Chapter II
Computer Security in Cybercafés

Oghenevwogaga Benson Adogbeji
Delta State University, Nigeria

ABSTRACT

The purpose of this chapter is to address the security breaches in cybercafés and also suggest measures of securing the unsecured computers. In order that cybercafés operate breach free Internet services, there is need for measures to be put in place to secure their network. This chapter of the book therefore unveils the security situation in cybercafés with the view to address network security, network breaches, and methods of protecting cybercafés' systems. The chapter reveals some ways through which cybercafés encountered breaches such as Trojan horse programs, back door and remote administration programs, unauthorized access, denial of service, and so forth, and equally suggests measures of protecting the computers or networks such as installation of firewalls, use of antivirus, avoidance of opening unknown attachments, disabling of hidden filename extensions, keeping all applications parched, disconnecting from the net when not in use, regular backup of data, virtual private networks, and so forth.

INTRODUCTION

Computer security is the process of preventing and detecting unauthorized use of a computer and to stop unauthorized users, also known as *intruders* from accessing our computer. It is the means and measures adopted to secure our computers from destruction and infections. *Computer insecurity* is higher when computers are open to share resources. The best way to keep an intruder from entering the network is to provide a security wall between the intruder and the corporate (cyberfaces) network (Hawkins, Yen, & Chou, 2000). This sharing of resources is mainly through a

computer network. *Computer network* therefore is the interconnection of two or more computers for the purpose of sharing resources such as hardware and software in the network; that need also to be secured. This involves sharing of data, network resources, message transmission, and sharing of Internet connection.

Network security is the process and means of protecting and detecting unauthorized users of having access to or tampering with the resources in the network. Resources in the Internet are so numerous and important that there comes the need to protect them. The *Internet* is not a single network, but a vast array of loosely connected networks situated all over the world, easily accessible by individual computer hosts in a variety of ways. The Internet, being a global tool through which information are accessed and provided among others, uses gateways, routers, dial-up connections, and Internet service providers (ISPs) to make itself readily available at all times. Therefore, individuals and organizations world wide can reach any point on the network without regard to national or geographic boundaries or time of day (GCIS, 2006). The fact that the Internet keeps up-to-date information, access to such information is so easy and quick; it then created open access to individuals and organizations. Therefore, when a company (cybercafé) is connected to the Internet, any user in cyberspace can have access to its Web site. Installing *firewalls*, intrusion detection systems (IDS), and user authentication software are the necessary precautions a company must take to protect themselves (Hawkins et al., 2000).

However, while using the Internet, along with convenience and speed of access to information, there are risks involved. Among these risks in the Internet are the risks that valuable information will be lost, stolen, corrupted, or misused and that the computer systems will be corrupted (GCIS, 2006). These risks manifest in the form of *network security breaches*. These security breaches create an avenue for insecurity in *computer networks*, mostly in cybercafés and other private users' computers.

Security breaches are the penetration of an unauthorized user into a computer or computer network with the view to access information in such computers or networks and sometimes cause damage to data or information in such computers or networks; security breaches are in every category according to a 1998 information security industry study. The study surveyed 1,050 readers who worked in computer, data processing education, finance, insurance, government, law, manufacturing, health care, or military. Three out of four organizations experienced a virus in 1998 (Shim, Qureshi, & Siegel, 2000).

Although it is difficult for intruders to have access to information printed on paper and kept in cabinet, access to such information becomes difficult because of lack of sharing, which the Internet offers. As a result of timeliness and quick access to information, it becomes vital to have the Internet, which offers services from different Web servers that share resources to the users. These resources become accessible to users and even the *intruders* and *hackers*, among others, hence there is need for network security. Nobody on the net is fully or completely immune to security breach. Those after use include banks and financial companies, insurance companies, brokerage courses consultants, government contractors, hospitals, and so forth (GCIS, 2006). The *intruders* can steal; tamper with information without torching a piece of paper. They can create new electronic files, run their own programs, and even hide all evidence of their unauthorized activity. This intrusion has become a thing of concern to every user of the Internet. Nevertheless, the three basic *security* concepts important to information on the net include confidentiality, integrity, and availability. It is expected that data on the net must be treated with element of confidentiality; one should not lose confidence in such data as there is need to secure such data to avoid unauthorized users having access to such data or information. Secondly, the integrity of the data must be guaranteed such that data are not modified or tampered