K. K. Wagh Polytechnic, Nasik-3
Department of Information Technology

Chapter 1: Introduction to Information Security

(12 Marks)
Information, Need and Importance of Information
Information Classification
Criteria for information classification
Security, Need of security,
Basics principles of information security
Three pillars of information security
Data Obfuscation
Event Classification

Information:

It is a resource fundamental to the success of any business.

Data: It is a collection of all types of information which can be stored and used as per requirement.

Knowledge: It is based on data that is organized, synthesized or summarized and it is carried by experienced employees in the organization.

Action: It is used to pass the required information to a person who needs it with the help of information system.

Information Systems (IS)

An information system(IS) is a set of inter-related components that collect, process, store and distribute information to support decision-making and control in an organization. IS is automated or manual

Need and importance of Information:

1. Information is essential in organization because damage to information/data can cause disruptions in a normal process of organization like financial loss.
2. Information is the most valuable resources of an organization so its management is crucial to making good business decision.
3. Main objective of an information system is to monitor and document the operations of other systems
4 To satisfy the decision making capability, the information system should be call for intensive and complex interaction between different units in the organization.

Information Classification:

- The main reason for classifying is that not all data/information have the same lvel of importance or same level of relevance/ criticality to an organization.
- Some data are more valuable to the people who make strategic decisions (senior management) because they aid them in making long-range or short range business direction decisions.
- Some data such as trade secrets, formulae (used by scientific and/or research organizations) and new product information (such as the one used by the marketing

staff and sales force) are so valuable that their loss could create a significant problem for the enterprise in the market.

- Thus it is obvious that information classification provides a higher, enterprise–level benefit.
- Classification of information is used to prevent the unauthorized disclosure and the resultant failure of confidentiality

Schemes for Information Classifications:

1) Government /Military Organisation
2) Private Organizations

Levels in Government /Military Organization for Information classification:

1. Unclassified

Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.

2. Sensitive but Unclassified (SBU)

Information that has been designated as a minor secret but may not create serious damage if disclosed.

3. Confidential

The unauthorized disclosure of confidential information could cause some damage to the country‘s national security.

4. Secret

The unauthorized disclosure of this information could cause serious damage to the countries national security.

5. Top secret

This is the highest level of information classification. Any unauthorized disclosure of top secret information will cause grave damage to the country‘s national security.

The organizations make data available to those concerned on a ‘need-to know’ basis. For this reason, the following data/information classification is also prevalent in most **private organizations**:

1) **Public :**
   Information that is similar to unclassified information. However if it is disclosed, it is not expected to seriously impact the company.
2) **Sensitive:**
   Information that requires a higher level of classification than normal data. This information is protected from a loss of confidentiality as well as from a loss of integrity owing to an unauthorized alteration.
3) **Private:**
   Typically this is the information i.e considered of a personal nature and is intended for company use only. Its disclosure could adversely affect the company or its employees salary levels and medical information could be considered as examples of ‘private information.

Criteria for information Classification:

1. Value

It is the most commonly used criteria for classifying data in private sector. If the Information is valuable to an organization it needs to be classified.

2. Age

The classification of the information may be lowered if the information value decreases over the time.

3. Useful Life

If the information has been made available to new information, important changes to the information can be often considered.

4. Personal association
If the information is personally associated with specific individual or is addressed by a privacy law then it may need to be classified.

Security
Security is the method which makes the accessibility of information or system more reliable. Security means to protect information or system from unauthorized user like attackers, who do harm to system or to network intentionally or unintentionally.
Security is not only to protect information or network, but also allow authorized user to access the system or network.

Need of Security:
1. Security protecting the Functionality of an Organization.
General Manager and IT Manager are responsible for implementing information security that protects the functionality of an organization. Implementing information security has more to do with management then technology.
For e.g. Managing payroll has more to do with management then Calculating wages, other things etc.
2. Enabling the safe operation of application.
Today organization operates on integrated efficient and capable applications. A modern organization need to create an environment that safeguards these Applications, specially operating system platform, email, instant messaging application etc.
3. Protecting data that organization use and collect.
Without data an organization losses its records of transaction and ability to deliver a value to its customer. Protecting data at motion and at rest are both critical aspects of information security. The value of data motivates attackers to steal and corrupt the data.
4. Safeguarding technology assets in organization.
To perform effectively, organizations must employ secure infrastructure service which appropriate to the size and the scope of the organization. For e.g. a small business uses an email service and secure with the personal encryption tool. When an organization grows, it must develop additional security service that uses system of software, encryption methodology and legal agreement that support entire information infrastructure.

