Article

Technology-Based Security Systems and Security of Information Resources in the University Library

Onyema Nsirim
https://orcid.org/0000-0002-9386-1699
Ignatius Ajuru University of Education
onyema.nsirim@iaue.edu.ng

Oluchi Cecilia Okeke
https://orcid.org/0000-0002-3295-1551
Enugu State University of Science and Technology
oluchukwu.okeke@esut.edu.ng

Ejiro Sandra Ukubeyinje
https://orcid.org/000-0002-9386-1699
College of Education
ukubeyinjesandra@gmail.com

Rita Dumbiri
https://orcid.org/0009-0008-5810-3754
College of Education
rita.dumbiri@descoem.edu.ng

Abstract

Securing information resources in a university library is crucial to protect sensitive data, academic materials, and the privacy of library users. As academic institutions increasingly rely on digital platforms for storing and disseminating information, the need for robust security measures becomes paramount. The paper examines technology-based security systems and the security of information resources in university libraries. The literature review was conducted to examine existing studies, academic papers, and articles related to Technology-Based Security Systems in library environments. Databases consulted in search of relevant literature include Google Scholar, Academia, and ResearchGate. Content analysis was used to determine the concepts and themes. The study discovered the types of information resources vulnerable to security threats in the university library, including book and non-book materials. It also determined the technology-based security systems for safeguarding information resources in university libraries, including RFID Technology for Asset Tracking, Access Control Systems, CCTV Surveillance in Libraries, Digital Rights Management, Cybersecurity Measures, Cloud-Based Library Services, and Artificial Intelligence for Anomaly Detection. In analysing the threat landscape, the study comprehensively examines both physical and digital risks posed to information resources. This includes cybersecurity threats, physical security risks, insider threats, and third-party risks. Recognising these threats, the study offers strategic insights through proposed strategies such as

UNISA
Southern African Journal of Security
#15883 | 20 pages
https://doi.org/10.25159/3005-4222/15883
ISSN 3005-4222 (Online)

risk assessment and planning, user training and awareness, regular system updates and patch management, data encryption and privacy and continuous monitoring. The study concludes that libraries can maximise the effectiveness of their technology-based security systems, fostering a resilient defence against potential security breaches in the dynamic landscape of information management

Keywords: technology; security; security system; electronic security system; information resources

Introduction

In the contemporary landscape of higher education, university libraries act as repositories of a wide variety of information resources from printed materials to digital archives. But because of their abundance of knowledge, they are also more appealing to attackers, which calls for the installation of strong technology-based security measures. Modern libraries have special issues because of the confluence of the physical and digital domains, especially with the growing complexity of information resource preservation. The need for comprehensive security procedures in university libraries is highlighted by the increasing amount of sensitive data and the frequency of cyber threats (Opara et al. 2023). Thus, preserving academic integrity, safeguarding the privacy of library patrons, and protecting intellectual property all depend on the use of cutting-edge technologies.

Libraries face a variety of security challenges as they adopt digital environments and new technologies, necessitating thoughtful and flexible solutions. Ensuring the confidentiality and integrity of academic material is constantly threatened by the interconnectedness of library systems and the increasing sophistication of cyber threats. Not only do cyberattacks, unauthorised access, and data breaches jeopardise the authenticity of intellectual assets, but they also damage the prestige of academic institutions. Because of this, having cutting-edge technological security measures that are especially made to handle the challenges that university libraries face is now absolutely important. It takes a comprehensive strategy to address these issues, including user education, extensive policies, and technological innovation to strengthen these academic repositories' defences against dynamic security threats. Moreover, the increasing reliance on digital resources and online platforms within university libraries amplifies the importance of securing information against unauthorised access and data breaches.

The interconnected nature of library databases, coupled with the diverse range of users accessing these resources, introduces complexities that demand a nuanced security framework (Lavrov et al. 2021). It can be difficult to strike a balance between strict security protocols and accessibility, as libraries work to create a welcoming and inclusive atmosphere while also taking precautions against potential threats. Thus, investigating the relationship between technology-based security systems and the

preservation of information resources in university libraries is essential to creating a solid foundation for students' and scholars' intellectual pursuits as well as a comprehensive understanding of the changing security landscape in academia.

Objectives of the Study

1. Identify the types of information resources vulnerable to security threats in the university library.

2. Determine the technology-based security systems for safeguarding information resources in university libraries.

3. Identify the threats to information resources.

4. Proffer strategies to overcome the challenges to the use of technology-based security systems in university libraries.

Literature Review

Information Resources Vulnerable to Security Threats in the University Library

Information resources, which make up a large portion of the library, are essential sources of information. In the past, most of these resources were books, periodicals, newspapers, and other editorials, but since the internet was developed, digital resources have proliferated. Thus, libraries serve as storage facilities and points of access for a wide range of print, audio, and visual materials in addition to many other electronic resources (Nsirim, Agina-Obu, and Braide). Examples of these materials include maps, print documents, microform (microform/microfiche), CDs, cassettes, videotapes, DVDs, videos, e-books, audiobooks, and many more. Information resources encompass a wide range, including books, journals, databases, websites, and multimedia materials. Libraries often offer access to electronic resources and the Internet. In the 21st century, libraries are evolving into places that provide unrestricted access to information in various formats from diverse sources. They extend services beyond physical locations by offering electronic access to materials and aiding users with digital tools for navigating and analysing vast amounts of information. Due to their diverse user base, libraries curate collections covering a broad spectrum of human knowledge and opinions.

