ALARMING THE CYBER SECURITY ON THE HORIZON OF VIRTUAL LIBRARY: A REGULATORY DIALOGUE

Sanjiv Kadyan* Raj Kumar Vats **

***Assistant professor,**
MDU,
Rohtak,
Haryana,
India.

****Research Scholar**
Dept. of Library &
Information Science,
MDU,
Rohtak,
Haryana,
India.

QR Code

ABSTRACT: - *In this paper the authors tried to address the need of regulations and safety zone in the virtual library and aware about the security breaches and unlawful acts created in cyberspace. This paper discusses the cyber security in libraries by using the conceptual approach. The paper is concluded with the efforts to harmonize the cyber security in library dealing with defensive tool as safeguard.*

KEY WORDS – Cyber crime, Virtual superhighway, Cyber security, cyber space, Information Technology Act 2008.

INTRODUCTION

Cyber space has broken many of the barriers improved by time and space. As a result numbers of relevant cyber security challenges are brought to lights. In 1996, internet access in Myanmar (Burma) was available only through a single state run internet service provider. The rapid development of computer network has compelled library and information centre to address the need for regulation to control the e-resources. The new opportunities of cyberspace have enhanced the capacity of e-resource offenders and criminal networks that have emerged to exploit vulnerabilities in the information database. Cyber crime is a traditional crime like fraud and malicious act and is executed rapidly which enhance the unauthorised access, damage the cyber security. With the proliferation

of e-resource new issues are also emerging like cybercrime. In the context of library does not create a situation where library users of the database are frustrated out and unable to benefit from the library.

Strategies must be taken to balance between security concerns and digital user needs. The libraries responsibilities for investigating a cybercrime may differ depending on the identity of the white colour criminal and a fact not known in a cyber-investigation because of delay. Today courts and lawmakers have constantly echoed that there is a global revolution looming on the horizon of the development of the effective law to secure the database of virtual libraries. A good deal of uncertainty exists about the needs of standardized law enforcement in addressing crimes with a cyber space.

DEFINITIONS

Cyber Crime is not defined in Information Technology Act 2000 or in the I.T. Amendment Act 2008 or in any other legislation in India. To put it in simple terms any offence or crime in which a computer is used is a cyber crime.

Nigerian cybercrime Branch Advisory (2007) defined cybercrime as ‘‘acts that are punishable by the Information Technology Act.’’ [8]This may not be suitable enough but went further to give a sturdy definition of cybercrime as ‘‘unlawful acts where in the computer is either a tool or a target of crime.’’[1]

According to R Broadhurst “Cyber-crime is often traditional crime (e.g. fraud, identify theft, child pornography) albeit executed swiftly and to vast numbers of potential victims, as well as unauthorized access, damage and interference to computer systems.” [2]

These definitions indicates that cybercrime reflects as internet crime which involves the use of computers and the internet as an instrument to commit unlawful act, such as committing fraud, hacking, pornography, IPR issues, violating privacy of database and denial of service in an organization as library or information centre.

According to cyber security Fundamentals Glossary - ISACA “The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.” [3]

According to Glossary of Key Information Terms, NIST 2013 “The ability to protect or defend the use of cyberspace from cyber-attacks.” [4]

Section 2, 1 (n b) of ITAA-2008 states that (n b) (Inserted Vide ITAA 2008) "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. [5]

According to International Telecommunication Union (2012) "Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and its searching tools. Organization and its searching tools include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and stored information in the cyber environment." [6]

NEED OF CYBER SECURITY IN LIBRARY OPERATIONS

Cyber security is important because it touches all aspects of the internet, World Wide Web and cyberspace and every action and reaction which are related to virtual superhighway. Today network attacks are becoming more serious when they are inflicted upon an organisational operation that store sensitive data on the server of an organisation such as library. The consequences of attacks may completely debilitate important data can be lost hence privacy can be violated. As we move toward electronic environment the security of electronic resources will become more essential. The only fear of security problems can be harmful to library database as actual security breaches. General fear and suspicion of computers still exists and can limit the library opportunities for its user, especially that database that are completely Web based. From the academic point of view, it is the burning issue in growing libraries of the country like India. It is the time need that cyber security of digital library must be sound and staff will be trained. Mishandling of enforcement can back fire. So care must be taken for that. Thus library must enact security policies and install safeguards effectively and be assured proper implement of CCC (Copyright Clearance Control). Libraries have met with some success but the pitfalls are many that are why we need to employ some defensive tool as safeguard. A random action is required to maintain the cyber security. Library must be able to communicate how they plan to protect their user's rights. In addition to protecting their user organisation must protect their employees and its consortia partnered from security breaches. **(Sheakh, 2012)** The university management agreed to explore the Turnitin plagiarism prevention tool as one of the measure to fight the plagiarism.

