# Role of Cyber Security in Library Information Centers in India

*Raghavendra P. Inganal**

DOI: https://doi.org/10.5281/zenodo.19478821

**ABSTRACT**

*Information and Communication Technology (ICT) has helped libraries make all their electronic resources accessible to their users. Securing library-subscribed resources from scammers or unauthorized users is a big challenge in the present era. Cyber security is an area that needs to be studied in the present scenario, and the library is no exception. Institutions, including libraries, are one of the targeted areas of ransomware attacks. Library computers, library patrons' data, and library-subscribed resources are the target of cybercriminals. To overcome this, there is a need for cyber security in academic libraries. With the advance of Information Technology, new threats and unauthorized actions arise each day. To be able to protect information assets against these threats and actions is one of the most important issues nowadays. But sometimes technical and technological measures are not enough to protect an information asset. Additional measures must be employed because there are a lot of parameters when it comes to information security. One of these parameters is people. These people can be system administrators, security professionals, employees, and users. These are the people that interact with the information system. In order to secure the people parameter in an information system, a measure that employs moral judgment must be introduced. Information is power. Nowadays, the main concern*

* **Raghavendra P. Inganal**, Librarian, Sri G.R. Gandhi Arts, Sri Y. A. Patil Commerce and Sri M. P. Doshi Science Degree College, Indi, Vijayapur.

*of the cyber community is to protect this valuable asset. Technical and technological security measures are sometimes insufficient to protect an information system. Because there is a human factor in an information system. Ethics are a set of moral rules that guide people. With the help of ethics, better and more robust security can be achieved. In this paper, the role of ethics in information security is discussed. First of all, law, ethics, and information security concepts are briefly introduced. Later, some ethical concerns and perspectives in information security are given.*

**KEYWORDS:** *Communication Technology, Exception, Information, Parameters.*

## Introduction:

"The science of today is the technology of tomorrow," says Edward Teller. What do you mean by cyber security? Cyber security is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of "cyber-threats" is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or a tool by a wide range of malevolent actors. Although it should be emphasized that these figures are extrapolations. Much of its vulnerability is explained by widespread computer illiteracy and easily pirated machines.

In the present modern world, a person is able to send and receive any kind of information or data, maybe an e-mail or a video or audio, just by the click of a button at the tip of his fingers, but do we think how secure his or her data is being transmitted or sent to the other person without any leakage of information? The answer lies in cybersecurity. In modern times, the Internet is the fastest-growing infrastructure in everyday life; many latest technologies are changing the face of humankind. With the rise in these emerging technologies, we are not able to safeguard our confidential information in a highly effective manner, and as a result, scams are showing their effects day by day. A recent research survey conducted shows that today more than 60% of the total commercial transactions are online, so this requires equality of unity, transparent, and best transactions. As a result, cyber security has become a latest issue. The scope of cyber

security is so vast that it is not limited to just securing information in the IT industry but also to various areas like cyberspace and the cloud.

Several modern-day technologies like cloud computing, mobile computing, e-commerce, net banking, etc., also require an elevated level of security. Since these technologies hold prominent information regarding a person, their security has become a key thing. Improving cyber security and safeguarding critical information, including infrastructures, are important to each nation's security and economic development. Making the Internet safer has been an integral part of the development of new services as well as government policies. The modern war against cybercrime needs a comprehensive and safer approach, for technical measures alone cannot prevent any crime. It is important that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Today, nations and governments are improving laws on security in order to prevent the leakage of information, which makes it important for every individual to possess basic knowledge to save themselves from these increasing cybercrimes and gain some knowledge on cyber security.

**Review of Literature:**

Ethics in Cyber Security Policy Development: The confluence of ethics and cyber-security policy development is not a novel concept. A substantial body of literature has delved into the ethical considerations surrounding the formulation of secure cyber-security policies. This review draws on these scholarly insights and empirical research to explore the intricate web of ethical dimensions in the field.

The Ethical Imperatives in Cyber-Security: Scholars such as Johnson (2018) and Sandel (2019) have articulated the ethical imperatives driving the need for secure cyber-security policies. They argue that the protection of critical data and digital infrastructure extends beyond mere technical concerns. It is, at its core, a moral obligation to safeguard the interests and privacy of individuals and organizations. The ethical foundation of "do no harm" forms the cornerstone of these policies, highlighting the duty to protect against cyber threats while upholding the dignity of individuals and

respecting their rights to privacy and security.

