JATLIM International
http://www.jatlim.org

INTERNATIONAL JOURNAL OF APPLIED TECHNOLOGIES IN LIBRARY AND INFORMATION MANAGEMENT

International Journal of Applied Technologies in Library and Information Management 3 (1) 5 - 42 - 46
ISSN: (online) 2467 - 8120

Manuscript Number: JATLIM - 2017-03.01/ 5-42

Cyber Attack: Issues, Challenges And Solutions For Digital Libraries in Developing Countries

Christopher Agbeniaru Omigie
cvchris72@gmail.com
Department of Library
and Information Science
Ambrose Alli University,
Ekpoma Edo State, Nigeria

Eunice, N. Nwadioha
Auchi Polytechnic Library,
Auchi, Edo State

Abstract
This paper discusses the cyber-attacks as online war that is targeted at computers, information and infrastructure with vulnerabilities. The paper identifies the perpetrators to include individuals, organizations and nation states especially with issues to grind. The attacks involve the use of sophisticated malicious software smart programs. The paper also looks at the history of cyber-attacks, types of attacks, methods of attacks and the implications especially for digital library development in developing countries. The ways forward to combating the virtual insurgency were also discussed.

Key words: *Cyber attacks, Digital libraries, computer information, Infrastructure, Document vulnerability*

1.1 Introduction

In today's world of dramatic advances in Information Technology (IT), cyber attack has become a growing phenomenon in scope and in sophistications. There is hardly a day without report of any attack. Cyber attack is an Internet-based conflict which involves the use of malicious software programs to attack computer information and network systems to cause significant damage and setback to the victims. Cyber attack is an uncoordinated online war which could be as devastating as the terrorist escapades.

Although cyber attack has been on for a long time, the degree, frequency and harm across the globe is increasing and frightening every day. Cyber attack is an organized crime that can be carried out by individual, organization or gangs of criminals for a big fee or even by nation states to settle scores. Anyone connected to the Internet is vulnerable to the attack which could range from individual credit card data to an entire infrastructure. It is obvious that we are all closely connected to the information superhighway. So, an attack on one ally, if not dealt with quickly and effectively, can affect us all.

2.1 Literature Review

Cyber warfare is not limited. It can be seen as a platform where some individuals carry out their own dubious schemes against unsuspecting persons, companies, banks, the military, educational institutions and other government agencies. So, educational institutions, major corporations, private persons and information infrastructure are all victims of the attacks. The Internet, by its pervasive nature, makes the method of attack to be so diverged that it is difficult to tell the source of attack except by mere suspicion.

Globally, cyber attack is a war that is continuously spreading online in different ways. Common methods of cyber attack include: software piracy, identity theft,

electronic fraud, online spam, intellectual property theft, flashlight, etc. In advanced countries, the damage and frequency of attacks in educational institutions are now such that it is difficult to tell the reality from fictions. The attack could disable official websites and networks, disrupt or disable essential services, steal or alter classified data and cripple research systems. Combating the war is not easy. Every day, the war continues to defile combating strategies. The sophistication of attack is growing with technological advances. Talking about cyberwarfare, Cook (2012) states thus:

> The term "cyberwarfare" refers to politically motivated hacking in order to conduct espionage and sabotage. It is well established that the use of computers to manipulate markets, organisations and governments has been occurring now for decades and evidence of cyberwarfare is apparent from as early as the 1970s in the form of "worm" attacks which have taken the form of extremely invasive viruses over time [1].

This means that cyberwarfare has been going in the computing industries as organized attack targeted at destroying computers and related software.

2.2 Some Cyber-attack Incidences

The frequency of attack is a multiplying organism that is now spreading vastly into institutions in the developing countries. The Nigerian Guardian Newspaper (2016) reports that Nigeria loses one hundred and twenty-seven billion Naira (N127b) to hackers and cyber bandits annually. Yet, despite the spread and threats to information infrastructure and even to educational institutions, developing countries are doing less to combat the attacks. A study of this nature therefore, becomes imperative, using analytical perspective to discuss the actors of the attacks, types of attack, methods used and possible implications on digital library development in developing countries like Nigeria. The ways forward is also postulated.

News reports and available literature have shown that no nation, educational institution, organization or individual is immune to cyber-attack; only the experiences vary. In advanced countries like the US, China, Russia, Iran, etc. the menace of cyber insurgence in higher education is on the increase. In August, 1986, Clifford Stoll, a US physics researcher at the University of California, Berkeley tracks down a hacker to Germany who had broken into computers at the Lawrence Berkeley National Laboratory.

In November, 1988, about 10% of the world`s Internet servers were temporarily shut down by Morris worm. Robert Tappan Morris, a student at Cornel University was confirmed to be behind the act and it was the first occurrence of an Internet worm. In 1999, the India and Pakistan prolong dispute over Kashmir was reported to have moved into cyber space with each nation's hackers repeatedly engaged in attacking each other`s computer database systems including those of universities.

Prichard and MacDonald (2004) affirm the Israel and Palestinian cyber-attacks in which Israeli hackers launched Denial-of-Service (DOS) attacks against Palestinian Resistance Organizations (Hamas) and Lebanese Resistance Organization (Hezbollah). In retaliation, several Israeli websites were crashed including those of universities by flooding them with bogus traffic. In 2016, a group that works with universities and technology companies and IT systems providers, Educause, announced that between 2005 and 2016 there were over 1000 data breaches at US universities. Also that year, Identity Theft Resource Center affirms 42 colleges and universities in US as victims of cyber-attacks. Universities are particularly vulnerable because they are the most open and

robust centers of information exchange in the world.

