ITEC 100

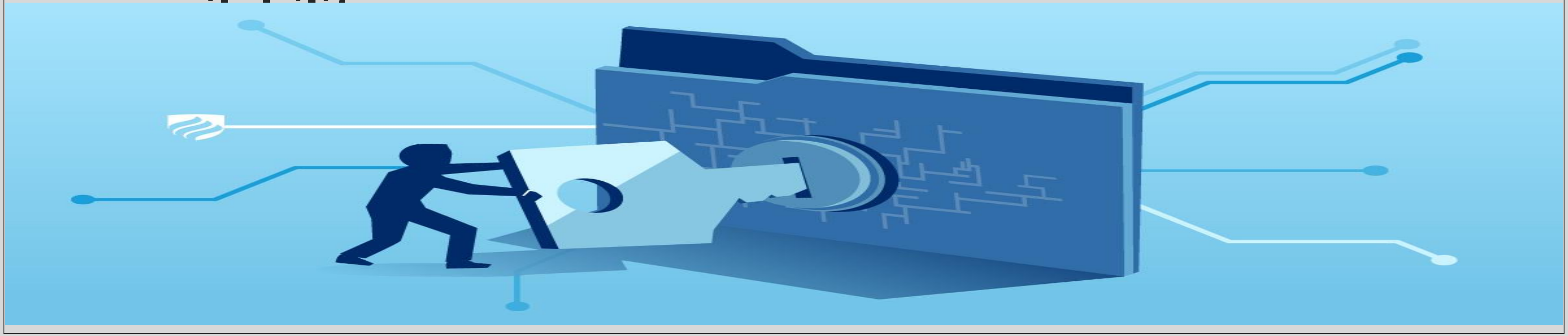
Information Assurance and Security 2

Information Assurance

- which focuses on ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of information and systems. These measures may include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Security

- which centers on the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability



Core of Information Assurance and Security

Confidentiality

Availability

Authenticity

Privacy

Non Repudiation

Integrity

Possession

Utility

Authorized Use

Confidentiality

- ***the state of being secret or of keeping secrets. An example of confidentiality is when a lawyer is not able to reveal the secrets of his clients because he has a duty to keep those secrets to himself.***

- Confidentiality, or not disclosing certain information, is important in a wide - range of jobs.

- Confidentiality matters for legal and reputational reasons, and it also matters because your future employment may depend on it.

- Some information is protected by law in several countries, including personally identifiable information and also 'trade secrets'.

Integrity

◦ integrity refers to the accuracy and completeness of data. Security controls focused on integrity are designed to prevent data from being modified or misused by an unauthorized party.

1. Encryption
2. User access controls
3. Version control
4. Backup and recovery procedures
5. Error detection software

Availability

- means that information is accessible to authorized users. It provides an assurance that your system and data can be accessed by authenticated users whenever they’re needed.

1.Off-site backups

2.Disaster recovery

3.Redundancy

4.Failover

5.Proper monitoring

6. Environmental controls
7. Virtualization
8. Server clustering
9. Continuity of operations planning

Possession

- is a category of user authentication credentials based on items that the user has with them, typically a hardware device such as a security token or a mobile phone used in conjunction with a software token.

Authenticity

- **The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.**

Utility

- a utility is a small program that provides an addition to the capabilities provided by the operating system. In some usages, a utility is a special and nonessential part of the operating system. ... In other usages, a utility is an application that is very specialized and relatively limited in capability.

Privacy

- is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties.

Authorized Use

- is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features. This is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.

Non Repudiation

- **Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.**

Information System Security

- **The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.**

Security Requirements of ISS

- **Data confidentiality - controlling who gets to read information in order to keep sensitive information from being disclosed to unauthorized recipients - e.g., preventing the disclosure of classified information to an adversary**
- **• Data integrity - assuring that information and programs are changed, altered, or modified only in a specified and authorized manner - e.g., preventing an adversary from modifying orders given to combat units so as to shape battlefield events to his advantage**
- **• System availability - assuring that authorized users have continued and timely access to information and resources - e.g., preventing an adversary from flooding a network with bogus traffic that delays legitimate traffic such as that containing new orders from being transmitted**
- **• System configuration- assuring that the configuration of a system or a network is changed only in accordance with established security guidelines and only by authorized users - e.g., detecting and reporting to higher authority the improper installation of a modem that can be used for remote access.**

Major Challenges to Information Systems Security

- **Networked Systems**
- **The Asymmetry Between Defence and Offense**
- **Ease-of-use compromises**
- **Perimeter defence**
- **Threats posed by insiders**
- **Passive defence**

Why we study Security?

- helps you understand how people, data, and technology work together within the business context. You will be able to apply what you learn to increase the effectiveness of business processes, secure organizational data, and enhance an organization's overall competitiveness.