All of the above information is considered crucial for the success of an organization. Information leaks could have catastrophic effects on organizations.

**Corporate Espionage: Insider/Outsider Threat**

Corporate espionage threats can be classified into the following two basic categories:

- **Insiders**: Insiders such as IT personnel, contractors, and other disgruntled employees who can be lured by monetary benefits are the main targets of corporate spies. An insider threat is always considered more potent than an outsider threat because insiders have legitimate access to the facilities, information, computers, and networks. According to the available study reports, almost 85% of espionage cases originate from within an organization. Insiders can easily misuse their privileges to leak sensitive information, and they can collaborate with an outsider. There are several factors that may prompt an insider to sell information to a competitor or spy, such as the following:
  - Lack of loyalty
  - Job dissatisfaction
  - Boredom
  - Mischief
  - Money

- **Outsiders**: Outsiders include corporate spies and attackers who have been hired by a competing organization or are motivated by personal gain. These people try to intrude into an organization’s affairs for the purpose of stealing sensitive information. An outsider can enter a company through Internet connection lines, physical break-ins, or partner (vendor, customer, or reseller) networks of the organization.

**Corporate Espionage Threat Due to Aggregation of Information**

Espionage is a great threat to organizations that practice information aggregation, where all information concerning an organization is brought together and stored in one location. Both insiders and outsiders can easily access critical information because there is only one point of infiltration.

In an insider attack, insiders with access privileges can tamper with, edit, overwrite, or send critical information to the organization’s competitors. In an outsider attack, an outsider who breaks into the private network of an organization can search, aggregate, and relate all the organization’s critical information.

**Techniques of Spying**

The following are some common spying techniques:

- **Hacking computers and networks**: This is an illegal technique for obtaining trade secrets and information. Hacking involves gaining unauthorized access to computers and networks.

- **Social engineering**: Social engineering is the use of influence and the art of manipulation to gain credentials. Individuals at any level of business or communicative interaction can make use of this method. All the security measures that organizations adopt are in vain when employees get socially engineered by strangers. Some examples of social engineering include unwittingly answering the questions of strangers, replying to spam e-mail, and bragging to coworkers.

- **Dumpster diving**: Dumpster diving is searching for sensitive information in the following places at a target organization:
  - Trash bins
  - Printer trash bins
  - User desks

- **Whacking**: Whacking is wireless hacking that is used to capture information passing through a wireless network.

- **Phone eavesdropping**: Phone eavesdropping is overhearing phone conversations while being physically present.