Protection of information assets

Q. Global Positioning System (GPS) is one of the most commonly used applications in modern communication systems.
Required:
(a) Briefly explain GPS. (03)
(b) From the list given below, rank three organisations which have most extensive usage of GPS. Explain the reason for your selection or omission in each case.
(i) Manufacturing company
(ii) Bank
(iii) Insurance company
(iv) Shipping company
(v) Ambulance service (04)

(a) A Global Positioning System (GPS) consists of one or more earth-based receivers that accept and analyse signals sent by satellites in order to determine the receiver's geographic location. A GPS receiver is a handheld or mountable device which can be secured to an automobile, boat, airplane, farm and construction equipment or a computer. Some GPS receivers include a screen display that shows your position on a map. Other GPS receivers send location information to a base station, where humans can give you personal directions.

(b) Ambulance service, shipping companies and insurance companies can use GPS in more important ways as discussed below:

Rank	Organisations	Reason for selection
1	Ambulance service.	The GPS is helpful in saving lives and rescuing people in need as the ambulance driver could use it to find the best possible route and/or to create a map to its destination. In some cases, the ambulance service could track the people in need of help i.e. on motorways, etc
2	Shipping company	GPS could be used in tracking of vessels which can help in providing assistance if necessary and knowing in advance about possible delays.
3	Insurance company.	The insurance company could use GPS to track lost/stolen assets embedded with GPS

Manufacturing companies and banks also use GPS but in most cases their use is in less critical areas.

Case study: Life Care Hospital (LCH) is one of the largest and best equipped hospitals of the country. Recently the IT system of LCH was hit by a ransomware that halted its functions, including consulting clinics, retail pharmacy and patients' operations. The hackers demanded ransom of Rs. 300,000 for recovery of entire data; however, LCH management rejected their demand and decided to retrieve the data from its backup. It started gradual recovery after
almost 24 hours and it took about a month in getting everything back to normal. LCH suffered an estimated loss of Rs. 25 million in revenue during this period.
Required:
(a) What are ransomware and how they work? Discuss LCH's decision to reject the hackers' demand. (06)
(b) Suggest course of action for LCH to mitigate the possibility of similar attack in future and to minimise the impact in case of any eventuality. (08)

Ransomware is malware that creates encrypted copies of files on the victim's computer and deletes the originals, leaving the victim with only the encrypted copies, which cannot be accessed without a decryption key. Data message are sent by hackers on victims' machine advising them to pay a certain amount mostly through virtual currency to prevent their files from being deleted permanently.

Ransomware exploits the unpatched vulnerabilities of the operating system. These are usually sent through emails. Once a user clicks on the link sent in the email, it gets downloaded and activated on that system. Some ransomware has the capability to replicate them onto the network and ultimately lock down the entire network.

Though LCH has to bear more than eighty times the financial loss, its decision to reject the hackers demand was correct as:

- To bow against criminals' demand is not correct. It strengthens them for more serious crimes.
- Some ransomware operators refuse to unlock the data even after receiving payment and demand more money or attempt to defraud the victim by other means with the financial information provided to them.
- LHC management may be confident to recover the data and restore the system in an acceptable time.
- LHC management might have made incorrect estimate loss in revenue.
- Paying the ransom could have adversely impact LHC reputation much more than the financial loss.

(b) LCH should follow the following course of action to mitigate the possibility of similar attacks:

(i) Review the adequacy of backup, recovery and continuity plan according to data and system classification and make necessary changes, if required.

(ii) Review the adequacy of installed antivirus and related security software.

(iii) Review the installed operating systems and upgrade any outdated operating systems.

(iv) Review the policies and configuration of firewall and routers and make necessary revisions.

(v) Review email and download policies. Prohibit download of executable files.

(vi) Configure automatic update of security patches and updates of operating systems, antivirus and related security software.

(vii) Review the listing of all application and system software and uninstall any unwanted software installed on the network.

(viii) Place centralised control over distribution and installation of software.

(ix) Regularly scan user PCs, either from the LAN or directly, to ensure that unwanted software have not been installed on their PC.

(x) Conduct users' training sessions to make them aware of such threats, and measures to prevent such threats.

(xi) Implement network monitoring mechanism and investigate any suspicious activity on network.

(xii) Develop and implement incident response mechanism to minimise the impact if similar situation is faced in future.

(xiii) Perform periodic risk assessment exercise for on time identification and resolution of emerging threats similar to ransomware.

Besides Scanners (P-266) , other types of antivirus software are described below:

(i) Active Monitors:

- They interprets DOS and ROM basic input-output system calls, looking for virus like actions.
- Active monitors can be annoying because they cannot distinguish between a user request and a program or virus request, so users are asked to confirm their action such as formatting a disk or deleting a file or set of files.

