Evaluating the Influence of National Cyber Security Policies on Digital Library Security, Governance, and Services in Select Academic Institutions of Lucknow, Uttar Pradesh

Zeba Khanam
College Librarian,
Karamat Husain Muslim Girls' P.G. College,
University of Lucknow, Lucknow
Email Id: zebakhanam2015@gmail.com

Abstract

This study assesses the influence of national cyber security policies on the governance and service delivery of digital libraries in Lucknow's academic institutions. As higher education rapidly adopts digital transformations, vulnerabilities to cyber threats, including data breaches and phishing, have increased. National guidelines, such as the National Cyber Security Policy (2013) and CERT-In directives, aim to protect critical information infrastructure. A mixed-methods approach was utilised, with data from 45 library professionals analysed through questionnaires and interviews. Results indicate moderate awareness and implementation of security measures, with basic tools in place but advanced practices like encryption underutilised. The study finds no significant correlation between policy awareness and governance effectiveness, implying that understanding policies does not always enhance performance. It concludes that while national frameworks improve data protection, their implementation is lacking, and recommends policy training, dedicated governance frameworks, and increased collaboration between library and IT departments to ensure more secure digital library services.

Keywords

Cyber security policy, digital libraries, governance, service delivery, SPSS analysis, academic institutions

Electronic access

The journal is available at www.jalis.in
DOI: 10.5281/zenodo.19437751

Journal of Advances in Library and Information Science
ISSN: 2277-2219 Vol. 15. No.2. 2026. pp.194-197

1. Introduction

Cyberspace is increasingly vulnerable to malicious activities, including data breaches, ransomware attacks, phishing, and denial-of-service attacks. These threats affect not only national infrastructure but also educational institutions, which rely heavily on digital platforms for service delivery. According to the Government of India (2013), cybersecurity is essential for protecting critical information infrastructure and ensuring the confidentiality, integrity, and availability of data.

The National Cyber Security Policy (2013) was introduced to create a secure and resilient cyberspace ecosystem in India (Government of India, 2013). It emphasises the protection of critical information infrastructure, capacity building, incident response, and awareness-raising. Similarly, the Indian Computer Emergency Response Team (CERT-In) provides operational frameworks for cyber incident reporting and response (CERT-In, 2021).

Higher Education Institutions (HEIs) are undergoing rapid digital transformation across e-learning systems, digital repositories, institutional websites, and library automation. However, this transformation has increased vulnerability to cyber threats (Sethi & Sethi, 2025). Digital libraries, as network-based repositories of academic resources, are particularly exposed to data breaches, unauthorized access, and system disruptions (Kumar & Sharma, 2019).

The integration of national cybersecurity policies into digital library governance structures is therefore critical. Despite the existence of national-level frameworks, empirical research has yet to examine their direct impact on digital library governance and service delivery in Indian academic institutions. This study addresses that gap.

2. Objectives of the Study

The primary objectives of this research are:

1. To assess the level of awareness of national cybersecurity policies among digital library professionals in academic institutions.
2. To examine the extent of implementation of cybersecurity measures in digital libraries.
3. To evaluate the effects of cybersecurity policies on the security and governance of digital library systems.

4. To investigate the influence of cybersecurity policies on the quality-of-service delivery in digital libraries.
5. To recommend strategies for improving cybersecurity compliance and digital library resilience.

3. Literature Review

3.1 Cybersecurity and Digital Libraries

Digital libraries depend on interconnected information systems, making them susceptible to cyber risks. Kumar and Sharma (2019) identified malware, phishing attacks, and unauthorised access as major threats to digital repositories. Balakrishnan (2020) observed that many Indian academic libraries adopt reactive cybersecurity practices rather than proactive frameworks. Gressel (2014) emphasised that libraries must implement structured privacy policies to safeguard patron data. Internationally, libraries operate under national cyber security and data protection regulations to ensure secure information systems and user authentication mechanisms.

These studies highlight the importance of integrating cybersecurity into digital library management. However, they primarily focus on technical vulnerabilities rather than policy-level influence.

3.2 National Cyber Security Policies

The Government of India (2013) introduced the National Cyber Security Policy to protect the nation's digital ecosystem through awareness creation, capacity development, and infrastructure protection. CERT-In (2021) further strengthened cybersecurity governance by mandating incident reporting mechanisms and compliance requirements. These frameworks provide macro-level guidance, but their institutional implementation remains uneven.

3.3 Governance and Service Delivery

Effective governance enhances institutional performance. Rajan and Verma (2021) found that structured governance models improve service efficiency in university libraries. However, limited research connects national cybersecurity directives to digital library governance and service delivery outcomes.

Research Gap

Although studies exist on digital library security and policy frameworks, there remains a research gap on the direct impact of national cybersecurity policies on digital library governance and service delivery in academic institutions.

4. Research Methodology

4.1 Research Design

1. A mixed-method approach was adopted.
2. Quantitative: Structured questionnaire surveys.
3. Qualitative: Semi-structured interviews and document analysis.

4.2 Population and Sampling

The study included selected academic institutions in Lucknow with established digital library systems, including:

- Tagore Library
- Isabella Thoburn College
- Institute of Engineering and Technology Lucknow
- Amity University Lucknow
- IILM Academy of Higher Learning, Lucknow

Sample Size: 45 respondents
Sampling Technique: Stratified purposive sampling

4.3 Data Collection Tools

- Questionnaire: Measured awareness and implementation of cybersecurity practices.
- Interviews: Captured in-depth insights on governance and policy challenges.

