Chapter VI
Cybercafé Physical and Electronic Security Issues

Adetoun A. Oyelude
University of Ibadan, Nigeria

Cecilia O. Bolajoko Adewumi
University of Ibadan, Nigeria

ABSTRACT

An overview of physical and electronic security issues in cybercafés in Ibadan city, Nigeria is presented in this chapter. The security measures taken by cybercafé managers for physical and electronic facilities and clients also, were observed in an in-depth study of sixty cybercafés purposively selected for location, popularity, and wide range of services offered, over a period of 2 months. Participatory observation, in-depth interview, and questionnaire methods were adopted, using trained research assistants. Results of the findings showed that cybercafé operators are having a hard time, some folding up due to activities of criminals, and the war against cyber crime can be better tackled if the operators have skilled staff to man the cafés; security measures like passwords that are hard to break, and especially monitor customers who do overnight browsing. Hackers and spammers caught should be handed over to law enforcement agents who will stick to the rule of law.

INTRODUCTION

The cybercafé is a café or shop open to the public, where a computer can be hired for a period of half an hour or more to access the Internet, write curriculum vitae, or play a game (Stewart, 1999). It serves as a rallying point for all sorts of information seekers and givers. Cybercafés have become so important that it is necessary to give a background to how they came into being.

Cybercafés are established in the public places of modern cities and towns and villages around the world. In December 1999 an online cybercafé guide listed 4397 cafés around the world. With the explosion in the use and profile of the Internet and personal use of new information and communications technology-'multimedia', cybercafés have become part of contemporary culture. In January 2000, there were about 72.4 million hosts on the Internet, and of these the third world is participating with a mere 3%. About 85% of worldwide Internet hosts are in the G7 countries, which make up only about 10% of world population. On the other hand, the most populated countries of the third world—China, India, Brazil, and Nigeria all together make up less than 1% of all hosts with more than 40% of world population. In developing countries there are only full Internet connections with all services in the capital cities and since there are three basic requirements for Internet access, that is, telephone connection, computer, and electricity, they are invaluable.

The reality however, is that one in three people lack electricity globally and 80% of the world population does not have a telephone line. The percentage of those who have is very low as shown.

Computers also suffer the same fate, as in year 2000, 28.32% of all computers were in the United States of America (USA), and Europe had 26.73% while countries like India and Mexico shared 1.08%. For countries without direct access to the Internet, costs of being connected are usually very high. Monthly fees for an Internet connection are often unreachable for common people in developing countries (Afemann, 2000). The costs of maintaining the facilities also posed problem. To overcome the big hurdles in financing individual Internet access, many civil organizations in developing nations found a more suitable way of using the Internet and decided to establish facilities called cybercafés, where several users at a fee could access the Internet.

In managing the cybercafés, security measures have to be taken to protect the equipment and the persons working as well as the clients. The equipment has to be physically protected by for example, labeling them through inscribing, and using iron bars on windows and doors to prevent theft. This helps protect staff and users.

Electronic security involves making the computers and the information on them, and received through them, safe for general use, and restricting usage of information that could be tampered with, or that could be used for criminal purposes, for example, keeping financial records away from open access.

This chapter discusses physical and security issues with respect to cybercafé management, as well as crimes committed using the Internet (now referred to as cyber crime). These issues would not be coming up if the incidence of cyber

Table 1. Telephone density in low & middle-income countries (Source: World Development Report 1998/99)

Region	No. of Tel.lines/100pers
East Asia & Pacific	4.1
Europe & Central Asia	18.5
Latin America & Caribbean	10.2
Middle East & N. Africa	6.5
South Asia	1.4
Sub-Saharan Africa	1.4