Security and Software for Cybercafés

Esharenana E. Adomi
Delta State University, Nigeria
Table of Contents

Foreword ............................................................................................................................................ xiv

Preface ................................................................................................................................................ xvi

Acknowledgment ............................................................................................................................... xxi

Section I
Cybercafé Security

Chapter I
Cybercafé Systems Security ................................................................................................................... 1
Lawan Ahmed Mohammed, King Fahd University of Petroleum and Minerals,
Saudi Arabia

Chapter II
Computer Security in Cybercafés ........................................................................................................ 18
Oghenevwogaga Benson Adogbeji, Delta State University, Nigeria

Chapter III
Enhancing Social Security through Appropriate Cybercafé Security Policy in Nigeria .................... 30
Samuel Chiedu Avemaria Utulu, Bells University of Technology, Nigeria

Chapter IV
Cyber Security of Children: Implications for Sub-Saharan Africa.................................................. 46
Stephen M. Mutula, University of Botswana, Botswana

Chapter V
Issues, Controversies, and Problems of Cybercafés Located in a University Campus...................... 62
Henrietta O.C. Otokunefor, University of Port Harcourt, Nigeria
Hudron K. Kari, University of Port Harcourt, Nigeria
Chapter VI
Cybercafé Physical and Electronic Security Issues .......................................................... 84
  Adetoun A. Oyelude, University of Ibadan, Nigeria
  Cecilia O. Bolajoko Adewumi, University of Ibadan, Nigeria

Chapter VII
Managing Cybercafés: Achieving Mutual Benefit through Partnership .................... 95
  Darlington Onojaefe, Nelson Mandela Metropolitan University, South Africa
  Marcus Leaning, Trinity College, University of Wales, UK

Section II
Cybercafé Software

Chapter VIII
Cybercafé Management Software ............................................................................. 113
  Alexander Ozoemelem Obuh, Delta State University, Nigeria

Chapter IX
Software Requirements for Cybercafés ..................................................................... 125
  Ayotokunbo I. Ajewole, Network Operations Center (NOC), Nigeria

Chapter X
Maleware: An Evolving Threat .................................................................................. 147
  Steven Furnell, University of Plymouth, UK
  Jeremy Ward, Symantec EMEA, UK

Chapter XI
Viruses and Virus Protection in Cybercafés ............................................................... 170
  Alexander Ozoemelem Obuh, Delta State University, Nigeria

Chapter XII
Computer Virus Phenomena in Cybercafés .............................................................. 186
  Garuba Abdul Rahman, University of Benin, Nigeria

Chapter XIII
A Case Study on the Selection and Evaluation of Software for an Internet Organisation .... 205
  Pieter van Staaden, Media24 Ltd., South Africa
Section III
Cybercafés, Cyber Laws, and Control of Cyber Crime

Chapter XIV
Cyber Laws and Cybercafés: Analysis of Operational Legislation in some Commonwealth Jurisdictions and the United States

Yemisi Dina, York University, Canada

Chapter XV
Prevention of Cyber Crime in Cybercafés

Ogochukwu Thaddaeus Emiri, Delta State University, Nigeria

Chapter XVI
Cybercafés of Nepal: Passage to Cyber Crime?

Deepak Rauniar, South Asia Partnership International, Nepal

Chapter XVII
Cybercafés and Prevention of Terrorist Activities

Esharenana E. Adomi, Delta State University, Nigeria
Williams P. Akpochafo, Delta State University, Nigeria

Chapter XVIII
Cyber Crime Control in Developing Countries’ Cybercafés

Stella E. Igun, Delta State University, Nigeria

Chapter XIX
Cybercafés and Cyber Crime in Nigeria

Pereware Aghwotu Tiemo, Delta State University, Nigeria
Christiana Uyoyou Charles-Iyoha, Centre for Policy and Development, Nigeria

Compilation of References

About the Contributors

Index
Detailed Table of Contents

Foreword ........................................................................................................................................................ xiv
Preface .......................................................................................................................................................... xvi
Acknowledgment ........................................................................................................................................... xxi

Section I
Cybercafe Security

Chapter I
Cybercafe Systems Security ......................................................................................................................... 1
Lawan Ahmed Mohammed, King Fahd University of Petroleum and Minerals,
Saudi Arabia

This chapter 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 especially
when using commercial Internet cafés in a way that renders the system or other systems inoperable. It
discusses the challenges facing those operating and managing Internet cafes, governments, parents, and
even educators to ensure proper preventive measures, guidelines, and laws needed to protect the system
against breaches, misuses, and abuses. It 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. In addition, virus, worms, Trojan horse, adware, malware, and spyware are spreading
beyond imagination. Further, the chapter discusses different defense mechanisms.