(ii) Integrity checkers:

- They compute a binary number on a known virus free program that is then stored in a database file. The number is called a cyclical redundancy check (CRC). When that program is called to execute, the checker computes the number and compares it to the number in the database. A match means no infection.
- They can detect virus only after infection has occurred. Further, they are ineffective against new files, copied/downloaded from somewhere else, that are already virus-infected.

(iii) Behavior blockers:

- They focus on detecting potentially abnormal behavior like writing to the boot sector or the master boot record, or making changes to executable files.
- They are not very effective in detecting worms.

(iv) Immunizers:

 They defend against viruses by appending sections of themselves to files; somewhat in the same way that file viruses append themselves. They continuously check the file for changes and report changes as possible viral behavior.
 Application of immunizers is not always practical since it is not possible to immunize files against all known viruses.

Although updated antivirus software has been installed on all computers of TA, it lacks sound policies and procedures to prevent viruses. Further, new viruses keep on coming and an updated antivirus may not detect all of them.

Weaknesses that may cause penetration of viruses into TA's LAN are discussed below:

Weakness	**Safeguards**
All users have installation rights	Installation rights should be restricted to limited users, say to IT support staff. Other users should seek their assistance for installation purpose.
Free games, clips and other media contents downloaded from social networking sites may contain viruses, some of which may not be detected by the installed antivirus software	Define appropriate policy in the firewall to blacklist websites that are more prone to viruses.
	Create awareness among users as regards downloading precautions. Always scan the downloaded contents with antivirus before use.
Viruses may be transported from clients' USBs into TA's systems. Similarly TA's USBs inserted into clients' systems may also import viruses in them and export these to TA's LAN when inserted into TA's systems.	There should be a separate standalone system with updated security patches and antivirus software. That system should be used for exchanging data with clients. All USBs exposed to other systems must be scanned first at that system and if no virus is found, they may be inserted into staff system.
Besides periodical virus scanning, the antivirus software always prompts to run a scan whenever a USB device is attached to a system. The user may ignore the alert and continue without scanning the USB.	The users should be trained to never ignore scan message and consider all aspects before deciding to forego the scan.
As there is no restriction on USB ports, the users may access internet by inserting portable internet devices and hence by pass firewall restrictions.	Prohibit use of Internet USB devices.
	Periodically scan users' machines for detection of prohibited software.
	Associate disciplinary action on detection of any violation.
Antivirus and firewall policies may not be updated.	Review antivirus and firewall policies at periodic intervals.
	Besides periodic review, these policies must be reviewed in case of major changes in IT infrastructure e.g., acquisition of new hardware or software.
Existing antivirus software may not be able to defend against new viruses.	Compare existing software with other available antivirus software and change it if it is performing below par.

The **techniques** which are most commonly **used by hackers** to affect the availability of e-banking websites are Denial-of-Service (DoS) and Unauthorised Privileged Access.

A **DoS** attack involves saturating the target machine with external communications requests, so that it cannot respond to legitimate traffic, or responds so slowly that for all practical purposes it becomes unavailable.

In **Unauthorised Privileged Access**, the attacker penetrates into the website by guessing its administrative password using different techniques such as brute force or dictionary attacks, removes the actual contents from the website, displays his own contents and making the website unavailable to its users.

Good practices to reduce risk from DoS and Hacking include:
(i) Webservers should not be run close to full capacity. Available processing capacity and storage space would provide flexibility and increase fault tolerance in the event of a DoS attack.
(ii) Packet filtering should be used to prevent obviously forged packets from entering into the company's network.
(iii) Keep the operating systems on the hosts updated and patched.
(iv) Keep the website's administrative password strong and change it periodically.
(v) Arrange periodic penetration testing of the website by a third party.
(vi) Periodic risk assessment and vulnerability management of hacking and DoS attacks should be made.
(vii) Network monitoring and traffic analysis tools should be installed.

Phishing is the **most commonly used social engineering technique** to victimise bank customers. Phishers attempt to fraudulently obtain sensitive/confidential information such as login credentials (User IDs and Passwords) and credit/debit card numbers including PIN codes and CVT numbers. They do so mostly by presenting themselves as genuine, trustworthy individuals mostly representing the customers, bank or any other well-known and trusted institution. Phishing is generally carried out through emails or instant messages, although phone contact has been used as well.

The bank may take the following measures to help its customers in avoiding phishing:
(i) Provide general awareness of social engineering including phishing to its customers through its website, emails, letters and awareness sessions.
(ii) Advise customers to enable phishing filter in their web browsers.
(iii) Advise customers to never respond to suspicious phone calls or emails asking them to disclose their secret information such as User IDs, passwords, credit/debit card details etc.
(iv) Advise customers to alert the bank if they receive any phone call or email as described above.
(v) Set up a security help desk that can respond to alerts from the customers.

