International Journal of Advance and Applied Research (IJAAR)
Peer Reviewed Bi-Monthly

ISSN – 2347-7075
Impact Factor – 0.899
Vol.6 No.1 Sept – Oct 2018

Use in Publications Information Security Procedures in Digital Technology

Prof. Pochanna M Jakku
Librarian. Bhagwantrao Art's College, Sironcha Dist.Gadchiroli (Maharashtra)
Email-.pmjakku@gmail.com

Abstract
It is not necessary to secure the hardware or the surrounding environment for electronic security. Information protection is the main concern here. Global attention has been drawn to the expanding problems and difficulties of privacy, security, and the possibility for fraud and deceit as a result of the recent development in the publishing and use of electronic resources. To evaluate the literature on these problems and challenges, a theoretical analysis was done. Only by using proper security measures and legal processes that guarantee their integrity and dependability can the dangers associated with e-publications be managed. It was discovered that a strict security strategy must be implemented, especially in cases of malicious attacks. When sharing information, a methodical approach should be used, including authentication, maintaining secrecy, and using encryption for optimal security.
KEYWORDS**:** Information Security, Digital Information Resources, Challenges of information Security.

Introduction

One of the most significant technical developments in the last two decades in every aspect of daily life has been the influx of digital media. News organizations, museums, libraries, artists, scientists, and writers of multimedia documents are just a few examples of the information producers and publishers who face a genuine danger from the simple transfer and modification of electronic publications. In electronic research, information security is a top priority. Owners of copyrights want to be paid each time their work is utilized. Additionally, they want to guarantee that their works are not improperly exploited, such as being altered or updated without their consent. Current issues with electronic publishing include how to protect information sources from threats and assaults, how to determine which information is useful and which is useless, and more. (Muneer, 2010).

The term "electronic publications" refers to all types of electronic information, its storage, and its communication, including content (such as files and documents, database records, multimedia clips, web pages, e-mail, voice mail, chat room and forum discussions, and news items), electronic storage media (such as disks, diskettes, CD-ROMs, DVDs, server shares, public folders, websites and news services, and computer screens), and electronic communications media. The list of electronic publications in the library now prioritizes dealing with complicated and challenging privacy and information security concerns. The coordination and communication between information security and privacy are frequently lacking, nevertheless. These limitations make managing information resources more complicated and difficult. Providing eligible people with access to information resources while maintaining the

confidentiality of those resources and reducing their exposure to threats and assaults are all components of good information security. There are eight constructs that guide good security procedures. The eight constructions are a collection of security procedures that help create highly secure data. As follows:

1. Website of the library: Go to the official website of your library. The majority of libraries offer online access to their electronic resources and publications. For electronic or digital collections, they frequently feature a special area.

2. library's online catalog: - Use the search function or the library's online catalog. The majority of the time, you may narrow your search to just display online resources, e-books, e-journals, or other digital content.

3. Library employees: library personnel Speak with the librarians or employees of the library. They are familiar with the library's resources and can offer assistance in locating certain electronic publications or resource recommendations.

4. Databases in the library: Libraries frequently pay subscription fees to a number of electronic databases and platforms that house a wide variety of publications. Academic journals, e-books, periodicals, newspapers, and other materials may be found in these databases. These databases include ProQuest, JSTOR, and EBSCOhost, as examples.

5. Library Cards and Access: Make sure you have a library card or the appropriate login information in order to access electronic publications. You might need to log into certain libraries' systems in order to access digital materials.

6. Approach for Recommendations: Don't be afraid to approach the library staff for suggestions or help in locating pertinent materials if you're seeking for particular sorts of electronic publications or themes.

To get the most accurate and recent information about your local library's digital collections, remember that the accessibility of electronic publications varies from one library to the next.

1. Essential For Information Security: -

A. Protection of Patron Data: Names, addresses, phone numbers, and, in some circumstances, even financial information are just a few of the sensitive and personal details that libraries hold about its users. To safeguard the privacy and confidence of library users, this data must be protected.

B. Preservation of Historical and Cultural Materials: A lot of libraries store precious and rare items, such as manuscripts, rare books, and old papers. These resources are protected by information security from theft, damage, and unauthorized access.