Opara et al. (2023) highlighted that information resources include printed materials like reference sets, novels, biographies, children's literature, histories, newspapers, and magazines, as well as visual and auditory materials like photographs, maps, art reproductions, sound recordings, and videos. Ibenne (2018) categorised information resources into print, non-print, and electronic formats. In the digital age, information resources are crucial to our interconnected world, influencing how we learn, work, and interact. The landscape of information resources is continually expanding, ranging from traditional print materials to extensive online databases. Libraries, whether physical or

digital, serve as repositories for these resources, encouraging intellectual curiosity and supporting the pursuit of knowledge. In academic settings, students and researchers heavily rely on scholarly articles, books, and databases for literature reviews, deepening their understanding, and contributing to academic discussions. Information resources also empower individuals to stay informed about current events, explore diverse perspectives, and engage critically with the world. Digital platforms have democratised access to information, overcoming geographical and socioeconomic barriers (Omehia et al. 2021).

While the digital era provides unprecedented access to information, it poses challenges in managing and preserving these resources. The sheer volume of digital information raises concerns about organisation, storage, and retrieval. Libraries and institutions face challenges in ensuring the authenticity and reliability of online information, combating misinformation, and addressing ethical considerations related to data collection and use. The rapid evolution of technology requires constant adaptation to new formats and platforms, demanding robust strategies for information resource management. Copyright issues, privacy concerns, and ethical use of data add complexity to the landscape, necessitating careful consideration and adherence to ethical standards.

Securing information resources is paramount in safeguarding sensitive and valuable data across various platforms and formats. Digital repositories, including databases and online archives, house vast amounts of information and intellectual property crucial to organisations and individuals. This includes proprietary research data, confidential business plans, and personal user information. Ensuring the security of these digital repositories is essential to prevent unauthorised access, data breaches, and intellectual property theft. As highlighted by Opara et al. (2023), protecting digital information resources involves implementing robust security measures such as access controls, encryption, and regular monitoring to detect and respond to potential threats promptly. Additionally, physical repositories, such as libraries and archives, house valuable printed materials, rare manuscripts, and historical documents that require protection from theft, damage, or unauthorised removal. Implementing security protocols for both digital and physical repositories is critical to preserving the integrity and confidentiality of information resources.

Furthermore, the proliferation of online communication channels and collaborative platforms has introduced additional challenges in securing information resources. Elejene, David, and Nsirim (2023) noted that email communication, cloud storage, and collaborative tools contain sensitive information that can be targeted by cyber threats. Effective cybersecurity measures, including email encryption, secure file sharing protocols, and employee training programmes, are essential in mitigating the risks associated with these digital communication channels. The significance of securing information resources is underscored by the potential legal and financial repercussions of data breaches, as well as the impact on organisational reputation and user trust. By addressing the unique security requirements of various information resources,

organisations can establish a comprehensive and resilient security posture that protects against a range of potential threats

Technology-Based Security Systems for Safeguarding Information Resources in University Libraries

University libraries play a pivotal role in academia by serving as repositories of vast information resources. With the digital transformation of libraries, the security of information resources has become a paramount concern. The technology-based security systems employed in university libraries to safeguard valuable information resources are reviewed below:

RFID Technology for Asset Tracking: Radio-frequency identification (RFID) technology has emerged as a pivotal tool in enhancing security systems and safeguarding information resources in university libraries. RFID offers a versatile and efficient means of tracking and managing library assets, ranging from books and journals to multimedia materials. By utilising RFID tags and readers, libraries can automate the inventory management process, streamline circulation workflows, and significantly reduce the risk of theft or misplacement of valuable information resources (Omehia et al. 2021). This technology not only improves the overall efficiency of library operations but also serves as a proactive measure to fortify the security of the library's intellectual assets. The implementation of RFID technology for resource tracking in university libraries has demonstrated a positive impact on security measures. RFID tags embedded in library materials allow for real-time tracking, enabling librarians to monitor the movement of items throughout the library premises. This not only aids in preventing the unauthorised removal of materials but also speeds up locating misplaced items. Echem and Okwu (2023) highlight the efficacy of RFID technology in reducing instances of theft and improving the overall security posture of university libraries. Moreover, the integration of RFID with access control systems provides an additional layer of security, ensuring that only authorised individuals have access to specific sections containing sensitive information resources. While RFID technology presents significant advantages for asset tracking and security in university libraries, challenges such as potential privacy concerns and initial implementation costs should be acknowledged. As libraries continue to evolve in the digital age, future research should explore ways to address these challenges and enhance the integration of RFID with other security measures. Additionally, ongoing assessment and adaptation of RFID systems will be crucial to staying ahead of emerging security threats. By investing in research and development, universities can optimise the use of RFID technology to fortify the security of their information resources, ensuring a resilient and technologically advanced library environment.

Access Control Systems: The term "access control" refers to the practice of managing and regulating access to and use of physical and digital spaces, devices, and data. To fortify their defences against unauthorised access, minimise risks, and preserve their valuable assets, individuals an organisation must implement robust access control

systems (Evans 2023). Access Control Systems (ACS) play a crucial role in fortifying the security of information resources in university libraries by regulating and monitoring access to sensitive areas. These systems encompass a range of technological solutions, such as biometric authentication, smart cards, and PIN codes, that collectively contribute to the safeguarding of intellectual assets. Access control could be physical and logical. Physical access control focuses on securing physical spaces such as buildings, rooms, or restricted areas. Traditional methods include lock and key systems, security guards, and surveillance cameras. However, modern physical access control incorporates advanced technologies like proximity cards, biometric scanners, smart locks, and video surveillance systems. These technologies enhance security, streamline access management, and provide an audit trail of activities. On the other hand, logical access control revolves around the management of digital resources such as computer networks, databases, and software applications. It ensures that only authorised individuals can access and use these resources. Techniques employed in logical access control include usernames and passwords, multi-factor authentication, role-based access control (RBAC), and encryption. Additionally, security measures like firewalls, intrusion detection systems (IDS), and data loss prevention (DLP) tools complement logical access control to safeguard against cyber threats

Opara, Irokah, and Nsirim (2023) underscore the significance of access control in libraries, emphasising its role in preventing unauthorised access to information resources. As university libraries increasingly digitise their collections, Access Control Systems become pivotal in protecting not only physical assets but also digital holdings and databases. One notable advancement in Access Control Systems for university libraries is the integration of biometric technologies. Biometric authentication methods, including fingerprint and iris scans, enhance security by uniquely identifying individuals. Despite the advantages, challenges such as privacy concerns and the need for continuous technological updates should be addressed in the deployment of Access Control Systems. There is, therefore, a need for a holistic approach in designing Access Control Systems that not only enhance security but also accommodate the evolving needs of library users.

