Question 1

What are the three (3) different factors that are used for authentication? For each factor, give an example. Finally, describe a situation where a combination of at least two factors is necessary and briefly explain why

Three diff factors

1. Sth a person knows (Pwd Pin)
2. Sth a person has (Token)
3. Sth a person is (Biometrics Thumbprint, Thumb, Iris)

Two Factors Necessary (Choose 2 from above)

* Companies Card access and Biometrics to verify identity
* Companies Pin and Thumbprint
* Internet Banking Pin and Message sent to phone

**Question 2**

One important requirement when assigning value to an identity is that the value must be non-descriptive.

Explain what it means by ‘‘non-descriptive” and why it is required so.

Neither piece of the cred set shld indicate the purpose of the acct

Eg. user id not (backup op, ceo, administrator) - does not show who it belongs to

**Question 3**

Describe two types of technical controls that can be used for building access and specify which one you would use for low-security set-up required to protect a generic PC lab against unauthorised entry.

Access cards, biometrics, Pin (personal id number)

Low security - Biometrics, Pin, Access Card,

\* Need to write what type of biometrics

**Question 4**

Describe two types of technical controls that can be used for building access and specify which one you would use for low-security set-up required to protect a generic PC lab against unauthorised entry.

To be able to

Detect intrusion

reconstruct events and system conditions

provide legal recourse material

**Question 5**

Physical controls are often neglected when security systems are developed but nonetheless they are a critical component of an effective security solution. Describe two physical preventive types of controls as well as two physical detective types of controls and specify a scenario in which a combination of the two is necessary.

Physical Preventives

* Turnstiles
* Automated barriers
* Bollards

Physical Detectives

* Cctv
* smoke detector

Scenario

CCTV and Biometrics (Data Centre)

Technical Real Life examples:

* Online banking includes the:
* technical preventive controls such as (Passwords)
* Technical deterrent (Message on website to prevent people from hacking
* Technical detective (Audit)
* School security system
* Technical preventive (Passwords)
* Technical deterrent (Message on website to prevent people from hacking)
* Technical detective (Antivirus software)
* Technical Corrective (Recycle bin)
* Technical Recovery (Recovery technologies)

Administrative Real life examples:

* Big organisations:
* Administrative deterrent (Penalty and termination policy)
* Administrative preventive (Security awareness and training)
* Administrative detective (Security reviews, performance evaluations)
* Administrative Corrective (Incident handling procedures)
* Administrative recovery (Contingency plans and Disaster recovery plans)

**Question 6**

When developing a security system, it is important to plan for cases which the preventive measures in place fail and, consequently, the system integrity is compromised. From a security perspective what are the two main avenues that are generally considered for continuity/restoration of services?

Access controls fail

If fail, integ comprom

(Backup - offsite storage backups(Offline)

Ensure restoration of services, test the backup so that the backup will not fail (once in 6 mths or once a yr)

**Question 7**

The integrity principle in the context of data security deals with the correctness of the data and the aim is to prevent damage from personnel inside or outside the organization. What is the first measure that needs to be put in place to help with the data integrity protection?

Implement access controls. Users will only have limited access, this reduces the chance that a basic mist can result in a maj damage to the data that is being protected.

**Question 8**

Explain the difference between corrective and recovery controls.

Recovery controls are for recovering more serious situations from damage.

**Corrective control**

Example:

Recycle bin in Windows helps to correct accidental deletion. When an item is accidentally deleted, it goes into the recycle bin and users are still able to retrieve the files within a specific amount of time.

**Recovery control**

Example:

Chkdsk which helps to recover files that have been erased.

**CHKDSK**

It is not a data recovery tool and will not recover lost or damaged files. CHKDSK will simply ensure the information currently on the disk is in a consistent and safe state. If files are damaged, the CHKDSK utility attempts to separate the damaged files and save the remnants as Filenn.chk. This reorganisation of bad sectors can cause further problems. There have been many discussions or forums whereby CHKDSK has failed to repair a file and made it worse! The best advice we can give is to never run CHKDSK with the automatic repair option enabled.

<http://www.datarecoveryspecialists.co.uk/blog/chkdsk-data-recovery#:~:text=Will%20CHKDSK%20recover%20data%3F,save%20the%20remnants%20as%20Filenn>.

**Question 9**

Many organizations develop security systems which are focused entirely on physical and technological security controls. Explain why this is insufficient and provide examples how the security could be compromised.

Cyber security has 3 main aspects: People, Process, Systems

We need **Administrative Controls** as well.

If overlooked, an experienced attacker will be able to breach the security set up because the issue of information ownership is properly handled.

Thus an attacker may not need to break into the better protector systems as the access to confidential information is unlikely to be thoroughly control.

Example of lack of **Administrative Control**

Email to all users instead of only those that should have access to it.

Disposal of older hardware is not done in a secure manner and harddrives are simply thrown into a bin in from which an attacker can extract critical information such as passwords or confidential records.

**Question 10**

What is CERT-Australia? What is AusCERT? What is ASD? Why is it important from a data security point of view to know about each of them?

**C.E.R.T -** Computer Emergency Response Team

**CERT Australia** is the national computer emergency response team. CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.

**AusCERT** is a non-profit organisation that provides advice and solutions to cybersecurity threats and vulnerabilities. The organisation covers their costs through member subscriptions, attendees to the annual AusCERT conference and service contracts.

CERT educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. Knowing about each of them allows us to be better prepared in tackling cyber-security threats.

**Question 11**

What is sender policy framework (SPF)? Explain the type of attacks that SPF addresses.

The Sender Policy Framework (SPF) is an email authentication protocol and part of email cybersecurity used to stop phishing attacks. It allows your company to specify who is allowed to send email on behalf of your domain.

This is useful because in a typical phishing attack, the threat actor spoofs the sender address to look like an official business account or someone the victim may know.

**Targets**

* Email spoofing
* Phishing attacks

**How**

The protection of your outbound email is implemented by configuring a TXT record in your public DNS which lists the servers that are allowed to send email from your mail domain. Nothing is configured on the mail server itself.

The Sender Policy Framework (SPF) email authentication method aims to reduce spam and fraud by making it harder for email senders to hide their identity. SPF detects email spoofing by providing a process to verify who is permitted to send emails on your behalf.