Chapter 06 : Security, Copyright and The Law

6.0 Overview

Q : 06-00-01 : Define Security ? Describe the means to give access to authorized persons ?

Answer :

Security : Security is a system of safeguards designed to protect a computer system and data from intentional, accidental damage or unauthorized access.

Authorized Access : Authorized persons can access using four approaches :

What you have ? : *You may have a key, badge, token, or plastic card to give you physical access to the locked-up server room or computer building*.

What you know ? : *Standard user-IDs and Passwords or some special combination of numbers are given to the users to logon the machine.*

What you do ? : *Normally, the users put their signatures on the documents to confirm their legitimacy as an authorized user.*

What You are ? : *Biometrics - biological means of identification i.e. fingerprints, voice recognition, eye retina etc.*

Important Note : Loss of hardware and software are not critical. The actual problem lies in the damage / loss of data. It is difficult (though not impossible) to recover it in time in case of transactions based computer systems.

6.1 Virus and Antivirus Issues

Q : 06-01-01 : Define Virus or Worm ? Describe its propagation ?

Answer :

Virus (Worm) : [A virus is a program that attaches itself with other executable files by modifying them so that the virus program is also loaded and executed with the execution of these programs]. A virus usually performs destructive operation by deleting or modifying data stored on the storage devices attached to the computer. A virus is a set of instructions so it cannot physically destroy hardware (common misconception). A virus is "**A destructive program containing code that can generate copies of itself and attaches itself with other program so that it is automatically executed when those programs are executed**".

Q : 06-01-02 : Describe the means through which virus propagates (reaches from one computer to the other) ?

Answer :

Email : Now a days, most of the virus programs spread by attaching themselves with emails. When a user opens such an infected message, virus is loaded into the computers memory and attaches copies with many files. This continues and virus reaches thousands of computers.

Networks : When we download or share files on internet or other networks, the infected files infect the computers.

Removable Storage Media : When we copy data from one computer to another by using a removable media, the infected files are transferred.

Pirated Software :Companies intentionally put some virus program into their software. This program will only activate when it does not find some special files like license files on your computer.

Q : 06-01-03 : Describe important types of viruses ?

Answer :

Boot Sector Virus : The disk is divided into tracks and sectors. Operating system disk has a special program in its first sector called the boot sector. When the computer is turned on, the program in the boot sector is automatically loaded into the memory. The boot sector virus modifies the program in the boot sector and is loaded into memory whenever computer is turned on. The virus is attached with the executable files i.e. .exe, .com an .dll files. When the user uses these executable files, the virus infects other files and performs destructive commands.

Chernobal Virus : The famous chernobal virus deletes all the Microsoft Office files and also the partition information form the disk hence causing a major loss of data.

Logic bomb : Logic bomb, differ From other viruses in that they are set to go off at a certain date and time.

Trojan Horse : The Trojan Horse covertly places illegal, instructions in the middle of a legitimate program. Once you run the program, the Trojan horse goes to work, doing its damage while you are blissfully unaware. An example of a Trojan horse is FormatC.

Redlof : The Redlof virus is a polymorphic virus, written in Visual Basic Script. The virus relies on the Microsoft ActiveX Component vulnerability to automatically execute itself. When executed the virus locates Folder.htt and infects that file.

Important Note

1 : Some viruses may make unnoticeable changes hence corrupting the data being used and some viruses may even make data unusable.

2 : A virus program may detect some special information like passwords, or any sensitive data and send it to some other user on a network.

3 : A virus may make resources and data unavailable to the users. For example, a virus after copying itself on all computers, will start sending data on the network so that other users cannot use the network.

Q : 06-01-04 : Describe the ways, How to safe guard against viruses ?

Answer :

Unknown Email Messages : Never open unknown email messages, and also scan (for virus) all email messages even if you know the sender of the message.

Data Transfer : Minimize the data transfer between computers through the use of floppy disks, flash drives and other removable media. Always scan removable media before using.

Internet : Do not download free-ware programs without first checking it for virus.

Antivirus Software : Always use a virus detecting software to detect and to delete the infected programs from your system. You should periodically update these programs.

Always Keep Backup : Another important way to save yourself from the destruction of virus attack is that you should always keep backup of your data. The backup will be useful if a virus attack deletes your data or modifies it.

6.2 Data Security

Q : 06-02-01 : Explain Data Security ?

Answer :

Data Security : The means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy and protect personal data.
Offering protection from data theft and data loss.
Protecting data from deliberate or accidental access by unauthorized persons.

Q : 06-02-02 : Describe the ways the Data Security may be violated ?

Answer :

Data Security Violations :

Physically Breaking Into Computer Center / Room : Someone may break into the computer room and take away all storage devices housing the sensitive data.

Unauthorized Access : Unauthorized users may take access to personal data of someone and then use it to gain some advantage. By accessing credit card number, online shopping from others account.

Unauthorized User : Unauthorized user may use an online mail server, like mail.yahoo.com to view email messages of other users hence causing privacy issue.

Virus on Network : Someone can send a virus onto a network causing the network to become very slow or even unusable.

Unauthorized Access to Bank Accounts : Some users may gain unauthorized access to bank accounts and transfer of money from other accounts to their personal accounts.

Computer Becomes Unavailable to Authorized Users : A person may make a computer so busy by sending many requests so that the computer becomes unavailable to authorized users. Its called denial of service situation.

