SECURITY ASPECTS IN KNOWLEDGE - SHARING PLATFORMS: A LIBRARY- CENTRIC PERSPECTIVE

Ruma Kumari Singh
PhD Scholar, RTMNU, Nagpur
Email : ruma.rumi@gmail.com

Dr. Satyaprakash Nikose
Prof. – Dept. of Library and Info. Science
Rashtrashant Tukadoji Maharaj Nagpur Univ.
Email: drsmnikose@gmail.com

Abstract :

At the center of scholarly communication and community learning, libraries have quickly transformed from physical repositories to digital knowledge-sharing platforms. Unprecedented access and collaboration are made possible by this shift, but it also brings with it a wide range of cybersecurity threats. The necessity of thorough security planning is highlighted by recent events that targeted academic and public libraries. The security features of knowledge-sharing platforms based in libraries are thoroughly examined in this article. It draws attention to the key risks, changing difficulties, and best practices while highlighting the fine balance that libraries need to keep between security, privacy, and accessibility. Practical suggestions for creating robust, reliable library systems are provided, drawing on case studies, expert frameworks, and current technological developments.

Keywords : Knowledge-Sharing Platforms, Academic Libraries, Cybersecurity Threat, Privacy & Security

---

Introduction :

Libraries have evolved significantly in last two decades and have embraced the digital platforms to fulfil their mission of serving communities of students, researchers, scholars etc. From being physical facilities, paper card catalogs and borrowed books the libraries have transformed to online repositories of e-resources through cloud-connected Integrated Library Systems (ILS) and consortia-driven knowledge exchange. While technology has given the new shape to modern libraries and democratize the access, the same technology has also exposed libraries to cybersecurity threats.

The adoption of technology and knowledge-sharing platforms took paradigm shift during the COVID-19 pandemic- means the libraries are managing millions of transactions daily through digital platforms across the world that link user accounts, users' personal information, contents and institutional systems. Perhaps digital adoption helps libraries to outreach millions of people across the world, but it has its own challenges. The libraries are more exposed to cybersecurity threats now than earlier time – means the libraries must not only marry technology but also to its values and standard security practices that brings robust privacy protections, equitable access and openness while fending internal and external threats.

This article seeks not only to catalogue contemporary risks and mitigations but also to demonstrate how libraries can take informed and actionable steps to safeguard their platforms, resources and most importantly their reputations.

Understanding the Library Knowledge-sharing Ecosystem :

1. Platforms and Infrastructure :

The digital ecosystem that is empowering libraries today :

1. ILS platforms for circulation, cataloging, and patron management
2. Central repositories that host the institutional and scholarly content
3. Research tools that enable remote access and collaboration
4. Cloud-connected integrated library systems for scalability, storage and analytics
5. In consortia models, the libraries share the same digital space with other libraries, magnifying both the resource efficiency and the need for harmonized security policies.

2. Emerging Technologie: RFID, Mobile and IOT :

Emerging technology has given new dimensions to the libraries like RFID tags that enables libraries in maintain the inventory and cataloging in more efficient way but carries the risk to expose the unencrypted data to attackers equipped with readily available readers. On the other hand, the integration of library with mobile or smart devices widens both the services and the attack surfaces.

3. The Cybersecurity Threat Landscape in Libraries :

High-Profile Incidents :

Recent attacks demonstrate the severity of modern threats :

- In 2023, the British Library lost access to almost 600 GB of patron, staff and operational data due to Rhsydia ransomware attack.
- In Toronto, a data breach impacted approximately 14,000 library staff and, due to the vulnerabilities found in 3rd party software and system integrations.
- The libraries connected through shared systems, such as BC Libraries Cooperative, have experienced breaches that cascaded across the institutions connected to the network, multiplying the impact.

4. Internal Threats and Human Factors :

The internal threats are one of the most common threats amongst the other different threats. The sheer negligence or intent either of staffs or students may compromise the privacy or system integrity. Considering the increase in remote access, bring your own device policies, and credential sharing complicates the data security further.

The institutions must have data retention, consent protocols, breach notification plans aligned to legal or statutory requirements in place that helps them to monitor and take preventive actions proactively against any probable data loss.

5. Endpoint and Supply Chain Vulnerabilities :

With the increase in digital adoption the dependency on third-party applications, open-source components, and managed infrastructure has also increased. Outdated software or unmonitored integrations often become entry points for attackers making libraries more vulnerable to security threats.

