VOL- XI | ISSUE- XII | DECEMBER | 2024 | PEER REVIEW e-JOURNAL | IMPACT FACTOR 8.02 | ISSN 2349-638x

Cyber Security and Its Application in Academic Libraries

Ajagekar R. H.*
Librarian,
Ajara, Mahavidyalaya, Ajara, Dist-Kolhapur

Abstract

In today's ICT era, there have been an ever increase in academic libraries embracing digital collections to provide access to a wealth of information to their users. However, the demerit of this digitization brings about the need to ensure the security of these valuable digital collections, especially in developing countries where cyber threats are rampant. This paper aims to address the challenges faced by academic libraries in developing countries with regards to best cyber security practices for securing digital collections. The paper also highlights the benefits of prioritizing cyber security in academic libraries. Besides protecting valuable digital collections, robust cyber security practices enhance users trust; promote collaboration among institutions, and support academic research in a secure environment. This paper serves as a valuable resource for academic libraries in developing countries, as it offers guidelines and insights to enhance their cyber security practices.

Keywords – *Cyber security, Cyber threats, Digital collections, Digital libraries*

Introduction

Information technology has enhanced academic activities over recent years especially in the area of information resources and dissemination. Universities around the world have employed digital technology in their academic libraries, which translates to various digital collections, such as digital libraries, special collections, and repositories. Digital collections play an important role in academic libraries by providing access to a wide range of scholarly resources, including electronic journals, databases, e-books, and multimedia content. These collections are often curate and managed by libraries to support research, teaching, and learning activities of faculty, students, and researchers.

However, with the increased reliance on digital technologies, academic libraries and their digital collections are vulnerable to cyber security threats. These threats and attacks mainly target the accessibility, availability and integrity of the various digital collections. Furthermore, due to the increasing amount of information that needs to be protected, expansion of regulatory laws and policies governing information security, coupled with the economic downtown developing countries face from time to time, it is becoming increasingly harder for institutions to get adequate funding needed to maintain a strong cyber security posture.

Therefore, the focus of this paper is geared towards the direction that academic libraries should see cyber security as a foundational and fundamental element when setting up their information system infrastructure however the budget may be, while also setting up policies that will enable every functional office in the academic institution to take responsibility for the security of information.

Overview of Digital Collections in Academic Libraries

Digital collections refer to curetted sets of digital resources or materials that are available in electronic format. These collections can include various types of digital content such as documents, images, videos, audio recordings, datasets, and more. Digital collections are typically created and maintained by libraries, archives, museums, educational institutions, government agencies, and other organizations that seek to preserve and provide access to valuable cultural, historical, scientific, or educational materials. Digital collections can cover a wide range of subjects and themes, providing to diverse interests and research needs.

Types of Digital Collections

There are various forms of digital collections, which perform different functions based on their nature and the purpose they were made for. Here are some types:

1. Digital libraries: They are databases consisting of digital objects (digitized books, journals, manuscripts, and other textual materials). They have functionalities like catalogs, search functionalities, and other advanced features for accessing and managing digital.

2.Digital archives: Digital archives serves a database to preserve, organize, retrieve and provide access to

historical records, photographs, audiovisual materials, and other archival resources.

3. Image galleries: Digital image galleries provide an online platform for showcasing collections of photographs, artwork, illustrations, and other visual media..

4.Audio Libraries: They consists only of collections available in audio formats, such as, podcasts, speeches, etc., while also offering streaming services, metadata, and searching options for easy navigation.

5.Video Archives: Digital video archives are a collection of categorized videos (movies, documentaries, TV shows, news broadcasts) and other audiovisual contents. They also offer streaming services, and search capabilities to facilitate easy access.

6. Data Repositories: Also referred to as Digital repositories, are information retrieval portal that provides access to digital collections such as datasets, research findings, scientific measurements, and other data-related resources that is of relevance to an institution or organization. They also provide storage and sharing capabilities for researchers and scientists.

