Winter 2-20-2019

A Review of Trends and Issues of Cybersecurity in Academic Libraries

Ifeoma Ajie
ifeomapeters9@gmail.com

Introduction

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term *security* implies cyber security. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Security remains near the top of the list of strategic issues facing higher education institutions. Given the increasing volume of information that needs to be protected, the expanding body of rules, regulations, and laws governing information security and privacy, and the current economic downturn, which makes it even harder for an institution to obtain the funding necessary to keep up with requirements, this is not at all surprising. Security is not strictly a technology matter; indeed, it is a foundational element for almost all academic libraries. Responsibility for security needs to extend beyond information technology to every functional office in the institution and to the highest level of management. IT professionals can assist in this endeavor by not limiting their own perspective to IT and by modeling behavior to treat security and privacy best practices as everybody's responsibility.

Purpose of paper

The importance of information resources cannot be overemphasized as users depend on library resources for knowledge and new ideas to enhance intellectual development. As a result, libraries faced varying degrees of delinquency in the use of their resources. The extent of this problem varies from one library to another. Previously theft and defacement were the order of the day but now that we are in the technology age, cyber threats have plagued academic libraries thereby making it necessary for the emergence of cyber security.

Structure of paper

There would be a brief background to security in general, perspective of cybersecurity, forms of cyber security, cyber security actions, consequences of inactions , cyber ethics, conclusion and recommendation.

Background to the study

Different libraries have adopted varying security measures for their collections' safety. McComb (2004) writes that physical (non-electronic) security, electronic security and security policies/procedures are substantial methods for securing information resources of all kinds of libraries. Physical security includes architectural considerations, the use of personnel, and security hardware to prevent crimes against library collections. Electronic security system refers to the use of equipment which typically provide alarm notification to the appropriate authority on entry control and site surveillance. Major elements of the electronic security system include burglary protection, collection security (hidden on materials), access control (systems that directly "read" unique personal characteristics such as voice quality, hand geometry, identity cards, etc.), and video surveillance, particularly the CCTV system. Sensors (detectors) to detect an intrusion and alarms (to notify appropriate authorities) are the facilities that make this type of security electronic (www.alarm.org). On the other hand, security policies and procedures include all created and implemented security policies, procedures, and plans for the library. These should, at least, include entry and exit procedures, room registration procedures, personal belonging restrictions, special collections use policies, and entry key management procedures (McComb, 2004).

Cybersecurity is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of "cyber-threat" is rather vague and implies the malicious use of information and communication technology (ICT) either as a target or as a tool by a wide range of malevolent actors. Cybersecurity is often confused with national security while national security, according

to the co-ordinator of NCWG, Udotai (2002) in Odumesi (2006) may often be implicated in some cases of cybersecurity. Cybersecurity as a term refers only to security of networks and systems- computers, electronics and ancillary devices. Typical cybersecurity issues, according to Udotai (2002) in Odumesi (2006) include: confidentiality of information; and integrity of systems and survivability of networks (CIS). Major objective of cybersecurity includes: protection of system/networks against unauthorised access and data alteration from within; and defense against intrusion from without. As commonly used, the term "cybersecurity" refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks,

related hardware and software devices, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to national security;

2. The degree of protection resulting from the application of these activities and measures;

3. The associate field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality.

Cybersecurity is thus more than just information security or data security, but is closely related to those two fields, because information security lies at the heart of the matter. Information security refers to all aspects of protecting information. Most often, these aspects are classified in three categories: confidentiality, integrity, and availability of information. Confidentiality" refers to the protection of information from disclosure to unauthenticated parties, while "integrity" refers to the protection of information from unauthorised changes. "Availability" means the information should be available to authorised parties when requested. Sometimes, "accountability" the requirement that the actions of an entity be uniquely traceable to that entity is added to the list.

The first goal of modern information security has, in effect, become to ensure that systems are predictably dependable in the face of all sorts of malice and particularly in the face of denial-of-service attacks. The dominance of network topologies has implications for the shape of the protection policies and, subsequently, in determining appropriate protection efforts, goals, strategies, and instruments for problem solution:

1. Cybersecurity as an Information Technology issue: Cybersecurity can be approached as an IT security or information assurance issue, with a strong focus on Internet security. Policies are thus aimed at countering threats to the information infrastructure by technical means such as firewalls, anti-virus software, or intrusion detection software. The main threats perceived range from accident, system failures, bad programming, and human failures to hacker attacks.