METHODOLOGY

The paper attempt on conceptual study and for doing this, several documents and literature are utilized in the field of cyber-crime. We also handle e-resource related document to learn the basics and potentially of internet foundation and cyber security utilization. To know the possibilities and current trends in library operation, several e-resource database and

websites have been searched, to learn the latest of cybercrime and its potentiality in information superhighway the discussion of ITAA, 2008 was valuable and provided the tail for this paper.

CYBER SECURITY: A GLOBAL VIEW

The international community realized the possibility consequences rate from the cyberspace and it was signed as the International Convention of cyber-criminal by the representatives of EC countries and also US, Canada and Japan in the November 2001. In the convention the crimes, which committed in the virtual superhighway ruled as cyber-crimes and ruled some estimated crime which are against the library policy and connected with IPR and copyright issue, unlawful access to information, intervention into the computer system, unlawful use of telecommunication equipment, and also covered the forgery and deceitfulness with use of digital object. At international level International Telecommunication Union founded some efforts for cyber security which provide the path to tackle the cybercrime. Currently all major international organizations host meetings to discuss cooperation regarding security in the cyberspace including specialized working groups within regional bodies such as

- The Asia-Pacific Economic Cooperation (APEC)
- The European Union (EU)
- The Group of 8 (G8)
- The Organization of American States (OAS)
- The Organization for Economic Cooperation and Development (OECD)
- The Association of South eastern Asian Nations (ASEAN)
- The Shanghai Cooperation Organization (SCO) **(Yliopisto, 2007)**

When we are talking about western European libraries we found that Western European libraries have crossed (25 per) medium level security problems and 40 percent web security is vulnerable.

CYBER SECURITY AND THE INFORMATION TECHNOLOGY ACT (AMENDED) 2008

When we talk about the infringements of cyber security the cybercrimes are among the most commonly committed offences on the internet and cause concern both to copyright holders and those who work professionally with computer networks. In the beginning of 2004, My Doom or Norvag worm was spread out in the form of malicious code. First recorded cyber crime tool place in the year 1820. Something we have seen that libraries are often unprepared for managing network and new technology. The Internet and Intranets enable the effective communication between employees and partners. An attack may directly cause several hours of downtime for employees, and networks must be taken down in order for damage to be repaired or

data to be restored. Clearly, loss of precious time and data can greatly impact employee efficiency and morale. The cyber crime can be as simple as clicking on a tainted web site and having SQL-injected code transfer a malicious payload on your Personal Computer and for more security. Library has to be made clear to their users, that what they are allowed to do on library computers, as well as what is prohibited for them. **(Zimerman, 2010)**

Legislation is a traditional force that drives the need for data security. National governments are therefore developing laws intended to regulate the virtual flow of electronic information. Furthermore to accommodate the regulations enacted by governments the computer industry has developed a collection of security standards to help to secure database. Libraries that do not have demonstrable security policies must maintain that to protect their databases. Indian Government must appreciate that for safe and secure access movement on cyberspace a sound legal framework is needed. India's cyber laws are contained in the Information Technology Act (amended) 2008. It is based on the Model Law framed by United Nations Commission on International Trade Law. This Act attempt to change outdated laws and provide ways to deal with the Virtual data lies on superhighway. The Act provided necessary legal framework so that information is not denied legal effect only on the ground that it is found in the form of digitally. The Act specifically stipulates that any subscriber may authenticate an electronic record under section 4 by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key under section 5of the Act. Today the libraries that collect, store, process and disseminate the data and tasked as intermediary has the vicarious liability for data protection. It is fact that the librarians are not involved in this access moment directly. The Section 43 (A) dealing with compensation for failure to protect database of library. As per this Section, where a outsource provider is negligent in implementing reasonable security practices and thereby causes wrongful loss or gain to any person, such vendor shall be liable to pay damages by way of compensation to the library. The Internet has certainly become the virtual data network, supporting and facilitating its user worldwide. While the Internet has changed and greatly improved the way we do library operations. Library network and its associated technologies have opened the door to an increasing number of security threats from which library must protect them. **(S. 4, 5 & 43(A), I TAA 2008).**

SILENT FEATURES OF THE ITAA 2008

1. Focussing on data security and data privacy.
2. Making digital signature technology neutral.
3. Defining reasonable security and cyber cafe practices used by the corporate.
4. Redefining the role of intermediaries.