7. Digital Museums: These are online platforms that gives users the experience of visiting a physical museum. Various collections such as artifacts, historical objects, artwork, and interactive exhibits are showcased and featured with detailed descriptions and multimedia elements.

8. Digital Exhibitions: Digital exhibitions are curate collections of presentations relating to specific themes or topics, often featuring multimedia content, narratives, and interactive elements.

9.Specialized Collections: These are digital collections that focus on specific subjects or fields, such as natural history findings, genealogical records, maps, rare books, educational resources, and more.

These are just a few examples of the types of digital collections that exist. The digital landscape continually evolves, and new types of collections may emerge as technology advances and new needs arise.

The advantages of digital collections include:

1. **Access and availability:** Digital collections enable wider access coverage to resources that were previously limited to physical locations. Users can access the materials remotely, anytime and anywhere with an internet connection.
2. **Preservation and conservation:** Valuable digital resources are preserved and protected of by reducing physical handling, exposure to light, and other potential risks associated with traditional formats. Digital preservation techniques ensure long-term access and prevent degradation.
3. **Search ability and discover ability:** Digital collections often provide extensive search functionalities, metadata descriptions, and indexing, which enables users to easily find specific resources based on their interests or research topics.
4. **Enhanced user experience:** Digital collections often offer additional features such as multimedia integration, interactive elements, and social sharing, thereby enhancing the overall users' experience and engagement.
5. **Collaborative research and interdisciplinary exploration:** Digital collections encourage collaborations among researchers, students, and institutions which promotes interdisciplinary studies and enabling the exchange of knowledge and insights

.

It's important to note that the specific features and accessibility of digital collections varies depending on the organization and platform hosting the collection. Some digital collections may be freely available to the public, while others might require registration, subscription, or institutional affiliation for full access.

Significance of digital collections to academic research, teaching, and learning

Digital collections have become increasingly significant to academic research, teaching, and learning due to some of the following reasons.

1. Access to a wide range of resources: Digital collections provide researchers, educators, and students with access to a large collection of resources (digitized books, journals, manuscripts, images, maps, audio recordings, videos) that may not be available physically or in their local libraries. This wealth of digital content broadens the scope of research possibilities and enhances teaching and learning materials.

2. Convenience and flexibility: Digital collections offer the convenience of 24/7 access from anywhere with an internet connection. This eliminates the need for physical visits to libraries or archives, saving time and effort. Researchers can access and analyze materials remotely, enabling collaboration across geographical boundaries. Students can also engage with digital collections at their own pace, allowing for flexible learning.

3.Enhanced research capabilities: Digital collections offer varieties of tools and technologies such as robust search functionalities, metadata tagging, data visualization tools, and text mining

techniques that enhance research capabilities. This will make researchers more efficient in identifying relevant materials and extracting valuable information.

4. Interdisciplinary research opportunities: Due to the way digital collections spans across several disciplines and subject areas, researchers and students can explore interdisciplinary studies by leveraging diverse digital resources which can lead to new perspectives, collaborations, and innovations across academic fields..

5. Long-term data availability: Digital collections provide a sustainable platform for storing and accessing research data. Scholars can deposit their research data in digital repositories, ensuring its long-term availability for validation, replication, and further analysis. This promotes transparency, reproducibility, and advances in research.

Overall, digital collections have really revolutionized the academic research, teaching, and learning landscape by expanding access to resources, fostering interdisciplinary collaborations, and enhancing research capabilities. They have become indispensable tools for scholars, educators, and students in the digital age.

Cyber security Threats to Digital Collections

Digital collections, such as online databases, archives, and libraries, are vulnerable to various cyber security threats. Here are some common threats that can affect digital collections

1.Data Breaches: Data breaches occur when unauthorized individuals gain access to sensitive information. In the context of digital collections, a data breach could lead to the exposure of personal data, research materials, or copyrighted content. Hackers may exploit vulnerabilities in the system to gain unauthorized access..

2.Malware Attacks: Malware, such as viruses, worms, and ransomware, can infect digital collections. Malicious software can damage or corrupt data, disrupt operations, or compromise the integrity, and availability of the collection. Ransomware attacks, in particular, can encrypt data and demand a ransom for its release, causing significant disruptions.

