FUNDAMENTALS OF CYBER SECURITY

UNIT 1

CYBER SECURITY GOALS

1. INTRODUCTION

This unit covers the details of cyber security goals. The unit has the objective of demonstrating the goals of cyber security enshrined in the need to protect the confidentiality of data, preserve the integrity of data and promote the availability of data for authorised users. These goals are referred to as the CIA triad that describes the major issues in data communication and security.

2. INTENDED LEARNING OUTCOMES (ILOS)

The intended learning outcome of this unit includes the following:

- Understanding the CIA triad of cyber security
- Describing the "C" in the CIA triad
- Explaining the "I" in the CIA triad
- Understanding the "A" in the CIA triad

3. Cyber Security Goals

The objective of Cybersecurity is to guard information from being stolen, compromised or attacked. Cybersecurity will be measured by a minimum of one among three goals-

1. Protect the confidentiality of information.
2. Preserve the integrity of knowledge.
3. Promote the provision of knowledge for authorized users.

These goals form the confidentiality, integrity, availability (CIA) triad,the idea of all security programs. The CIA triad could be a security model that's designed to guide policies for information security within the premises of a corporation or company. This model is additionally stated because the AIC (Availability, Integrity, and Confidentiality) triad to avoid the confusion with the American Central intelligence service.

the weather of the triad is considered the three most vital components of security.

The CIA criteria are one that the majority of the organizations and corporations use after they have installed a replacement application, creates a database or when guaranteeing access to some data. For data to be completely secure, all of those security goals must get effect. These are security policies where everyone works together, and thus it will be wrong to overlook one policy. The CIA is shown in Figure 1.2.

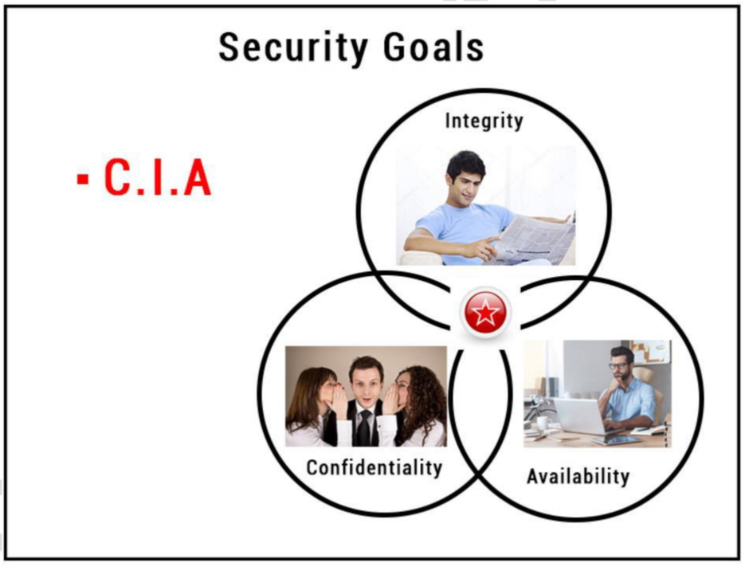

Figure 1.2: The CIA

3.1. Confidentiality

Confidentiality roughly corresponds to privacy and avoids the unauthorized disclosure of knowledge. It involves the protection of knowledge, providing access for people who can access it while disallowing others from learning anything about its content. It prevents essential information from reaching the inapt people while ensuring the correct people can access it. Encryption may be an ideal example to confirm confidentiality.

Tools for Confidentiality

a. Encryption

Encryption may be a method of reworking information to form it unreadable for unauthorized users by using an algorithm. The transformation of information uses a secret key (an encryption key) so the transformed data can only be read by using another secret key (decryption key). It protects sensitive data like the MasterCard numbers by encoding and remodelling data into incomprehensible cipher text. This encrypted data can only be read by decrypting it. Asymmetric-key and symmetric-key are the 2 primary kinds of encryption.

b. Access control

Access control outlines the rules and policies for limiting access to a system, physical or virtual resources. it's a process by which users are allowed access and given certain privileges to systems, resources or information. In access control systems, users must present their credentials before they will be granted access like the personality's name or a computer's serial number. In physical systems, these credentials may be available in many forms, but credentials that cannot be transferred provide the foremost security.

c. Authentication

An authentication may be a process that certifies and confirms a user's identity or applicable role that somebody has.

Authentication is often accomplished in a number of ways, but it's usually reinforced by a mix of something the user – has (e.g. a smart card or a radio key for keeping secret keys), knows (e.g. a password), is (e.g. a human biometric, fingerprint).

Authentication is an inevitable requirement of each establishment because it enables organizations to have their networks secured by permitting only authenticated users to access its secure resources. These resources may include networks, computer systems, websites, databases and other network-based applications or services.

d. Authorization

Authorization could be a security mechanism that grants permission to carry out something or take something. It's wont to determine what someone or a system is allowed access to resources, depending on the access control policy, including computer programs, services, files, information and application features. It's usually preceded by authentication for user biometric identification. System administrators are normally assigned permission levels that covers all system and user resources. During authorisation, users are either granted or refused resource access based on the results of system verified authenticated user's access rules.

e. Physical Security

Physical security describes measures designed to deny the unauthorised access of information technology assets like equipment, facilities, personnel, resources and other properties from damage. It safeguards these assets from physical threats including vandalism, theft, fire and natural disasters.

3.2 Integrity

Integrity refers to the methods for ensuring that data is real, correct and safeguarded from unauthorised user alteration. It’s the property that data has not be altered in an unauthorised way with a guarantee that the source of the obtained information is genuine.

Tools for Integrity

a. Backups

Backup is that process of periodically archiving of information. It's a process of creating copies of information or data files to use within the event when the first data or data files are lost or destroyed. it's also wont to make copies for historical purposes, like for longitudinal studies, statistics or for historical records or to fulfil the wants of an information retention policy. Many applications particularly within the Windows environment, produce backup files with the .BAK file extension.

b. Checksums

A checksum could be a numerical value for verifying the integrity of a file or an information transfer. Alternatively, it's the computation of a function that maps the contents of a file to a numerical value. They're typically applied in comparing two sets of information to confirm that they're identical. A checksum function depends on the whole contents of a file. It's designed in a special way that even a little or low change to the computer file (such as flipping one bit) is likely to leads to different output value.

c. Data Correcting Codes

It is a way of storing data such that little changes can be easily detected and corrected automatically.

3.3 Availability

Availability is that property wherein information is accessible and amendable in a timely manner by authorised users. It's the guarantee of consistent and continual access to sensitive data by authorised users.

Tools for Availability

a. **Physical Protections**

Physical safeguard means to preserve and make information available even within the event of physical challenges. It guarantees sensitive data and critical information technology resources are housed in secure areas.

b. **Computational Redundancies**

This is applied as fault tolerant against inadvertent faults. It protects computers and storage devices that function as fallbacks in the event of failures.