4.4 Data Analysis Methods

- Quantitative data: Analysed using descriptive statistics (percentages, mean scores).
- Qualitative data: Thematic analysis.

5. Data Analysis and Interpretation

5.1 Awareness of Cyber Security Policies

Table 1: Awareness of Cyber Security Policies

Awareness Level	Frequency	Percentage
High	14	30%
Moderate	23	50%
Low	8	20%

Most library professionals demonstrated moderate awareness, indicating the need for enhanced training programs.

5.2 Implementation of Security Measures

- Firewall & Antivirus: Installed in 85% of institutions
- Encryption protocols: Active in 45%
- User authentication systems: Implemented in 63%

Core infrastructure protections are relatively widespread, but advanced security measures remain inconsistently applied.

5.3 Governance Frameworks

Thematic analysis revealed:

- Lack of formal cybersecurity governance policies at the institutional level.
- Insufficient coordination between library and IT departments.
- Reactive rather than proactive risk management.

5.4 Effect on Service Delivery

Respondents reported:

- Frequent system downtimes due to security updates.
- User access issues attributed to multi-layered authentication protocols.
- Positive perception of enhanced data safety.

While cybersecurity measures improve trust, they can also impede seamless access if not effectively managed.

6. SPSS Statistical Analysis Results

Impact of National Cyber Security Policies on the Security, Governance, and Service Delivery of Digital Libraries: A Study of Academic Institutions in India.

Table 2: Descriptive Statistics of Study Variables (N = 45)

Variable	Mean	SD	Minimum	Maximum
Awareness Score	3.13	0.75	1.1	5
Implementation Score	3.49	0.72	1.23	5
Governance Effectiveness	3.11	0.88	1.19	5
Service Delivery Impact	3.18	0.81	1.32	5

Note. Scores measured on a 5-point Likert scale (1 = Very Low, 5 = Very High).

The descriptive statistics for the study variables (N = 45) indicate that the mean scores for Awareness (M = 3.08, SD = 0.78), Implementation (M = 3.49, SD = 0.72), Governance Effectiveness (M = 3.11, SD = 0.88), and Service Delivery Impact (M = 3.18, SD = 0.81) are all above the midpoint of the scale. This suggests a generally moderate to moderately high level of awareness, implementation practices, governance effectiveness, and perceived service delivery impact among the respondents. The standard deviation values indicate moderate variability in responses, implying that participants' perceptions were relatively consistent, though some variation exists. Overall, the findings reflect a reasonably positive trend across all study variables.

Table 3: Pearson Correlation Matrix

Variable	1	2	3	4
Awareness Score	1			
Implementation Score	-.04	1		
Governance Effectiveness	-.04	.05	1	
Service Delivery Impact	-.11	-.03	-.04	1

Note. None of the correlations were statistically significant at $p < .05$.

All correlation coefficients are very close to zero, and none are statistically significant at $p < .05$. This indicates:

There is no meaningful linear relationship among awareness, implementation, governance effectiveness, and service delivery impact.

Awareness does not significantly translate into implementation.

Implementation does not significantly improve governance.

Governance does not significantly influence service delivery.

The correlation analysis indicates that national cybersecurity policies have not yet created a statistically measurable integrated impact across security, governance, and service delivery dimensions in the studied institutions.

7. Discussion

This study confirms that national cybersecurity policies have influenced digital library practices, though implementation varies widely across institutions. Awareness is moderate due to limited policy dissemination. Security tools like firewalls are common, but encryption and advanced governance frameworks lag due to budgetary constraints and technical skill gaps.

The policy impact is evident in improved incident response procedures; however, the lack of institutional policies tailored to digital libraries undermines governance effectiveness. Service delivery outcomes are mixed: security has improved, but user experience suffers where systems are overly restrictive.

8. Findings

I. Moderate policy awareness among professionals.
II. Partial policy implementation in digital libraries.
III. Significant governance gaps, with weak institutional cybersecurity structures.
IV. Service delivery affected both positively (data protection) and negatively (access barriers).
V. Key barriers include limited training, funding, and policy integration.

9. Conclusion

National cyber security policies in India have a noticeable impact on digital library management, with benefits in data protection and structured incident handling. Yet, inconsistent implementation and weak governance frameworks limit their full potential. Digital libraries must align their policies with national directives to deliver secure, user-centric services.

10. Recommendations

I. Capacity-building programs focused on cybersecurity for librarians.
II. Institutional cybersecurity governance frameworks tailored to library contexts.
III. Collaborative planning between the library and IT departments.
IV. Continuous monitoring and evaluation of digital library security systems.

References

1) Balakrishnan, R. (2020). Cybersecurity practices in Indian academic libraries. *Journal of Library Security, 12*(2), 45–57.
2) CERT-In. (2021). *Guidelines for incident reporting and response*. Ministry of Electronics and Information Technology, Government of India.
3) Government of India. (2013). *National Cyber Security Policy 2013*. Department of Electronics and Information Technology.
4) Gressel, M. (2014). Are libraries doing enough to safeguard their patrons' digital privacy? *The Serials Librarian, 67*(2), 137–151. https://doi.org/10.1080/0361526X.2014.939324
5) Kumar, S., & Sharma, G. (2019). Security challenges of digital libraries. *International Journal of Digital Information Management, 17*(4), 12–22.
6) Rajan, P., & Verma, A. (2021). Governance frameworks in university libraries. *Library Management Review, 9*(1), 77–92.
7) Sethi, A., & Sethi, P. K. (2025). Addressing security challenges in the digital transformation of higher education: Strategies and solutions. *International Journal of Engineering in Computer Science, 7*(1), 52–59