CCTV Surveillance in Libraries: Closed-circuit television (CCTV) surveillance stands as a fundamental technology-based security system employed in university libraries to safeguard information resources. The integration of CCTV systems provides a visual monitoring mechanism, allowing libraries to actively observe and record activities in designated areas. Okwu and Echem (2023) underscore the importance of CCTV surveillance in deterring potential security breaches, including theft and vandalism, by creating a visible and documented security presence within the library environment. In addition to physical assets, CCTV plays a crucial role in protecting digital resources by monitoring computer workstations and other technology-infused spaces within the library. CCTV surveillance has proven to be effective in both deterring and detecting security incidents within university libraries. The mere presence of visible cameras can act as a deterrent, discouraging individuals from engaging in illicit

activities. In cases where incidents occur, the recorded footage becomes valuable evidence for investigations and potential legal actions. A study by Ezeabasili (2018) discusses the impact of CCTV surveillance in deterring theft and enhancing overall security measures in university libraries. Moreover, the integration of advanced analytics and artificial intelligence in CCTV systems allows for real-time threat detection, further enhancing the proactive security capabilities of these systems. While CCTV systems contribute significantly to security, there are important considerations regarding user privacy. Igwela and Nsirim (2018) emphasise the need for policies and practices that strike a balance between security and privacy concerns. Future developments in CCTV technology for library security should focus on enhancing privacy protections, perhaps through anonymisation techniques or selective monitoring. Additionally, exploring the integration of CCTV with other security systems, such as access control and alarm systems, can create a more comprehensive and adaptive security infrastructure for university libraries, addressing emerging threats and evolving user needs.

Digital Rights Management (DRM): Digital Rights Management (DRM) emerges as a crucial technology-based security system for safeguarding information resources in university libraries, especially in the context of digital collections and electronic resources. DRM encompasses a set of technologies and protocols designed to control access, distribution, and usage of digital content. In the academic environment, DRM plays a pivotal role in ensuring that intellectual property rights are respected and that access to sensitive information resources is carefully managed. Endouware and Okwu (2023) indicate that DRM enables libraries to protect digital assets from unauthorised copying, distribution, and other forms of misuse, thereby preserving the integrity and value of the information within their collections. One specific application of DRM in university libraries is the protection of e-books and digital journals. Libraries often procure digital content that requires secure distribution and controlled access to adhere to licensing agreements and copyright regulations. DRM technologies, such as encryption and access controls, are instrumental in managing digital content licences and preventing unauthorised duplication or dissemination. Effective DRM implementation ensures that only authorised users, such as students, faculty, and staff, can access and use digital resources within the bounds defined by licensing agreements. Despite its benefits, DRM implementation in university libraries is not without challenges. Rana and Mishra (2021) confirmed that DRM systems either provide authentication or constrain access rights, but access control with legal authentication in digital content distribution has remained a challenging issue for public-key cryptography (PKC) or identity-based public-key cryptography (ID-PKC). PKC associates certificate management, which includes revocation, storage, distribution and verification of certificates, has become the bottleneck in a large network. Thus, balancing the need for security with user convenience and the evolving landscape of digital publishing requires ongoing research and adaptability. Addressing user concerns about limitations imposed by DRM and exploring interoperability standards are critical aspects for future development.

Cybersecurity Measures: As university libraries increasingly rely on digital infrastructure and information technologies, robust cybersecurity measures have become indispensable for safeguarding information resources. Cybersecurity encompasses a range of technologies and practices aimed at protecting computer systems, networks, and digital assets from unauthorised access, data breaches, and cyber threats. In the context of university libraries, the implementation of comprehensive cybersecurity measures is essential to secure both physical and digital collections. Borky et al. (2019) highlights the significance of cybersecurity in balancing act involving an adequate level of protection against known or postulated threats while still allowing systems and their users to carry out their legitimate functions and accomplish their objectives as well as preventing unauthorised access to sensitive information resources, mitigating the risk of data breaches, and ensuring the confidentiality, integrity, and availability of digital assets. A fundamental aspect of cybersecurity in university libraries involves securing the library's network infrastructure. Effective network security measures, such as firewalls, intrusion detection systems, and encryption protocols, play a pivotal role in preventing unauthorised access and protecting against cyber threats. Aregbesola and Nwaolise (2023) emphasise the importance of network security in the context of academic libraries, highlighting the need for continuous monitoring and proactive measures to detect and mitigate potential security incidents. By implementing advanced threat detection technologies, libraries can identify and respond to cyber threats in real time, thereby safeguarding information resources and maintaining the integrity of digital collections.

