**UNIT – 1**

**Introduction**

Information technology is the vehicle that stores and transports information—a company’s most valuable resource—from one business unit to another. But what happens if the vehicle breaks down, even for a little while? As businesses have become more fluid, the concept of computer security has been replaced by the concept of information security.

Because this new concept covers a broader range of issues, from the protection of data to the protection of human resources, information security is no longer the sole responsibility of a discrete group of people in the company; rather, it is the responsibility of every employee, and especially managers.

Organizations must realize that information security funding and planning decisions involve more than just technical managers: Rather, the process should involve three distinct groups of decision makers, or communities of interest:

   Information security managers and professionals

   Information technology managers and professionals

Nontechnical business managers and professionals These communities of interest fulfill the following roles:

The information security community protects the organization’s information assets from the many threats they face.

The information technology community supports the business objectives of the organization by supplying and supporting information technology appropriate to the business’ needs.

The nontechnical general business community articulates and communicates organizational policy and objectives and allocates resources to the other groups.

**WHAT IS SECURITY?**

Understanding the technical aspects of information security requires that you know the definitions of certain information technology terms and concepts. In general, security is defined as “the quality or state of being secure—to be free from danger.”

Security is often achieved by means of several strategies usually undertaken simultaneously or used in combination with one another.

Specialized areas of security

o   **Physical security**, which encompasses strategies to protect people, physical assets, andthe workplace from various threats including fire, unauthorized access, or natural disasters

o   **Personal security**, which overlaps with physical security in the protection of the peoplewithin the organization

o   **Operations security**, which focuses on securing the organization’s ability to carry out itsoperational activities without interruption or compromise

o   **Communications security**, which encompasses the protection ofan organization’scommunications media, technology, and content, and its ability to use these tools to achieve the organization’s objectives

o   **Network security**, which addresses the protection of an organization’s data networkingdevices, connections, and contents, and the ability to use that network to accomplish the organization’s data communication functions

o   **Information security**includes the broad areas of information security management,computer and data security, and network security.

**Where it has been used?**

ü Governments, military, financial institutions, hospitals, and private businesses.

ü Protecting confidential information is a business requirement.

**Information Security components:**

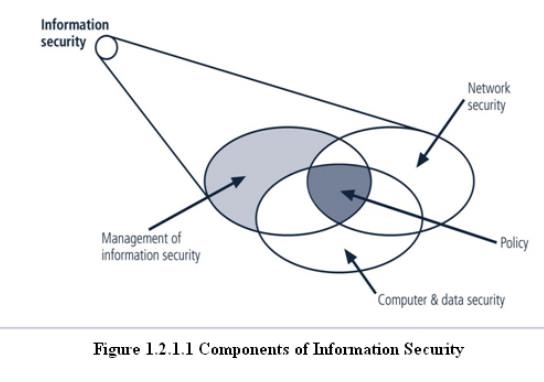
ü Confidentiality

ü Integrity

ü Availability(CIA)

**CIA Triangle**

The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a more comprehensive list of critical characteristics of information. At the heart of the study of information security is the concept of policy. Policy, awareness, training, education, and technology are vital concepts for the protection of information and for keeping information systems from danger.



**Critical Characteristics of Information** • The value of information comes from its characteristics: – Confidentiality: self-explanatory – Integrity: (Bitwise) identical to the original – Availability: of info, services, etc. – Authenticity: “it is what it claims to be” – Accuracy: free from mistakes and errors – Utility: self-explanatory – Possession: different from confidentiality

**There are three components of information security**, otherwise known as the CIA triad. They guide organizations on protecting important data through those three pillars of data security:

**Sign up for our newsletter!!**

Top of Form

Bottom of Form

1. Confidentiality
2. Integrity
3. Availability

The [CIA triad](https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA) is a framework for safeguarding data and is a fundamental cybersecurity standard.

The three elements of the CIA triad are confidentiality, integrity, and availability. These three aspects of information security work together to give your organization more comprehensive security strategies that protect sensitive information from multiple attack vectors.

Let’s take a deeper look into each of these pillars and how they fit into the full CIA triad.

