Large Organizations work at large amount of data [Basic values or facts organized in a database]

Information → consists of data that has been organized to help answers questions and to solve problems.

Info' System is defined as a software that helps organize and analyze data, so the purpose of IS is it to turn raw data into useful info' that can be used for decision making in an organization. The intersection of technology, people and processes within an organization.

Data Base Management System → Combination of S/W and data that makes it possible to organize and analyze data.
General purpose info' System.

Electronic spreadsheet - A tool for basic data analysis based on formulas that define relationships among the data. [specific purpose info' System]

Technology [H/W, S/W, data and n/w comm'] → set of info'
Physical Tech. ↓ Program run within H/W

People [who are generating the management tools]

Processes [How the raw data is converting into info']

Main motive of Info' System → Providing the right info' to the right people at the right time.

Info' System components → [n/w comm'] → [where]

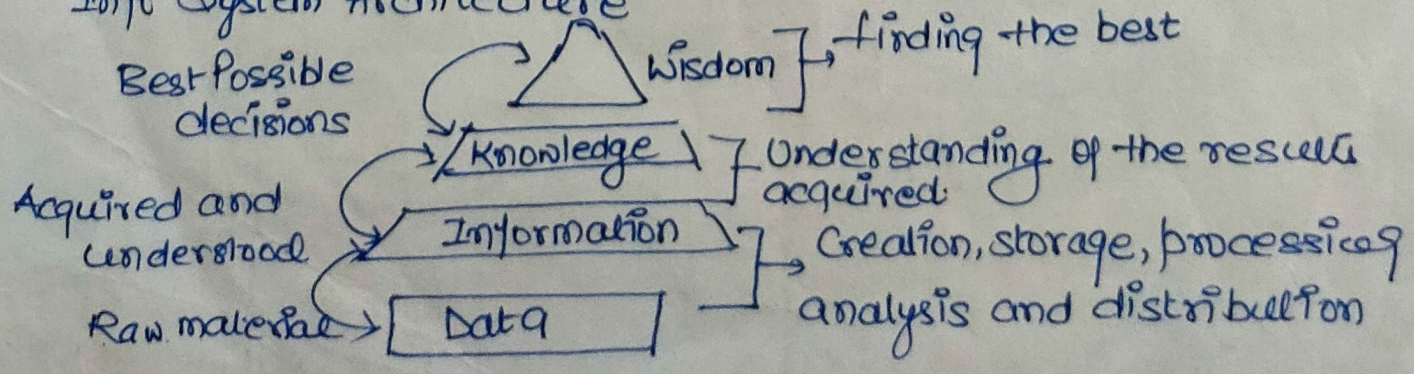
[What] Input → Process → Output → Storage [saving data for a period of time.

Input ↓ Embed data in a system for any use

Process [Internal] Act of Taking inputted data and converting it into something usable [How]

Output ↓ Processed info' [Why as why the output is best possible decision made]

Info' System Architecture



Advantages → (1)- Communication → With the help of Infor Tech. the Instant Messaging, Emails, voice and video calls becomes quicker cheaper and much efficient.
Improves Data storage, file management and Data Analysis
Globlazation and cultural gap- Sharing the info b/w different regions around the globe become much more easier.
Improves financial Management → Accounting s/w provides easy maintainance of financial info of organization.
Availability → 24x7 available purchasing and deliveries
Improves Business to consumer relationship-
Creation of new types of jobs → System analyzers, H/W & S/W developers are some of it.
Improves Business competitive Advantage - Technology has been used to gain competitive advantage over other.
Cost effectiveness and productivity - Promotes more efficient use of company and improves the info for decision making.

Disadvantages →
Unemployment and lacks of job security.
Dominant culture → While providing a global reach to every other culture, it made one culture dominating another weaker one. As English is the language dominate other languages and is becoming the primary mode of comm^n
Security Issues - Thieves and hackers get access to identity and target sensitive data of any organization that can include any personal info like bank details, personal details.
Implementation Expenses → to setup the Info System a good amount of cost in case of S/w, H/w and people. To train the employees for handling the new technology and softwares.

Types of Info System →
(1)- Transaction Processing System → [Used for Record Keeping] Such as Sales order entry, payroll. Used for scheduled generation of periodic records

(2)- Decision support System → Serves Management of any organization. These Systems have data-Analyzing tools, which support decision making in context of Individual problem. Where the info is difficult and complex to use, to enhance the decision making DSS are being used.