Q : 06-02-03 : Describe the main threats to Data Security ?

Answer :

Security Threats :

Unintentional Damage : Some authorized user of the data may unintentionally delete or change sensitive data. Assigning proper rights to users and periodical backup can minimize the loss.

Proper Password Protection : Proper password protection should be used to access any resource. A log file should also be maintained to keep track of all the activities on the data / files.

Encryption Algorithm : Encryption algorithm should be used, so that if someone gets access to the data, he / she should not be able to make any sense out of it.

Virus Scanning Software : Proper virus scanning software should be used to scan all data coming into the organization.

Safe Rooms : Computers and all hacking storage devices should be placed in locked rooms with only authorized access to these resources.

Periodically Change Passwords : Authorized users must he asked to change their passwords periodically.

Q : 06-02-04 : Describe Data Protection ?

Answer :

Data Protection :

Prevention of misuse of computer data; legal safeguards to prevent misuse of information stored on computers, particularly information about individual people.
Installation of safeguards for computer data: the adoption of administrative, technical, or physical deterrents to safeguard computer data.

Q : 06-02-04 : Describe Data Privacy Issue ?

Answer :

Data Privacy Issue :

Right to See Personal Data : An individual has a right to see the data kept about him.
Right to Stop the Processing : He has the right to stop the processing of his data by the organization.
Compensation for Discloser : He has the right to claim a compensation from the organization for any kind of disclosure of data disallowed by the law.
Discloser is a Crime : No worker of the organization is allowed to disclose or use the data kept by its organization, failing to abide by, is committing a crime.
Safeguard Against Crime : Data protection act tries to minimize the misuse of personal information to provide a safeguard against such crime.
Adequate / Necessary Data : An organization collecting data should collect only the data adequate and necessary for its working and should not collect un-necessary data.

Q : 06-02-05 : Describe the points necessary to ensure Individual's Privacy ?

Answer :

Individual's Privacy :

Responsibility : The organization is responsible for keeping the data updated.
Life of Data : The organization should keep data for the specified period of time only and can not keep it longer than necessary.
Rights of Individual : During the processing of data, the rights of the individual should not be violated.
Security of Data : The organization is responsible for all kinds of security of data.

6.3 Data Protection Legislation and Copyright Issues

Q : 06-03-01 : Define Data Protection Legislation ? And state principles of Data Protection Act ?

Answer :

Data Protection Legislation : [The data protection legislation defines the laws that ensure data protection]. Many countries have defined the data protection legislation and in some advanced western countries; this law is enforced properly as well.

The Principles of Data Protection Acts :

Purpose : The purpose of keeping and distributing personal data must be clearly defined by organization obtaining that data.
Identity of Keeping Organization : The individual must be informed about the identity of the organization / individual maintaining data.
Necessity : The processing is necessary to fulfill the contract between two parties.
Individual's Interest : The processing is required by law or is necessary to carry out interest of the individual.

6.4 Important Privacy Acts

Q : 06-04-01 : Describe various Important Privacy Acts ?

Answer :

The 1980 Privacy Protection Act : This prohibits agents of federal government from making unannounced, searches of press office if no one there is suspected of a crime.

The 1984 Cable Communications Policy Act : This restricts cable companies in the collection and sharing of information about their customers. The "Data Protection Act 1984" is intended to protect the individual from unauthorized use and disclosure of personal information held on a computer system.

It consists of eight principles :

Fair / Lawful Processing : The information shall be obtained and the data shall be processed, fairly and lawfully.

Specified and Lawful Purpose : Personal data shall be held only for one or more specified and lawful purposes.

Incompatible Use / Discloser : Personal data held for any purpose shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

Adequate / Relevant Holding : Personal data held for any purpose shall be adequate, relevant and not excessive in relation to that purpose(s).

Accurate and Up To Date : Personal data shall be accurate and kept up to date.

Duration : Personal data held for any purpose(s) shall not be kept for longer than is necessary.

Entitlement : An individual shall be entitled, at reasonable intervals and without undue delay or expense, to be informed by any data user whether he holds personal data of which that individual is the subject.

Security : Appropriate security measures shall he taken against unauthorized access to, or alteration, disclosure, accidental loss, or destruction of personal data.

The 1987 Computer Security Act : It makes actions that affect the computer security files and telecommunication illegal.

The 1988 Video Privacy Protection Act 1988 : It prevents retailers from disclosing a person's video rental records without a court order; privacy supporters want the same rule for medical and insurance files.

Computer Matching and Privacy Protection Act of 1988 : It prevents the government from comparing certain records in an attempt to find a match. However, most comparisons are still unregulated.

The Computer Misuse Act 1990 : It makes provision for securing computer material against unauthorized access or modification; and for connected purposes. It was passed to deal with the problem of hacking of computer systems. This was introduced to recognize three key offences :

Unauthorized access to computer material.

Unauthorized access with intent to commit or facilitate commission of further offences.

Unauthorized modification of computer material.

The 1998 Data Protection Act : It came into force early in 1999 and covers how information about living identifiable persons is used. The 1998 Act applies to :

Computerized personal data.

Personal data held in structured manual files.

It applies to anything at all done to personal data (“processing”), including collection, use, disclosure, destruction and merely holding personal data.