The firewalls **may not succeed** in all setups due to one or more of the following **reasons**:
(i)The firewall is poorly configured or miss-configured.
(ii)If proper testing processes/procedures are not carried out to monitor firewall security.
(iii)The organization relies too much on perimeter firewall security.
(iv)All traffic is not required to pass through the firewall.

Bastion Host Configuration:
In this configuration all internal and external communication must pass through the bastion host. The bastion host is exposed to the external network; therefore it must be locked down, removing any unnecessary applications or services. It can use filtering, proxy or a combination. It is not a specific type of hardware, software or device.
Screened Host Configuration:
This configuration generally consists of a screening router (border router) configured with access control lists. The router employees packet filtering to screen packets, which are then typically passed to the bastion host and then to the internal network. The screened host (the bastion host in this example) is the only device that receives traffic from the border router. This configuration provides an additional layer of protection for the second host.

Screened Subnet Configuration:
The bastion host is sandwiched between two routers (the exterior router and the interior router). The exterior router provides packet filtering and passes the traffic to the bastion. After the traffic is processed, the bastion passes the traffic to the interior router for additional filtering. The screened subnet provides a buffer between the internal and external networks. This configuration is used when an external population needs access to services that can be allowed through the exterior router, but the interior router will not allow those requests to the internal network.

Proxy Firewall: A proxy firewall works as an intermediary between in-house clients and servers on the internet. All packets passing to the network are delivered through the proxy. The communication is checked for access authorization according to a rule-base and then passed to the receiving system or discarded. A proxy impersonates the internal (receiving) system to review packets before forwarding.
A proxy firewall can look at all the information in the packet, all the way to the application layer whereas a packet filtering firewall can look into just the header of the packet and compares the header information against its rules.
A proxy firewall inspects all seven OSI layers of network traffic whereas packet-filtering firewall is restricted to OSI layer 3 (Network Layer). The above differences between proxy and packet filtering firewall clearly show that a proxy firewall provides greater degree of protection and control than packet filtering firewall and hence ET should deploy it instead of packet filtering firewall.

Measures to reduce vulnerabilities of the operating system:
Software-based firewalls are installed on top of an operating system. The operating system may have its own vulnerability. A robust and fully functioning operating system poses a greater risk of firewall compromise. To mitigate this risk,
(i) either the operating system should be properly locked down and a process should be in place to ensure continued installation of security patches. Any unnecessary services or applications, as well as, unneeded protocols, must be removed or disabled from the operating system; or
(ii) the firewall software should be installed onto a system using an operating system that has very limited functionality, providing only the services necessary to support the firewall software.

Importance of other two suggestions:
The implementation of other two suggestions is equally important because if network users are allowed to bypass firewall while connecting to Internet or are allowed to access the Internet through separate Internet devices, they would not be subject to the firewall security policies. It will make the entire network vulnerable to external threats and the deployment of firewall will become ineffective.

Measures to mitigate the insiders' threats to its IT resources and the main objective/benefit of each such measure:

(i) Carry out periodic risk assessments of the entire organization: Periodic risk assessment procedure helps to identify new risks and update the managements understanding.
(ii) Carry out periodic security awareness training for all employees: If the employees are trained and understand security policies and procedures, and why they exist, they remain motivated to follow the policies and avert security lapses.
(iii) Enforce segregation/separation of duties: This reduces the possibilities of collusion and fraud.
(iv) Monitor and respond to suspicious or disruptive behavior: In addition to monitoring online actions, organizations should closely monitor other suspicious or disruptive behavior by employees to ensure that any potential loss is avoided.
(v) Deactivate computer access immediately after termination of employees or their transfer to another job/department etc: Immediate deactivation policy is essential to avoid lapses and slackness.
(vi) Controls on usage of CDs and USBs: Restricting the use of CDs and USBs etc. to authorized personnel only on need basis with proper monitoring reduces the risk of viruses and information theft.

The **information security policy** typically contains:
(i) a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing.
(ii) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives.
(iii) a framework for setting control objectives and controls, including the structure of risk assessment and risk management.

(iv) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization including:
 compliance with legislative, regulatory and contractual requirements
 security education, training and awareness requirements
 business continuity management
 consequences of information security policy violations
(v) a definition of general and specific responsibilities for information security management, including reporting information security incidents.
(vi) references to documentation which may support the policy; e.g. more detailed security policies, standards, and procedures for specific information systems or security rules with which users should comply.

The ISP should be **reviewed** when significant changes occur in the IT function and related technologies. Even if there is no such significant change the ISP should be reviewed at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The review of ISP should include:
 identifying weakness in the current policy and assessing opportunities for improvement to the policy.
 assessing the completeness of ISP and the approach to managing information security in response to the change in organizational environment, business circumstances, legal conditions or technical environment.

