Cybercafés, which are places where Internet access is provided for a fee, provide the opportunity for people without access to the Internet or who are traveling to access Web mail and instant messages, read newspapers, and explore other resources of the Net (Adomi, 2005; Adomi, 2007; Adomi, Okiy, & Ruteyan, 2003; Adomi, Omodeko, & Otolo, 2004). As noted by Stewart (2000), the explosion in the use and profile of the Internet and personal use of new information and communications technology—multimedia—has made cybercafés to become part of contemporary culture, established among the public places of modern cities, towns, and villages around the world.

In the contemporary era, it is very difficult to think of an urban area that is not connected with the Internet, especially for people who use the medium for routine communication, transactions, and so forth. A cybercafé’s facilities access to the Internet through computers in a relaxed atmosphere for people belonging to different age groups and having diverse socio-economic backgrounds. Cybercafés are often not selective about the clientele and satisfying users’ varying needs for example, besides providing Internet, consultation, and publishing, some serve food and liquor. In some areas, cybercafés have become a preferred gathering place for the people of different ages, income, and level of computer knowledge and skills (Rathore & Alhabshi, 2005).

It should be noted that cybercafé is not a transitory phenomenon but the evolution an extension of an old and traditional institution, the café. Cybercafés may service and reflect the communication and information needs of people living in a global society, but they place this in a local context through provision of a social space and a convenient and hospitable location for technology access (Stewart, 2000).

Though cybercafés have been used as places for facilitating e-communication and socialization in different parts of the world, they like other Internet based organizations experience “local” security problems and can be used as avenues to caused/launch security breaches/attacks to others (individuals and organizations) that are connected to the Internet. Whenever computers are connected to the Internet, they are exposed to attacks from intruders (Liverpool John Mores University, 2007). This is because the technology user group had changed from one consisting mainly of researchers and academics which has resulted in a shift from the desired results of improving economics to increase in the risk of using information technology as well (Rudasill & Moyer, 2004). Cybercafés can experience systems/network security breaches such as cracking, hacking, virus, worms, and so forth (see for example, chapter one of this book, by Lawan Mohammed), security breaches can cause computers and network malfunction and even breakdown of the systems and network of an affected cybercafé. Security is a key factor for organizations when adopting Web services in their mission critical business transactions. Without taking cares of security, enterprises like cybercafés could not use Web services in the insecure Internet environment (Rosado, Gutierrez, Fernandez-Medina, & Piattini, 2006). The Internet has become increasingly
complex, leaving many organizations vulnerable to malicious attacks. Organizations are therefore faced with trying to protect their infrastructure against network security attacks, as well as attacks that are specific to the security layer (F5 Networks Inc., 2004).

Cybercafés are set up in order for the entrepreneurs to make money and to enable their clients to access the Net. When security breaches occur in the cafes, this could lead to dissatisfaction of clients which eventually may affect income, especially if measures are not taken to correct such breaches quickly. It would even be better for cybercafés to put security measures in place to prevent occurrence of breaches. Installation of antivirus software, firewall, and so forth, could assist cybercafés to prevent occurrence of network attacks. Knowledge of network security would also enhance cybercafé security as it has been found that few café personnel know little about hacking/Internet security (ApiAP, 2005).

Apart from cybercafés being potential victims of cyber attack, cybercafés can be used by cybercriminals to launch attacks on individuals and organizations. Criminals can explore the anonymity provided by cybercafés to commit cyber defamation, terrorism, hacking, and so forth (Gruenwald, 2001). In order to stem the activities of cyber criminals who use cybercafés to carry out their negative acts, governments of some countries have taken steps to regulate the operations of cafes within their jurisdictions (Gruenwald, 2001; Hong Kong Legislative Council Panel on Home Affairs, 2002; Glaser, 2003; Rathore & Alhabshi, 2005). The regulations include requiring cybercafés to install software filters to block some sites, compelling clients to show identity cards among others. Several cafes have been raided and even closed down for failing to comply with government orders. While restrictions on and closure of cybercafés may hamper Internet access for some users in the short term, such moves have not been able to hurt cafes popularity down the road (Gruenwald, 2001).

Software which is the detailed instrument that controls the operation of the computer system (Laudon & Laudon, 2001) is very crucial to the smooth and successful operations of computers that are connected to the Internet. Software is a necessary requirement in a cybercafé. As noted by Ajewole in chapter two of this book, it is essential to install necessary software in a café because the demands of the typical cybercafé user are numerous, that besides the basic software usually bundled with operating systems, there are other software required to make customers visit to a café a successful one. A cybercafé operator needs to install software that should ensure the smooth operation and management of the systems, network, and enhance client satisfaction.

The objective of this book is to:

- Be a source book on cybercafé systems/network security and software
- Provide background information to scholars and researchers who are interested in carrying out research on cybercafé security and software
- Furnish teachers of information technology with necessary knowledge of systems/network security which they can impart to their students/trainees
- Be a source book on cyber crime perpetration, detection, and prevention in cybercafés and other network environments
- Acquaint cybercafé operators and personnel with necessary information on security and software required to run and manage a café successfully

**ORGANIZATION OF THE BOOK**

The book is organized into XIX chapters. A brief description of each of the chapters follows:

**Chapter I** introduces the vulnerability and security issues associated with the use and operations of Internet cafés or cybercafés by demonstrating different methods of launching different attacks. The
author discusses the challenges facing those operating and managing Internet cafes. He also argues that defense mechanism against breaches should be dynamic and strong enough due to the increasing number of new freely available cracking tools and harmful Web sites.