Chapter II
Computer Security in Cybercafés .................................................................................................................. 18
Oghenevwogaga Benson Adogbeji, Delta State University, Nigeria

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.

Chapter III
Enhancing Social Security through Appropriate Cybercafé Security Policy in Nigeria

Samuel Chiedu Avernia Utulu, Bells University of Technology, Nigeria

The crucial role cybercafés play in the use of the Internet for business necessitates the development of appropriate cybercafé security policy in Nigeria. This chapter looks at how cybercafé security policy can be used to reduce criminal activities perpetrated in Nigerian cybercafés against individuals and organizations who use the Internet for various business transactions. The chapter proposes that, if Nigeria and Nigerians are to benefit from the highly electronized modern business environment, developing and implementing an all-encompassing cybercafé security policy has become a must. It was therefore concluded that such a policy should be a part of National Information Policy and should cover both technical security needs and social security needs.

Chapter IV
Cyber Security of Children: Implications for Sub-Saharan Africa

Stephen M. Mutula, University of Botswana, Botswana

This author discusses issues and threats to children’s cyber security vis-à-vis access to useful children online literature and the implications for sub-saharan Africa. The author points out that whereas the benefits of online children literature are immense especially in Africa where there is paucity of print literature, increasing cyber security and crime targeting children is of growing concern to governments, school teachers, parents, and Internet service providers. The chapter observes that whereas the developed world has made attempts to put in place mechanisms and systems such as acceptable user policies and protection software to mitigate undesirable consequences of online insecurity to which children are the most vulnerable, Africa is lagging behind despite the pervading Internet on the continent. The author notes that censorship of online literature is not the panacea to cyber insecurity, but parents should work closely with teachers and service providers to find pragmatic ways of protecting children online. Africa could learn a lot from developed countries on how to balance between access to useful online information resources against the growing cyber crime targeting children. The author cautions that the future of online security with regard to children’s safety in cyberspace is bound to become more complex as technologies become more advanced and online predators evolve sophisticated ways to circumvent online security measures, calling for the development of a proactive security strategy to protect children online.
Chapter V
Issues, Controversies, and Problems of Cybercafés Located in a University Campus

Henrietta O.C. Otokunefor, University of Port Harcourt, Nigeria
Hudron K. Kari, University of Port Harcourt, Nigeria

This chapter takes a look at the use of campus cybercafés as a possible solution to the inadequate or lack of Internet facilities in Nigerian university libraries. It argues that campus cybercafés are most likely for now the avenue whereby their faculty, students, researchers, and other members of the university community can have online access to the world’s leading peer-reviewed journals. This is because some of the libraries are yet to have Internet facilities while those that do have, do not have enough to cater for the large population of users. Secondly, these libraries through three or more global initiatives are provided with free online journal access in support of the UN millennium development goals making campus cybercafés partners in the provision of Internet facilities to the university communities in which they are located. The chapter therefore discusses the issues, controversies, and problems of their operations in relation to cyber security in order to know 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
Cybercafé Physical and Electronic Security Issues

Adetoun A. Oyelude, University of Ibadan, Nigeria
Cecilia O. Bolajoko Adewumi, University of Ibadan, Nigeria

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 being 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.

Chapter VII
Managing Cybercafés: Achieving Mutual Benefit through Partnership

Darlington Onojaefe, Nelson Mandela Metropolitan University, South Africa
Marcus Leaning, Trinity College, University of Wales, UK

This chapter offers an alternate perspective upon issues of management and security in cybercafés. Here attention is placed upon the wider social environment in which the cybercafé operates and the development of ‘soft’ skills in cybercafé management in order to mitigate security risks. Three key arguments are made: first, it is noted that cybercafés offer a key means by which small business may
access ICT. Second, that the relationships that cybercafés may foster are beneficial to all parties and that such relationships bring additional benefits in terms of trust and social capital. Third, that in order to develop such partnerships, new skill sets may be required.

