***Organization***

**Types of organizational data**

Traditional data

This is typically generated and maintained by all organizations. It includes:

- **transactional data**  
 details relating to buying and selling, production activities and basic operations such as inf. Used to make employment decisions  
 - **intellectual property**  
 Patents, trademarks, product plans   
 (smt to help organization to gain economic advantage over competitors)  
 - **financial data**  
 income statements, balance sheets and cash flow statements

**IoT**  = large network of physical objects, such as sensors, software and other equipment  
 All of them are connected to the internet, with ability to collect and share data.  
 The increase of size has led to creation of new area of interest in technology and business called ‘Big Data’

**The cube**

McCumber Cube

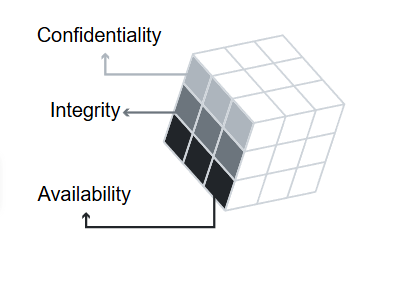
- is a model framework created to help organizations establish and evaluate information security initiatives by considering all of the related factors that impact them

It has **3 dimensions**:

**1 The foundational principles for protecting information systems  
 2 The protection of information in each of its possible states**

**3 The security measures used to protect data**

The foundational principles for protecting information



Confidentiality - set of rules that prevents sensitive information from being   
 disclosed to unauthorized people, resources and processes.   
  
 Method to ensure confidentiality   
 include **- data encryption,   
 - identity proofing**

**- two factor authentication**

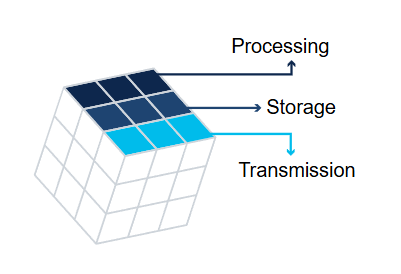
Integrity - ensures that system information/processes are protected from   
 intentional/accidental modification

One way  
 use **hash function / checksum**

Availability - authorized users are able to access systems and data when and where needed   
   
 Ways:

**Maintaining equipment   
 performing hardware repairs  
 keeping operating systems and softwear up to date  
 creating backups**

The protection of information in each state

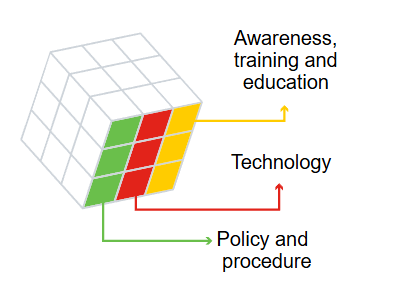


Processing - refers to data that is being used to perform an operation such as updating a   
 database record

Storage - refers to data stored in menory or on a permanent storage device such as a HDD, USB…

Transmission - refers to data traveling between information systems

The security measures used to protect data



Awareness, training and education - measures put in place by an organization to ensure that users are knowledgeable about potential security threats   
 and the actions they can take to protect information systems

Technology - software and hardware based solutions to protect information systems such as   
 firewalls,…

Policy and procedure - refers to administrative controls that provide a foundation for how an  
 organization implements information assurance,   
 (incident response, plans and practice guidelines)

**Consequences of a security breach**

Potential consequences of a security breach can be:

1. **Reputation damage**  
    - it can have a negative long-term impact on an organization’s reputation  
    - customers particularly those impacted, will need to be notified and may seek   
    compensation and/or turn to a competitor
2. **Vandalism**  
    - hacker/group may vandalize an organization’s website, minor like changing email   
    or phone to big ones
3. **Theft**  
    - it often involves an incident where sensitive personal data has been stolen  
    - cybercriminals can make this information public or exploit it to steal individuals   
    money or identity
4. **Loss of revenue**  
    - financial impact of security breach can be devastating  
    - example hacker takes down online shop’s website, demand of further investment I  
    in an organization’s security, large fines or penalties
5. **Damaged intellectual property** - devastating impact on the competitiveness of an organization, particularly if   
    hackers are able to get their hands on confidential documents, trade secrets or   
    intellectual property