Alpha Synopsys Inc
Advanced solutions-powered sourcing

Guide to IT Security

Over the years, Information and Technology (IT) has become an integral process of businesses and large organizations. IT systems include telecommunications equipments and computers for retrieval, storage, transfer or transmission, and manipulation of different types of data related to an organization or business. The question is: Are IT systems in organizations secure?

The truth is that IT systems are as much prone to security issues as are computers. Ensuring the security of IT system is a complex and extensive task and requires knowledge, time, and resources. Information and Technology systems in organizations store valuable data, loss of which can cripple the company or specific business processes. This brings us to the second question - What type of measures need to be put in place to ensure the security of IT systems in organizations?.

Layered Security Approach For IT Systems

In order to understand the security systems required for IT system, the possible threats need to be identified. There are basically 6 types of threats that can affect organizational information and technology systems and render them useless. These threats are often used for information theft. These threats include viruses, worms, trojan, rootkits, riskware, and spyware. These security threats can be transferred to the IT systems when they are connected to the internet or an external device like USB drives or infected hard disks.

In order to ensure security against these threats and to make an organizational IT system secure, a layered approach to security needs to be incorporated. The layered approach should consist of the following:

- **Physical security:**

There are times when people can physically break into a system and steal data. Hence, it is important to password protect valuable data on an employee's computer. Alternatively, the data can be encrypted in such a manner that only the users of those systems can decrypt. There are two types of encryption procedures that can be followed. The first is encryption of individual files and the second is full hard disk encryption.

- **Virus and other malware:**

Normally, spreading of virus and malware is deliberate. These are programs created to de-capacitate an IT system or to extract specific important data and information from them. The solution to this is available in the form of multiple firewalls and anti-virus or anti-malware programs. Regular scanning of computers and the network connecting the IT system will ensure that it is protected. Firewalls provide defense against intrusion by hackers or crackers.

❑ Access control:

The more number of people have access to the various IT systems, the higher the probability of a security lapse. There are many ways in which individuals outside the organization attack the IT systems and one of the most common methods is by initiating a brute force password attack. The solution is to create stronger passwords and restrict access to as few employees as possible.

❑ Segmentation:

This is a process by which you can limit access between the various network components. It also involves separating network components like separating the primary web server from the primary file server. This simply means that if a hacker were to attack your website then at least the primary data location of the organization will not be compromised due to separation from the network and restricted access.