**Chapter II** looks at security situations in cybercafes with the view to unveil network security, network breaches, and methods of protecting cybercafes’ systems. The author explores various ways through which cybercafes experience breaches and the methods of protecting the cybercafes computers from such attacks.

**Chapter III** focuses on how cyber cafe security policy can be used to reduce criminal activities perpetrated in Nigerian cybercafes against individuals and organizations. The author proposes that, if Nigeria and Nigerians are to benefit from the highly electronic modern business environment, it is essential for relevant authorities to develop and implement an all-encompassing cybercafe security policy.

**Chapter IV** concentrates on issues and threats to children cyber security vis-à-vis access to useful children online literature and the implications for sub Saharan Africa. The author points out that Africa could learn a lot from developed countries on how to balance between accesses to useful online information resources against the growing cyber crime targeting children.

**Chapter V** takes a look at the use of campus cybercafes as a possible solution to the inadequate or lack of Internet facilities in university libraries. The authors discusses the issues, controversies, and problems of the cafe operations in relation to cyber security in order to determine the level of security awareness among their users, identify serious security threats, and to find out the type of anti-virus software used.

**Chapter VI** investigates physical and electronic security issues in cybercafes in Ibadan city, Nigeria. The security measures taken by cybercafe managers for physical and electronic facilities and clients also were investigated in an in-depth study. Participatory observation, interview, and questionnaire methods were adopted.

**Chapter VII** offers an alternate perspective upon issues of management and security in cybercafes. It places attention upon the wider social environment in which cybercafes operate and the development of ‘soft’ skills in cybercafe management in order to mitigate security risks.

**Chapter VIII** provides an insight into the meaning of cybercafe management software, eatures of cybercafe management software, cybercafe management software systems requirement, criteria for selecting cybercafe management software, some examples of cybercafe management software, the role of cybercafe management software in enhancing Internet security, limitations of cybercafe software, future trends, and future research direction.

**Chapter IX** discusses basic software that should be found in a typical cybercafe setup. The author broadly divides software required for a cafe into those for the server side and client side of the network. He states that though a whole lot of software could be used in a cafe, the actual software installed and used depends on general client’s requirements and/or the operator’s amount of know-how/preferences which may vary across different environments

**Chapter X** examines the nature of maleware evolution and various facets of maleware threats. The authors further present appropriate strategies for maleware detection, prevention, and mitigation through appropriate use of safeguards.

**Chapter XI** dwells on viruses, types of viruses, classification of viruses, sources of viruses in cybercafes, why cybercafe systems are vulnerable to attacks or infections, and how to detect virus infections or symptoms of virus infection in cybercafe systems/ networks. It also focuses on virus prevention and control in cybercafes.
Chapter XII examines computer viruses, some of the devices used by hackers to circumvent the security of cybercafé systems. The history, sources, spread, detection, and removal of viruses are set forth.

Chapter XIII focuses on a research intended to determine certain evaluation and selection processes used to acquire software to meet business objectives and the requirement of users in an Internet based organization. The results confirmed that the organization, Media24 uses the suggested protocol as noted in the theory of for software acquisition in most cases.

Chapter XIV examines the existing cyber laws in some commonwealth countries and the United States jurisdictions. The author compares the various definitions accorded to cyber crimes in these countries. She examines and discusses when cyber crime occurs in the various jurisdictions, the significance of jurisdiction for Internet criminals in all these countries, as well as when cybercafé operators are liable in cyber related crimes

Chapter XV looks at the concept of cyber crimes as it relates to cyber café. The author discusses various forms of cyber crimes, what cyber crimes are as they relate to cybercafés, finds out how cyber crimes are perpetrated, identifies the various forms of cyber crimes, and explores how cyber crimes can be controlled and prevented in cybercafés.

Chapter XVI introduces the cybercafés of Nepal and explores the prospect of criminals exploiting them to commit global cyber crimes. The author discusses cybercafés and cyber crimes and introduces them with specific reference to Nepal, based on research carried out, he argues that they can be easily exploited to commit cyber crimes. Further, in terms of the facts that have emerged from the research, appropriate recommendations have also been derived and presented.

Chapter XVII describes the use of the Internet by terrorists in cybercafés and explores measures intended to stem the use of cybercafes for terrorist activities. Specifically, the authors x-ray the reasons terrorists use of the Internet, how they use the Net, their motivations for utilization of cybercafés, various measures adopted in different countries for combating terrorists’ use of cafes for their acts, and impediments to prevention of terrorism via cybercafés.

Chapter XVIII discusses the challenges and problems governments and other stakeholders are facing in fighting and controlling cyber crimes in developing countries’ cybercafés. It reveals reasons for the increase in the incidences of cyber crimes in developing countries; strategies to control and tackle the problem of cyber crimes are also highlighted.

Chapter XIX highlights the various categories of persons involved in cyber crime in Nigeria. It identifies the different agencies established by the government to curb the crime and their roles and the factors affecting cyber crimes in Nigeria. The author makes recommendations on how cyber crime can be prevented in cybercafés.

REFERENCES