2. Cybersecurity as an economic issue: Cybersecurity is relevant to the business continuity, and especially to e- business, which requires permanent access to ICT infrastructures and permanently available business processes to ensure satisfactory business performance. The main actors are representatives of the private sector. The main threats are viruses and worms, human failures, but also hacker attacks of all sorts, and acts of cybercrime.

3. Cybersecurity as a law enforcement issue: Cybersecurity is seen as relevant to cybercrime. Cybercrime is a very broad term with various meanings, and definition can include everything from technology-enabled crimes to crimes committed against individual computers. The main actors are law enforcers. The main threats are acts of computer criminality, but also cyber terrorism.

4. Cybersecurity is a national security issue: Society as a whole and its core values are endangered, due to their dependence on ICT. Action against the threat is aimed at several levels (the technical, legislative, organisational, or international levels). The main actors are security specialists. The main threats are terrorists, but also information warfare threats from other states.

Forms of cyber threats

(a) Hardware Security Threats

Hardware, form as a physical component in an information system is also prone to security attacks. Previous study results (Ke, 1997; Lin and Huang, 1999; and Shen, 1999) revealed several factors that jeopardise hardware security including:

a) Natural disasters such as earthquakes, fires, floods and thunder strokes;

b) Changes in temperature or humidity;

c) Accidents, such as stealing and vandalism;

d) Malicious intrusion and destruction;

e) Defects of the hardware itself, such as bugs or errors generated from routers or firewalls;

f) Faults in the manufacture of the equipment;

g) Air-conditioning failure;

h) Loss of essential services such as telecommunications or power. Other hardware security threats include electromagnetic interference, failure of communication equipment and services, hardware equipment failure, installation of unauthorised hardware, maintenance errors, physical sabotage or intentional destruction of computing equipment, theft, physical sabotage and vandalism of ICT hardware equipment.

Farahmand, et al. (2003) indicated that hardware attacks can be mounted against hardware for the purpose of using the hardware as a means of denying use of the system. These may include a physical attack against the equipment, a bug implanted within the hardware or an attack against the supporting utilities. Computer hardware infected with malware (i.e. computer viruses, worms and Trojan horses) may suffer some sort of damage such as making it impossible to boot the computer, repeated error messages, hardware malfunctions and lowered the computing speed.

(b) Software Security Threats

In terms of jeopardising software security, the threats can be divided into operating systems and related applications. Security threats associate with operating systems might include the security loopholes due to improper design and improper management. Whereas, software security threats related with applications include stealing or copying software from the Internet which might contain viruses (Shen, 1999). Computer software infected with malware (i.e. computer viruses, worms and Trojan horses) may suffer some sort of damage such as periodically automatic reboots, program crashes or malfunctions, repeated error messages and poorer system performance or unusual behavior.

Other software security threats include corruption by system, system failure, maintenance errors, cyber-terrorism, software piracy, unauthorised access, unauthorised changes to software settings, adware, spyware, hacking, password sniffing, weak passwords and abuse of computer access control. Farahmand, et al. (2003) reported that software attacks can range from discreet alterations to less discreet changes. They indicated that for the discreet alterations, attacks are subtly imposed for the purpose of compromising the system. In contrast, for the less discreet changes, attacks are intended to destruct of data or other important systems features. There are several software security threats that could jeopardise software security such as follows:

i. Abuse of computer access control refers to employees or patrons abusing their access controls rights and privileges for personal reasons or to obtain more data than needed for their jobs;

ii. Adware and Spyware is a type of malware that can be installed on computers to collect information about users without their knowledge. Specifically, adware is used as a marketing tool to monitor people's behaviour on the Internet, to determine which products they are interested in. Whereas, the functions of spyware extend well beyond simple monitoring. Spyware programs can change computer settings, resulting in slow connection speeds and loss of Internet connection or functionality of other programs;

iii. Corruption by system, system errors, or failure of system software. According to Laprie et al. (1992) “a system failure occurs when the delivered service no longer complies with the specifications". Whereas, an error is defined by Laprie et al. (1992) as that part of the system which is liable to lead to subsequent failure, and an error affecting the service is an indication that a failure occurs or has occurred. If the system comprises of multiple components, errors can lead to a component failure. As various components in the system interact, failure of one component might introduce one or more faults in another;

iv. Hacking refers to unauthorised attempts to bypass the security mechanisms of an information system or network either skilled or unskilled persons.