3.Phishing and Social Engineering: Phishing attacks involve tricking users into revealing sensitive information by impersonating trusted entities. Digital collection users, including administrators and researchers, may be targeted through phishing emails, messages, or websites. Social engineering techniques can manipulate individuals into disclosing login credentials or other valuable data.

4. Denial-of-Service (DoS) Attacks: DoS attacks aim to overload a system's resources, making it unavailable to legitimate users. Such attacks can disrupt access to digital collections, preventing researchers, students, or the public from accessing valuable resources. Distributed Denial-of-Service (DDoS) attacks, where multiple systems flood the target, are particularly potent.

5. Insider Threats: Insider threats refer to individuals within an organization or institution who abuse their authorized access to digital collections. This could be employees, contractors, or volunteers who intentionally or unintentionally misuse or leak sensitive information. Insider threats pose a significant risk due to their proximity to the data and systems.

5.Zero-day Vulnerabilities: Zero-day vulnerabilities are software vulnerabilities that are unknown to the vendor and, therefore, lack available patches or fixes. Cybercriminals can exploit these vulnerabilities before they are discovered and addressed, potentially gaining unauthorized access to digital collections..

6.Third-Party Risks: Digital collections often rely on third-party vendors or service providers for various aspects, such as hosting, data storage, or content management systems. Inadequate security measures or vulnerabilities in these third-party systems can pose risks to the digital collection's security. It is essential to ensure that these partners follow robust cybersecurity practices.

7. Data Loss or Corruption: Accidental data loss or corruption can occur due to hardware or software failures, power outages, natural disasters, or human errors (Ajie, 2019). Without proper backups and data recovery mechanisms, digital collections can suffer irreparable damage, resulting in the loss of valuable information.

Cyber security breaches in academic libraries can have significant consequences, particularly in developing countries. These breaches can result in data loss, reputational damage, and legal implications. Let's explore each of these consequences in detail.

1. **Data Loss:** Cyber security breaches can lead to the loss or theft of sensitive data stored in academic libraries. This data may include personally identifiable information (PII) of students, faculty and staff, research data, financial records, and other valuable intellectual property. The loss of such data can have serious implications, including identity theft, financial fraud, and compromised research integrity. It can also disrupt library services and hinder the

institution's ability to support academic activities

2. **Reputational Damage:** A cyber security breach can severely damage the reputation of an academic library and the institution it serves. If news of the breach becomes public, it can erode trust and confidence among students, faculty, and other stakeholders. The perception of inadequate security measures and inability to protect sensitive information can tarnish the institution's image and make it less attractive to prospective students, faculty, and donors. Rebuilding a damaged reputation can be a lengthy and challenging process.
3. **Legal Implications:** A cyber security breach in an academic library can have legal ramifications. Depending on the jurisdiction, the institution may be subject to various data protection and privacy laws. If personal data is compromised, the library or the institution it serves, may face legal actions, such as fines and penalties for non-compliance with regulations. Additionally, affected individuals may file lawsuits seeking damages for the loss or misuse of their personal information. These legal battles can be costly and time-consuming for the institution.

Best Practices for Cyber security in Academic Libraries in developing countries

Cyber security is a crucial concern for academic libraries in developing countries, as they often face resource constraints and limited expertise in this area. However, there are several best practices that can help improve cyber security in academic libraries in developing countries.

Creating a campaign for information security literacy

1. Regular cyber security awareness programs should be conducted for library staff and users. They should be trained on basic cyber security practices, such as creating strong passwords, identifying phishing attempts, and protecting sensitive information. The importance of data privacy and safe online practices should be continually emphasized. Inform and educate faculty, staff and students on steps they should take if they discover that their credentials have been compromised
2. Librarians should refresh their knowledge of the institution's information security policies. Other areas of the policies in relation to the library not fully understood should also be researched, while also taking advantage of any information security trainings from the office of the chief information security officer of the institution
3. The library and ICT unit should be in constant communication to discuss ways the library can participate in improving the overall security posture of the institution
4. Encourage and promote the use of legitimate websites in collecting primary sources, from both authors' and publishers' site. Likewise, the use of pirated websites should be discouraged, as sources gotten from there cannot be guaranteed
5. Remind faculties, staff and students of the risks that can come when sharing account passwords and campus credentials, as they are likely linked to other personal information and may unknowingly enable access beyond the single system they are trying to share.
6. The information security policies should include a provision of a clear, easy to understand operational methods for securely accessing library resources from off campus.