Cloud-Based Library Services: Cloud-based library services have become integral technology-based security systems for safeguarding information resources in university libraries. These services leverage cloud computing infrastructure to store, manage, and deliver digital content, offering scalability, flexibility, and enhanced security features. Taneja and Tyagi (2017) highlight the transformative impact of cloud-based services, providing libraries with the ability to optimise resource management, enhance accessibility, and implement robust security measures. As university libraries increasingly adopt cloud solutions, it is crucial to examine the role of these services in ensuring the confidentiality, integrity, and availability of information resources. Cloud-based library services offer secure data storage solutions that allow libraries to store and manage digital collections with enhanced security features. The cloud infrastructure employs encryption protocols, access controls, and authentication mechanisms to protect sensitive information resources from unauthorised access. These security measures contribute to the overall integrity of the digital assets stored in the cloud. Daniels et al. (2023) discuss the implementation of cloud-based systems in academic libraries, highlighting the importance of access controls in ensuring that only authorised users can retrieve and manipulate digital resources. As libraries transition to cloud-based solutions, the implementation of robust access controls becomes paramount in safeguarding against potential security threats. Cloud-based library services also play a critical role in disaster recovery and ensuring data redundancy. The cloud infrastructure allows for automated and regular backups of digital collections, mitigating the risk of

data loss in the event of hardware failures, natural disasters, or other unforeseen incidents. Opara et al. (2023) underscore the importance of cloud-based disaster recovery strategies in preserving the availability and accessibility of information resources. By leveraging cloud services, university libraries can enhance their resilience against potential disruptions, contributing to the overall security and continuity of library operations.

Mobile Device Management (MDM): Mobile Device Management, or MDM, is a specialised solution that allows educational institutions to manage, monitor, and secure mobile devices such as smartphones, tablets, and laptops from a centralised platform. Mobile Device Management (MDM) serves as a crucial technology-based security system for safeguarding information resources in university libraries, particularly in an era where users increasingly rely on mobile devices for accessing digital content. MDM solutions provide libraries with the means to monitor, secure, and manage mobile devices, ensuring that they adhere to security policies and standards. The integration of MDM systems in university libraries addresses the challenges associated with the proliferation of smartphones and tablets, enhancing overall security measures. Stating the importance of MDM in the academic environment, including its role in mitigating security risks associated with the use of mobile devices in library settings, Ghosh (2023) asserted that MDM is not confined to addressing administrative challenges, it goes well beyond confronting the biggest threat for students, the malicious side of the Internet, cyberbullying, online sexual abuse and harassment, and violent, hateful, or pornographic content, among others. Furthermore, MDM solutions offer plenty of features that ensure a safe, secure, and focused learning experience on mobile devices, apart from easing the device management perspective for IT admins. By implementing MDM protocols, libraries can enforce security measures such as device encryption, password policies, and remote data wiping in the event of a lost or stolen device. Samochadin et al. (2014) discuss MDM-based mobile services in universities, emphasising their role in enhancing the security of mobile devices used for accessing services. Secure mobile access management not only protects sensitive information resources but also contributes to the privacy and data integrity of users engaging with digital content on their mobile devices. MDM systems enable the enforcement of security policies within the library's digital environment. Libraries can establish policies related to data access, application usage, and network connectivity on mobile devices. MDM solutions also facilitate robust user authentication mechanisms, ensuring that only authorised individuals can access library resources through their mobile devices. Alam (2023) explores the role of MDM in enforcing security policies and enhancing user authentication, underscoring its significance in protecting information resources from unauthorised access or misuse. As libraries increasingly adapt to the mobile-centric habits of their users, MDM systems play a pivotal role in maintaining a secure and user-friendly digital environment.

Artificial Intelligence for Anomaly Detection: Artificial Intelligence (AI) is increasingly being leveraged as a technology-based security system for safeguarding

information resources in university libraries, particularly through the application of anomaly detection algorithms. Anomaly detection involves identifying patterns that deviate from the norm, making it a powerful tool for detecting unusual activities or potential security threats within a library's digital infrastructure. With the growing complexity of cyber threats and the critical role libraries play in preserving and disseminating knowledge, the integration of AI-driven anomaly detection systems becomes imperative. Oyetola et al. (2023) underscore the significance of AI in anomaly detection, emphasising its ability to adapt to evolving security challenges and enhance the overall resilience of information systems. AI-driven anomaly detection systems find practical applications in library security by continuously monitoring network traffic, user behaviour, and access patterns to identify deviations indicative of potential security breaches. These systems can analyse vast amounts of data in real time, enabling swift identification of abnormal activities that may go unnoticed through traditional security measures. In the context of university libraries, protecting sensitive information resources from unauthorised access or data breaches is paramount. Trilles, Hammad, and Iskandaryan (2024) discuss that the integration of AI for anomaly detection analysis on Internet of Things (IoT) devices produces clear benefits as it ensures the use of accurate data from the initial stage. This highlights its effectiveness in mitigating security risks and ensuring the confidentiality and integrity of digital collections. By employing machine learning algorithms, these systems learn and adapt to the unique patterns of normal behaviour, providing a proactive defence against emerging threats. While the adoption of AI for anomaly detection in university libraries presents significant advantages, it is not without challenges. Ensuring the privacy of user data, addressing false positives, and optimising system performance are areas that require ongoing research and refinement. Lee and Park (2019) explore the challenges associated with implementing AI-based security systems and stress the need for continuous advancements to keep pace with evolving threats. Future directions should focus on developing AI models that are tailored to the specific needs and characteristics of university libraries, considering the diverse nature of information resources and user behaviours.