Section II
Cybercafé Software

Chapter VIII
Cybercafé Management Software

Alexander Ozoemelem Obuh, Delta State University, Nigeria

This chapter is intended to provide an insight into cybercafé management software. Specifically, it gives the meaning of cybercafé management software, features of cybercafé management software, cybercafé management software systems requirement, criteria for selecting cybercafé management software, some examples of cybercafé management software, the role of cybercafé management software in enhancing Internet security, limitations of cybercafé software, future trends, and future research direction. It is argued that cybercafé management software has the capability of keeping a large client database with which it draws its strength for asset tracking, calculating client’s bonus on patronage, and in keeping an audit trail thus securing financial transactions.

Chapter IX
Software Requirements for Cybercafés

Ayotokunbo I. Ajewole, Network Operations Center (NOC), Nigeria

This chapter discusses basic software that should be found in a typical cybercafé setup. ‘Software requirements’ are broadly divided into requirements for the server side and client side of the network. As a commercial venture, it is of great importance that only necessary software be found installed in a cybercafé, to meet the café user’s need. Starting with an introduction, a general overview of the café user’s needs are set forth, thereby leading to the division into two broad areas: server and client side. An outline of the chapter is given. The background section gives some details on some basic terminologies (server, client, operating system, etc.) that a cybercafé user/prospective operator might want to get acquainted with. Software requirements for the server side of the café network are discussed first; general features of timing softwares, notes on Internet security, viruses, and spyware. As the café server is a very important element in café management, it is necessary that the server is not overwhelmed by unnecessary tasks thereby leading to a generally slow network. Software for the client side of the café network is discussed next with emphasis on basic software applications often used/requested by café users. Examples of such are word processing applications and graphics viewing software. Since a lot of computer literate people are familiar with the Windows operating system, all software discussed for client use derives from such a perspective. Some security issues necessary for maintaining crisp client computers are also discussed. Due to lack of in-depth knowledge about information security among internet users, the future trends section discusses the applicability of the personal Internet communicator in the Nigerian environment, because of its portability and built in security. Other possible trends in security and cyber-crime are also discussed. The chapter ends with a note that café users will continue to demand faster Internet speeds,
and therefore operators must be on the search for latest software to meet their needs, latest security software to keep their café network always clean and secure. Future research directions include software development research to allow café users modify or design their desktops to their own taste while in the café. Complete café solution software is also proposed to cater for everything from operating systems to end-user applications which can be installed once, and from a single source. Literature used for this chapter is sourced mainly from the Internet, and from personal experience of the author, as there are not literatures dealing with ‘cybercafé software’ on a specific note. A whole lot of software are been used, and could be used in a café. This depends actually on general client’s requirements and/or the operator’s amount of know-how preferences which may vary across different environments.

Chapter X
Maleware: An Evolving Threat................................................................. 147

Steven Furnell, University of Plymouth, UK
Jeremy Ward, Symantec EMEA, UK

In the two decades since its first significant appearance, malware has become the most prominent and costly threat to modern IT systems. This chapter examines the nature of malware evolution. It highlights that, as well as the more obvious development of propagation techniques, the nature of payload activities (and the related motivations of the malware creators) is also significantly changing, as is the ability of the malware to defeat defences. Having established the various facets of the threat, the discussion proceeds to consider appropriate strategies for malware detection and prevention, considering the role of modern antivirus software, and its use alongside other network security technologies to give more comprehensive protection. It is concluded that although malware is likely to remain a significant and ever-present threat, the risk and resultant impacts can be substantially mitigated by appropriate use of such safeguards.

Chapter XI
Viruses and Virus Protection in Cybercafes.............................................. 170

Alexander Ozoemelem Obuh, Delta State University, Nigeria

The objective of this chapter is to give an insight to virus, virus infection, and prevention in cybercafes. Specifically, it gives the meaning of virus, types of viruses, classification of viruses, sources of viruses in cybercafes, why cybercafé systems are vulnerable to attacks or infections, how to detect virus infections or symptoms of virus infection in cybercafé systems or networks, virus prevention and control, and future trends. It is argued that with the advent of WiFi technologies, virus writers can launch their dubious malcode from just about anywhere in the world, and as such there exist a form of cyber-terrorism that cannot be easily stopped.