Developing mature information security practices

1. Secure network infrastructure: Ensure that the library's network infrastructure is secure by implementing firewalls, intrusion detection and prevention systems, and regularly updating network equipment and software. Separate the library's network from the general academic network to minimize potential risks.

2. Develop a cyber security policy: Create a comprehensive cyber security policy that outlines the guidelines, procedures, and responsibilities related to cyber security. This policy should cover areas such as data protection, access controls, network security, and incident response.

3. Use encryption and secure protocols: Encrypt sensitive data and communications using robust encryption algorithms. Implement secure protocols (such as HTTPS) for online services and websites to protect data during transmission.

3. Maintain up-to-date software: Regularly update and patch software applications, operating systems, and security solutions to address known vulnerabilities. Outdated software can be an easy target for cyber attacks.

4. Backup and disaster recovery: Implement a regular backup strategy to ensure data can be restored in case of a cyber incident or data loss. Store backups in secure off-site locations to prevent data loss due to physical damage or theft.

5. User access controls: Implement strong access controls to limit user privileges and prevent

unauthorized access. Use role-based access control. Regularly review and revoke unnecessary user accounts especially faculty, staff and students that have left the institution.

6. Regular security assessments: Conduct periodic security assessments and audits to identify vulnerabilities and weaknesses in the library's systems and infrastructure. This can include vulnerability scanning, penetration testing, and security risk assessments. Address any identified issues promptly..

7. Incident response plan: Develop an incident response plan that outlines the steps to be taken in case of a cyber security incident. This plan should include procedures for reporting incidents, containing and mitigating damage, and recovering normal operations. Regularly test and update the plan as needed.

8. Collaborate with other institutions: Establish partnerships and collaborations with other academic libraries, cybersecurity organizations, and relevant stakeholders. Share information, best practices, and lessons learned to collectively improve cybersecurity in the academic library sector.

Remember that cybersecurity is an ongoing process, and it's important to stay updated with the latest practices, threats, and technologies. By implementing these best practices, academic libraries in developing countries can enhance their cybersecurity posture and protect their valuable digital assets

Challenges and Future Directions

Implementing cybersecurity best practices for digital collections can be a challenging task for academic libraries in developing countries. Some of the challenges and limitations they may face include:

1. **Limited resources:** Developing countries often have limited financial and technical resources to allocate towards cybersecurity measures. This can make it difficult for academic libraries to invest in the necessary infrastructure, tools, and expertise needed to implement robust cybersecurity practices.
2. **Lack of expertise:** Developing countries may face a shortage of cybersecurity professionals with the necessary skills and knowledge to implement and maintain effective cybersecurity practices. This shortage of expertise can make it challenging for academic libraries to develop and execute comprehensive cybersecurity strategies.
3. **Outdated technology:** Many academic libraries in developing countries may still rely on outdated technology infrastructure, including legacy systems and software. Such outdated systems may have known vulnerabilities that can be exploited by cyber attackers, making it difficult to ensure the security of digital collections.
4. **Limited awareness and training:** Awareness and training programs related to cybersecurity may be inadequate or lacking in developing countries. Academic library staff members may not be sufficiently trained or aware of the latest cybersecurity threats, preventive measures, and best practices. This lack of awareness and training can increase the risk of security breaches
5. **Regulatory and legal challenges:** Developing countries may have less mature or clear comprehensive cybersecurity regulations and legal frameworks in place. This can create uncertainty regarding responsibilities, data protection, and compliance requirements for academic libraries (Etse & Boateng, 2019). This can also hinder their ability to implement effective cybersecurity practices.
6. **Connectivity and infrastructure limitations:** Developing countries may have problem of limited internet connectivity and unreliable infrastructure. This can pose challenges for implementing and managing cybersecurity measures, including timely software updates, patch management, and access to threat intelligence resources.
7. **Increased targeting:** Academic libraries in developing countries may be targeted by cybercriminals due to perceived vulnerabilities and lower security defenses compared to their counterparts in developed countries. This increased targeting puts additional pressure on these libraries to strengthen their cybersecurity practices.