v. Intrusion refers to unauthorised access to system resources such as public access workstations to obtain unauthorised access to resources and can cause damage or loss of data;

vi. Installation or use of unauthorised programmes or software can cause security threat as it associated with the risk of introducing viruses and other unwanted risks into the public-access and administrative library computers. Malicious software can be accidentally or intentionally installed on computers from portable drives, email accounts and web browsing. Allowing these programs to run on workstations presents a serious challenge to the IT administrator’s.

vii. Internet threats such as malicious code, Trojans and spyware could make desktop vulnerable to leakage of important corporate information (Gawde, 2004);

viii. A password is also vulnerable to sniffing or stealing every time it sent across a network such as when users are using remote access to access computers, printers, databases, emails or Internet banking;

ix. The integrity, reliability, confidentiality and availability of the information processed by programme or software could be threatened if errors are made during the programme or software development, maintenance or installation process. For instance, Microsoft has released software which made systems vulnerable to security breaches such as Hotmail,

Microsoft Outlook and Outlook Express software. Microsoft Outlook and Outlook Express software had a bug that could allow malicious code to run on a computer without the knowledge of the user and allow the hacker to use the user's access rights to reformat the disk drive, change data or communicate with other external sites;

x. The use of pirated or unauthorised software on the library network is illegal and places the library in danger of legal action by the software supplier. Thus, ensuring that the software on library computer systems is fully licensed is a responsibility of the IT personnel as f libraries are found to be in noncompliance, the consequences can be quite expensive;

xi. Unauthorised changes to software settings or to program code can be used to commit fraud, destroy data or compromise the integrity of a computer system. This would involve a manipulation of settings in the browser such as to delete history files, change security settings or enable private browsing. In order to prevent users from accidentally changing their system settings, a clear separation of functions between software programming staff and operational IT staff who implement all authorised changes should be made clear;

xii. Use of library Internet for illegal or illicit communications or activities such (e.g. porn surfing, e-mail harassment or porn surfing)

xiii. Cyber-terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored on cyberspace which can cause fear and violence against persons or property (Denning, 2000).

(c) Network Security Threats

Yeh and Chang (2007) reported that networks were rated as contributing the most severe among IS security threats but had the lowest level of protection among Taiwanese enterprises. Williams (2001) listed the most common network security threats in small libraries such as;

a) Cracking of passwords;

b) Damage to equipment or data due to lightning strike, surges or inadequate power;

c) Internet based attacks of internal network resources;

d) Local patron tampering workstation desktop and systems that the intruder has found to be vulnerable (Eisenberg and Lawthers, 2005);

ix. Transmission errors may occur due to the failure of any of the network components that are used for the transmission of data. These errors can destroy the integrity and reliability of data and can lead to a loss of availability;

x. Website defacement is an attack usually initiate by a system cracker who breaks into a web server and changes the visual appearance of the website. Penetration and hacking of web sites is increasing due to the growth of virtual private networks and online business.

(d) Data Security Threats

Data security is the practice of protecting and ensuring privacy of personal or corporate data resides in databases, network servers or personal computers from corruption and unauthorised access. The ISO 7498-2:1989 (1989) document considers the threats to data as:

1) Destruction of information and other resources,

2) Corruption or modification of information,

3) Theft, removal or loss of information and other resources,

4) Disclosure of information;

5) Interruption of services.

There are several other threats that could jeopardise data security such as follows:

a) Data diddling or changing of data before or during input into a computer system;

b) Data loss due to wrong procedures of updating, storage or backup;

c) Data manipulation;

e) Delay in updating or dissemination;

f) Destruction due to natural disaster;

g) Exposure of patrons sensitive data through web attack;

h) Impersonation or social engineering;

i)Loss of patron data or privacy ideas;

j) Malware and Malicious code (e.g. virus, worm, Trojan horse, logic/time bombs and trapdoor);

k) Masquerading of user identity;

l) Password attacks, sniffing, stealing, phishing or pharming;

m) Theft of proprietary data;

n) Unauthorised access;

o) Unauthorised data copying;

p) Unauthorised transfer of data; and

q) Unauthorised, accidental disclosure, modifications or alteration of data.

