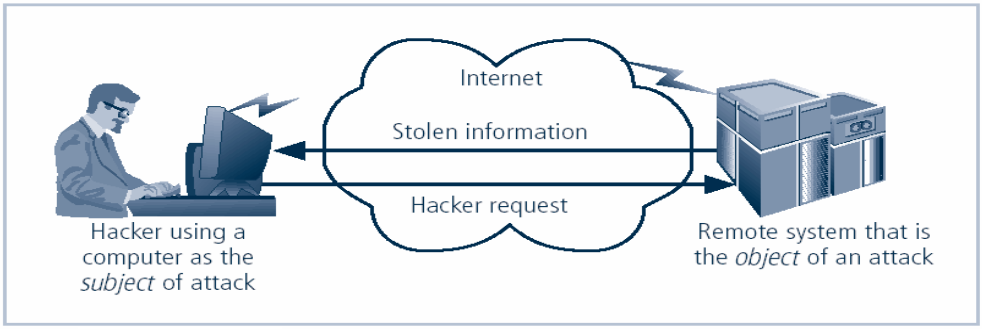
1. **Why C.I.A triangle is commonly used in information security? (MAY/JUNE 2014)**

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.

2. **When can a computer be a subject and an object of an attack respectively? (Nov/Dec 2012)**
   - A **subject** is an active entity which interacts with information system and can be an individual, technical component or computer process.
   - An **object** is a passive entity that receives or contains information and they are assigned with specific controls that restrict or prevent access by unauthorized subjects.



FIGU puter as the Subject and Object of an Attack

3. **How can organizations effectively mitigate and respond to the ever-evolving landscape of Information Security threats?**
   1. **Implement Robust Security Policies:** Organizations can mitigate information security threats by establishing and enforcing comprehensive security policies. These policies should cover aspects such as data access controls, password management, and acceptable use of organizational resources.
   2. **Continuous Employee Training:** Regular and up-to-date training programs can educate employees about the latest security threats and best practices. This helps in creating a security-aware culture within the organization, reducing the likelihood of human errors that could lead to security breaches.

4. **What is policy? How is it different from law? (NOV/DEC 2011, MAY/JUNE 2013)**

In an organization professionals help to maintain security through establishment and enforcement of policies. This policy is a body of expectations that describe acceptable and unacceptable employee behaviors in the workplace. The main difference between policy and law is that the ignorance of a policy is an acceptable defense.

5. **In risk management strategies, why does a periodic review have to be a part of process? (May/June 2012, May/June 2013)**

- The first focus is asset inventory
- The completeness and accuracy of the asset inventory has to be verified
- The threats and vulnerabilities that are dangerous to asset inventory must be verified.
- It is a constant process for safeguards and controls to be devised and implemented, and not to be installed and forget devices.

6. **What do you mean by Confinement problem?**

The confinement problem is a security issue that arises in a **multi-user** environment where **users** are allowed to **run programs** on a **shared system**. The problem is that a user may be able to **access data** or resources that they are not authorized to access. The confinement problem is the problem of **preventing a user** from **accessing data** or **resources** that they are not authorized to access.

7. **Define policy and standards.**

A policy is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters. Standards, on the other hand, are more detailed statements of what must be done to comply with policy. The organizational rules for acceptable/unacceptable behavior.

- Penalties for violations
- Appeals process

8. **Mention the Drawbacks of ISO 17799/BS 7799.**

Several countries have not adopted 17799 claiming there are fundamental problems:

- The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799

- 17799 lack “The necessary measurement precision of a technical standard”.
- There is no reason to believe that 17799 is more useful than any other approach currently available
- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls
- There is no reason to believe that 17799 is more useful than any other approach currently available
- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

9. **What are the advantages and disadvantages of using honey pot or padded cell approach?**

Advantages:

- Attackers can be diverted to targets that they cannot damage
- Administrators have time to decide how to respond to an attacker
- Attacker’s action can be easily and extensively monitored
- Honey pots may be effective at catching insiders who are snooping around a network

Disadvantages:

- The legal implications of using such devices are not well defined
- Honey pots and Padded cells have not yet been shown to be generally useful security technologies
- An expert attacker, once diverted into a decoy system, may become angry and launch a hostile attack against an organization’s systems
- Security managers will need a high level of expertise to use these systems

10. Distinguish between symmetric and asymmetric encryption.

Symmetric	Asymmetric
Uses the same secret (private) key to encrypt and decrypt its data	Uses both a public and private key.
Requires that the secret key be known by the party encrypting the data and the party decrypting the data.	Asymmetric allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be Decoded by the person having the private key.
Fast	1000 times slower than symmetric