on the registered mobile number of the user. It is very useful for IT managers IT administrators of any business organization and secures for the users as well as for customers of the company. The advantage of OTP is that they become invalid in seconds thus it prevents unauthorized attackers from obtaining the secret codes and reuse it hack the business data illegally.

Check Your Progress D

Part A: Multiple Choice Questions

1) What is Cyber Crime?
   a) The virus attack
   b) The worm attack
   c) Hacking the system
   d) All the above
2) Use of internet to harass a person or group of individuals known as:
   a) The cabernet
   b) The cyber policing
   c) The cyber stalking
   d) The cyber space

3) We should follow below steps to stop harassment using internet
   a) By installing Anti-Virus
   b) By taking regular back-up
   c) By not clicking on unknown links
   d) All the above

4) An unsolicited mail sent to a large number of persons without their consent, is known as
   a) The worm
   b) The spam
   c) The trojan
   d) The online marketing

Part B: Short Answer Type Questions

1) Explain the term Digitization.

2) What are CAPTCHA’s? Explain their use in user authentication.

3) Explain the impact of digitization & IT Security in Business organizations.
4) What is the full form of OTP? How it is used for online transaction in banking sector?

……………………………………………………………………………………
……………………………………………………………………………………
……………………………………………………………………………………
……………………………………………………………………………………
……………………………………………………………………………………

6.12 LET US SUM UP

Identification, authentication and authorization are the main prerogatives for the data contents security and for the safe communication among the users of the open distributed systems, as well. These measures are performed on the physical and logical level, and special attention is paid to communication between the Internet and intranet. The implementation itself, without adhering to security principles important for their introduction and use, does not guarantee security – neither of the data contents in database, or the one in communication.

Data contents should be protected by means of cryptographic algorithms, where complexity and speed depend on the required security level. The example of this is an electronic signature, the means of accuracy confirmation and message credibility. Authenticity protocols, even complete authentication systems were generated as the means of cryptographic algorithm implementation, security methods and principles (of data contents) in dynamic and distributed systems, which become very important in the case of electronic financial transactions, i.e. electronic cash payment protocols.

6.13 KEY WORDS

**Key:** In cryptography, a key is a piece of information that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into cipher text, and vice versa for decryption algorithms.

**Private Key:** A private key is a tiny bit of code that is paired with a public key to set off algorithms for text encryption and decryption.

**Public Key:** Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.

**Encryption:** Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.
Decryption: Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or un-encrypting the data using the proper codes or keys.

OTP: OTP is a password which can be used only once to login into the computer system and also to make secure online transactions. It is numeric or alphanumerical automatic generated string.

CAPTCHA: CAPTCHA based methods for Human Verification can be roughly divided into text and image-based CAPTCHA, audio CAPTCHA, mathematical CAPTCHA, logic CAPTCHA, and gamification CAPTCHA.

Authentication: Authentication is the process to check the credentials of users before they are given access to use the resources of the system. It is ability to prove that a user or application is genuine on this basis it can use the resources of the organization or network.

Authorization: Authorization is methodology adopted by software companies to allow lawful users to system resources including files, services, computer programs, data and application programs. It is the processes to grant or deny access to a network resource based on the user's identity.

6.14 ANSWER TO CHECK YOUR PROGRESS

Check Your Progress A
1) d 2) d 3) c 4) c

Check Your Progress B
1) d 2) d 3) e 4) a

Check Your Progress C
1) b 2) c 3) b

Check Your Progress D
1) d 2) c 3) d 4) b

6.15 TERMINAL QUESTIONS

1) What is phishing?
2) List some security attacks.
3) Which technique is based on Vernam Cipher?
4) Define Cryptanalysis.
5) What is plain text cipher text and coded text? Explain.
6) Explain digital signature.
7) Define integrity & non repudiation.
8) Explain any two classical ciphers.
9) Explain one time password.
10) What are active and passive attacks? Explain with suitable example.
11) What do you mean DES in cryptography?
12) Explain the use Hash function in cryptography.
13) What do you mean by Private and public key?
14) What do you mean by hackers? Also explain ethical hacking.
15) Discuss Digital Signature.

**Note:** These questions are helpful to understand this unit. Do efforts for writing the answer of these questions but do not send your answer to university. It is only for yours practice.