Malware refers to computer viruses, worms, Trojans and any other kinds of malicious program designed to damage data by infecting open files and program libraries on an operating system, deleting data and files in the hard drives, steal information and send it to third parties for illegitimate reasons.

(e) Physical Facilities and Environmental Threats

The most common problem of physical threats that must be factored into a security program includes natural disaster and theft. It has been reported that the relationship between physical threats and virtual threats is most apparent as both physical infrastructure and systems are needed to provide an access point to the virtual world (Lindstrom, 2003). Tittel et al. (2003) listed the most common types of physical threats including:

1) Fire and smoke;

2) Water (rising or falling);

3) Earth movement (earthquakes, landslides or volcanoes);

4) Storms (wind, lightning, rain, snow, sleet or ice);

5) Sabotage or vandalism;

6) Explosion or destruction;

7) Building collapse;

8) Toxic materials;

9) Utility loss (power, heating, cooling, air or water);

10) Equipment failure; and

11) Personnel loss (strikes, illness, access or transport).

Perhaps the most prevalent threat is the natural calamity caused by natural and manmade environmental problems. Computing equipment, physical infrastructure assets and data can be destroyed due to fire, floods, electricity spikes and power outages.

Besides that, chemical, radiological and biological hazards can also cause damage to electronic equipment both from intentional attack or accidental discharge in an information system environment (Vacca, 2009). Intrusion or authorised access into library building is seen as another threatening threat which can lead to theft of valuable materials. For instance, stolen computing and network equipment can be resold on the black market for the value of its computing power. In addition, physical attacks can also occur at system consoles through available ethernet ports and in network equipment or wiring closets rooms (Lindstrom, 2003).

(f) Human Related Threats

Prior literature consistently reports that human errors are the most highly ranked security threats (Loch, Carr and Warkentin,1992; Whitman, 2004; Im and Baskerville, 2005). Instances of poor security practices that may put an organisations's IS security at risk caused by human are human errors, poor passwords selection, piggybacking, shoulder surfing, dumpster diving, installing unauthorised hardware and software, access by unauthorised users and social engineering, lack of discipline or knowledge among library staff and patrons (e.g. no data backups) (Pipkin, 2000 and Conklin, et. al., 2005). Dhillon's study (1999) indicated that

computer fraud by insiders is recognised as a severe problem which could be difficult to prevent especially when it blends with legitimate transactions.

Human errors including data entry errors or carelessness, though often not considered as threats but they are highly likely to occur. Lindstrom (2003) revealed that erroneous actions by employees or users can threaten the integrity, availability, confidentiality and reliability of data. Examples include:

1) Incorrect set-up of security features could result in loss of confidentiality, integrity and availability of data;

2) Switching off computers when an error is displayed instead of correctly closing all current applications;

3) Deletion of files;

4) Inadequate back-ups; and

5) Processing of incorrect versions of data.

Employee misconducts especially in large corporation may be the most difficult problem to manage, as use of perfect intrusion detection controls become irrelevant when trusted employees either accidentally or unknowingly do something they should not do (Swartz, 2006). Gawde (2004) reported that as much as 80% of the security compromises are due to actions by insiders. The effects of employees' misuses to or negligence. Yeh and Chang (2007) listed seven countermeasures for protecting the data including use of information backup, authentication for data access controls, authorisation for user access rights, enforced path, event logging, procedures for information handling, management of removable media and disposal of media.

(g) Physical Facilities and Environmental Security Measure

The term physical and environmental security refers to measures taken to protect the library systems, buildings and related supporting infrastructures or resources (including air

conditioning, power supply, water supply and lighting) against physical damage associated with fire, flood and physical intrusion (INTOSAI, 1995). The use of security personnel to undertake patrol within the library and to enforce appropriate library access at the main lobby has become increasingly common (Rajendran and Rathinasabapathy, 2007). However, they should not necessarily have access rights to IS, sensitive output and secure areas during quiet hours to prevent abuse of privilege (INTOSAI, 1995).

