**Question 1**

* Give an example of administrative preventive controls that addresses Confidentiality and briefly explain how.
* Give an example of technical corrective controls that addresses Integrity and briefly explain how.

Confidentiality - No leak (the secrecy of the data is maintained at all times)

Availability - Users must be able to use the system when they need to (The systems and networks should provide adequate capacity to perform in a predictable manner with an acceptable level of performance.)

Integrity - No modifications and Accuracy( Accuracy and reliability of information

Prevent unauthorised and improper modifications)

Three types of control

* Administrative controls
* Technical (Software part eg. penetration testing) controls
* Physical controls

**Preventive controls**:

Training of employees about security awareness. Eg. enhances security awareness of phishing attacks.

How: With security awareness training, users will be able to identify and spot phishing emails that attempt to steal account information

**Technical Controls**:

Recycle bin in windows helps to recover files that are accidentally deleted by authorised users.

**Question 2**

Describe one (1) example of administrative preventive controls and one (1) example of physical recovery controls, both of which must address Availability. For each example, briefly explain how it helps address availability.

**Availability**

Definition: The systems and networks should provide adequate capacity to perform in a predictable manner with an acceptable level of performance.

**Administrative**

(The soft part of things: Policy, trainings, procedures, software based)

* Policy that prevent unauthorised people from entering
* Change control procedure, change management ensure that new software development will not crash existing appication due to thorough testing.
* Penetration testing

**Physical**

(Physical part of things, Physical infrastructure)

Backup sites, Backup systems, Warm site, cold site, UPS (Uninterruptible Power Supply), Hot sites, Backup power so that when a system is down, data can be retrieved from the backup sites and will thus will make the data available as quickly as possible. (Example + how it addresses availability)

**Question 3**

A small health organization has asked for advice in regards to improving its security system. The organization is already implementing a defense-in-depth mechanism which combines a firewall with the encryption of traffic to prevent confidential information being accessed by unauthorised personnel. The company has very limited funding and you can only suggest two additional security mechanisms (security methods) to be considered. Describe the mechanism you have selected and justify your selection.

\* Defence in depth - Different layers of controls

Small organisation and limited funding (sugg solutions must address these constraints)

Touches on commonly used security methods

**Minimisation (similar to least privilege)**

* applies to system configuration
* States that one should not run any software, applications or services that are not strictly required to the entrusted job
* Eg. computer which only function is to serve as an email server, should only have the email server and software installed on the computer, all other services as per protocols should either be disabled or not installed at all to eliminate any possibility of the compromise or misuse
* Advantages: Increases security and improve performance, save storage space and is also a good system administration in practice.
* Principle: hardening the organisation server by disabling the services that are redundant or removing programs that are not necessary in order to reduce the attacks on the server
* Summary: able to harden org server, disable unnecessary services, restrict accesses, perform on a need to basis, use the least privilege principal
* Does not need require company to buy solutions, only need to use the current system that the organization has and enforce such principals

**Leverage unpredictability**

* Eg. announce on the organisation website web that using firewall that logs all traffic to and from the network and the logs are reviewed by the organisation
* No need to disclose the type and vendor of the firewall, where it is located, the frequency of use and any backup firewalls or network disruption detections are put in place
* Principle in this case: telling the public about the existence of such security controls, public able to get the gist of what is happening in the organisation and warn them about the effects of trying to compromise the security of the organisation

**Question 4**

A retailer is selling goods via both physical and online stores. The online store allows customers to create their own accounts, update personal and financial information, order goods, and track order status. It also links to the inventory management back-end. It has been suggested that three universal security methods; Least privileges, Compartmentalisation, and Defense-in-depth need to be used to enhance the security of the system. Describe your interpretation of these three (3) security methods in this particular scenario. (Definition, Example, Principle, Advantage and Disadvantages)

\*Physical and online store

**Least privileges**

Do not grant users or the staff more privilege than they should have. Only give them the privileges they need for their duties.

**Compartmentalisation**

Definition: Putting things into different categories

Parts

Web server ( in demilitarised zone DMZ)

Front end systems and Backend systems

**Compartmentalise :**

* segregation of front end systems from the back end systems
* If they are not in physical servers, they can be on virtual machines
* Users able to retrieve webpage from web servers without accessing any materials on the backend
* Pulling happens when information is transferred from one system to another (eg. info keyed in -> inventory -> management -> system -> person reads and sends order to warehouse -> ship)

**Defence in depth**

Multiple layers to the defence: Online stall has personal and financial information. In order to protect the info, multiple layers need to be used.

Layers : (Outer to inner layer) Firewall. Intrusion detection system (IDS). Secure data with encryption. Search for more information and examples on these layers

(two layer firewall: internet facing and internal facing firewall)

**Question 5**

With the help of an example, explain the principle Fail securely.