Three pillars of information security:

1) Confidentiality
2) Integrity
3) Availability

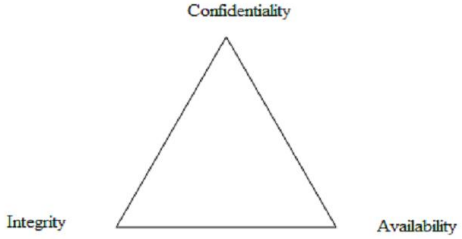

Fig: Three pillars of Information Security

1) Confidentiality:

It is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways such as through the intentional release of private company information or through a misapplication of networks right.

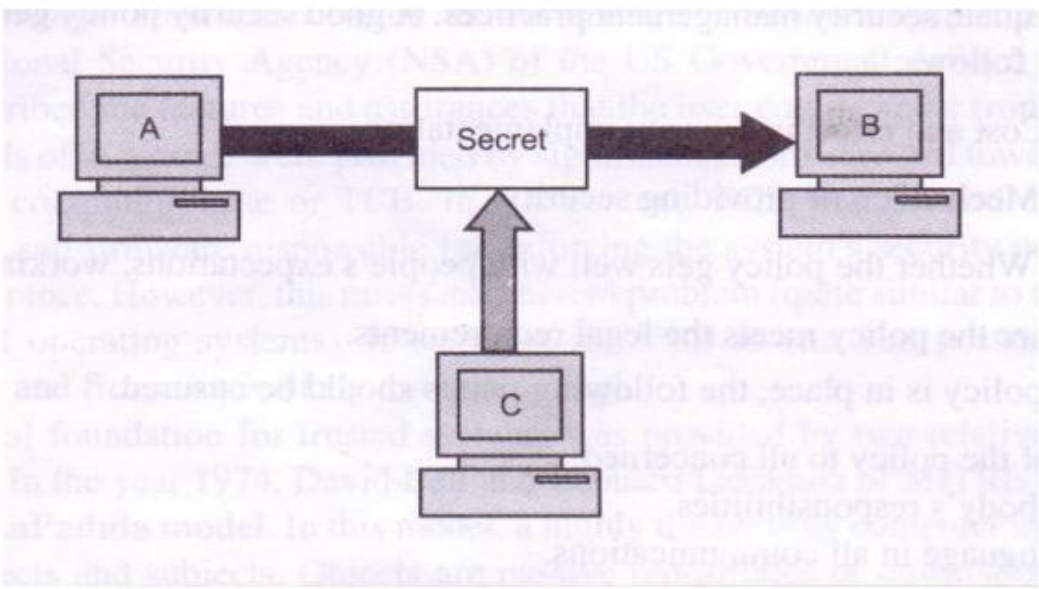

Fig: Loss of Confidentiality

2) Integrity:

The concept of integrity ensures that

i. Modifications are not made to data by unauthorized person or processes.

ii. Unauthorized modifications are not made to the data by authorized person or processes.

iii. The data is internally and externally consistent.

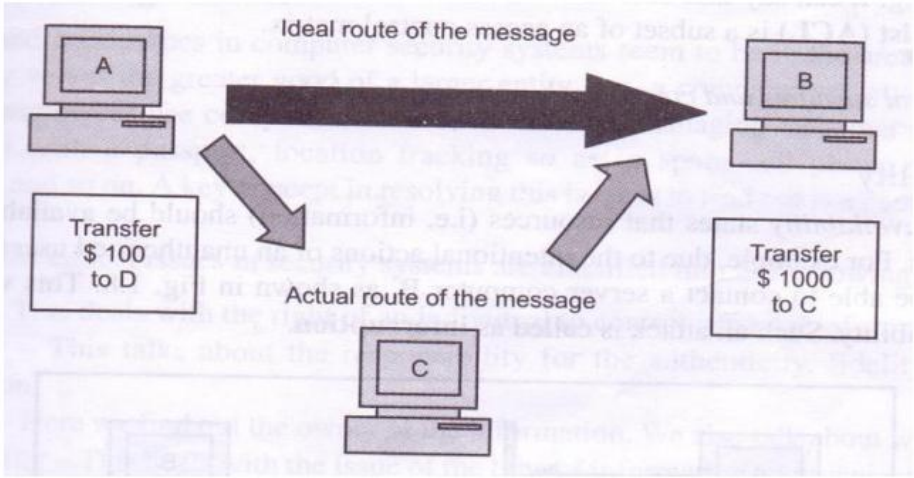

Fig: Loss of Integrity

3) Availability:

The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate person. Availability guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.