Other use of physical security systems or the non-electronic systems in libraries include:

a) inspection of bags and other belongings of library users while entering and leaving the library by security or library staff,

b) visual inspection by library staff through floor walks to overcome the unethical practices,

c) the use of window protection with locks, grills, guards, bars, screens and films, door protection, display case protection and dummy security devises to controlled access to the library buildings and library collections.

Rajendran and Rathinasabapathy (2007) also suggest the use of electronic security systems to overcome the security threats in the library by using the following tools:

1) Burglar protection to provide alarm notification to the appropriate authorities,

2) Electromagnetic system to combat library material theft,

3) Electronic surveillance cameras to monitor the library entry control and site surveillance,

4) Radio Frequency Identification (RFID) system for easy handling and security of the library collection. These electronic security systems are believed to be effective in reducing the levels of theft and unethical practices within the library premises at reasonable cost for many libraries.

Another popular physical security measure in libraries is the use of air conditioner.

This is because the computers and their peripherals often have specific environmental requirements. Failing to comply with the environmental conditions specified by the manufacturer may lead to machine failure and disputes over maintenance (INTOSAI, 1995).

Beside air conditioners, Yeh and Chang (2007) also encouraged the use of lightning protectors, fireproof installations, waterproof installations and quakeproof installations to protect the IS against physical damage due to natural disasters.

Cyber Safety Actions

(Davis n.d) highlighted seven safety actions that academic libraries can adopt and they are:-

1) Install software updates: - Updates sometime called *patches* fix problems with operating systems and software programmes.
2) Run Anti-virus Software: - To avoid computer problems caused by viruses, its necessary to install and run anti-virus programmes periodically and to always update it. Antivirus software removes viruses, quarantines and repairs infected files and can help prevent future viruses.
3) Prevent Identity Theft:- Financial account numbers, Social security numbers and details on drivers license or personal identity information should not be given out. Another thing to look out for is phishing scams which is a form of fraud that uses email messages that appear to be from a reputable business in attempt to gain personal or account information.
4) Turn on Personal Firewalls :- Firewalls act as protective barriers between computers and the internet. If computers have built in fire walls, hackers who search the internet by sending out pings(calls) to random computers and wait for response will wait in vain. Firewalls prevent your computer from responding to these calls.
5) Avoid Spyware/ Adware:- Spyware and Adware should be avoided because they take up memory ad can slow down your computer or cause other problems.
6) Protect Passwords:- Passwords should not be shared and new passwords should be difficult to guess by avoiding dictionary words, mixing letters, numbers and

punctuation. Passwords should be a mixture of upper and lower case letters, minimum of 8 characters and mnemonics to help remember a difficult password.

7) Back up important files:- To reduce the risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.

Consequences of Inactions

(Davis n.d) gave three consequences of inaction and they are:-

1) Loss of access to the libraries computing network
2) Loss of confidentiality, integrity and/ or availability of valuable university information, research and /or personal electronic data.
3) Lawsuits , loss of public trust and / or grant opportunities, prosecution, internal disciplinary action or termination of employment.

Cyber Ethics

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. (Reddy 2014) noted some cyber ethics, below are a few of them:

Do use the Internet to communicate and interact with other people**.** Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world.

Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.

Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.

Do not operate others accounts using their passwords.

Never try to send any kind of malware to other's systems and make them corrupt.

Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.

When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.

Always adhere to copyrighted information and download games or videos only if they are permissible.

Conclusion

The issue of cyber security in university libraries is an issue that requires serious managerial and strategic attention. Cyber security should not be allowed to flourish in academic libraries due to their financial and social consequences. Cyber security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each new year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging academic libraries with not only how they secure their information resources, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

Recommendation

Cybercrime is definitely a threat to academic libraries and there is therefore need for a holistic approach to combat this crime and ensure cybersecurity in all ramifications. To this end, the

researcher suggests the following as mechanisms to combat cybercrime and ensure cybersecurity in academic libraries.