Several emerging technologies and future directions show promise in enhancing cybersecurity measures in academic libraries. Here are a few potential areas of impact:

1. **Artificial Intelligence (AI) and Machine Learning:** AI and machine learning can play a crucial role in cybersecurity by automating threat detection and response. These technologies can analyze large amounts of data to identify patterns, anomalies, and potential security breaches. AI-powered systems can aid in real-time monitoring of network traffic, identifying malicious activities, and providing proactive defense mechanisms against cyber threats

2. **Blockchain Technology:** Blockchain offers a decentralized and tamper-resistant platform that can enhance data integrity, privacy, and authentication mechanisms. Academic libraries deal with sensitive user information, research data, and academic records. Blockchain can enable secure and transparent transactions, protect intellectual property rights, and prevent unauthorized access or modifications to critical data.
3. **Zero Trust Architecture:** Zero Trust Architecture (ZTA) is an emerging security framework that treats all users, devices, and network components as potential threats. ZTA employs multifactor authentication, micro-segmentation, and continuous monitoring to ensure security at every level.. Implementing ZTA in academic libraries can provide granular access controls, isolate sensitive data, and minimize the impact of potential breaches.
4. **User Behavior Analytics (UBA):** UBA involves analyzing user behavior patterns to identify anomalies and potential security risks. By monitoring user activities, libraries can detect unauthorized access attempts, suspicious behavior, or compromised accounts. UBA systems can provide early warnings and generate alerts for further investigation, thereby enhancing the cybersecurity posture of academic libraries.
5. **Cloud Security and Data Protection:** As academic libraries increasingly adopt cloud-based services for storage, collaboration, and data management, robust cloud security measures are essential. Technologies such as encryption, access controls, secure application programming interfaces (APIs), and data loss prevention (DLP) solutions are critical to protect sensitive information and ensure compliance with privacy regulations..
6. **Internet of Things (IoT) Security:** The mass usage of IoT devices in libraries, such as smart sensors, beacons, and self-checkout systems, introduces new security challenges. It is essential to implement strong security protocols, device authentication, and regular patch management to mitigate potential vulnerabilities and prevent unauthorized access.

Conclusion

Cybersecurity is rooted in global insecurity. It concerns manipulating data over network that is detrimental to organization and its clienteles but lucrative to the perpetrators. Libraries and librarians are challenged to keep abreast with the emerging threats over cyberspace. It is clear from the above that, digital natives due to the psycho-social problems or economic situations (they are in), find it useful to engage in cybercrimes a consequence of exposing the weaknesses of organizations affected and the strengths of the cybercriminals. This is true as information needs-seeking-use of organizational workers seems to be linear against the non-linear information needs-seeking-use of cybercriminals. In other words, while organizational workers use makerspace particularly designed for students to interact with one another, cybercriminals have sophisticated hackerspace that is highly equipped, and can access, share, and retrieve valuable information of the organization itself or its clienteles according to the crime at hand. Unless librarians get up to the challenge of cybersecurity threats, the cybercrimes will continue. A slight mistake done by programmers or metadata developers can risk the relevance of organizations especially with regards to metadata terminology or vocabulary. This also gives hackers opportunities to have unauthorized access to databases or manipulate data