C. Keeping Information Secure: Libraries give patrons access to priceless digital resources including databases, e-books, and e-journals. Information security procedures guard against illegal downloads and dissemination and guarantee that only authorized users may access these resources.

D. Protection of Intellectual Property: Since libraries frequently license digital content, it is crucial to safeguard the authors' and publishers' legal rights to their works. Information security aids in the prevention of copyright infringement and unauthorized distribution of protected works.

E. Security online: Just like any other business, libraries are susceptible to online threats. Data and library systems are shielded from internet risks such as malware, ransomware, and hacking by cybersecurity safeguards.

F. Data Integrity: Data integrity for libraries is protected by information security. It guards against data theft, illegal alterations, and record and cataloging information

corruption.

G. Regulation Compliance: Libraries are required to abide by a number of data protection laws, including the Children's Online Privacy Protection Act (COPPA) and the General Data Protection Regulation (GDPR). There may be legal repercussions if these restrictions are broken.

2. Important Issues And Challenges Of Information Security

In recent years, information security has received considerable attention. Despite increasing concerns about the use of electronic information resources, there are numerous issues and challenges related to information security. Some of these issues and challenges are discussed below:

1. Data Privacy and Confidentiality: Libraries keep a ton of private and sensitive data about its patrons, including personal data and borrowing history. A key concern is ensuring the security and privacy of this data.
2. Cybersecurity Threats: Data breaches and cyberattacks are not unheard of in libraries. Hackers may target them in an effort to steal user data, launch ransomware attacks, or interfere with library services.
3. Libraries offer access to digital resources like e-books, which are subject to strict licensing conditions and digital rights management (DRM) systems. It might be difficult to manage these agreements while maintaining security.
4. Controlling access to sensitive information and library systems is essential. A constant problem is ensuring that only authorized users and professionals have access.
5. Phishing and social engineering: Phishing emails and social engineering attacks may target library employees and patrons, resulting in data breaches or malware infections.
6. Insider Threats: Insider threats from library personnel or volunteers can be quite dangerous, as they can for any institution. Security can be jeopardized by malicious behavior or unintended data disclosures.
7. Libraries may still use outdated hardware and software, which makes them more susceptible to security risks because there aren't as many security updates and fixes available.
8. Public Wi-Fi and network security: Libraries frequently provide public Wi-Fi, which can serve as an attack vector for cybercriminals. It might be difficult to maintain network security while allowing users unrestricted access.
9. User Education: Libraries must instruct its patrons on the best ways to safeguard their personal information and privacy, as well as how to spot and stay clear of security dangers.
10. Compliance and Regulations: Privacy and data protection rules must be complied with by libraries. Non-compliance may have legal repercussions and harm one's image.
11. Resources: Many libraries, especially smaller ones, may not have the money or IT resources to put strong security measures in place and keep current with emerging threats.
12. Digital collection preservation is the responsibility of libraries, who must also guarantee the collections' long-term security and accessibility. Protecting against data loss, corruption, and illegal access is part of this.
13. Initiatives for Collaboration: Libraries frequently work with other institutions and groups, which might present security issues when transferring data and resources.

14. Security of Vendors: Libraries collaborate with a range of vendors to obtain software, systems, and services. In order to avoid supply chain vulnerabilities, it is crucial to ensure the security of these third-party interactions.
15. Emerging Technologies: Libraries are implementing cutting-edge innovations including cloud-based services, machine learning, and artificial intelligence. It can be difficult to implement these technologies securely.

Recommendations For The Effective Information Security

a. Develop Information Security Policies: Construct thorough information security guidelines and practices that are suited to your library's particular requirements. Data protection, access restriction, incident response, and user education should all be covered by these rules.

b. Risk Assessment: Perform routine risk analyses to find risks and vulnerabilities unique to your library. This will enable you to deploy resources wisely and prioritize security measures.

c. Implement stringent access controls to make sure that only authorized staff have access to private user information and library systems. When feasible, use robust authentication techniques like multi-factor authentication (MFA).

d. Encrypt sensitive data both in transit and at rest by using data encryption. This includes encrypting backups, user data stored on servers, and communication across library systems.