5. Recognising the role of Indian Computer Emergency Response Team.
6. Inclusion of some additional cyber crimes like child pornography and cyber terrorism.
7. Authorizing an Inspector to investigate cyber offences. **(Sumanjeet, 2010)**

SECURITY TIPS FOR LIBRARIES

1. Encourage the users and employees to choose passwords that are not noticeable.

2. Require employees as well as users to change passwords every month.

3. Educate employees about the security risks in every section like site certification, awareness training

4. Implement a proper and comprehensive network security solution in library.

5. Assess library security regularly with policies like password policy, access control, and e-mail policy.

6. If you allow student to use Wi-Fi in campus, provide a secure, centrally managed server in remote areas.

7. Update your Web server software regularly.

8. Make sure your virus protection subscription is up to date.

9. When an employee leaves the library, remove that employee's network access immediately.

10. Do not run any unnecessary library services and databases.

WE ADOPT CERTAIN METHODS FOR INTERNET SECURITY

Fire wall

User authentication

Data encryption

Key management

Digital certificate

Intrusion and virus detective system

Virtual Private Network (VPN)

Extranets

CONCLUDING REMARKS:

In the library the traditional preserving and policies are not adequate for proper enforcement. So we need to policing computer related crime and adequate amendments to execute the exiting legislation. Many libraries and data centre have addressed the problem of cyber-crime and laws exist that criminalise unauthorised access and unlawful use of computers but such laws are neither universal nor uniform. Now the concerns remain focused on the weakest links in the hypothetically security chain necessary to prevent cyber-crime and a swift action is required to protect the cyber security. So today library may be expected to recruit IT specialists and experts to obtain access to IT systems and encryption in cyber security. The library coupled with the digital revolution to begin recording the incidence of illegality in cyberspace. Librarians and the institutions they serve need to do more to get involved in the creation of policy and regulations that will affect the way we do our work in the future. We need to educate ourselves on the ways

in which cyber attack might occur and appear as well as our options when we become aware of such an attack. The software and systems used need to be made as solid as possible to virtual attack and plans should be in place to provide quick recovery of systems when a concerned attack is successful. It should be the duty of the library and its users to take care of information security playing their respective role within the permitted parameters and ensuring compliance with the cyberspace. There should be appointed CERT (Computer Emergency Response Team) to resolve the basic problems faced in the E-environment specially related to hacking and cracking of ID, password and websites.

REFERENCES:-

1. Babatunde Ajala ,Emmanual(2007) Cybercafes, Cybercrime Detection and Prevention. *Library hi tech news*, 7, 26-29.
2. Broadhurst,Roderic (2006) Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29 (3) 408-433.
3. Cyber security Fundamentals Glossary- ISACA Retrieved From http://www.isaca.org/knowledgecenter/documents/glossary/cybersecurity/fundamentals/glossary.pdf on dated 25/06/2015.
4. NIST (2013). Glossary of Key Information Terms. NISTR 7298, Revision 2, Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf on dated 25/06/2015.
5. The Information Technology Act (Amended) 2008. S. 2,1 (nb)
6. Alexander Klimburg (Ed.). (2012) National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn Retrieved from https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf on dated 25/06/2015
7. Sheakh, Taraq Hussain (2012) Cyber Law: Provisions and Anticipation *International Journal of Computer Applications*, 53 (7), 10.
8. Yliopisto, Turun (2007) International Actions against Cybercrime:NetworkingLegal Systems in the Networked Crime Scene. Webology, 4(3) Retrieved from http://www.webology.org/2007/v4n3/a45.html on dated 25/06/2015.
9. Zimerman, Martin. (2010). Protect your library's computers. *New Library World*, 111 (5/6), 203-212.
10. op. cit. , S.4, S.5 & S.43 (A)
11. Sumanjeet (2010). The state of e-commerce laws in India: a review of InformationTechnology Act. *International Journal of Law and Management* , 52 (4), 265-282
12. Hawkins, Steve; Yen & Chou, D. C. (2000) Awareness and challenges of internet security. *Information Management & Computer Security*, 8/3, 131-143. Retrieved from on dated 23/07/2015. http://www.emeraldinsight.com/doi/pdfplus/10.1108/09685220010372564