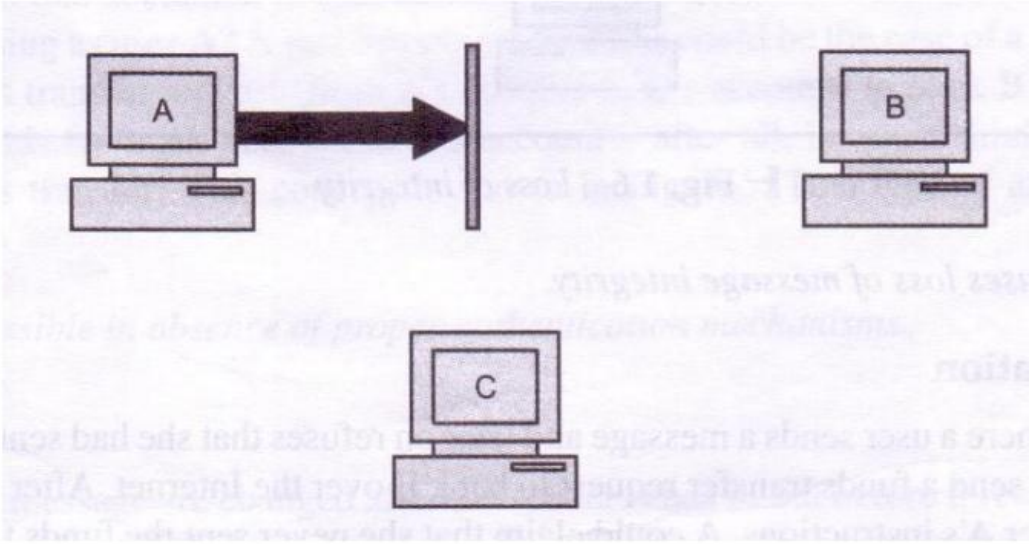

Fig: Attack on availability

Data Obfuscation:

1) It involves protection of sensitive information with techniques other than encryption.
2) Data Obfuscation is one of the solutions for data theft.
3) Protecting credit card numbers, medical data and other sensitive information has become more important.
4) It is important to keep in mind that encryption refers to some method of modifying data so that they are meaningless and unreadable in their encrypted form. They also must be reasonably secure that is they must not be easily decrypted without the proper key. Anything less than that will be referred as obfuscation.
5) Data obfuscation makes the data unusable by some means, but are not considered as a serious form of encryption.
6) A good example would be an audit report on a medical system. This report may be generated for an external auditor and contains sensitive information.
7) The auditor will be examining the report for information that indicated possible cases of fraud or abuse.
8) Assume that the management has required that patient names, permanent account number (PAN) and other personal information (PI) should not be available to the auditor except on an as needed basis.
9) The data need to be presented to auditor but in a way that allows the examination of all data, so that only patterns in the data may be detected.
10) When the auditor finds a possible case of abuse, he will need the real name and PAN of the party involved. He could obtain this by calling a customer service representative at the insurance company that supplied the report and ask for the real information.
11) The obfuscated data re read to the customer service representative, who then inputs it into an application that supplies the real data.

12) To summarize, data obfuscation, it would not be very difficult to decipher the obfuscation scheme given enough data.

Event Classification:

Events that can result in damage to IS are typically classified as:

1) **Crisis:** An abnormal situation that presents some extra ordinary high risks to a business and that will develop into a disaster unless carefully managed.
2) **Disaster:** An event that causes permanent and substantial damage or destruction to the property, equipment, information staff or services of the business.
3) **Catastrophe:** Major disruptions resulting from the destruction of critical equipment in processing. (Major Earthquake, Hurricane)

Crisis -> Disaster- > Catastrophe

MSBTE Questions:

Summer 2016

1. List down three pillars of information security. Describe any one in detail with neat labelled diagram.
2. Define information. State need and importance of information
3. Define security. State the needs of security.
4. Elaborate what is information classification? Describe any two criterias for the information classification.

Winter 2015

1. Mention basics principles of information security.
2. What is information? Describe the need and importance of information (6M)
3. State and describe the three pillars of information security with neat diagram.

Summer 2015

1. State pillars of information security. Describe with neat diagram. (Diagram 1M, each point 1M)
2. Give classification of information. Describe different criteria for information Classification. (Classification- 3M (any 3), Criteria-3M(any 3)).

Winter 2014

1. Define information. State need and importance of information.(Definition - 1 Mark, Need and importance - 1 Mark each (any 3))
2. Explain importance of pillars of information security.(Pillars - 2 Marks each)
3. Explain basic principles of information security. (Diagram - 2 Marks, Each principles - 2 Marks).
4. Define the term confidentiality. Explain with example. (Definition - 2 Marks, Description - 2 Marks).