The Information Security Policy (ISP) should be **communicated** to all employees, service providers and business partners/suppliers. The IS auditors may use it as a reference framework for performing various IS audit assignments.

Case study: You have been appointed as a consultant by Nava Communications (NC) which recently faced a network security breach as User IDs and passwords of all the employees were published by a hacker on the individual's web page. During the initial discussion, the management has identified that the following controls are in place to avoid such instances:
(i) The network is protected by a well configured firewall.
(ii) There is a central repository for Antivirus from where antivirus definitions on all computers on the network are periodically updated.
(iii) Complex password policy is in place.
(iv) All users have been assigned a unique User ID and password.
(v) There exists a shared network drive on the data server, on which the users can create their own folders and share their data with other users. No individual user can otherwise access any other user's computer through LAN.
While going through the previous IS audit report, you noted that the auditor had recommended NC to undertake a penetration testing exercise; however, this exercise has not been carried out to this date.

The hacker may have been able to penetrate NC's network due to following reasons:
(i) Though the firewall was well configured, its default password may not have been changed. This gives hacker an easy opportunity to break in the network.
(ii) The firewall logs may not be reviewed vigilantly or may not be reviewed periodically at an appropriate level. Hence any unauthorized attempt to violate the firewall policy may remain undetected which gives hacker ample opportunity to find and exploit the weaknesses in the firewall policy.
(iii) There may exist some systems on the network that may connect to the Internet bypassing the firewall. Such systems give the hacker a firewall free passage to attack the network.
(iv) The method and periodicity of antivirus repository updates is not specified. The larger the difference between two successive updates of antivirus repository, the greater the chances for a hacker to inject his code in the system.
(v) No software is installed at NC that can analyse and detect files/objects with suspected behavior. This gives rise to the possibility of advance attacks like zero-day or advanced persistent threat attacks as having a properly configured firewall and updated antivirus definitions are not capable to counter such attacks.
(vi) Users may not be aware of the risks associated with sharing of passwords and or keeping a common password for official and all personal/social networking sites. Such mistakes by users give hackers an opportunity to exploit.

(vii) Controls as regards the terminated employees are not specified. If the user IDs of terminated employees is not deleted immediately, such employees may access the company's network using their credentials.
(viii) Users may not be aware of the risks of storing confidential documents on the shared drive. Some high privilege user may have stored such information on the shared network drive which may have been exposed to low privilege users and hence reached in the hands of unauthorized users.

Penetration Testing: A penetration test is an authorized, carefully managed and structured analysis of the security of a system or network. The purpose of a penetration test is to simulate the type of attack that an unethical hacker would conduct in order to determine if the client is vulnerable to a hacking attack.
NC should undertake penetration testing because it would help to:
(i) determine the effectiveness of the security controls NC has put into place;
(ii) determine the vulnerabilities relating to a particular threat;
(iii) alert the upper management to the security threat that may exist in its systems or operations;
(iv) identify the areas for improvement or areas where additional countermeasures are required;
(v) regain its lost trust and confidence after the network security breach and enhance its position in the marketplace; and
(vi) fulfill the audit recommendation.

Benefits of Penetration Testing
(i) Goes beyond surface vulnerabilities and demonstrates how these vulnerabilities can be exploited iteratively to gain greater access.
(ii) Allows for testing the susceptibility of the human element by the use of social engineering.
(iii) Enables testing in real environment.
(iv) Demonstrates that vulnerabilities are not just theoretical.
Risks of Network Penetration Testing
(i) It may slow the organization's network response time.
(ii) The possibility exists that systems may be damaged.
(iii) Sensitive information may be disclosed.
(iv) Some unknown backdoors may be created.
(v) Future attackers may be created because, it gives an idea to employees "How to hack?"
Five components of an Information System are as follows:

Sr.no	Component	Associated key security issues	Controls
1	Software comprising of applications, operating systems and other utilities software.	Undetected errors/bugs. Failure to incorporate security features at the development stage. Back doors left by developers	Thorough testing. Keeping security features at the time of development. Independent review of source code. / Security assessment.
2	Hardware comprises of computers, printers, switches etc.	Theft. Unauthorized access .	Lock and key including casing locks and door locks. Restricted access.
3	Data	Lost/deleted. Corrupted. Leaked. Modified.	Encryption. Passwords. Restricted access.
4	People	Errors. Override controls. Social engineering.	Checks. Controls. Training.
5	Procedures comprises of defined/documented instructions for using computer systems and implementing	Inadequate. Obsolete/outdated. Leaked.	Review. Timely updation. Dissemination on need-to know basis.

	controls		

How would you verify the effectiveness of policies given below?

Password policy:

 Check whether appropriate controls over setting of password are in place to avoid the use of weak passwords.