6. Social Engineering and Privacy Loss :

Phishing, social media, or impersonating attacks where cybercriminals use clever emails, malicious attachments or fraudulent login pages to harvest sensitive data by targeting the librarians or the end users.

Core Security Challenges Faced by Libraries :

1. Authentication and Access Control :

A wide range of people, including kids, students, researchers, and the general public use the library. It is both technical and moral challenge to guarantee that every user has valid access without overwhelming them with authentication obstacles.

While multi-factor authentication (MFA) or dual factor authentication increases security, loosely integrated systems run the risk of decreasing usability and drive users away. Hence, it is very important to consider both the factors of security and user experience while enabling scope bases access to the users.

2. Cloud Security and Third-Party Risks :

The service providers help in securing the infrastructure, the libraries must configure their platforms, manage data permissions, and monitor any suspicious activity. Miscommunication or misunderstanding of shared responsibilities leaves critical gaps and huge cost.

3. Regulatory Compliances :

Privacy regulations like GDPR, CCPA, PDPA, and Data Protection law are very stringent. However, there are many libraries that are far behind having transparent policy development and implementation.

4. Digital Preservation :

Libraries must guarantee both the accessibility and authenticity of digital collections.

As knowledge sharing platforms, metadata schemas, and storage technologies evolve, preserving integrity demands proactive security measures.

1. **Security Frameworks: Best Practices for Resilience :**

1. Adopting Robust Frameworks :

The modern libraries are aligned with the NIST (National Institute of Standards and Technology) Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) , Privacy regulations, and other security standards as appropriate and customizing it as required to ensure the data security.

Similarly, ITSM (IT Service Management) protocols help libraires with standardized change management, incident management and risk management- essential for system stability and compliance.

2. Zero Trust Architecture :

Modern challenges require modern solutions. The zero trust approach where every device and user must authenticate themselves before accessing the library internal network. Unless they are not verified, the access shall not be granted. However, the libraires needs to balance the security and service both while implementing such framework so that the security and user experience both are compromised.

3. Encryption and Data Classification :

With the help of data classification tools, the libraries encrypt the data during transit and rest which further helps in having better control over the sensitive data. Automated solutions help in flagging the risk or anomaly access, reducing the risk of breaches.

4. Monitoring and Proactive Response :

The continuous monitoring, routine vulnerability assessments, audit logs, and user training helps libraries in preventing any security risk proactively. The Incident response plans, ensure rapid, coordinated actions minimize the risk and maintain the patrons trust.

5. Institutional Policies and Professional Guidelines :

Guidelines from the American Library Association and OCLC underscore foundational practices: strong password policies, clear privacy statements, regular IT audits, staff onboarding that addresses cyber risks, and public education efforts.

Advanced Threats and Leading-Edge Solutions :

1. Artificial Intelligence and Automation :

As technology is advancing, libraries also need to explore new technologies and see how to leverage AI/ML for predictive threat detection, anomaly spotting and workflow optimization. The library needs to be vigilant towards these systems, poor oversight during training or in deployment may lead to blind spots or give way to new vulnerabilities.

2. Privacy-Preserving Analytics :

Techniques such as federated learning allow institutions to contribute analytics or share best practices while maintaining local control over patron data. This serves regulatory mandates and fosters broader innovation within consortia.

3. Security-Oriented Design (“Privacy by Design”) :

Security is most effective when baked into system architecture while planning and not post implementation. Tools and interfaces should default to privacy by design that requires deliberate action for unusual access.

Case Studies :

1. Academic Libraries :

Manipal Academy of Higher Education (MAHE) implemented a multi-tiered cybersecurity program: deploying firewalls, monitoring remote access, and conducting mandatory seminars for faculty and staff. The results included reduced incidents and higher user confidence

Cornell and MIT libraries have published explicit statements regarding user privacy, data collection, and incident handling, inviting patron feedback to foster trust and transparency.

Routine digital literacy sessions—focusing on phishing, password management, and safe browsing—have demonstrably reduced staff-targeted cyber risks.

2. Public Libraries :

Limitations in resources present significant difficulties. However, the Toronto Public Library's breach demonstrated the value of having established connections with outside IT providers and public information officers in order to respond quickly and efficiently. Pierce County and Calgary Public Library systems implemented ITSM-aligned frameworks and used E-Rate and LSTA funding to launch multi-year training initiatives, purchase endpoint protection, and upgrade digital infrastructure. These institutions proved that investing in assessment and planning—not merely technology—improves system resilience and recovery after events.