* Definition : If a security measure or control has failed, the system is not rendered to an insecure state.
* Eg. firewall fails, shld fall towards a deny all rule instead of permit all ( Firewall: There are many firewall rules. Person whos job is to key,delete, amend and add firewall rule. Eg. users cannot access the database servers and only the web servers. Because database server is in the internal network. Firewall rule states who can access what etc. on 80, there is http protocol bec access the webpage stored in web server. Firewall has a particular deny all rule : unless all rules are followed, deny all rule is activated)

\* Does not mean close everything in all cases

* Physical example: Building access control system: Doors should open when there is a fire should default to open doors when humans are trapped in the buildings instead of close as human lives takes priority over the risk of unauthorised access which may be dealt with using other forms of controls that does not endanger the lives of people during emergency situations.

**Question 6**

With the help of an example, explain why the principle of minimization is important from the point of view of system security. (Definition, Example, Principle, Advantage, Importance)

Minimisation Principle: Only run applications that are strictly necessary to perform its tasks and nothing more because when there are more applications running, the higher the chance for something to go wrong and the security will be compromised

A common approach to breach security is to attack services which are running on a host machine, such as Telnet.

TELNET is commonly used by terminal emulation programs that allow you to log into a remote host. However, TELNET can also be used for terminal-to-terminal communication and interprocess communication. TELNET is also used by other protocols (for example, FTP) for establishing a protocol control channel.

To limit the number of options for hackers, it is imperative to shut down all services that are not essential to improve the running of the system.

An application may have weaknesses that can be exploited and thus, if they are not running, the system will be more secure.

Disabling redundant services is a major task to server hardening. With minimisation principle, the priority is to have the least privileges as possible

Example:

In the case of the Firewall Rule in minimisation principle, port 80, HTTP is the protocol. Inside the firewall, there are alot of protocols and ports. For example:

* FTP(File Transfer Protocol: works on a client-server model, it is a standard communication protocol used for the transfer of computer files from a server to a client on a computer. FTP is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections.) protocol in port 21.
* TELNET is in port 23.
* SSH is another service is in port 22.
* SMTP (Simple Mail Transfer Protocol: for mail services) in port 25

Minimisation: disable services that you do not need, unnecessary services should be disabled eg. If an organisation does not need to use FTP, disable FTP bec FTP is not secure as FTP transfer files in clear files.

* Instead of having FTP, use SFTP (Secure File Transfer Protocol)
* Since TELNET is also not secure as TELNET also send files in clear text, disable TELNET and enable SSH (Secure Shell) instead.

**Ports and Protocols**

As per its word definition, a protocol is a set of rules. In computer networking, a protocol defines a standard way for computers to exchange information. Most common protocols used in computer networks and the internet are TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and IP (Internet Protocol).

A port in computer networking is a logical access channel for communication between two devices. Bi-directional communications and more complex connections may use multiple ports (channels) simultaneously.

Data on the Internet is organised into standard TCP or UDP packets. Network clients use different ports (or channels) to transfer this data. Generally one port is used to send data and another to receive it, so packets don't collide. The port number (and the destination IP address) is included as part of the header each packet is given. Ports range from 1 to 65535 for the TCP and UDP protocols.

**Question 7**

You are asked to give an advice on the security set-up for a medical research laboratory which has computer terminals connected to a server that stores sensitive information. a) Suggest two physical preventive controls and two physical detective controls that can be used and explain your choice. b) The laboratory is going to provide an Internet presence to assist researchers in finding information online. However, this raises a serious concern that the sensitive information is accessed by intruders from the outside world. Under the defense-in-depth principle, suggest specific security solutions for at least two layers of defense that may be deployed to mitigate the risk.

**Physical Preventive:**

(Since it is in a medical research lab, assume that it is a physical site)

Security guards, Bollard, Biometrics Access Control

Backup Files (in case of an attack)

**Physical Detective** :

CCTV, Smoke Detectors, Fire alarm

**Defense-in-depth:**

**(**eg. having a preventive, detective and corrective control)

* Preventive - firewall (stops bad traffic before it enters the network)
* Detective - Intrusion detection system, Logging (helps to detect malicious activities)
* Corrective - Backups (helps to restore the data damaged or modified by intruders)

**Question 8**

It is often suggested to suspend or delay access capability after a number of unsuccessful login attempts. Describe the reason behind this suggestion and clearly indicate what security threat this recommended practice addresses.

This helps prevent hackers from carrying out Brute force attack, Password guessing when it is done automatically.

**Question 9**

With the help of examples explain the differences between three universal security principles/methods:

Least privilege, Minimization, and Keep things simple. (Definition, Advantages and Disadvantages, Principles, Importance)

**Least Privilege**

Normal users do not have the same level of power as compared to administrators. Normal users should not be able to change, view system critical files. Normal users are given as least privilege as possible.

**Minimisation**

Disable redundant services or services that are unnecessary for example FTP, TELNET.

**Keep things simple**

For making decisions between different choices, pick the one that does the job but simple. Not making things difficult.

**Question 10**

The logon screen of workstations in an organisation reads ”Warning: All activity is constantly monitored and logged, including hostname and IP address.”

Explain the purpose of this notice and determine the type of security control and the universal security method of this practice.

(Types of security control - Preventive, Deterrent, Detective, Corrective, Recovery)

(Universal security method - Commonly used security methods)

**Purpose: (based on this scenario)**

**Deterrent control**

This is used to discourage malicious activities by users. Users will know that people at the backend will be able to see their activities.This security method leverages unpredictability.