Ethical Dilemmas in Decision-Making: The development of cyber-security policies often entails complex ethical dilemmas. As discussed by Jones et al. (2020), the trade-offs between security and privacy, surveillance and civil liberties, and the balance between national security and individual rights present intricate ethical challenges. Decision-makers must navigate this intricate ethical landscape, making choices that not only ensure security but also uphold ethical principles. The tension between the collective good and individual rights is a recurrent theme in the literature, emphasizing the need for ethical frameworks to guide decision-making.

Ethical Implications of Emerging Technologies: The speedy advancement of the era introduces new ethical dilemmas in the cyber-security domain. Ethicists like Florida (2021) have examined the moral implications of emerging technologies consisting of synthetic intelligence, quantum computing, and the Internet of Things (IoT). These technologies introduce novel demanding situations associated with records protection, privacy, and duty. The literature highlights the necessity of adapting ethical principles to address these evolving threats. In sum, the existing literature provides valuable insights into the ethical foundations, dilemmas, and implications within the realm of cyber-security policy development. This review builds upon these foundational works to present a comprehensive analysis of the role of ethics in shaping secure and morally responsible cyber-security policies. By doing so, it seeks to contribute to the ongoing discourse on how ethics can guide and fortify the cyber-security landscape in an ever-evolving digital world.

**Objectives of the Study**

- To examine the current level of cyber security awareness and digital literacy among Indian citizens.
- To study the cybercrimes in academic libraries in India.
- To study the cyber security in academic libraries.

**Methodology:**

To write this paper, the data has mainly concentrated on a textual approach; books written by eminent scholars and articles, and

papers written in various National and International Journals have been considered to do the framework of this paper. Thus, secondary data has been used; the literature included journal articles, books, chapters in edited volumes, electronic sources, and conference papers to write this paper.

**Results and Discussion:**

**I. Cyber Crime in Academic Libraries:**

Health, finance, military, social media, public institutions, and many others are the most common sectors targeted by cybercrime. Institutions, including libraries, are one of the targeted areas of ransomware attacks. In this attack, cybercriminals target library computers, library patron personal data, and library-subscribed resources.

**Misuse of Library Subscribed Resources:** Most of the libraries used to provide usernames and passwords to access e-resources from its subscribed platforms. Since many library users misused that system, now the libraries have implemented remote access software. Email addresses provided by the organization are enabled to access electronic resources. Sharing e-mail IDs and passwords with friends and family to access library e-resources who are not part of the institutions and sending downloaded articles to others is now a risk for users.

**Social Media Frauds:** The library has started using social media platforms to give current awareness services, and new arrivals notifications, update its users about library activities, promote library services, and many more. This platform allows cybercriminals to share and receive information from library users. Social engineering attacks may increase by using social media. Displaying students' contact details or personal information leads to phishing attacks, credential theft, data theft, and other crimes. Sharing of links to library resources or articles is a loss for the library.

**Software Crimes:** Digital library usage can be done with the help of software. The library subscribes to many software to provide adequate services to its users. Unauthorized access, virus attacks, intellectual property crime, software piracy, wiretapping, and many other crimes come under software crimes. Librarians should be aware and trained to protect library software from such crimes.

**Data Crimes:** Data is an essential part of the digital library. In digital libraries, user information and the content of library resources are considered data. Data diddling, data leakage, data spying, and scavenging are some of the most important data crimes.

**Physical Crimes:** To access the digital content of the digital library, computers, the internet, smart devices, and many physical equipment are necessary. Almost all libraries in the country have separate computer labs or information centers that help users access e-resources from the library. Theft of physical library resources, breaking of library equipment, and destroying data manually by deleting the contents become physical crimes. Monitoring users' activity in the library is very important to overcome this crime.

**Internet and Computer Crimes:** The Internet has become a part of our life. Every work is dependent on the Internet. Digital libraries are meaningless without the Internet and computers. E-mail bombing, e-mail spoofing, internet time theft, password attacks, hacking, fraud, and many others come under internet and computer crimes. Using some security software helps to overcome the effects of these types of crimes.

**Cyber Security:** Cyber security means protecting individuals, institutions, or organizations from cyber-attacks or cybercriminals. It mainly defends internet-connected devices and services from various cybercrimes. Cyber security's role is to protect networks, devices, and data from cyber criminals and unauthorized access. Cyber security is needed to protect data from criminals.

**Cyber Security in Academic Libraries:**

- **Network Security:** Network security secures library networks from unauthorized access, misuse, and modification of academic library computer networks. Firewall, e-mail security, remote access security, data loss prevention, etc., are a few types of network security aspects of the library.
- **Application Security:** Application security is the process of developing, adding, and testing security features in an application. The library subscribes to many applications to access e-resources. Securing applications from unauthorized users is very important for academic libraries.