Chapter XII
Computer Virus Phenomena in Cybercafes ............................................. 186

Garuba Abdul Rahman, University of Benin, Nigeria

The chapter examines the concepts, history, sources, spread, detection, and removal of computer viruses. The increase in the number of computers and accessibility to Internet has made it easy for hackers to
Chapter XIII
A Case Study on the Selection and Evaluation of Software for an Internet Organisation

Pieter van Staaden, Media24 Ltd., South Africa

The author conducted research to determine whether IT managers, IT auditors, users, management, etc. (all decision-makers) use a certain evaluation and selection process to acquire software to meet business objectives and the requirement of users. An argument was used that the more thorough the software evaluation and selection process, the more likely it would be that the organisation will chose software that meets these targets. The main objective of the research was therefore to determine whether Media24 uses evaluation methods and obtains the desired results. The results confirmed that Media24 uses suggested protocol as noted in the theory for software acquisition correctly during most stages.

Section III

Cybercafés, Cyber Laws, and Control of Cyber Crime

Chapter XIV
Cyber Laws and Cybercafés: Analysis of Operational Legislation in some Commonwealth Jurisdictions and the United States

Yemisi Dina, York University, Canada

This chapter will discuss the existing cyber laws in some commonwealth countries and the United States jurisdictions. It compares the various definitions accorded to cyber crimes in these countries. It examines and discusses when cyber crime occurs in the various jurisdictions regardless of where it originates, the laws that apply to pornography, 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
Prevention of Cyber Crime in Cybercafés

Ogochukwu Thaddaeus Emiri, Delta State University, Nigeria

The purpose of this chapter is to examine the concept of cyber crime as it relates to cybercafés, forms of cyber crime, the role of the Internet, and suggest measures of cyber crime control and prevention in cybercafés. This chapter unveils the various forms of cyber crime and preventive measures with the view to addressing insecurity on the Internet and methods of protecting cybercafés systems. This chapter revealed some forms of cyber crimes to include computer viruses, data dwindling, hacking, data leakages,
trapdoors, scavenging, e-mail bombing, and so forth, and equally suggested preventive measures such as user education, legal regulations against cyber crimes, international cooperation, restricting system use, limiting access to certain programs, and so forth.

Chapter XVI
Cybercafés of Nepal: Passage to Cyber Crime? ................................................................. 253

Deepak Rauniar, South Asia Partnership International, Nepal

The chapter introduces the cybercafés of Nepal and explores the prospect of someone (persons, criminals) exploiting them to commit global cyber crimes. Cybercafés are public places of Internet and are considered important tools of society for access to information and e-services of all kinds. However, by the virtue of being public places, they also stand vulnerable to misuse in terms of cyber crimes. The chapter discusses cybercafés and cyber crimes and introduces them with specific reference to Nepal—a country in south Asia nestled between two information technology giants, India and China. The chapter also discusses the cyber law of the country. Based on research carried out with the objectives of assessing the scenario in which the cybercafés operate in Nepal, it has been argued 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
Cybercafés and Prevention of Terrorist Activities ............................................................ 270

Esharenana E. Adomi, Delta State University, Nigeria
William P. Akpochafo, Delta State University, Nigeria

The purpose of this chapter is to describe the use of the Internet by terrorists in cybercafés and explore measures intended to stem the use of cybercafés for terrorist activities. Specifically, 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 cafés for their acts, impediment to prevention of terrorism via cybercafés, and future trends are set forth.

Chapter XVIII
Cyber Crime Control in Developing Countries’ Cybercafés .............................................. 283

Stella E. Igun, Delta State University, Nigeria

This chapter discusses the challenges and problems governments and other stakeholders are facing in fighting and controlling cyber crimes in developing countries cybercafés. The chapter’s main focus is on the developing countries vulnerability to cyber crimes; these countries lack major infrastructural devices for controlling cyber crimes at the moment. The nature of cyber crime and Internet in developing countries is pathetic, in that the cyber crime rate is high and transnational (affecting the developing countries all the same) and the developing countries are still very low in Internet connection. Furthermore, the chapter reveals reasons for the increase in the incidences of cyber crimes in developing countries; cyber crime laws that have been enacted to control and tackle the problem of cyber crimes are also highlighted.
Chapter XIX
Cybercafés and Cyber Crime in Nigeria

Pereware Aghwotu Tiemo, Delta State University, Nigeria
Christiana Uyoyou Charles-Iyoha, Centre for Policy and Development, Nigeria

This chapter discusses cybercafés and cyber crime in Nigeria. It also identifies the various cyber criminals in Nigeria. The working groups set up by the government to redeem the image of Nigerians by monitoring cybercafés and handling cases of cyber criminals and cyber victims are also discussed. Some major factors affecting the rise in cyber crime in Nigeria and methods of preventing cyber crimes (scam mail) are outlined. It was recommended that there is need to educate the populace on café fraud and in fighting cyber crime, the working group established by the government needed to be adequately equipped with ICT knowledge and facilities.