(3)- Executive Info System → Graphical Representation
(4)- Management IS → Deals with Production, sales
(5)- Workflow System → monitor the execution of interrelated set of tasks arranged for a business process.
(6)- Expert System → Ability to make suggestions and act like an expert in a particular or

curity Trends → 2018-19

1)- Indetity as the default perimeter → perimeter less security With identity and access management technologies, orgdnizations can define policies based on specific users and applications, limiting worker access to only the info they need to do their jobs. As the identity changes moment to moment, such as different on laptop and then in a smart-phone, its all about the role you are in at that moment. ## John N. Stewart, Cisco chief security and trust officer.

(2)- Privacy → As how we have little privacy with major companies

(3)- Disinfo will likely persist → A big negative on the predicted security trends as their is a lot of fake info curling around the globe to influence the economical, political and religious views of any country or particular person. From election influencing to deep fake videos that use AI to manulate images, The security council sees efforts to confuse people's perceptions of trusted info as a key threat.

(4)- Phishing through email → giving up personal info, login credentials or transaction. Phishing involves general sms is called as [~~smishing~~ smishing], via phone calls [vishing]

(5)- Increasing use of mobile landed as an attack vector.

(6)- Targeting of local governments and enterprises via ransomware attacks.

(7)- ## Informing individuals about how their info will be used.
Providing individuals with a way to disallow their info from being shared.
Developing and implementing policies and procedures to become compliant
Increasing the security of data and personal info through the use of encryption and other mechanisms

(7)- Increasing investment in cyber security automation - Helps to perform tasks →
collecting data about components of your info system that can be used to monitoring and analysis
Keeping track of all S/W and H/W asset within your organisation.
Keep those physical and virtual assets up to date.
This movement increases efficiency of a system and decreases the burden on understuffed cyber security team.

in-house expertise]

for 2020 → [Spending on security will increase]

AI & ML effect security → It provides quick responses to-
wards cyber threats Advantages of AI for Systems

Work round the clocks.

Response in milliseconds.

Simplify the process of data collection and analysis.

Enhanced the logistics to Analysis and detect the attacks and provide prevention.

Helping in building much better accurate biometric based login techniques.

Disadvantages → Costly, can be used by attackers also not fit for all solutions. Cyber security staff needs more training to operate AI solutions more effectively.

Expansion of cloud-Based Security → Consumer and business have grown dependent on storing sensitive data in cloud environments.

Avancement in Data Encryption → Data and identity Encryption. As the technology updated so the compromising ie data encreases We have to update the encryption techniques according to the advancement in technology.
Cyber insurance

The growth in 'passwordless'-Authentication

Need for cybersecurity Talent.

The Melissa Attack-(1999). MS-Word document got affected and attached as a email. It would mail out to the first 50 email-Addresses saved ie the outlook email box.
Solar Sunrise (1998) → Solar Solaris OS [Defense Info' Systems] no Iraqi operatives but 3 teenagers from California. However the case was closed but it shows how our effort can affect an IT infrastructure.

The OSI Security Architecture-
ITU-T [Telecomm² Standardization sector of the International Telecomm' Union]
Systematic way of providing security services to an organization. It helps in managing the tasks of security provision for the firm manager.
OSI security Architecture Provide different services and mechanisms to deal with the issues in an organization.
(1)-Security Attacks → Defined as any act of Info' compromising when somehow info' of an organization is modified without any knowledge, the situation formed as the organization is dealing with an attack.

(2)- Security Mechanism → (Control)- A method followed or established for an organization to prevent Info' from any modifications and to know when are the possibilities

occurices for info Alteration. and if happened than how to Overcome it.

(3)- Security services → These services are used to respond security attcks and used the mechanisms or methods for providing the security services.

Principles of security → OR Security Services → (X.800)

(1)- Confidentiality- It states that the info should be in blw the sender and the receiver, any third party should not have any access to info ie blw the data on air.

(2)- Authentication → The Affirmation or the guartee that the communicating person is the one who it he or sher is claiming to be.

(3)- Integrity → the confirmation of the info as it has not been modified, Deleted or added any info in it and is the same by Authorized Entity.

(4)- Availability

Identification of the Sender & Receiver.

→ # Resources or Applications must be available to Authentic users all the time.

RFC(2828) →

Threat → A Potential of variation of security which exists or happend only when there is a circumstance, capability or action, event that cause harm and breach the security.

Attack → An act of violating the security services policies of a system and by avoiding the security services which is being derived by an threat.

#(4)- Non Repudiation → None of the sender or Reciever be able to deny the transmission.

(5)- Access Control → Access to the Info Resources must be controlled by the System.

