International Journal of Information Movement **Vol. 8 Issue IV (August 2023)**
Website: www.ijim.in ISSN: 2456-0553 (online) Pages 36-41

CYBERCRIME PREVENTION AND THE ROLE OF THE ODISHA HIGH COURT LIBRARY: IMPACT OF A LEGAL USER'S AND THEIR PRIVACY

Mr. Karna Singh
Research Scholar
Sambalpur University, Jyotivihar, Burla, Odisha
Email Id: karan4u358@gmail.com
and
Prof. (Dr.) Bulu Maharana
Head Of Dept. Lib & Info. Science
Sambalpur University, Jyotivihar, Burla, Odisha
Email Id: bulumaharana@gmail.com

Abstract: Modernization is a never-ending process of improvement. The Internet of Things (IoT) has altered many aspects of how the world runs, including financial, military, and defence services, as well as routine stock purchases. It is complicated to transact for medical and health services. The library is not left out in any of these. Online threats, attacks, and crimes, as well as an evil associated with modern internet growth, the invisibility of human contact has made combating cyber attacks difficult. However, the same technical innovation has been created by cyberspace and is associated with advancing technologies. The concept of cybercrime or cyber attack, which was previously more familiar in Western countries, has gained traction in India. It has become more prevalent and may face major difficulties among internet users. The internet's popularity and accessibility have grown in recent years. Now India is moving in the right direction to address the crisis. This paper's goal is to examine the existing situation of supportive actions taken in response to the rise in cybercrime and how they thwart such crimes. This essay emphasises the high court library's function of assisting its legal users and community in preventing white collar crimes.

Keywords: cybercrime, information technology, library, information security, prevention, cyber attacks

1.0 Introduction

Modernization is a continuous process of change for the better, which is taking place in every field of library activity due to extensive use of information and communication technology (ICT) applications. Libraries in the pre-industrial period, mostly had manuscripts and printed materials and their main function been to keep the materials as a storehouse of information. The information available to the users was on demand basis. Cyber crime is a new term used in the ICT era. ICT is applicable in every sector knowledge and service sector. Cybercrime in plain words can be summarized as crime committed due to use of computers and technologies associated with it. There are different natures of cybercrimes like cyber stalking, cyber bullying, cyber warfare; frauds, hacking, etc. are creating social issues and harms to society in general as well as intellectual activities.

Cybercrime halls in detecting theft, phishing, ransom wares, spam and fake messages, etc. Presently, cybercrime is an ever increasing phenomenon, not only in India but all over the world. The incidence of cybercrime is directly proportional to the level of progress made by a country in computer technology.

The library and Information sector are not escaped from the cyber thefts and crimes. There are some issues in which cyber crimes are playing a role like stealing data and information of others or from other sources, passwords, audio video books or literature, pirating literature, altering literature, hacking cites etc. The information and knowledge community as well as information users need the safe environment for information handling and for this purpose library professionals need to have literacy about the cybercrime. If library professionals are fully aware of cyber laws and crime detection measures they also develop literacy among the users and educate them.

2.0 Meaning and Definition of Cyber Crime

The Information Technology Act 2000 has not been statutorily defined by any statute or law as yet.

The IT Act, 2000 does not contain a specific definition of cybercrime. However, cybercrimes are defined as those types of crimes in which a computer is either an object or a subject of the criminal conduct, or both. Thus, any activity that uses computers as an instrumentality, target, or means for perpetrating further crime, falls within the ambit of cybercrime. Prof. S.T. Viswanathan has given possible definitions of cyber crimes, and these are :Any illegal action in which a computer is the tool or object of the crime, i.e., any crime, the means or purpose of which is to influence the function of a computer, Any incident involving computer technology in which a victim suffered or could have suffered loss and a perpetrator made or could have made a gain on purpose. Computer abuse is considered any illegal, unethical, or unauthorized behaviour relating to the automatic processing and transmission of data.