Compilation of References

About the Contributors

Index
Foreword

The importance of information and the protection of its integrity against ever-increasing cyber risks and threats necessitate that businesses ensure that reasonable steps are taken to secure their information assets, resources, and systems, failing which may render them legally liable. In recent years considerable effort has been made to protect information assets, especially in the form of customer, client, and patient information against unauthorised disclosure and misuse. However, it is not often that one comes across a study focusing on cybercafés and the importance of its cyber security infrastructure. This topic is often ignored and/or neglected as focus is generally placed on the importance of corporate cyber security. This book, however, correctly highlights the importance of cybercafés. Cybercafés are often used in various countries to conduct day-to-day business and conclude important transactions. Cybercafés are in fact one of the best ways in which the digital divide can be breached. It is therefore encouraging that this topic is highlighted in the book.

In the preface to this book the editor pronounces the purpose of this work as being to provide essential information on cybercafé systems/network security and software. In evaluating this expressed intention it must be stated that this work definitely succeeds in meeting this objectives, as is evident in the practical style of the book. While network and system administrators are provided with an in-depth and detailed explanation of the conceptual basis and practical aspects of cyber security in cybercafés, I cannot help but feel that educators and students interested and specialising in cyber security will also derive great value from this work.

Security and software for cybercafés aims to provide a thorough exposition of all the aspects of cyber security in cybercafés. This is evident from the work’s scope and structure. The work’s layout is very organised. A number of characteristics are evident from this work as a whole. Firstly, the emphasis is on practicality. When one has regard to the contents of the work it is clear that its purpose is to make cyber security in specifically cybercafé’s more accessible to the reader. This work not only provides network and system administrators with a detailed background knowledge of cyber security, but also guides them on how to apply it in cybercafés. Secondly, it must be noted that in my opinion the value of this work for students and practitioners is to be found in the manner in which the contributors succeeds to combine theory with practice. Thirdly, I am of the opinion that this book will prove to be a valuable contribution not only to developing countries but also to first world countries as this will enable the latter to better understand the numerous challenges facing cyber security in developing countries. The
research contained in this book is comprehensive and thorough and should be viewed as a stepping stone for further studies on this subject-matter.

Verine Etsebeth  
Information Security Specialist  
University of Johannesburg  
South Africa

Verine Etsebeth lectures at the University of Johannesburg, South Africa. She holds a L.L.B. degree, Hdip labour law (cum laude) and Hdip corporate law (cum laude) and L.L.M. (cum laude) entitled “The Legal Implication of Information Security Governance.” She has completed her LLD entitled “Corporate and Individual Civil Liability for Information Security Breaches and Incidents” and handed it for external examination in September, 2007. She is also finishing a higher diploma in tax law this year. She has also published various articles in legal journals and has presented papers at national and international conferences.
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 cyber criminals 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 cybercafés with the view to unveil network security, network breaches, and methods of protecting cybercafés’ systems. The author explores various ways through which cybercafés experience breaches and the methods of protecting the cybercafés computers from such attacks.

**Chapter III** focuses on how cyber café security policy can be used to reduce criminal activities perpetrated in Nigerian cybercafés 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 cybercafé 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 cybercafés 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 café 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 cybercafés in Ibadan city, Nigeria. The security measures taken by cybercafé 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 cybercafés. It places attention upon the wider social environment in which cybercafés operate and the development of ‘soft’ skills in cybercafé management in order to mitigate security risks.

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

**Chapter IX** discusses basic software that should be found in a typical cybercafé setup. The author broadly divides software required for a café 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 café, 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 malware evolution and various facets of malware threats. The authors further present appropriate strategies for malware detection, prevention, and mitigation through appropriate use of safeguards.

**Chapter XI** dwells on viruses, types of viruses, classification of viruses, sources of viruses in cybercafés, why cybercafé systems are vulnerable to attacks or infections, and how to detect virus infections or symptoms of virus infection in cybercafé systems/ networks. It also focuses on virus prevention and control in cybercafés.
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 cybercafés 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