2.3 Types of Cyber Attacks

There are various types of attacks. Paganini et al (2012) groups the attacks as they affect information access into two: sabotage and espionage attacks. Clapper (2015) avers the sabotage attack as the most alarming. This attack primarily aims at destroying critical infrastructure such as information and communication systems, electricity generation grids, transportation and the economic systems.

The espionage attack, Paganini et al (2012) notes involve secretly intercepting and even modifying classified information that is not securely handled. It involves use of malicious software programs to infiltrate computers with virus so as to cripple or disrupt essential network services. Espionage attack could be targeted against government, educational institution, corporate organization, enemy group, the military, political, religious and economic groups using exploitative means on Internet, networks, software, etc.

3.1 **Methods of Cyber-Attacks**

Various methods of attacks exist. Pakim (2015) affirms that attack can range from installing spyware on a personal computer to destroy a set target in a sophisticated smart ways. This can be done by using a computer network tool to shut down critical computer networks like that which control power grids, water system, transportation system, the military and government agencies so as to disrupt their essential services.

Another method is through the use of malicious code through computer network to deface a webpage so as to disrupt the integrity or authenticity of a critical data of an organization and make the organization vulnerable to denial-of-service attack.

Professional hackers can trace computer systems with vulnerabilities like those of universities that are the most robust open centers of research and information exchange and then infect the systems with malicious code, get control of the systems, view the content of the system to gain detail information and then attack. Professional hackers can use self-replicating viruses to attack files. Computer virus is a harmful software program intentionally designed to infect a computer system. It has the ability to replicate itself and continue to spread. The virus can hide in the memory of a computer system and execute it code on whatever file it finds. The virus can change its digital form each time it reproduces making it difficult to track down in the system. Some examples include: Flashlight spy, Memory Resident, Overwrite, Direct Action, Directory web Scripting, Multipartite, Fat, Polymorphic, Browser Hijacker, Boot Infector, etc.

Worm, on the other hand, has similar characteristics as the virus. Worm is program design to monitor and collect server activities and then transmit it back to its creator. Worm is self-replicating, but in different ways. Worm is a stand-alone virus and when it is infected on a computer system, it searches for other computers connected via Local Area Network (LAN) or Internet connection. When it finds another computer, it replicates itself to the new computer and continues to search for other computers on the network to replicate. It is a self-replicating running program that replicates over a network using protocol. Examples of worms include: Trojan horse, Sky wiper, Flame, Morris, sniffer, flight, bullet, Code Red, Titan Rain, flashlight, and so no.

4.1 Implications for Digital Library development

In developing countries, the use of

computers, mobile phones and the Internet have opened the windows of opportunity for cyber attacks. Every day, millions of students are accessing their institutional library databases or connecting to other global network information systems with little or no knowledge of the security implications. This exposes them to the myriad of risks as hackers are now aggressively attacking even the cell phones where users blindly allow applications to access their personal information.

Unlike the advanced countries, university libraries in developing countries like Nigeria have relatively weak surveillance capacity to monitor what comes into their computer systems and this makes their systems more vulnerable to cyber attacks. Also, it is very possible for criminals in other countries like China, Russia, Iran, etc to installed spyware into the computer systems that access information in their country`s library databases. This becomes an open window for the cyber criminals in those to launch their nefarious activities against the computer systems that visit them. Again, poor security infrastructure and human capacity development in IT are making digital library users in developing countries to be unable to identify the red line they should not cross. This again hinders the libraries ability to shift destructive attacks back to sender. So, any attack easily sails through their defenseless systems and the consequence is total disaster and setback.

Another problem is over dependence on foreign nations for all solutions. Libraries in developing countries lack the human capacity and international research projects to improve their ability to uncover and neutralize cyber threats. So, any attack on their digital library system at this stage of their development would be very devastating and colossal.

Conclusions and Ways forward

Cyber welfare as a cankerworm is already eating deep into the fibers of developing countries. There is urgent need for more awareness campaigns about the consequences and the actors of this new method of war and fraud. Digital libraries in developing countries are at risk. University libraries in the developing countries are already under serious threats as the hackers are now invading into their cyber space and information systems. The criminals can bring down any operating system by force and even wipe out an entire economy system. There is need for urgent push for human capacity building in cyber security systems to protect the library information systems from sudden attacks. Over dependence on the advanced nations for aids on security protection is no longer fashionable.

Digital librarians should be trained on cyber security systems and have synergy with international research laboratories on cyber security matters. The situation where library development is greeted with apathy by university management is unprogressive and inimical to her mission of teaching, learning and research. In fact, it is time, and now is the time, for university management to look inward, using their cyber security librarians, in tackling their growing menace of cyber insurgency.

References

Clapper, J.R. (2015). *Espionage and National Security Breaches*. United States: National Security Law. Retrieved from: http://nationalsecuritylawbrief.com/espionage-and-the-21st-century-data-breaches/

Cook, D. (2012). The History of Cyber Warfare. Retrieved from http://www.pannone.com/media-centre/blog/hcyb

Nigerian Guardian Newspaper (2016) Nigeria loses 127 billion Naira to hackers and cyber bandits annually. *Publication of the Guardian Newspaper, July 20th 2016,*

New York Times (2010). Malware Hits Computerized Industrial Equipment. *New York Times; September*, 24th 2010.

Paganini, P. Kelson, R., Gittins, B. & Pace, D. (2012). The `Cyber War` Era Began Long Ago. Retrieved from: www.securityaffairs.com/word

Pakim, P.S.I. (2015) Spyware Attack. *Tech. Journal of Computer Science*. 2(1) June, 2015.

Prichard, J.J. and MacDonald, *L.* E. (2004). Cyber Terrorism: A Study of the Extent of Coverage in Computer Science Textbooks. *Journal of Information Technology Education*, 3,279-289