Computer security by s

Business

Why Organizations need security? As discussed above, the organizations in this century more increasingly depend on data communication for the daily business communication, database information retrieval and the internetworking of LAN's. This led the management into more consideration on converting manual operations into computerized systems and relay on them. In fact, organizations then considered that "..

.. many potential hazards such as fraud, errors, lost data, breaches of privacy and the disastrous events that can occur in a data communication" (3) The above consideration statement was considered about fifteen years ago but still holds valid reasons. Computer and network address three requirements: 1. Security Requires that the information in a computer system only be accessible for reading by authorized personnel or parties. This type of access includes printing, displaying , and other form of disclosure, including simply revealing the existence of an object.

2. Integrity Requires that the computer system access can vibe modified only by authorized personals. Modification includes writing, chaining, changing status, deleting, and creating. 3. Availability Requires that the computer system access are available to authorized personnel. The essence of security operations is managing and controlling access to equipment and facilities within an organization.

The crux of the security problem is providing simple and inexpensive access on a wide-reach basis even protect the physical securities from harm and sensitive information from unauthorized users. Therefore, the organizations can define their own security policies and responsibilities for various aspects of security within, which would lead to a great successful in reducing the threat of the organization. (1). In an article called ' Strategic Dimensions of Networking Behavior (5) brings the same argument that the first step should be either to devise or to revise a comprehensive security policy for the organizations and that should be educated to the employees about their responsibilities for protecting the organization's information. Types of Network Security There are two types of attacks involved in release of message contents and traffic analysis. A release of message contents is easily understood.

A telephone conversation, an electronic mail message, a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions. The second passive attack, traffic analysis is more sublet. Suppose that we had a way of masking the contents of messages or other information traffic so that opponent, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages.

The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be use full in guessing the nature of the communication that was taking place. Passive attacks are very difficult to detect because they do not involve any alteration of the data. However, it is feasible to prevent the success of these attacks. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

One is Passive attack and active attacks. Passive attacks mean the eavesdropping on, or monitoring of, transmission. The goal of the opponent is to obtain information that is being transmitted. …