Identification of Vulnerabilities and Threats:

University libraries, as repositories of valuable and diverse information resources, are susceptible to various vulnerabilities and threats that can compromise the confidentiality, integrity, and availability of these resources. Understanding these challenges is crucial for developing effective security measures. Some of the common vulnerabilities and threats faced by information resources in university libraries are as explained below:

Cybersecurity Threats: In the modern library landscape, information resources are increasingly vulnerable to cybersecurity threats, posing significant risks to the integrity, confidentiality, and availability of valuable data. Cybersecurity threats can manifest in various forms, including malware attacks, phishing schemes, and ransomware incidents, all of which have the potential to compromise sensitive information stored in library

databases and systems (Opara et al. 2023). Malware, such as viruses and spyware, can infiltrate library networks, leading to data breaches and unauthorised access to patrons' personal information. Phishing attacks, often disguised as legitimate communication, may trick library staff into divulging login credentials, providing cybercriminals with unauthorised access to critical systems. Furthermore, ransomware attacks can encrypt information resources, rendering them inaccessible until a ransom is paid, disrupting library services and compromising the availability of essential resources. To mitigate these cybersecurity threats, libraries must adopt robust security measures, including regular software updates, employee training programmes, and the implementation of advanced intrusion detection systems (Aregbesola and Nwaolise 2023). Ensuring that library staff are well-informed about the latest cybersecurity risks and best practices is crucial in building a human firewall against potential threats. Additionally, the use of encryption technologies and secure authentication methods can enhance the protection of sensitive information resources in the library, safeguarding them from unauthorised access and data breaches. By adopting a comprehensive cybersecurity strategy, libraries can uphold their commitment to safeguarding the confidentiality and integrity of information resources, preserving the trust of patrons and stakeholders in an increasingly digitalised information environment.

Physical Security Risks: Physical security risks present significant threats to the preservation and accessibility of information resources within library environments. Instances of theft, vandalism, or unauthorised access to physical spaces can lead to the compromise of valuable library collections and resources. Inadequate surveillance and security measures may expose libraries to increased risks of theft, where rare and valuable materials can be targeted by criminals for illicit gains (Omoike and Alabi 2020). Additionally, vandalism poses a threat to both physical and digital resources within the library, potentially disrupting services and compromising the usability of materials. Libraries need to address these physical security risks through the implementation of robust access control systems, surveillance technologies, and security personnel to ensure the protection of information resources. To safeguard information resources from physical security threats, libraries should adopt a multi-faceted approach that combines technological solutions with staff training and awareness programmes. Access control systems, including electronic key card systems and biometric authentication, can help restrict entry to authorised personnel, reducing the risk of unauthorised access and theft (Marvin 2023). Moreover, surveillance technologies such as CCTV cameras play a crucial role in monitoring and deterring potential physical security threats. Regular staff training on emergency response procedures and the importance of maintaining a secure environment can further enhance the library's overall resilience to physical security risks, ensuring the longevity and accessibility of information resources for patrons and researchers.

Insider Threats: Insider threats represent a formidable challenge to the security of information resources within library settings. These threats emanate from individuals within the organisation, such as library staff or contractors, who exploit their access

privileges to intentionally or unintentionally compromise the confidentiality, integrity, or availability of information resources. Insider threats can take various forms, including data theft, unauthorised access, or the dissemination of sensitive information (Voss 2023). In libraries, where access to a vast array of valuable information is granted to staff members, the potential for insider threats is heightened. For instance, a disgruntled employee might intentionally leak sensitive patron information, or a well-meaning staff member could inadvertently introduce malware into the library's systems through a compromised device. Vigilance against insider threats requires a combination of technological controls, comprehensive access management policies, and ongoing employee education to foster a culture of cybersecurity awareness and responsibility. Ferreira et al. (2008) noted that access controls are likely to increase the barrier to acceptance since their design and implementation are very complex and thus costly. Mitigating insider threats in libraries involves implementing proactive measures to detect, prevent, and respond to potential risks. Regular security awareness training for library staff is crucial in cultivating a cybersecurity-conscious workforce that can recognise and report suspicious activities. Additionally, the implementation of access controls, least privilege principles, and monitoring systems can help restrict unauthorised access and detect unusual patterns of behaviour indicative of insider threats (Atlan et al. 2018). By adopting a holistic approach that combines technological solutions with employee training and awareness programmes, libraries can enhance their resilience to insider threats, safeguarding the integrity of information resources and maintaining the trust of patrons and stakeholders.

Third-Party Risk: Third-party risks pose a significant threat to the security of information resources within library environments, as libraries often collaborate with external vendors and service providers for various technological solutions and resources. These third-party relationships introduce vulnerabilities that can be exploited by malicious actors, potentially compromising the confidentiality and integrity of library data. For instance, when libraries rely on external cloud service providers to host and manage digital collections, the security of those collections becomes contingent on the practices and policies of the third-party provider (Tom-George and Nsirim 2020). Issues such as data breaches, service outages, or inadequate security measures on the part of third-party vendors can have direct implications for the availability and privacy of the library's information resources. To address third-party risks effectively, libraries must implement robust vendor management practices that encompass thorough due diligence, contractual agreements, and ongoing monitoring of third-party security measures. This includes conducting risk assessments of potential vendors to evaluate their security protocols and ensuring that contractual agreements explicitly outline the security standards and responsibilities of both parties. Kimpel (2023) hoped that regular audits and assessments of third-party vendors could help libraries proactively identify and address potential vulnerabilities before they lead to security incidents. By adopting a comprehensive approach to managing third-party risks, libraries can foster a secure environment for their information resources and uphold the trust of patrons and stakeholders in the face of an ever-evolving threat landscape. If third-party vendors

providing library services have weak security measures, they may inadvertently expose the library's information resources to external threats. Libraries using cloud-based services may face risks related to data breaches, data loss, or insufficiently protected servers, emphasising the importance of robust cloud security practices.

