Name: Yuvraj Singh Gill **Student ID:** 000560556

Assignment 1

Scenario: Company XYZ has recently experienced a data breach where sensitive customer information was accessed by unauthorized individuals. As part of the incident response, the company is evaluating its security measures to prevent future breaches.

Tasks:

1. **Confidentiality:** Explain how the breach could have compromised the confidentiality of customer information. Suggest two security measures that could enhance confidentiality in this scenario. (3 points)
2. **Integrity:** Discuss the potential impact of the breach on the integrity of the company's data. Provide two examples of controls that could help maintain data integrity. (3 points)
3. **Availability:** Describe how the breach might affect the availability of the company's services. Recommend two strategies to ensure high availability of services even during a security incident. (3 points)

(**NB:** 1 point for organizing and formatting your writeup properly)

The company's initial step in response to this breach is to trace back vulnerabilities and identify what is most important among confidentiality, integrity, and availability (CIA) to strengthen its security measures as it depends on security risks that the company faces.

Example:

- ➔ **Confidentiality:** If a company is dealing with sensitive customer information such as personal information, financial information or trade secrets then confidentiality is crucial for a company as it could lead to identity theft or financial loss.
- ➔ **Integrity:** If a company handles data which needs to be accurate and trustworthy such as health records or financial records. Any unauthorized modifications or inconsistencies with data could do serious harm. Therefore, Integrity is important.
- ➔ **Availability:** If a company provides online services or conducts online business such as e-commerce, or third-party data provider then availability is the key when a company needs 99.9% uptime. If the site goes down due to an attack it could lead to revenue loss and damage to reputation.

Choosing the right factor and balance between confidentiality, integrity, and availability is important and it should be relevant to the company's nature of business.

Confidentiality: It ensures that sensitive information is only accessible to authorized individuals. A data breach can expose personal or sensitive details. This means unauthorized users can misuse private information, leading to identity theft or financial fraud. For example, if an unauthorized access to credit card details, they can make unauthorized purchases. Confidential data needs to be tightly secured or it might get spread elsewhere through unauthorized channels.

Two security measures that could enhance confidentiality:

1. **Encryption** – By adding an encryption layer on top of sensitive data such as personal information, passwords, and payment information protects data by turning it into unreadable code or ciphertext without a key which makes it difficult for an attacker to comprehend. For example, when sending payment details online, encryption ensures only the bank can read it.
2. **Multi-Factor Authentication (MFA)** – MFA adds an extra layer of security. The user requires a one-time password on the phone or email to log in to the system, preventing unauthorized access even if a password is stolen.

Integrity: It ensures that data remains accurate and free from unauthorized modifications. Unauthorized gained access can change or delete sensitive data, making it incorrect or inconsistent. For example, if an attacker modifies financial records, it could lead to incorrect customer balances or unauthorized transactions.

Two controls that will keep or maintain data integrity:

1. **Access Controls** – Implementing access controls that who can edit information, making sure that only authorized users with specific roles can update records. It helps to prevent unauthorized modifications.
2. **Hashing and Checksums** – Implementing hashing and checksums helps in detecting unauthorized changes by comparing hash values before and after data transmission. If a file's hash value has changed, it means the file has been altered.

Availability: It ensures that information and systems are accessible when needed. The data breach can affect the availability of the company's services by causing system downtime, slowing down operations, or completely shutting down the services. For example, if a company's website is down, authorized users might not be able to access the data when they require it.

Two strategies to keep services highly available:

1. **Redundant Servers** – Setting up redundant servers ensures that services remain available even if the main system is affected by a breach.

2. **Backup Data Centres** – Setting up backup data centres helps restore services quickly after an attack.

References:

- *What is a Data Breach and How to Prevent It? | Fortinet*. (n.d.). Fortinet. *https://www.fortinet.com/resources/cyberglossary/data-breach*
- *St John, C. (2024, December 10). CIA triad in cloud security (Part 1: Confidentiality). Medium. https://medium.com/@csjcode/cia-triad-in-cloud-security-part-1-confidentiality-b7ec5dcf21a2*
- Pryimenko, L. (2025, January 16). *8 steps for data breach response and investigation | Syteca*. *https://www.syteca.com/en/blog/data-breach-investigation-best-practices*