3. Consortia and Shared Systems

Shared infrastructures increase risks and efficiency. By reducing the cascading effect on member libraries, the BC Libraries Cooperative breach demonstrated the necessity of standardized security standards and quick, coordinated incident response plans.

In order to stay up to date, consortiums now regularly conduct cross-institutional risk assessments and use shared threat intelligence platforms.

2. **Strategic Recommendations :**

1. **Regular Risk Assessment:** The regular self-assessments and external audits, focus on both technical vulnerabilities and organizational preparedness ensure readiness against cyberthreats.
2. **Staff Training and Engagement:** Awareness campaigns, regular staff training, and simulation exercises like phishing tests etc help build a culture of vigilance.
3. **Policy and Governance:** Libraries need clear, enforced policies, authenticated access control, data retention and third-party engagement.
4. **User Centric Security:** Ease of access and user experience must remain a core value while ensuring security solutions in place to manage cybersecurity threats. There should be clear communication to all the patrons regarding the acceptable usage policy, risks and rights.
5. **Collaboration and Resource Sharing:** Peer-to-peer exchanges, consortia engagement, and participation in industry-wide intelligence networks amplify defense capabilities and knowledge transfer.
6. **Incident Preparedness:** Tested and documented incident response protocols minimize the impact of breaches. Pre-arranged partnerships with IT, legal, and public communication experts speed recovery.
7. **Technology Investment:** Libraries should invest in tools with proven privacy and security credentials, adapting their procurement strategies to prioritize resilience over cost alone.
8. **Continuous Improvement:** Cybersecurity is a living discipline. Libraries must iterate policies and procedures in response to changing technologies and threat profiles, using lessons from real incidents.

Future Outlook :

Libraries are facing new challenges every day due to change in technology every day and the emerging threats along with. The traditional security systems need to be upgraded with Artificial intelligence, quantum computing, and advanced privacy tools to tackle the emerging threats with emerging technology. These advanced tools will further open up new ways to protect sensitive data.

Whether libraries can turn these security challenges into an opportunity to further their mission of outreaching and enabling resources to the people will depend on the skills acquired by their staff, their funding and their professional culture. To build resilience, one needs to put cybersecurity first, undergo the required training, and encourage open communication with the end users.

With the help of technology, the libraries can build a strong secure environment and enable the end user with required resources without any hassle.

Conclusion :

It is said that great power comes with great responsibility, so the adoption of digital platforms and knowledge-sharing ecosystems. Libraries are the pillars of open knowledge and community services and hence every aspect of library operations, from platform design and technology acquisition to policy developments, needs to be incorporated into cybersecurity.

The libraries prepared against the increasing cybersecurity threats based on the NIST framework, continuous staff training, and open policymaking and proactive cooperation yielded better results. The importance of preparation, continuous learning, and inter institutional connects ae highlighted in case studies.

Libraries hold a unique position by not just providing access to information but also spreading awareness of security and digital citizenship, which benefits both their patrons and the community.

References :

- Ajie, I. (2019). A review of trends and issues of cybersecurity in academic libraries. *Library Philosophy and Practice*.
- American Library Association. (2006). RFID in Libraries: Privacy and Confidentiality Guidelines.
- Cariboo Regional District Library. (2024). Integrated Library System impacted by data breach.
- CISA. (2024). Cybersecurity Best Practices.
- Cornell University Library. (2023). Privacy & Confidentiality at the Library.
- IMD. (2025). Full transparency: 10 lessons from the cyberattack on the British Library.
- IPC Ontario. (2025). Toronto Public Library cyberattack: A wake-up call for public sector cybersecurity.
- Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors, 22*(2).
- 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).
- OCLC. (2023). Security—Protecting library information and systems.
- OCLC. (2025). Safeguarding public libraries: Cybersecurity best practices and solutions.

- Pooja, & Pai, R. D. (2025). Best Practices for Cyber Security in Academic Libraries. *Information Security Education Journal, 12*(1).
- Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *J. Comput. Commun, 9*, 80–102.
- Saha, R. (2024). Data Privacy and Cyber Security in Digital Library Perspective: Safeguarding User Information. *International Journal of Scientific Research in Engineering and Management, 8*(4).
- Singh, V., & Margam, M. (2018). Information security measures of libraries of central universities of Delhi: A study. *DESIDOC Journal of Library and Information Technology, 38*(2), 102–109.
- Techtarget. (2025). 10 Cybersecurity Best Practices for Organizations in 2025.
- Tsesis, A. (2019). Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure. *University of Colorado Law Review, 90*, 593–629.
- Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*, 583–592.