Strategies to Overcome the Security Threats to the Use of Technology-Based Security Systems

Overcoming challenges related to the use of technology-based security systems requires a comprehensive approach that addresses various aspects of implementation, integration, and ongoing management. Some strategies to help overcome these challenges are:

Risk Assessment and Planning: Risk Assessment and Planning are fundamental strategies in mitigating security threats associated with the use of Technology-Based Security Systems. Conducting a comprehensive risk assessment is a critical first step in identifying potential vulnerabilities and threats. As emphasised by Hayes (2023), an effective risk assessment involves the systematic identification, analysis, and evaluation of potential risks, allowing organisations to prioritise and implement appropriate security measures. By understanding the unique risk landscape, organisations can tailor their security strategies to address specific challenges and allocate resources efficiently. This proactive approach not only helps in preventing security incidents but also facilitates the development of a robust security plan that aligns with organisational objectives and regulatory requirements. The importance of planning cannot be overstated in the context of technology-based security systems. A well-developed security plan encompasses not only risk mitigation strategies but also outlines the organisation's approach to incident response, compliance, and ongoing monitoring. Mmejim and Nsirim (2023) emphasise the role of planning in establishing a structured framework for managing security risks and ensuring the resilience of technology-based security systems. This planning should involve collaboration among stakeholders, including IT professionals, security experts, and organisational leadership. Additionally, the plan should be dynamic, evolving in response to changes in technology, organisational structure, and the threat landscape. Through systematic risk assessment and strategic planning, organisations can build a resilient security posture that effectively addresses and mitigates the dynamic and evolving nature of security threats in technology-based environments

User Training and Awareness: User Training and Awareness play a pivotal role in mitigating security threats associated with the use of Technology-Based Security Systems. Human error and lack of awareness are significant contributors to security incidents; thus, the need for user education. Implementing regular training programmes for employees helps in cultivating a security-conscious culture within an organisation. Such programmes should cover topics such as phishing awareness, password hygiene, and the importance of reporting suspicious activities promptly. By equipping users with the knowledge and skills to recognise and respond to security threats, organisations can

significantly reduce the likelihood of successful cyberattacks. Terra (2023) highlighted the importance of security awareness training. As noted, users are often the weakest link in the security chain, and improving their awareness and understanding of security issues is crucial for overall system resilience. Training should not be a one-time effort but an ongoing process that adapts to emerging threats and technologies. Additionally, creating a positive security culture where employees feel encouraged to report security concerns without fear of reprisal fosters a collaborative approach to security within the organisation. By investing in user training and awareness, organisations can build a human firewall that complements the technological aspects of security, creating a more robust defence against evolving cyber threats.

Regular System Updates and Patch Management: Regular System Updates and Patch Management are critical strategies in mitigating security threats associated with the use of Technology-Based Security Systems. The importance of timely updates is underscored by the ever-evolving nature of cyber threats. Philips (2023) noted that by implementing patch management, organisations can mitigate vulnerabilities, protect against exploits and malware, meet compliance requirements, enhance cyber security, and improve system stability and performance. Libraries can, through regular updates, ensure that security vulnerabilities identified in software or operating systems are promptly addressed, reducing the risk of exploitation by malicious actors. Libraries could also establish a systematic and well-defined patch management process that includes testing patches in a controlled environment before deployment to production systems. This approach helps to avoid potential issues that may arise from the application of patches without proper validation. Mildenberger (2023) states that by staying proactive in system updates and patch management, organisations can significantly enhance their resilience against emerging threats and reduce the attack surface of their technology-based security systems.

Data Encryption and Privacy: Data encryption and privacy measures are integral strategies to counter security threats associated with the use of Technology-Based Security Systems. Encryption serves as a powerful safeguard for sensitive information, ensuring that even if unauthorised access occurs, the data remains indecipherable without the appropriate cryptographic keys (Van Daalen 2023). By encrypting data both in transit and at rest, organisations add a layer of defence against data breaches and unauthorised access to critical information. Privacy considerations, closely intertwined with encryption, are equally vital. Adhering to privacy principles and regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA), ensures that organisations handle personal information responsibly, minimising the risk of privacy breaches. Moreover, encryption and privacy measures are particularly crucial in light of the increasing volume of data transmitted and stored in cloud environments. Seth et al. (2022) emphasise the significance of encryption in cloud security, recommending the use of encryption to protect data both at rest and in transit within cloud services. With the growing prevalence of data breaches and cyber-attacks, organisations must prioritise the

integration of robust encryption and privacy practices into their technology-based security systems to safeguard sensitive information and maintain the trust of their stakeholders.

Continuous Monitoring: Continuous monitoring serves as a crucial strategy in overcoming security threats associated with the use of Technology-Based Security Systems. The concept of continuous monitoring, as advocated, involves the real-time assessment of security controls and the information system, enabling organisations to detect and respond to potential threats promptly (Sahoo 2023). This approach acknowledges the dynamic nature of cyber threats and provides a proactive means to identify vulnerabilities and unauthorised activities. Moreover, it plays a significant role in compliance efforts, ensuring that security controls remain effective over time and align with regulatory requirements. The integration of advanced technologies such as artificial intelligence and machine learning further enhances the capabilities of continuous monitoring systems by identifying anomalous patterns and behaviours indicative of security threats (Coole, Evan, and Medbury 2021). By adopting continuous monitoring as a central component of their security strategy, organisations can strengthen their overall security posture, respond proactively to emerging threats, and maintain a vigilant defence against evolving cybersecurity challenges.

Methodology

This study aims to investigate the implementation of technology-based security systems and their role in ensuring the security of information resources within a university library. The research methodology involves a multi-faceted approach to comprehensively analyse the complex interactions between technology, security frameworks, and information resources in the university library context. A literature review was conducted to examine existing studies, academic papers, and articles related to Technology-Based Security Systems in library environments. Databases consulted in search of relevant literature include Google Scholar, Academia, and ResearchGate. Content analysis was used to determine the concepts and themes. This review provides insights into established best practices, emerging trends, security threats posed by university libraries in securing their information resources and the strategies to curb the security threats.

Implications of the Study

The study's identification of particular information resources in university libraries that are susceptible to security risks is one of its main implications. Academic organisations now store a wide variety of sensitive materials in the digital age, including book and non-book materials. It is imperative to comprehend the characteristics of these assets and their vulnerability to unapproved entry or cyber hazards to execute focused security protocols. By shedding light on the possible threats that different kinds of information resources may encounter, the study helps libraries prioritise their security measures according to the content's sensitivity and criticality.