 Check whether password settings include maximum age and password history, e.g., password may be changed after every 30 days and that new passwords should not be any of the last ten passwords.

 Check whether password policy includes appropriate account lockout e.g., users accounts may be locked after certain number of unsuccessful attempts and then unlocking is only done by the administrator after investigation.

User access authorisation policy:

 Check whether user accounts for new recruits (joiners) are set up only on appropriate formal/documented authorization.

 Check whether user accounts of Terminated (leavers) and/or Transferred employees have been disabled/removed from the network and all applications, as appropriate.

 Check whether User Authorisation Matrix (UAM) exists and is updated.

Monitoring of logical access control procedures:

 Check whether system generated log is maintained for each logical access attempt i.e., for both success and failure.

 Check whether logical access logs are checked at appropriate level.

 Check whether logical access logs can be edited.

Information Security incident handling procedures:

 Assess the adequacy of procedures for timely reporting, resolution and containment of the security incidents.

 Interview relevant users and assess their understanding as regards the said procedures.

 Enquire about any past security incident and review its documentation to check how it was handled.

Case Study: Your firm is conducting IS audit of Bolan Foods Limited (BFL). The observations reported by the audit staff and response of the IT head are given below:

Observation (i): Certain key functions are performed by sharing User IDs.

Response of the IT head: During the last month, few key employees left BFL and presently their work is being performed jointly by their respective team-mates who share the workload as per their convenience. Therefore, for the time being, such User IDs are being used by more than one person of the respective teams.

Observation (ii): As per BFL's IT policy, staff is prohibited to use instant messaging service, browsing social networking sites and downloading all types of files. While testing the compliance of Internet use policy, it was observed that staff of IT department has unwritten immunity from the policy.

Response of the IT head:

His team uses instant messages to exchange views with their professional friends, during development and support activities. They often get very useful tips for their work from social sites and discussion forums. Moreover, the permission to download files is necessary as they have to download various types of security patches/updates and virus definitions regularly. Rest of the users are not allowed these relaxations as their productivity is likely to be affected as well as it is likely that most of them would misuse such rights and unnecessarily occupy the Internet bandwidth.

Following **implications** may arise due to **shared User IDs:**

(i) User accountability may not be established.

(ii) An unauthorized user may use the shared User ID to gain access to confidential or critical records.

(iii) It may encourage others users to share their User ID as and when needed.

(iv) It also increases the risk (though not with certainty) that passwords are not changed frequently.

Risks and their corresponding implications, if BFL allows its all employees to visit social networking sites and/or discussion forums, are as follows:

Risks	Implications
They may click on links, promotions and advertisements running on the social networking sites without understanding the consequences.	Some such links may cause virus/malware attacks or make them victim of hacking.
They may share their social networking site's login credentials with their family members, friends or associates. Sometimes people use same or similar passwords for personal and official use.	Sharing of login details may ease hackers to break into the organization's computer network.
Hackers may gather employees' personal information from such sites like date of birth, names of children and spouse etc.	These may be used to compromise organization's logical security.
Employees of IT department may share the source code of some proprietary program or key of a licensed program on a discussion forum or a social networking site.	This may lead to legal repercussion and or give way to hackers to compromise the organization's logical security.
Employees may become victim of social engineering.	They may share some confidential information on a social network/discussion forum. They may experience identity theft.
Some employees may post negative or offensive comments on social / professional forums.	Such comments may cause legal repercussions and/or negative impact on the public image of the organization.
Some employees may accept contact invitation from people they do not know.	Making such blind contacts may share their personal information available on social networking sites with the employees of competitor and or hackers.

Risk (i), (iv) and (v) may be avoided/mitigated if the employees are strictly prohibited to visit such sites from office.

Comments on IT head's response on observation (i):

The IT head's comments seem unreasonable. The practice followed is not correct. It should be ensured that User IDs should not be shared. If certain key functions are to be performed jointly by different users then instead of sharing the user account, such users should be given rights to perform those functions using their own IDs.

Comments on IT head's response on observation (ii):

There may be some exceptions to the policy; however, all such exceptions must be documented. Use of instant messaging services must be restricted and allowed only on genuine reasons with prior authorization. Employees of all departments, including IT department, are equally vulnerable to the risks associated with the social networking sites. Moreover, as in the case of IT employees there may be exception requirements in the case of other employees also. Hence browsing of social networking sites and discussion forums may be allowed in a controlled manner by guiding all users (providing a comprehensive policy) about the risks associated with such sites and precautionary measures to minimize such risks. Risk of losing productivity and misusing the download facility is equally applicable for employees of IT department.