References

1. Akamai's State of the Internet Security Report Q2 (2015).media.scmagazine.com /documents/144/q2_2015_soti_security_report_-_35820.pdf
2. Akokpari, J. (2007). The political economy of human insecurity in sub-Saharan Africa. V.R.F. Series, No. 431
3. Alleyne, B. (2011). Challenging code: A sociological reading of the KDE Free Software project. *Sociology*, 45(3), 496–511;
4. Baca, M. (2000). Introduction to metadata: Pathways to digital information, 2nd ed., Getty Information Institute, Los Angeles, pp.12, available at: http://www.slis.kent.edu /~mzeng/metadata/Gilland.pdf
5. Bada, M., & Nurse, J.R.C. (2019). The social and psychological impact of cyber-attacks. In \Benson & McAlaney (2019/20) *Emerging Cyber Threats and Cognitive Vulnerabilities*, Academic Press
6. Barlow, J. (1996). Declaration of the independence of cyberspace. Retrieved July 30,2011 from http://homes.eff.org/~barlow/Declaration-Final.html
7. Bensmann, L. (2009). *Intelligent search strategies on human chosen passwords*. Technische Universtat, Fakultat für Informatik, Dortmond

8. Bennett, S. (2012). Digital natives. In Z. Yan (Eds.), *Encyclopedia of cyber behaviour*: Vol. 1 (pp. 212-219). United States: IGI Global.
9. Canbek, G., & Sağıroğlu, Ş. (2006). A review on information, information security and security processes. Journal of Polytechnic, 9, 165-174.
10. Castells, M. (1996). *The rise of the network society, the information age – economy, society and culture*, Vol I, Blackwell: Oxford, Great Britain
11. Chan, G.R.Y.C. (2018). Scholarly communication at the crossroad: From subscription to open access? IFLA WLIC Kuala Lumpur.
12. Chandler, A. (1996). The changing definition and image of hackers in popular discourse.*International Journal of the Sociology of Law*, 24(2), 229–251.
13. Choo, C.W. (2001). Environmental scanning as information seeking and organizational learning. *Information Research*, 7(1).
14. Cohen, M. (2017). Learning the basics of scholarly communication: A guide for new subject liaison librarians. *Codex: the Journal of the Louisiana Chapter of the ACRL*, 4(3): 4-38
15. Dell, S. (2010). Mediation and Immediacy: The Press, the Popular Front in France, and the Spanish Civil War. In edited by C. Young, *The Mexican suitcase: The Rediscovered Spanish Civil War Negatives of Capa, Chim, and Taro* 1, 37–49. Göttingen: Steidl.
16. Farley, T. (2015). Introduction. In Rosenquist, M. *Navigating the digital age: The definitive cybersecurity guide for directors and officers*. Caxton: Business & Legal Incorporation.
17. Feather, J., & Sturges, P., (eds.) (2003).Scholarly communication. International encyclopedia of information and library science (2nd ed.) London: Routledge: 563-567.
18. Foster, A. (2005). Non-linear information seeking. In Fisher, K.E., Erdelez, S., & McKechnie, L.E.F. (eds.) *Theories of information behaviour.* American Society for Information Science and Technology
19. Frand, J. L. (2000). The information-age mindset. Changes in students and implications for higher education. *EDUCAUSE Review*, 35(5), 15-24. http://www.educause.edu/ir/library/pdf/ERM0051.pdf
20. Giddens, A. (1990). *The consequences of modernity: Self and society in the late modern age*. Cambridge: Polity Press.
21. Gilliland-Swetland, A. J. (2000). Setting the stage: Defining metadata, in Baca, M. (Ed.), *Introduction to metadata: Pathways to digital information*, 2nd ed., Getty Information Institute, Los Angeles, pp.12, available at: http://www.slis.kent.edu/~mzeng/metadata/Gilland.pdf
22. Godfray, H., *et al*. (2010). Food security: The challenge of feeding 9 billion people. *Science*. 327 (5967), 812-18
23. Goldsmith, D., & Siegel, M. (n.d). Systematic approaches to cyber insecurity. Funded by Office of Naval Research under award number N00014-09-1-0597
24. Henk, D. (2005). Human security relevance and implications. *Parameters*, *US Army War College*, 35(2), 91-106.
25. Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, 46(4), 757–780.