Introduction to Information Security

Security can be defined as the degree of protection against criminal activity, danger, damage, and/or loss. Following this broad defi nition, information security refers to all of the processes and policies designed to protect an organization's information and information systems (IS) from unauthorized access, use, disclosure, disruption, modification, or destruction.

Before continuing, let's consider these key concepts. Organizations collect huge amounts of information and employ numerous information systems that are subject to myriad threats. A threat to an information resource is any danger to which a system may be exposed. The exposure of an information resource is the harm, loss, or damage that can result if a threat compromises that resource. An information resource's vulnerability is the possibility that the system will be harmed by a threat.

Today, fIve key factors are contributing to the increasing vulnerability of organizational information resources, making it much more diffi cult to secure them:

• Today's interconnected, interdependent, wirelessly networked business environment;

• Smaller, faster, cheaper computers and storage devices;

• Decreasing skills necessary to be a computer hacker

• International organized crime taking over cybercrime;

• Lack of management support

The first factor is the evolution of the IT resource from mainframe-only to today's highly complex, interconnected, interdependent, wirelessly networked business environment. The Internet now enables millions of computers and computer networks to communicate freely and seamlessly with one another. Organizations and individuals are exposed to a world of untrusted networks and potential attackers. A trusted network, in general, is any network within your organization. An untrusted network, in general, is any network external to your organization. In addition, wireless technologies enable employees to compute, communicate, and access the Internet anywhere and anytime. Significantly, wireless is an inherently nonsecure broadcast communications medium.

The second factor reflects the fact that modern computers and storage devices (e.g., thumb drives or flash drives) continue to become smaller, faster, cheaper, and more portable, with greater storage capacity. These characteristics make it

much easier to steal or lose a computer or storage device that contains huge amounts of sensitive information. Also, far more people are able to afford powerful computers and connect inexpensively to the Internet, thus raising the potential of an attack on information assets

The third factor is that the computing skills necessary to be a hacker are decreasing. The reason is that the Internet contains information and computer programs called scripts that users with few skills can download and use to attack any information system connected to the Internet. (Security experts can also use these scripts for legitimate purposes, such as testing the security of various systems.)

The fourth factor is that international organized crime is taking over cybercrime. Cybercrime refers to illegal activities conducted over computer networks, particularly the Internet. iDefense (http://labs.idefense.com), a company that specializes in providing security information to governments and Fortune 500 companies, maintains that groups of well-organized criminal organizations have taken control of a global billion-dollar crime network. The network, powered by skillful hackers, targets known software security weaknesses. These crimes are typically nonviolent, but quite lucrative. For example, the losses from armed robberies average hundreds of dollars, and those from white-collar crimes average tens of thousands of dollars. In contrast, losses from computer crimes average hundreds of thousands of dollars. Also, computer crimes can be committed from anywhere in the world, at any time, effectively providing an international safe haven for cybercriminals. Computer-based crimes cause billions of dollars in damages to businesses each year, including the costs to repair information systems and the costs of lost business

The fi fth, and fi nal, factor is lack of management support. For the entire organization to take security policies and procedures seriously, senior managers must set the tone. Ultimately, however, lower-level managers may be even more important. These managers are in close contact with employees every day and thus are in a better position to determine whether employees are following security procedures