For all kind of security patches/updates and virus definitions, a list of trusted sites should be developed and incorporated in the firewall policy. Employees of IT department may be allowed to download the security updates and virus definitions from trusted sites only. On other sites, download of certain file types like executable, video and audio should not be allowed to any employee, unless authorized by appropriate authority on genuine reasons.

Computer based crimes are used to steal money, goods, corporate information, etc. Some of the common methods used to commit a computer crime by the perpetrators are Rounding Down Technique, Phishing, Denial of Service and Brute-force Attack.

Rounding Down Technique: It involves drawing off small amounts of money by rounding down small fractions of a denomination and transferring these small fractions into an unauthorized account.
The risk could be mitigated by periodic generation of reports identifying the accounts where often very small amounts are being credited and by checking the trail of those amounts. Such reports must be reviewed at an appropriate level.
Phishing: Phishers attempt to fraudulently acquire sensitive information, such as user name, password and credit card details by masquerading as a trustworthy entity in an electronic communication, sometimes phone contact has been used as well. For example, by posing as a banker, regulator, friend etc.
Such risk could be mitigated by creating awareness among users about such risks and giving them useful tips like any bank official is not authorized to ask a customer's PIN.
Denial of Service Attack: It is an attack that disrupts, denies or slows the services to legitimate users, networks, systems or other resources. It can be done in many ways, for example, by subjecting a network to hostile pinging by different attackers over an extended time period.
Appropriate network and firewall policies can be helpful to prevent or minimize the effect of such attacks, for example, blocking the unusual traffic inflow or alerting the network administrator about any unusual network activity that is consuming more than normal network resources. Regular scanning of network through appropriate antivirus with updated definitions may also detect such attacks. Developing clustered systems also mitigate the impact of such threats, however, active clustering is usually restricted to servers.
Brute Force Attack: Such attacks are launched by an intruder, using many of the password-cracking tools which are available at little or no cost, to gain unauthorized access to an organization's network.
Possibility of the success of such attacks can be mitigated by limiting password input attempts and or generating an image containing some random text which the user is required to input before entering the password.

Social Engineering is the act of interacting with people and deceiving them to obtain important/sensitive information or perform any other act that is harmful.
A social engineer can use the phone, the Internet, or even show up personally to induce a person to disclose ID number, username, password, server name(s), machine name(s), remote connection settings, schedules, credit card number(s) etc.
Piggybacking, shoulder surfing, faux service, dialing for passwords, bribery, fascination and bullying are some examples of social engineering.

Phishing attacks use email or malicious web sites to solicit personal, often financial, information Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing can be **avoided** by taking following measures:
(i)Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
(ii)Do not provide personal information or information about your organization, unless you are certain of a person's authority to have the information.
(iii)Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
(iv)Don't send sensitive information over the Internet before checking a website's security.
(v)Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
(vi)Ongoing security awareness program can be helpful in creating awareness among employees about phishing attacks.

Single sign-on: Single sign-on (SSO) is a user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications whose rights have been given to him and eliminates further prompts when they switch applications during a particular session.
The information resource or SSO server handling this function is referred to as the primary domain. Every other information resource, application or platform that used those credentials is called a secondary domain.

SSO **advantages** include:
(i)It reduces the time taken by users to log into multiple applications and platforms.

(ii)Multiple passwords are no longer required; therefore; a user may be more inclined and motivated to select a stronger password.
(iii)It reduces administrative overhead in resetting forgotten passwords over multiple platforms and applications.
(iv)It improves an administrator's ability to manage users' accounts and authorizations to all associated systems.

SSO **disadvantages** include:
(i)The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information assets.
(ii)The costs associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary.
(iii)Support for all major operating system environments is difficult. SSO implementations will often require a number of solutions integrated into a total solution for an enterprise's IT architecture.

Voice-over Internet protocol (VoIP), also known as Internet telephony, is a technology that enables data packet networks to transport real time voice traffic. VoIP makes it possible to have a voice conversation over the Internet or any dedicated IP network instead of dedicated voice transmission lines. Sounds are digitized into IP packets and transferred through the network layer before being decoded back into the original voice.

Disadvantages related to the use of VoIP
(i) It is more prone to virus attacks.
(ii) Possibility of hacking and disclosure of sensitive information may increase.
(iii) Denial of service on account of flooding of the data network.
(iv) Extra cost of infra-structure.

Best practices for handling 'Classified Information' include:
(i) Classification of information must be communicated to all users.
(ii) As far as possible, classified information should be kept in encrypted form.
(iii) Access to classified information should be given on need to have basis.
(iv) Classified material shall not be taken home/outside the office premises.
(v) Classified working papers such as notes and rough drafts should be dated and inventoried.
(vi) Classified information should not be disposed of in the waste basket. It must be placed in a designated container for destruction by shredding or burning etc.
(vii) When information is transmitted from one official to another, the receipt should be recorded and acknowledged.
(viii) Classified information should be kept under an approved security arrangement.
(ix) Activities of users should be logged while they are accessing classified information and the logs should be reviewed periodically.
(x) At the end-of-day a security check should be conducted to ensure that all classified material is properly secured.