2.1 How cybercrime can affect on library and national development: The library has a large number of e-resource subscriptions. Besides e-resources; the library also creates user databases, holds and maintains catalogue databases. These details should be kept safe from unauthorised library users. Students, the teaching community, researchers, managers, policymakers, the intelligence department, and any educated person in a country rely heavily on the e-resources that institutional libraries subscribe to. They are involved in accessing a large number of e-resources. Among these e-resources, some are very sensitive in nature, like defence and R & D related e-resources. Libraries are sensitive locations where transactions involving both less sensitive and highly sensitive e-resources can take place. At Law libraries, users run the risk of experiencing cyber attacks or committing crimes online. It is the duty of libraries to offer user education regarding safe access to online data. the following problems where

- Violation of intellectual property rights:
- Misuse of data by unauthorised persons:
- National Security Information:

2.2 Preventive measures for libraries: Most cybercrime cases in India are committed by educated individuals (some cybercrime requires skills). Therefore, to prevent it, deep knowledge of cybercrime is required. In addition, most crimes in India are committed due to a lack of knowledge or a mistake.

- To safeguard the large amount of information, the law libraries should adhere to the following security procedures.
- Hardware must be kept in locked, safe areas, and an inventory system must be put in place for simple tracking.
- Users should not be permitted to install unauthorised network equipment in order to maintain the security of physical networks.
- To protect the library's data from viruses and malware, use up-to-date antivirus software.
- Use of firewalls
- Databases ought to be able to grant access to resources that are specified by roles and profiles and ought to be based on those roles' and profiles' respective functions.
- The invention of software that converts files in out-of date formats to workable files and public registries of format standards
- Taking up the regular data backups.
- Privacy and confidentiality should be maintained with regard to library users and their use.
- Not to initiate contact with strangers via the Internet.
- Passwords and credit card information shouldn't be shared during any online transactions.
- Providing access to library data while promoting user authentication techniques (user name and password, biometrics).

3.0 **Probable Measures To Prevent Cyber Crimes**

3.1 Cyber Laws and Information Security: "India passed the Information Technology Act 2000 in May 2000 and notified it for effectiveness on October 17, 2000. The act has also been amended in 2008 and is currently known as the IT (Amendment) Act, 2008, and was notified for enactment on October 27, 2009 The Act's Sections 65 through 74 discuss the punishment for cybercrime". (Kumar, 2013)

3.2 Online Awareness Programs Indian websites offer information security awareness training. To raise public : awareness, the Indian government's Department of Information Technology has developed the website http://deity.gov.in/content/cyber-laws-security. This website has offered information security awareness for kids, students, and parents.

3.3 Cybercrime cells: India has nine cybercrime cells that are actively involved in the investigation of the cyber attacks, and they are located in Mumbai, Chennai, Bangalore, Hyderabad, Delhi, Thane, Pune, Gujarat, and Gurgaon (as of 2013). The Indian educational system covers topics like information security. Information security concerns and courses on cybercrime awareness must be added immediately to college and university curricula.

3.4 Topics being included in the syllabus : India's education sector is expanding. Computer literacy is necessary in basic and secondary education. Even though there are more than 500 universities and the colleges that make up those universities, very little is understood about the risks associated with computer threats.

3.5 Responsibilities of the Police Department: "The IT (Amendment) Act, 2008 of India grants the right to enter any public place, search without a warrant, and detain without a warrant any person found there who is reasonably suspected of having committed, of committing, or of being about to commit any crime, to any police officer not below the rank of Deputy Superintendent of Police or any other officer of the Central Government or a State Government authorised by the Central Government." (Kumar, 2013) In light of this, the suspects must be identified clearly by the police department. They might also run initiatives to educate the public about cyber crime.