1) Establishment of an institutional framework that will be responsible for the monitoring of the information security situation, dissemination of advisories on latest information security alerts and management of information security risks including the reporting of information security breaches and incidents.
2) Academic libraries should secure their network information. When organization provides security for their networks, it becomes possible to enforce property rights laws and punishment for whoever interferes with their property.
3) Improving awareness and competence in information security and sharing of best practices through the development of a culture of Cybersecurity at all levels in the
4) Safeguarding the privacy rights of individuals when using electronic communications
5) Formalize the coordination and prioritization of cyber security research and development activities; disseminate vulnerability advisories and threat warnings in a timely manner.
6) Implement an evaluation/certification programme for cyber security product and systems.

References

Adewole .S.K and Olayemi.R (2011). An inquiry into the awareness level of cyber security policy and measures in Nigeria. International Journal of Science and Advanced Technology Volume 1 No 1.

Davis (n.d), Cyber –Safety Basics

Denning, D. (2000). Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism. *U.S. House of Representatives, Comm. Armed Services*. Retrieved March 20, 2016, from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Dhillon, G. (2001). Challenges in Managing Information Security in the New Millennium, In, Dhillon, G. (2002). Information Security Management: Global Challenges in the New Millennium, Hershey, PA: Idea Group Publishing: pp. 1-8.

Eisenberg, J. and Lawthers, C. (2005).Library computer and network security. *Infopeople.* Retrieved Feb 5, 2016, from http://www.infopeople.org/resources/security/.

Farahmand, F., Navathe, S. B., Sharp, G. P., and Enslow, P. H. (2003). Managing Vulnerabilities Of information systems to security incidents, Pittsburgh.

Gawde, V. (2004). Information Systems Misuse - Threats & Countermeasures. *Infosecwriters.* Retrieved April 11, 2016, from http://infosecwriters.com/text_resources/pdf/information_systems_misuse.pdf.

Im, G. P. and Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *SIGMIS Database*. 36(4): 68-79.

INTOSAI. (1995). *Information System Security Review Methodology: A Guide for Reviewing Information System Security in Government Organizations.*

Ke, X.R. (1997). *Gist of Banking Law*. Banchiau City, Taipei. Publisher of LiJian, Taiwan.

Lin, Y.C., and Huang, M.X. (1999). Technology of Internet system security. *Communication of Information Security* (15:3): 12–22.

Lindstrom, P. (2003). Let's Get Physical: The Emergence Of The Physical Threat. *A Spire Research Report*. Retrieved April 10, 2016 http://www.netbotz.com/library/Physical_Threat_Security.pdf.

Loch, K.D., Carr, H.H. and Warkentin, M.E., (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*. 16 (2): 173-186.

McComb, M. (2004). Library security. San Francisco: RLS Inc.

Odumesi J.O (2006). Combating the menace of cybercrime: The Nigerian Approach (Project), Department of Sociology, University of Abuja, Nigeria p.45.

Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*. Prentice Hall PTR: Upper Saddle River, New Jersey.

Rajendran, L. and G. Rathinasabapathy (2007). Role of Electronic Surveillance and Security Systems in Academic Libraries. In: *Proceedings of the Conference on Recent Advances in Information Science and Technology (READIT 2007), MALA & IGCAR, Kalpakkam. pp. 111-117.*

Reddy ,G.N & Reddy,G.U (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. International Journal of Engineering and Technology Volume 4 No. 1.

Schwartz, M. (2006). *Employees Cause Most Security Breaches, Yet Response Lags.*

Shen, W.Z. (1999). Attack and protection with Hacker. *Communication of Information Security*. 5(3):86–96.

Tittel, E., Chapple, M., and Stewart, J. M. (2003). *CISSP: Certified Information Systems Security Professional study guide.* 3rd. ed. Sybex: Wiley Publishing.

Vacca, J.R. (2009). *Computer and information security handbook*. Burlington: Morgan Kaufmann Publication. p.632.

Whitman, M.E. (2003). Enemy at the gates: threats to information security. *Communication of the ACM*. 46 (8):91–95.

Williams, R. L. (2001). Computer and network security in small libraries: A guide for planning. *Texas State Library & Archives Commission*. Retrieved April 5 2016, from http://www.tsl.state.tx.us/ld/pubs/compsecurity/.

Yeh, Q. and Chang, A.J. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management.* 44:480-491.