The **benefits** of maintaining the classification of information assets are as follows:
(i) It helps in identifying the appropriate level of access controls to each class of information asset.
(ii) It reduces the risk and cost of under or over protecting information resources.
(iii) Formulation of a consistent and homogenous policy for the security of information assets, throughout the organization.
(iv) Assists in formulation and implementation of appropriate DRP and BCP policies.

Benefits of good privacy controls
- Protecting the organization's public image and brand.
- Protecting valuable data of customers and employees.
- Achieving a competitive advantage in the market place.
- Avoiding legal repercussions.
- Promoting confidence and goodwill.

Best Practices
- Performing adequate and regular privacy risk assessments.
- Developing awareness among the users about the need to follow the specified procedures.

 Proper implementation of login IDs and passwords.
 Masking personal identification numbers and other sensitive information when possible.
 Creating awareness about Web, and e-mail vulnerabilities.
 Developing record retention and destruction policies.
 Implementing a data classification scheme based on the sensitivity and data mapping.
 Implementing intrusion detection and prevention technologies.
 Control over use of removable media.
 For keeping safe custody of the laptops, undertaking is to be signed by employees carrying company's laptop.
 Supervising and training staff to prevent social engineering and similar risks.
 Establishing a privacy ombudsman, officer, or organization to be available to act as the focal point for the coordination of privacy-related activities and the handling of complaints and issues.

Case study: Jay Tech provides cloud and mobile app solutions and is planning to construct a centralized Data Centre to connect its offices across the country. Management has formed a committee to evaluate different tasks of this assignment. One of the tasks which the company is looking at is the physical exposure which the Data Centre may face.
Required:
(a) Identify any six physical exposures which may be faced by the Data Centre. (03)
(b) Identify four types of perpetrators who may physically perpetrate the Data Centre without authorization. (02)
(c) Suggest any two controls to minimise the risks presented by each exposure identified by you in part (a) above.

(a) The Data Centre may face following physical exposures:
(i) Unauthorised physical access
(ii) Fire damage
(iii) Water damage
(iv) Energy variation
(v) Environmental threat (temperature and humidity)
(vi) Terrorist attack
(vii) Accidental damage
(viii) Natural threats (earthquake, flood, torrential rains etc.)

(b) Following types of perpetrators could physically perpetrate the Data Centre without authorization:
(i) Professional intruders
(ii) Interested/informed outsiders
(iii) Accidental ignorant person
(iv) Employees
 Former employees
 Existing employees - facing financial/emotional problems
 Existing employees - threatened for disciplinary action/disgruntled

(c) Controls to minimise the risks presented by the exposures identified in part (a) are as follows:

Physical exposure	**Mitigating Control**
Unauthorised physical access	Placing security guards at the main entrance. Building deadman doors. Restricting main entrance access with RFID card enabled electronic/electronic password/biometric lock. Installing surveillance cameras to monitor the entire facility.
Fire damage	Placement of fire exit map and emergency helpline numbers at prominent places. Installation of both manual and automatic fire alarms throughout the facility. Installation of automatic fire extinguishers at strategic places agreed with the clients.

	□ Periodic inspection and testing of fire suppressing system.
Water damage	□ Proper drainage system throughout the facility. □ Installation of water alarms at strategic places agreed with the clients. □ Raised floors.
Energy variation	□ Installation of voltage stabilisers/regulators and circuit breakers. □ Installation of UPS. □ Arrangement of alternate power supply i.e., generator.
Environmental threat (temperature and humidity)	□ Installation of temperature monitoring system. □ Periodic inspection of air conditioning system.
Terrorist attack	□ Placement of secure barriers □ Controlled physical access to the facility. □ Installation of walk through gate. □ Installing surveillance cameras to monitor the entire facility.
Accidental damage	□ Restricting food items and drinks in the clients' area. □ Placement of hardware in an intelligent manner with minimum chances of accidental damage.
Natural threats (earthquake, flood, torrential rains etc.)	□ Selection of venue in less affected area. □ Insurance cover.

Q. Modern Hospital (MH) has ninety computers, including three servers, which are connected through LAN. There is one vacant network point in each department and in each of the four wards. Senior doctors use these points for connecting their laptops to the network to view patients' history. Internet facility is available to all users through LAN. Entrance to server room is through IT Manager's room. MH has deployed customised user access control software developed by a local software house.
Required:
(a) Identify any five physical access controls which could help to ensure physical security of the server room. (05 marks)
(b) Identify six general functions which user access control software deployed at MH should contain. (03 marks)
(c) List the type of information (seven points) that you would require to assess MH's logical access controls. (07 marks)

(a)Following physical controls may help to ensure physical security of the server room:
(i) Installation of a biometric/electronic door lock at the entrance.
(ii) Manual / electronic log of all people accessing the server room.
(iii) Review of such logs by an appropriate authority.
(iv) Installation of surveillance cameras in the server room to monitor the entrance and the room.
(v) All visitors such as outside technical support persons are escorted by an authorized employee during their stay in the server room.