The study emphasises how crucial it is to use technology-based security measures to successfully protect university libraries' information resources. It explores the several kinds of security technologies that can be used to strengthen the safety of sensitive data, including RFID Technology for Asset Tracking, Access Control Systems, CCTV Surveillance in Libraries, Digital Rights Management, Cybersecurity Measures, Cloud-Based Library Services, and Artificial Intelligence for Anomaly Detection. In analysing the threat landscape, libraries can choose the best combination of security measures by being aware of the advantages and disadvantages of each technology. Libraries can build a strong security infrastructure that reduces risks and guarantees the confidentiality and integrity of their priceless information resources by adopting these cutting-edge technologies.

A critical component of the research is the thorough examination of possible risks to the information resources found in university libraries. These dangers include cybersecurity threats, physical security risks, insider threats and third-party risk. Understanding the complexity of these threats is essential to creating comprehensive security plans. Through the study's insights into the changing security threat landscape, libraries will be able to keep ahead of new developments and take proactive steps to mitigate risks to their information resources.

The study acknowledges that the adoption of technology-based security systems in university libraries may face some security threats. Therefore, to overcome these obstacles, the study suggests strategies such as risk assessment and planning, user training and awareness, regular system updates and patch management, data encryption and privacy and continuous monitoring. By addressing these challenges head-on, libraries can maximise the effectiveness of their technology-based security systems and ensure a resilient defence against potential security breaches.

Conclusion

One of the most important things a university library can do to protect its information resources is to integrate Technology-Based Security Systems. Libraries are depending more and more on technology as they digitise their collections and services, which makes strong security measures necessary to safeguard sensitive and priceless data. Together, the techniques covered—which include encryption, user education, constant monitoring, and frequent updates—help to build a strong security posture. While user training makes sure that people are prepared to identify and address security issues, continuous monitoring offers real-time information about possible threats. Sensitive data is protected by encryption, and vulnerabilities are reduced by patch management and frequent upgrades. University libraries must adopt a holistic approach, incorporating these strategies into their security framework to effectively counter the evolving landscape of cyber threats. Furthermore, recognising the importance of privacy and compliance with regulations is vital in the context of information resources within a university library. Libraries often handle personally identifiable information and must adhere to stringent privacy standards. By aligning security measures with these

regulations, libraries not only protect information but also demonstrate a commitment to ethical and responsible data stewardship. As technology continues to advance, university libraries must stay proactive in adapting their security strategies to address emerging challenges. Ultimately, the successful implementation of Technology-Based Security Systems ensures the confidentiality, integrity, and availability of information resources, fostering a secure and conducive environment for academic pursuits within the university community. By optimising the performance of technology-based security systems, libraries may create a strong defence against any security breaches in the ever-changing field of information management.

References

Akam, R. 2023. "MDM Security Best Practices." https://alamrabiul.medium.com/mobile-device-management-mdm-cybersecurity-securing-mobile-workforces-ea8f5e21bced

Aregbesola, A., and Nwaolise, E.L. 2023. "Securing Digital Collections: Cyber Security Best Practices for Academic Libraries in Developing Countries." *Library Philosophy and Practice* (ejournal). 7822. https://digitalcommons.unl.edu/libphilprac/7822

Atlam, H.F., Alenezi, A., Hussein, R.K., and Wills, G.B. 2018. "Validation of An Adaptive Risk-based Access Control Model for the Internet of Things." *International Journal of Computer Network and Information Security* 12(1):26.

Borky, J.M., Bradley, T.H., Borky, J.M., and Bradley, T.H. 2019. "Protecting Information with Cybersecurity." *Effective Model-Based Systems Engineering* 345–404.

Coole, M., Evan, D., and Medbury, J. 2021. "Artificial Intelligence and Security Technologies Adoption Guidance Document: Opportunities and Implications of Using Artificial Intelligence in the Establishment of Secure Physical Environments." https://www.asisonline.org/globalassets/foundation/documents/digital-transformation-series/ai-guidance-document-final.pdf

Daniels, G. N., Wiche, H., and Nsirim, O. 2023. "Librarians' ICT Skills and Effective Library Service Delivery in University Libraries in Rivers State, Nigeria." https://digitalcommons.unl.edu/libphilprac/7501

Echem, M.E., and Okwu, E. 2023. "Library Security and Sustainable Service Delivery in Donald Ekong Library, University of Port Harcourt, Rivers State, Nigeria." *Communicate: Journal of Library and Information Science* 25(1):89–101.

Elejene, A. O., H. David, and O. Nsirim. 2023. "Information and Communication Technology and Knowledge Sharing: The Role of the Library." In *Library, ICT and Information Management*, edited by Mmejim, I. C., H. Wiche, I. Idoniboye-Obu, O. Nsirim, and B. O. Umahi, 25–31. Port Harcourt: Super Print Concept.

Endouware, B.E., and Okwu, E. 2023. “Librarians’ Perceptions of the Security of Library Resources in University Libraries in Bayelsa State, Nigeria.” *Southern African Journal of Security* 1: 1–18.

Evans, S. 2023. “Strengthening Security: The Importance of Access Control.” https://www.linkedin.com/pulse/strengthening-security-importance-access-control-shervin-evans/

Ezeabasili, C.A. 2018. “Impact of Electronic Security Systems in the Security of Information Resources in Federal University Libraries in Southern Nigeria.” *Library Philosophy and Practice (e-journal)* 2110.

Ferreira, A., Cruz-Correia, R., Chadwick, D., and Antunes, L. 2008. “Improving the Implementation of Access Control in EMR.” In *2008 42nd Annual IEEE International Carnahan Conference on Security Technology* (pp. 47–50). IEEE.