3.6 Role of Media in Creating Awareness: In terms of educating people about computer crime and raising their knowledge of its various forms, the media may play a significant role. More than 100 news channels broadcast news in various languages throughout India. The main source for informing the general public about news is news networks. This might be an effective medium for raising awareness of the crimes perpetrated online

4.0 Cyber Security In The Library And Users' Privacy

Cyber security measures are designed to protect data, programs, and computer networks from unauthorised access or attacks.Securing cyberspace ensures the confidentiality and integrity of data stored on and accessed through these technological devices.Reddy and Reddy (2014) listed some cyber security techniques to include: access control and passwords, authentication of data, malware scanners, firewalls, and anti-virus software. Also, installing updates of applications regularly as they are released helps prevent or guard against attacks (Bhavsar & Bhavsar, 2017). This is due to the fact that most updates are made to address issues such as bugs and vulnerability to specific malware, as well as to create a better and more secure version of a programme or application than the previous version.The library and its users can also adopt a strong, difficult-to-decipher password to secure their information.

According to Romdhani (2017), while security and privacy are closely related and are often used interchangeably, they actually differ. According to him, privacy is concerned with people.It has to do with the control that the person has over the information that he/she discloses in the context of an application and ensuring that the information is not used or disclosed for other purposes or used by other unauthorised entities aside from the ones for which it was disclosed by the person/user. Security, on the other hand, is how the different properties of data are guaranteed. Properties, such as confidentiality, integrity, and authenticity, availability, non repudiation, and access controls.

The issue of security and privacy is more embedded as mobile devices too have become mini-computers capable of running user programmes and third party software (Clarke, Symes, Saevanee, & Furnell, 2016). Mobile devices have become so common that they are used in commerce as electronic commerce transactions, the military, governance, and even health care and medical services (ITU, Organization Internationale De La Francophonie, and Africa Cert, n.d.).A study about the associated threat of invasion of privacy where users' data may become

The dilemma of users, including many library users, in choosing to be vulnerable to cyber attacks or to adopt cyber security applications that will likely compromise their privacy by accessing personal and sometimes sensitive data was a subject examined by Chassidim, Perentis, Toch, and Lepri (2020). The study identified that users were willing to open up their privacy moderately in exchange for a medium level of protection. However, the result from the study supports the idea that users' understanding that lesser exposure of private data translates into a lesser level of protection by cyber security applications, was a decisive factor in determining which cyber security application to choose; though there was no such positive effect in choosing an application with a higher level of privacy invasion.

Caches and web cookies collect data on and about the library users (browsing history, IP addresses, device identification, etc.). While some sites have cookie privacy settings where the user can control the type and amount of data that can be collected or stored about him or her, some do not. Where a user has such control and is not comfortable with the policy terms and conditions of the site, s/he has the option to reject or decline, in which case s/he may not be able to gain access to the information or data sought on the site. A library user has the right to share personal data under his or her control as a result of this. In contrast to when data is collected without the user's consent or prior notification of such data collection, Toch et al. (2017) in their study on dealing with privacy invasion opined that it could be viewed in three categories: (1) the no control category, where due to the configuration of the system, the user cannot interact in a straightforward manner with it and, as such, has no control or means of choosing a preference as it relates to privacy policies because such policies are not displayed at all to the view of the user. (2) indirect control where there is a potential for interaction between the system and the user and so there is the possibility of the user controlling the privacy aspect; and (3) full control where the user can interact with the system to modify or control the settings of the privacy aspects as the infrastructure or configuration allows the user to view the privacy policy and gives room to set privacy preferences.

5.0 **Information security**:

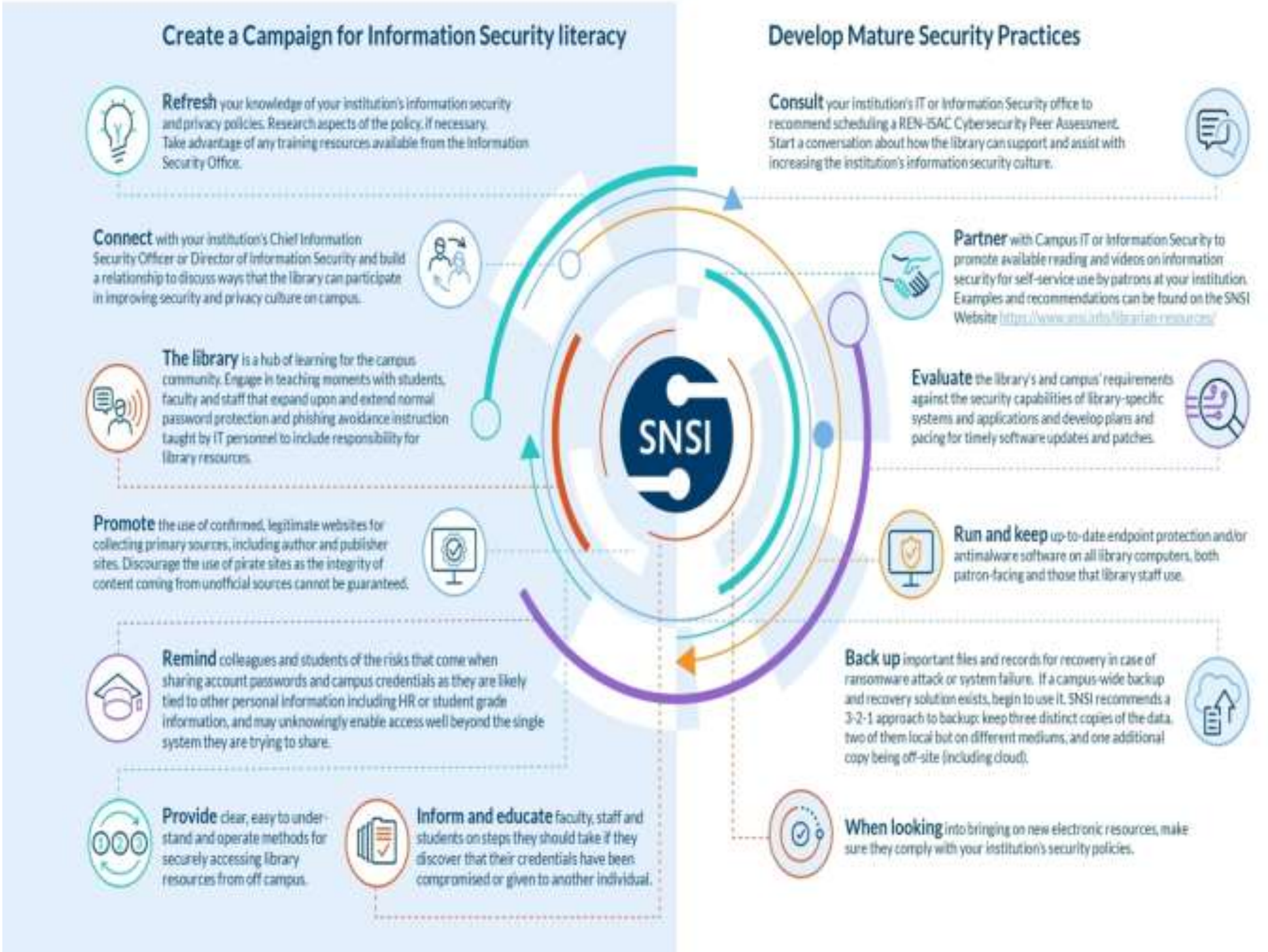
"Libraries have made significant investments in computer-based resources, training and services. However, such investments need to be protected from misuse or mistake by taking an active role in information security" .

"Information security is not simply computer security. Whereas computer security relates to securing computing systems against unwanted access and use, information security also includes issues such as information, information privacy and data integrity. For example, information security in a library would include personnel security and policies, steps taken for effective backups, and the physical integrity of computing facilities.

Minimally, effective information security in libraries should include:

Staff assigned to information security tasks

- Training all personnel in information security issues and procedures
- Specific policies dealing with information privacy, physical security of equipment, and computer security procedures
- Physical security plans
- Data integrity measures Levels of access to data or equipment, and monitoring for different types of access". (Newby,2002)



Create a Campaign for Information Security literacy

Refresh your knowledge of your institution's information security and privacy policies. Research aspects of the policy, if necessary. Take advantage of any training resources available from the Information Security Office.