(b) The user access control software of MH should contain the following general functions:
(i) Creating user ID and password.
(ii) Creating or changing user profile.
(iii) Applying user login limitation rules.
(iv) Assigning and verifying user authorization to applications/transactions.
(v) Logging events.
(vi) Reporting exceptions.

(c) While assessing logical access controls of MH, knowledge of following information would be useful:
Whether;
(i) there is a proper Information Security Policy in place?
(ii) the Information Security Policy has been communicated to all users?
(iii) a proper User Authorization Matrix (UAM) is in place?

(iv) and how the patients' history is updated and whether there is proper segregation principle in place between updating patient history and reviewing it.
(v) there is limit to the senior doctors' rights. Besides patients' history, can they access other departments' data as well?
(vi) the empty network ports in wards and other departments can be used for accessing data other than patients' history? Can patients' history be edited from these ports.
(vii) there is a system to handle logical access breaches / attempts to logical access breaches.

Q. Internet has developed systems for storage and sharing of information in a convenient, efficient and economical manner. Consequently, various organizations have demonstrated widespread reliance on use of Internet facilities. However, storage and exchange of sensitive information on Internet exposes the organisation to various types of threats. A firewall is considered an appropriate safeguard for companies whose networks are connected to the Internet.
Required:
(a) Distinguish between passive and active attacks. Briefly describe any three passive and three active attacks to which an organisation is exposed due to the connection of its network with the Internet. (08 marks)
(b) Identify the primary functions of a firewall and briefly describe any three types of firewall. (09 marks)

In **Passive Attack** network information is gathered by probing/observing various activities performed through the network. When the attack is actually launched (either using the information gained through passive attack or otherwise) it is called Active Attack.

Examples of passive attacks are as follows:

Network Threat	Explanation
(i) Eavesdropping	The attacker gathers the information flowing through the network. Such information may include emails, passwords and in some cases keystrokes, in real time.
(ii) Traffic analysis	The attacker determines the nature of traffic flow between defined hosts and through an analysis of session length, frequency and message length. Such analysis enables the attacker to guess the type of communication taking place even if it is encrypted.
(iii) Network analysis / foot printing	Initially the attacker uses a combination of tools and techniques to build a repository of information about a particular company's internal network. Later, the attacker focuses on systems within the targeted address space that responded to these network queries when targeting a system for actual attack. Once a system has been targeted, the attacker scans the system's ports to determine what services and operating system are running on the targeted system, possibly revealing vulnerable services that could be exploited.

Examples of active attacks are as follows:

Network Threat	Explanation
(i) Masquerading	The attacker impersonates as an authorized user and thereby gains certain unauthorized privileges.
(ii) Denial-of-service	It occurs when a computer connected to the Internet is flooded with data and/or requests that must be serviced. The machine becomes so tied up with these messages that it is rendered useless.
(iii) Brute-force attack	The attacker launches an attack using any of the password breaking tools.

(b) Primary **functions** of a firewall are as follows:
(i) Allows only authorized traffic to pass.
(ii) Keeps information related to all access attempts undertaken.

Different **types** of firewalls are described below:

 Router Packet Filtering

Such firewalls are essentially routers operating at OSI layer 3, using set access control lists (ACLs). Decisions are made to allow or disallow traffic based on the source and destination IP address, protocol and port number. Such type of firewalls can compare the header information in packets only against their rules. As a result they provide relatively low security as compared to other options.

 Stateful Inspection

They keep track of all packets through all OSI layers until that communication session is closed. It tracks communication (or sessions) from both internal and external sources. The rules are changed dynamically when an outbound connection is established to enable packets from the destination IP address to return back to origin. All other traffic is stopped from reaching origin computer, protecting it from dangers of the Internet.

 Application Firewall

Such firewalls manage conversations between hosts, acting as an intermediary at the application level of the OSI model. All packets passing to the network are delivered through the proxy, which is acting on behalf of the receiving computer. The communication is checked for access authorization according to a rule-base and then passed on to the receiving system or discarded. The proxy receives each packet, reviews it, and then changes the source address to protect the identity of the receiving computer before forwarding. Proxy firewalls can look at all the information in the packet (not just header) all the way to the application layer. They provide greatest degree of protection and control because they inspect all seven OSI layers of network traffic.