- **Information Security:** This security in libraries involves library resources security, policy security, computer security, internet security, cloud security, database security, and many others.
- **Hardware Security:** Hardware security involves protecting hardware systems like computers, CD-ROMs, network cables, and many others. Digital libraries mainly run on computers and their components. Protecting them from criminals is very important.
- **Software Security:** A digital library has a bundle of software collections. Virus attacks, malware attacks, and corruption of library software are basic software crimes in an academic library. Securing software from cyber criminals through other software or communication with other systems over networks is helpful to overcome this.
- **Data Security:** A library is a collection of data, including library user data, library resources data, library hardware or software data, and many others. Data security safeguards library data from corruption, theft, or unauthorized access.

**Librarian's Role in Cyber Security:**

Librarians play a major role as managers who manage the entire library, which includes resources management, service management, enquiries management, and many others, with the help of other team members. Librarians can play several roles in academic libraries' cyber security. Some are listed below.

- Librarian as an Educator/Trainer: The Librarian is called the teacher of teachers. He/she can educate the library user in many ways. The Librarian of an academic library can educate his/her library users, such as students, faculty, and research scholars, about library e-resources, library policies, library services, and the do's and don'ts of the library. In controlling cybercrime, the librarian should educate the users by conducting awareness programs for the users.
- Librarian as Policy Developer: Policy provides detailed information. Librarians can develop cybercrime or cyber security policies to avoid cybercrimes in the academic library. A set of guidelines helps library users minimize cybercrime.

- Librarian as Learner: Learning is a lifelong process. Librarians should explore new technologies, new updates about the software, cybercrimes, and security measures which help them to control cybercrimes in the library.

**Best Practices for Cyber Security in Academic Libraries**

- Creating strong passwords can avoid most e-mail crimes, unauthorized access, and fraud cases.
- The password should include a combination of special characters, capital letters, small letters, and numbers instead of the date of birth or name.
- Avoiding phishing emails from unknown persons/unknown sites.
- Usage of anti-virus software/updating software regularly to prevent software attacks. Librarians should monitor library software frequently.
- Avoiding illegal software installation in the library computer systems.
- Blocking unwanted websites, non-educational internet sites, and some social media sites, and avoiding unauthorized links helps not to become the victims of cybercrime.
- Avoiding the use of public Wi-Fi and securing mobile devices.
- Installing and updating the latest version of operating systems in the library.
- Protecting wireless networks by using strong passwords in the library.
- Regularly monitor library-subscribed software and maintain usage reports of e-resources.
- Strictly prohibit sharing library and library user personal data with anyone.

**Conclusions:**

Higher educational institutions such as engineering college libraries, medical college libraries, university libraries, etc., are investing huge amounts of money in e-resources. The institution needs to take some measures to protect its subscribed resources with the support of a library/librarian. Making institutional-level

policies, giving awareness about cybercrimes and cyber security, and organizing certificate courses for the students and staff of the institution can help to control cybercrimes. Librarians should be flexible in learning new technology and should be aware of the latest trends in the cyber world. Only then can library resources be saved from cybercrime. Ethics play an important role in our lives and also in the cyber technology domain. Ethics fill gaps in an information system that laws cannot be able to fill. In this paper, the importance of ethical principles in information security has been discussed. Different ethical perspectives in literature are inspected to show how an ethical layer can be built on a security layer. Also, in this paper, to provide solid proof that ethics complete information security, several ethical frameworks are inspected. Finally, methods to make ethical rules effective in a community are given. Several examined studies showed that awareness training and codes of conduct are effective in this manner.

## References:

1. Ngwum, N., Raina, S., Aguon, S., Taylor, B., & Kaza, S. (2020). A model for security evaluation of digital libraries. Journal of The Colloquium for Information Systems Security Education, 7(1)
2. Aregbesola, A., & Nwaolise, E. L. (2023). Securing digital collections: Cyber security best practices for academic libraries in developing countries.
3. Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. Sensors, 22(2), 1–35. https://doi.org/10.3390/s22020538
4. Bendiek, A. (2012). European cyber-security policy (SWP Research Paper No. RP 13/2012). Stiftung Wissenschaft und Politik (SWP). https://www.aura.com/learn/how-to-find-out-if-my-information-is-on-the-dark-web
5. Osho, O., & Onoja, A. D. (2015). National cyber-security policy and strategy of Nigeria: A qualitative analysis. International Journal of Cyber Criminology, 9(1), 120
6. Brito, J., & Watkins, T. (2011). Loving the cyber bomb: The dangers of threat inflation in cybersecurity policy. Harvard National Security Journal, 3, 39