Connect with your institution's Chief Information Security Officer or Director of Information Security and build a relationship to discuss ways that the library can participate in improving security and privacy culture on campus.

The library is a hub of learning for the campus community. Engage in teaching moments with students, faculty and staff that expand upon and extend normal password protection and phishing avoidance instruction taught by IT personnel to include responsibility for library resources.

Promote the use of confirmed, legitimate websites for collecting primary sources, including author and publisher sites. Discourage the use of pirate sites as the integrity of content coming from unofficial sources cannot be guaranteed.

Remind colleagues and students of the risks that come when sharing account passwords and campus credentials as they are likely tied to other personal information including HR or student grade information, and may unknowingly enable access well beyond the single system they are trying to share.

Provide clear, easy to understand and operate methods for securely accessing library resources from off campus.

Inform and educate faculty, staff and students on steps they should take if they discover that their credentials have been compromised or given to another individual.

Develop Mature Security Practices

Consult your institution's IT or Information Security office to recommend scheduling a REN-ISAC Cybersecurity Peer Assessment. Start a conversation about how the library can support and assist with increasing the institution's information security culture.

Partner with Campus IT or Information Security to promote available reading and videos on information security for self-service use by patrons at your institution. Examples and recommendations can be found on the SNSI Website https://www.snsi.info/librarian-resources/

Evaluate the library's and campus' requirements against the security capabilities of library-specific systems and applications and develop plans and pacing for timely software updates and patches.

Run and keep up-to-date endpoint protection and/or antimalware software on all library computers, both patron-facing and those that library staff use.

Back up important files and records for recovery in case of ransomware attack or system failure. If a campus-wide backup and recovery solution exists, begin to use it. SNSI recommends a 3-2-1 approach to backup: keep three distinct copies of the data, two of them local but on different mediums, and one additional copy being off-site (including cloud).

When looking into bringing on new electronic resources, make sure they comply with your institution's security policies.

Librarians and libraries have long been champions of good security to uphold the values core to the library. The campus-wide efforts to protect data are increasing as threats against institutions' data rise. Libraries, in partnership with other administrative units across campus including IT and Information Security, can educate patrons on how to protect institutional and personal information, access genuine resources to support their research, and build strong relationships between the Library and campus Information Security colleagues. Scholarly Networks Security Initiative (SNSI) brings together publishers and institutions to solve cyber-challenges threatening the integrity of the scientific record, scholarly systems and the safety of personal data. www.snsi.info

6.0 What Is Your Privacy Guarantee?

"Libraries, especially public libraries, have an outstanding record of protecting the privacy of their patrons. The American Library Association's Intellectual Freedom Manual (ALA, 1996) assists librarians in defending the Library Bill of Rights. More recently, the ALA has taken strong stand against the use of filtering software in libraries (see ALA, 1998), and specified guidelines for the freedom of computer and Internet use in libraries.

Recommendations are simple, but could be time consuming or difficult to implement:

- Maintain a comprehensive list of data that may be collected and the circumstances.
- For each type of data, what risks of misuse exist?
- Specify a policy for the collection of data and possible misuses.
- Identify personnel responsible for ensuring the policies are followed, and for remediation as needed".(Newby, 2002)

The Scholarly Networks Security Initiative recommends these rules of thumb when considering how libraries can contribute and support information security practices in higher education. These same recommendations can also be applied to nearly any other organization too. The investment of time, focus, and technology in prevention efforts is far more useful than the significant costs that result after a security intrusion or data breach.

7.0 Role of the High Court Library of Odisha

"All law libraries and the high court library are the ones who subscribe to e-resources in large numbers" (Haddagali, and Mulla). Libraries, like e-resources, are creating user databases and holding and maintaining catalogue databases. These details should be kept safe from unauthorised library users.

The electronic resources that the institutional libraries subscribe to are extremely important to students and the teaching community. A significant portion of the e-resources accessed by patrons of university and college libraries are electronic.