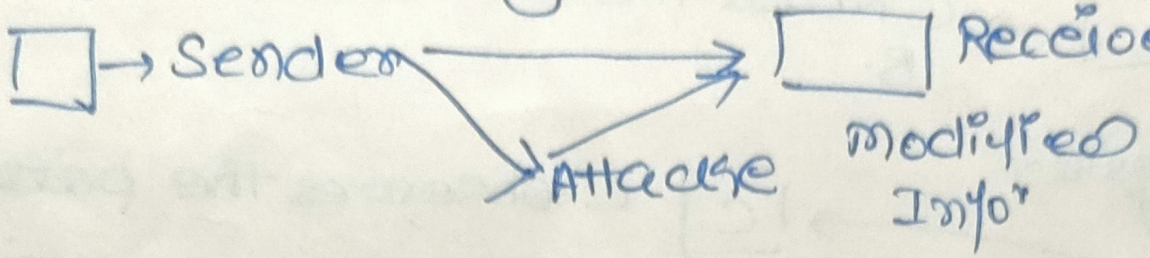
Authentication Types →

Peer Entity → Used to identify the Authencity of the entities connected to a System.

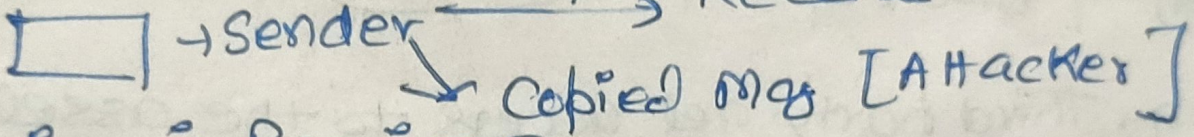
Data Origin Authentication- In an connectioness transfer Provide assurance that the source of received data is as same as it claims to be.

Web Site (Answer)

Active Attacks→ These Attacks involve some modification of the data stream or the creation of a false stream.
Dangerous for integrity and availability. [Detection is Required]



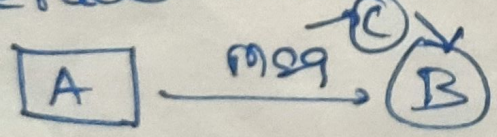
Passive Attacks→ When there is an exploitation ie the confidentiality of a msg or the content is copied by the third party the attack is passive as it does not harm the overall system an the victim is also unaware of the attack happened



Prevention is Required

Types of Active Attacks→

(1). Masquerade→ Predentiag to be someone, one is not→ C is pretendiag to be A



Modification of Msg → C ↓ Altered info producing unAuthorised effect.

A —msg→ B

As Allow B to read this msg
Modification ⇒ Don't Allow B to read the msg.

Repudiation → Denial of truth. Can be done from Sender or Receiver's side. As both can deny later that the info being send or received is not from their side.

Replay → Repeatation of same info again & again to make the other side believe that the Msg is from Authorized user.

Denial of Service → Prevention from use of comm facilities.
Overloading of the services by repeatation of false requests.

Types of Passive Attacks →

(1)- The Release of Msg content →

A —msg→ B
↓
C → C Reads the content which A sends to B.

(2)- Traffic Analysis →

A —msg→ B
C → C observes the pattern of Messages Exchanged b/w the A. & B.

Security Attacks →

Interruption → Attack on Availability

Sender — Block of Info — Receiver

Interception → Third party get access to the asset.

Sender → R

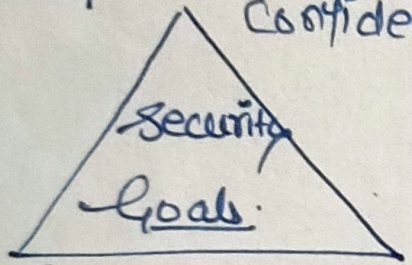
Attack on confidentiality

Modification → Integrity Attacks

Fabrication → Authencity Attacks

Security Goals → Info^r Security measures try to address at least one of three goals → Protect the confidentiality of data
Preserve the integrity of data
Promote the availability of data for Authorized use.

These goals for CIA Triad, basis of all security programs. Info^r security Professionals must consider these three things before creating a plan for protecting the info^r system.



CIA Triad is basically the principle of Info^r security Protection of confi, Integrity & availability can not be over emphasized. This is the central point for security Part of view for any IS. Used to illustrate the overall goals for IS throughout any task related to research or any firm.

Depends on Two Types of Requirements → functional and Assurance-
Verification - Process of confirmation whether predetermined Requirements or specifications are met.
Validation -
↓ what a system should do
↓ How functional requirements are needed to implent and test.