**1. Confidentiality**

Data confidentiality means that data should only be available to those with authorized access. In your organization, employees need easy access to the data and information that they require to do their job. Keeping data confidential, though, means that employees only have access to the data that’s they absolutely need.

Limiting how many people have access to different data sets improves your organization's ability to keep sensitive information confidential.

Data confidentiality is also a major consideration in [identity and access management](https://dotsecurity.com/insights/blog-identity-access-management-standards) standards.

To achieve confidentiality, businesses can take advantage of data encryption technology and implement [MFA (multi-factor authentication)](https://dotsecurity.com/insights/blog-what-is-multifactor-authentication-and-what-are-some-examples). Data encryption is the process of “scrambling” data to make it unreadable until it is delivered to the right person or user, at which point a decryption key is used.

MFA requires a user to validate their identity through multiple methods, such as using a code delivered to a device or a biometric like a fingerprint.

**2. Integrity**

Data integrity means information should be intact, complete, and accurate.

To ensure data integrity, businesses can maintain and optimize their IT infrastructure, back up their data, and create a [data loss prevention plan](https://dotsecurity.com/cybersecurity-services/secure-data-protection) that protects them in case of a severe data breach.

Data integrity is crucial for employees who use insights drawn from that data in their day-to-day decision making. In turn, data integrity is critical for organizations who are looking to remain efficient, measure things like productivity, and want to develop a competitive edge.

If your data is corrupt, modified without authorization, or otherwise inaccurate you’ll have no real way of knowing if what your business is doing is working.

**3. Availability**

The last of the three CIA components of information security is data availability. Data availability means that a network, system, and necessary devices are ready to use as intended by authorized personnel.

Essentially, data availability refers to your employees' ability to access the data they need at any given moment without delay. There are several factors that can hinder access to data, even for authorized users – especially in the era of cloud technology wherein so much data is hosted off-site.

Cyberattacks, data leaks, and even neglected IT tech stacks can lead to delays in accessing data, or worse, non-operational downtime.

By prioritizing information security as a core aspect of your cybersecurity strategy, you can drastically improve the employee experience and the overall security of your network.

**SECURING COMPONENTS**

Protecting the components from potential misuse and abuse by unauthorized users.

ü **Subject of an attack**

Computer is used as an active tool to conduct the attack.

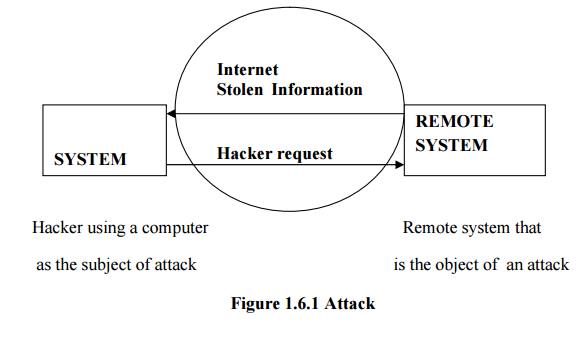
ü **Object of an attack**

Computer itself is the entity being attacked

**Two types of attacks:**

**1.**     **Direct attack**

**2.**     **Indirect attack**



**1.**  **Direct attack**

When a Hacker uses his personal computer to break into a system.[Originate from the threat itself]

**2.**  **Indirect attack**

When a system is compromised and used to attack other system.

[Originate from a system or resource that itself has been attacked, and is malfunctioning or working under the control of a threat].

A computer can, therefore, be both the subject and object of an attack when ,for example, it is first the object of an attack and then compromised and used to attack other systems, at which point it becomes the subject of an attack.

**BALANCING INFORMATION SECURITY AND ACCESS**

Impossible to obtain perfect security: it’s a process, not an absolute • Security should be considered balance between protection and availability • To achieve balance, level of security must allow reasonable access, yet protect against threats

 Security vs. Access Security • CIO: Two-factor authentication is necessary to protect private data • Auditor: We need to comply with laws/regulations … Access • Student 1: I forgot my authentication device • Student 2: It’s a hassle

**Approaches to Information Security Implementation**

ü Bottom- up- approach.

ü Top-down-approach

- Has higher probability of success.

- Project is initiated by upper level managers who issue policy & procedures & processes.

- Dictate the goals & expected outcomes of the project.

- Determine who is suitable for each of the required action.