Users may be the target of cyber attacks or engage in illegal online activity in libraries because of their vulnerability. The task of educating users about safe access to online material falls on libraries.

To safeguard the vast volume of information, the following security precautions should be observed in libraries: The same can be explained to library patrons in order to defend libraries against online criminals.

- Refrain from making online contact with strangers.
- Employing up-to-date antivirus software to safeguard the library's data from malware and viruses.
- Understanding the origins of cybercrime
- To avoid disclosing passwords and credit card information during any online transactions.
- Doing routine data backups
- Using firewalls
- Providing access to library data while promoting user authentication techniques (user name and password, biometrics).

7.1 Cybercrime prevention strategies and information environment:

There are a few measures that librarians and information specialists can take, including:

- Blocking users from downloading information from the library computers; obtaining authentic information sources from licensed publications;
- Librarians must regularly verify the functionality of antivirus software and ensure that it is updated.
- Use firewalls to prevent virus attacks on the servers.
- Upgrade security maintenance tools to the most recent versions as needed. Safeguard passwords and update them on a regular basis. Add an extra layer of security to passwords by using verification codes, etc.
- Be careful not to click on strange or questionable links in emails because they can contain malware.
- Avoid using public WiFi for managing personal or financial information.

8.0 Conclusion

In the information society, internet usage is on the increasing. Additionally, it enables criminal activity in the networked environment. Cybercrime is becoming a significant threat. The governments, police forces, and intelligence agencies have begun to take action to stop this crime, according to Gandhi. Government departments have launched initiatives to stop white collar crime. It may be stated that computers and the Internet are now commonplace in both our daily lives and any modern library. We wouldn't be able to cope with the excessive amount of information that seems to characterise our society without the assistance of any of these instruments. However, the issue of security places restrictions on the accuracy of data and computer systems. The proper usage of computers and the safeguards that are constantly provided for the secure processing of information need to be more widely known. By setting up orientation programmes, meetings, lectures, and other events, judicial libraries play a significant role in educating their patrons in this area. It is frequently very beneficial to manage information in a seamless fashion for both the judicial library and its legal users. All judicial libraries today, as well as judicial, law, and academic libraries, need to be aware of this. The sources of cybercrimes should be understood, and this knowledge should be disseminated to the legal practitioners, general public, academic institution faculty members, and students who spend a lot of time online.

9.0 References

i. Gandhi, V.K. (2012). An overview study on Cyber Crimes ininternet. *Journal of Information Engineering and Applications*,2(1),www.iiste.org/Journals/index.php/JIEA/article/download d/1201/1122

ii. Hadagali, G.S. et al. (2012). Use of electronic resources by post-graduate students in different universities of Karnataka State. *International Journal of Information Dissemination and Technology*, 2(3), 189-195.

iii. Mulla, K.R. (2011). Use of Electronic Resources by Faculty Members in HKBK College of Engineering: A Survey. *Library Philosophy and Practice*, http://www.webpages.uidaho.edu~mbolin/mulla.htm

iv. Kumar, V.D. (2013). Cyber crime prevention and role of libraries. *International Journal of Information Dissemination and Technology*, 3(3), 222-224.

v. Bhavsar and Bhavsar (2017)CYBER CRIME AND MEASURES TO PREVENT IN librariesknowledge Librarian" An International Peer Reviewed Bilingual E-Journal of Library and Information Science, Volume: 03, Issue: 05, Sept. – Oct. 2017 Pg. Nos. 38-47

vi. Biswal, B and Datta, S. (2017)Cybercrime in Context to Library Modernization in India: A Threat to National Development, *International Research:* Journal of Library & Information Science | Vol.7 No.3, Sep., 2017

vii. Kumar, V. D(2013) Cybercrime prevention and Role of Libraries, International Journal of information Dissemination and Technology,3(3), 222-224

viii. https://www.igi-global.com/chapter/big-data-analytics-with-machine-learning-and-deep-learning-methods-for-detection-of-anomalies-in-network-traffic/235048

ix. Newby, G B (2002)information security of Libraries, IGI publishers,(5)pp11