**Importance of Data Accuracy**

1. Supports informed decision making

* Accurate data ensures what well informed decisions are made

1. Enhances Security Measures

* Accurate data is essential in authentication and authentication processes

1. Protects Organisational Reputation

* Organisations found to handle data incorrectly may lose customer trust

**Potential Results of Incorrect Data**

1. Legal Consequences

* If incorrect data leads to violations of data protection laws, organisations could face lawsuits

1. Loss of Customer Trust

* Errors in customer data can negatively affect the customer, which will lead to the customer lose trust in the organisation

**Measures to Maintain Data Accuracy**

1. Training and Awareness

* Staff should be trained to recognise and report inconsistencies or anomalies

1. Data Backup and Recovery

* Regular backups ensure data can be restored to a known accurate state after corruption or loss

**Significance of Authenticity**

Authenticity means that the source of information is confirmed to be legitimate. It works alongside confidentiality, integrity and availability to ensure the trustworthiness of data preventing unauthorised access.

**Why Authenticity Matters**

1. Prevents impersonation

* Ensures that users or systems are who they claim to be, reducing risks like phishing

1. Supports Trust in Digital Transactions

* Verifying authenticity is essential in online banking, e-commerce and communication

1. Enables Reliable System Access

* Helps organisations enforce secure access to resources, minimizing unauthorised entry

**Examples of Authentication Measures**

* Passwords/PINs
* Biometrics
* Two-Factor Authentication (2FA)

**Security Measures to Safeguard the Integrity of Records**

1. Access Control

* Ensuring that only authorised individuals can modify sensitive records

1. Logs

* Maintain logs of who accessed or modified data and when

1. Encryption

* Protects data during transmission and storage from being read or seen by unauthorised users

**Shoulder Surfing**

Shoulder Surfing is when an attacker steals information by watching a user’s screen or keyboard

**Measures to Avoid Falling Victim to Shoulder Surfing**

1. Be Aware of your surroundings

* Avoid accessing sensitive information in crowded or open areas

1. Use biometric authentication

* Reduces risk even if login credentials are observed

1. Use privacy screens

* Physical filter that blocks side view of screens

**Why Effective Planning is Vital to Prevent Technology from Becoming Obsolete**

1. Ensures scalability and future proofing

* Anticipates future growth and avoids the need for completely changing the system in order to improve it

1. Maintains Compatibility

* Helps align new purchases with existing systems

1. Reduces Long-Term Costs

* Promotes strategic investment in technology that lasts

**Cybersecurity Threats Faced by the Financial Industry**

1. Phishing and Social Engineering

* Attackers trick employees or customers into revealing sensitive data

1. Ransomware Attacks

* Criminals encrypt financial records or systems and demand payment to restore access

1. Insider Threats

* Malicious or careless employees may leak confidential data or bypass internal controls

**Reasons for Security Education**

1. Reduces Human Error

* Educating staff on security practices like avoiding suspicious links minimises the risk of breaches

1. Improves Incident Response

* Staff who are trained in recognising threats can respond more quickly and effectively to minimise damage

1. Combats Social Engineering

* Awareness training helps users recognise and resist phishing, baiting and other manipulation techniques

**Elements of a Good Security Awareness Program**

1. Regular Updates

* Content should reflect current threats, technologies and compliance requirements

1. Continuous Reinforcement

* Regular reminders and tips to help reinforce safe behaviour

1. Assessment and Feedback

* Surveys or simulations to assess understanding and finding room for improvement

**Top-Down vs Bottom-Up Approach in Security Implementation**

**Top-Down Approach**

A strategic and management driven method where senior leadership initiates and supports the development of an information security program

Characteristics:

* Starts with executive support
* Security policies and budgets are developed by management
* Better resource allocation

**Bottom-Up Approach**

Begins at operational level, where staff attempt to implement security solutions without much involvement from upper management.

**Different Between Top-Down and Bottom-Up**

|  |  |
| --- | --- |
| Top-Down | Bottom-Up |
| Initiated by senior management | Initiated by staff |
| Aligns with business objectives | Focuses on technical issues |
| Strong budget and management support | Limited or lacking budget or support |

**Risk Appetite**

The amount of risk an organisation is willing to accept in pursuit of its objectives

**Residual Risk**

The remaining risk after controls have been implemented to reduce inherent risks. (e.g. even after installing antivirus software, there is still a risk a new virus can breach the system).

**Discretionary Access Control (DAC)**

An access control method where the owner of the resource decides who can access it and what operations they are allowed to perform.

Example:

A manager creates a document and manually gives read/write permissions to certain employees.

**Non-Discretionary Access Control (NDAC)**

Access control is managed by a security administrator based on an individual’s role.

Example:

A HR staff member automatically gets access to payroll files due to their job role, not because someone gave them access like in DAC.

**Differences Between DAC and NDAC**

|  |  |  |
| --- | --- | --- |
| Aspect | DAC | NDAC |
| Control Over Access | Resource owner decides | Authority defines access |
| Security | Less secure | More secure |
| Common Usage | Personal or small business systems | Government or large enterprises |