e. Updates to software frequently: Maintain the most recent security patches and upgrades for all library operating systems, programs, and software. By doing this, known vulnerabilities are protected against.

f. User Instruction: Inform users and library employees about security best practices. Give advice on how to create secure passwords, spot phishing scams, and protect personal data.

g. Response to Incident Plan: Create and maintain an incident response strategy. Steps to be taken in the case of a security issue, such as how to notify and mitigate breaches, should be outlined in this plan.

h. Vendor Security Assessment: When working with outside vendors for software and library services, evaluate their security procedures to make sure they abide by your library's security standards.

i. Data Backups: To guard against data loss due to cyberattacks or system failures, implement reliable data backup and recovery protocols. Test your backups often to make sure they can be restored if necessary.

j. Network Security: Use firewalls, intrusion detection and prevention tools, and routine network monitoring to safeguard your library's network. To reduce dangers, separate internal networks from public Wi-Fi.

k. Establish a methodical strategy to handling software updates and patches with the help of patch management. Set essential security upgrades as a priority and implement them right away.

l. Physical Security: Ensure that only authorized staff are permitted physical access to servers, networking hardware, and critical parts of the library. Use access control systems and security cameras as necessary.

m. Implement logging and monitoring systems to look for unusual activity and take appropriate action. Examine logs often for indicators of possible security problems.

n. adherence to regulations: Learn about applicable data protection laws and make sure your library is in compliance, especially if it handles personally identifiable

information (PII).

o. Information security is a process that requires constant training. To keep your personnel up to date on new dangers and best practices, provide them frequent training and awareness initiatives.

p. Conduct frequent security audits and vulnerability assessments of the networks and systems in your library. To find flaws, think about doing a penetration test.

q. Collaboration: Exchange knowledge about security dangers and best practices with other libraries and organizations. Join security consortiums or groups geared for libraries.

r. Budget Allocation: Set aside some money for information security. Think of it as an investment in maintaining the reliability of your library's services and the patrons' confidence.

s. Documentation: Keep the documentation for your library's security policies, practices, and incident response plans clear and up to date.

t. Create a communication strategy for alerting users and other stakeholders in the case of a serious security issue. Rebuilding trust can be aided by openness.

Conclusion

Everyone is liable for information security. The possible hazards associated with data and information security must be understood by everyone. However, concerns from problematic people, theft, and censorship continue to dominate security and privacy issues. When information security is discussed, the corporate information security management environment may be used as a starting point rather than the library setting. However, at the moment, libraries frequently don't value information security enough. Information security solutions that are adaptable and expressive will be necessary for the effective creation and use of online learning content. Therefore, the task is to support the joint development of information security solutions for electronic publications as well as appropriate procedures for controlling online learning content. It is advised that all libraries take action to evaluate and reduce information security concerns.

References

1. Arora, J. 2001. Indian National Digital Library of Engineering Science and Technology: A proposal for strategic co-operation for consortia-based access to electronic resources. The International Information &Library Review 33(2–3): 149–165.

(19) (PDF) Digital Libraries in India: A Review.

2. Das, A.K. and B. Dutta. 2004. An introduction to auditing and control of digital library systems. Annals of Library and Information Studies 51(3): 99–103. *(19) (PDF) Digital Libraries in India: A Review*.

3. Jayaprakash, M, B. M., & Chidananda, S. (2010). Preservation strategies in digital era. *KKBNET 2010* (pp. 395- 397). Mangalore: National Institute of Technology Karnataka, Surathkal.

4. Gupta, S. and G. Singh. 2006. Management of digital libraries: Issues and strategies. Journal of Library and Information Science 13(1).

5. Gopal, K. (2000). Digital libraries in electronic information era. New Delhi: Author Press.

6. Shukla, V.N. 2005. New trends in IT: Content Creation. Herald of Library Science 44(1–2): 87–90.

7. NCIHE. (1997). *National Committee of Inquiry into Higher Education.* London: HMSO.

Oppenheim, C. (1998). *A balance in electronic copyright law.* London: The times higher.
8. Urs, S.R. and K.S. Raghavan. 2001. Vidyanidhi: Indian digital library of electronic theses. Communications of the ACM 44(5): 88–89.