Ghosh, A. 2023. “Understanding the Role of MDM in Education 4.0. Scalefusion.” https://blog.scalefusion.com/mdm-in-education-4-0/

Hayes, A. 2023. “Risk Analysis: Definition, Types, Limitations, and Examples.” *Investopedia*. https://www.investopedia.com/terms/r/risk-analysis.asp

Ibenne, S. K. 2018. *Information Resources Development and Management*. Okigwe: Justman Publishers.

Igwela, J.N.B., and Nsirim, O. 2018. “Library and Information Services for National Security and Fight against Insurgency.” Paper presentation. National Conference/Annual General Meeting of the Nigerian Library Association, Olusegun Obasanjo Presidential Library, Abeokuta, Ogun State. Compendium of NLA 2018 Conferences papers. 124–240

Kimpel, H. 2023. “Mitigate the Hidden Security Risks of Open Source Software Libraries.” https://newrelic.com/blog/how-to-relic/mitigate-open-source-library-security-risks

Larrimore, N.P. 2018. “Risk Management Strategies to Prevent and Mitigate Emerging Operational Security Threats.” Doctoral dissertation, Walden University.

Lavrov, E.A., Zolkin, A.L., Aygumov, T.G., Chistyakov, M.S., and Akhmetov, I.V. 2021. “Analysis of Information Security Issues in Corporate Computer Networks.” *In IOP Conference Series: Materials Science and Engineering* 1047(1): 012–117. IOP Publishing.

Lee, D., and Park, J.H. 2019. “Future Trends of AI-based Smart Systems and Services: Challenges, Opportunities, and Solutions.” *Journal of Information Processing Systems* 15(4):717–723.

Marvin, M. 2023. “Securing Your Digital Eco-System: The Role of Access Control in Network Security.” https://www.portnox.com/blog/network-access-control/securing-your-digital-eco-system-the-role-of-access-control-in-network-security/

Mildenberger, T. 2023. “The Importance of Patching and Patching Best Practices.” https://contabo.com/blog/the-importance-of-patching-and-patching-best-practices-linux-windows/

Mmejim, I.C., and Nsirim, O. 2023. “Managing the University Library System: Assessment National Security and Fight against Insurgency.” Paper presentation. National Conference/Annual General Meeting of the Nigerian Library Association, Olusegun Obasanjo Presidential Library, Abeokuta, Ogun State. Compendium of NLA 2018 Conferences Papers. 124–240

Nsirim, O., Agina-Obu, R., and Braid, D. 2023. “Information Resources Development: The Heart of Library Existence.” In *Library, ICT and Information Management*, edited by Mmejim, I. C., H. Wiche, I. Idoniboye-Obu, O. Nsirim, and B. O. Umahi, 25–31. Port Harcourt: Super Print Concept.

Omehia, A. E., Okwu, E., and Nsirim, O. 2021. “Librarians’ ICT Competencies and Utilisation of Emerging Technologies in Academic Libraries in Rivers State.” *Library Philosophy and Practice*. https://digitalcommons.unl.edu/libphilprac/5410

Omoike, A., and Alabi, R. 2020. “Theft, Mutilation and Abuse of Library and Information Materials by Undergraduates of University of Ibadan, Nigeria.” *Information Impact: Journal of Information and Knowledge Management* 11(2): 1–12. .doi.org/10.4314/iijikm.v11i2

Opara, O.O. Nsirim, O, and Irokah. P. L. 2023. “Technological Methods and Security of Information Resources in Dame Patience Goodluck Jonathan Automated Library, Ignatius Ajuru University of Education.” *Southern African Journal of Security* 1:1–17. https://doi.org/10.25159/3005-4222/14506

Oyetola, S.O., Oladokun, B.D., Maxwell, C.E., and Akor, S.O., 2023. “Artificial Intelligence in the Library: Gauging the Potential Application and Implications for Contemporary Library Services in Nigeria.” *Data and Metadata 2*:36–36.

Rana, S., and Mishra, D. 2021. “An Authenticated Access Control Framework for Digital Right Management System.” *Multimedia Tools and Applications* 80: 25255–25270.

Sahoo, N. 2023. “The Advantages of Continuous Cybersecurity Monitoring.” LinkedIn. https://www.linkedin.com/pulse/advantages-continuous-cybersecurity-monitoring-narendra-sahoo/

Samochadin, A., Raychuk, D., Voinov, N., Ivanchenko, D., and Khmelkov, I. 2014. “MDM Based Mobile Services in Universities.” *International Journal of Information Technology and Computer Science (IJITCS)* 13(2):35–41.

Seth, B., Dalal, S., Jaglan, V., Le, D.N., Mohan, S., and Srivastava, G. 2022. Integrating Encryption Techniques for Secure Data Storage in the Cloud.” *Transactions on Emerging Telecommunications Technologies* 33(4): p.e4108.

Taneja, D., and Tyagi, S.S. 2017. “Information Security in Cloud Computing: A Systematic Literature Review and Analysis.” *International Journal of Scientific Engineering and Technology* 6(1): 50–55.

Terra, J. 2023. “The Importance of Security Awareness Training.” Simplilearn. https://www.simplilearn.com/importance-of-security-awareness-training-article

Trilles, S., Hammad, S.S., and Iskandaryan, D. 2024. “Anomaly Detection Based on Artificial Intelligence of Things: A Systematic Literature Mapping.” *Internet of Things* 101063.

Van Daalen, O.L. 2023. “The Right to Encryption: Privacy as Preventing Unlawful Access.” *Computer Law and Security Review* 49: 1–19. https://doi.org/10.1016/j.clsr.2023.105804

Voss, E. 2023. “Insider Threat: A Case Study, Recognizing the Early Warnings Signs by Humans.” Doctoral dissertation, Northcentral University.