Library Security Systems and Management in Academic Libraries in Nigeria

Odaro Osayande
Edo State University, Iyamho, Edo State.
odaroosayande80@gmail.com

Abstract

Security has become a major management concern in academic libraries as their collections, services and operating environments expand beyond printed resources to digital collections, information and communication technology (ICT) infrastructure, electronic databases, institutional repositories, networked systems, surveillance technologies and user data. In Nigeria, library security has traditionally been associated with theft, mutilation, vandalism and unauthorised removal of library materials. Although these threats remain significant, the contemporary academic library faces a broader spectrum of physical, technological, environmental, cyber and privacy risks. This opinion paper critically examines library security systems and their management in Nigerian academic libraries, drawing primarily on recent Nigerian empirical evidence and selectively on international studies for comparative insight. Evidence indicates ongoing losses through theft, mutilation, and vandalism, alongside uneven deployment of closed-circuit television (CCTV), radio-frequency identification (RFID), electronic security gates, biometric, and other access-control technologies. Studies also highlight emerging concerns about cybersecurity, institutional repositories, privacy, disaster preparedness, and continuity of digital services. The paper argues that acquiring security technologies does not, by itself, constitute effective security management. Sustainable protection requires integration of technology with governance, policy, risk assessment, competent personnel, user education, cybersecurity, data protection, maintenance, incident response and institutional commitment. As its principal conceptual contribution, the paper proposes an original Integrated Library Security Systems and Management Framework (ILSSMF) comprising seven interrelated components: security governance and policy; risk identification and assessment; physical and environmental protection; collection and asset protection; digital, cyber and data security; people, security culture and partnerships; and incident response, recovery and continuous improvement. Monitoring, evaluation, learning and improvement operate across the framework. The paper concludes that Nigerian academic libraries should move from reactive, collection-centered security to integrated, risk-based, and resilient security management capable of protecting people, collections, facilities, technologies, data, and continuity of library services.

Keywords: academic libraries; library security; security management; electronic security systems; cybersecurity; RFID; CCTV; disaster preparedness; data privacy; Nigeria; ILSSMF

Introduction

Academic libraries are fundamental to the teaching, learning, research and community service mandates of universities and other tertiary institutions. They acquire, organise, preserve and provide access to information resources required by students, researchers and academic staff. Their ability to perform these functions depends partly on how well their human, informational, technological and physical assets are protected.

The contemporary academic library, however, is considerably different from the conventional library whose security concerns centred primarily on books, journals and buildings. Academic libraries now function simultaneously as physical learning spaces, repositories of print collections, digital information environments, technology

centres, institutional repositories and processors of user information. Their infrastructure may include computers, servers, wireless networks, integrated library management systems, electronic databases, digitisation facilities, surveillance systems and access-control technologies. This transformation has expanded both the assets requiring protection and the range of threats confronting libraries.

Historically, security discourse in Nigerian academic libraries has concentrated largely on theft, mutilation, vandalism, non-return of borrowed materials and unauthorised removal of library resources. These remain important concerns. Recent empirical evidence confirms their persistence. Osayande, Mutula and Izuagbe (2024), in a study of 197 librarians and paraprofessional staff from four public and private universities in South-West Nigeria, reported substantial losses from theft, mutilation and vandalism. Their findings further demonstrated differences in the deployment and condition of electronic security systems across the institutions studied.

The security environment has nevertheless become more complex. Fatade, Ajiboye and Ogunjimi (2023), in their investigation of 169 staff in two academic libraries in South-West Nigeria, identified hacking as a significant security threat, particularly to e-libraries, while fire was among the important disaster risks confronting the libraries. Njoku et al. (2023), based on responses from librarians and ICT personnel associated with Nigerian institutional repositories, similarly highlighted viruses, cyberattacks, and risks to the confidentiality, integrity, and availability of digital scholarly resources.

These findings demonstrate an important transformation in library security. A stolen textbook represents a security breach, but so does unauthorised access to an institutional repository. Mutilation of a journal is a security problem, but so is loss of a digital collection because of malware, ransomware or inadequate backup. Unauthorised removal of a book is a breach, but inappropriate disclosure of a user's personal or borrowing information may equally constitute a security failure.

International evidence reflects similar developments. Asim et al. (2022), using an exploratory sequential mixed-method approach and quantitative responses from 122 university librarians in Pakistan, found that smart security doors, automatic fire alarms, RFID tags, card-recognition systems, and automated circulation technologies were deployed. However, inadequate networking infrastructure, funding, the absence of policy and strategic planning, and shortages of technical personnel constrained implementation.

This paper therefore advances the position that library security should be conceptualised as an integrated institutional risk-management responsibility concerned with protecting people, physical collections, digital resources, facilities, technologies and data while ensuring continuity of access to library services. The paper examines the changing security environment of Nigerian academic libraries, evaluates conventional and emerging security systems, discusses security governance and management, and proposes an original Integrated Library Security Systems and Management Framework (ILSSMF) appropriate to Nigerian academic library environments.

Concept and Scope of Library Security

Library security encompasses the policies, procedures, personnel, technologies and management practices established to protect library users, staff, collections, facilities, equipment, information systems and data against deliberate and accidental threats. It includes measures intended to prevent security incidents as well as arrangements for detecting, responding to and recovering from incidents when they occur.

Contemporary library security has at least six dimensions: human security, collection security, physical and environmental security, asset security, digital and cybersecurity, and information/privacy security. Nigerian empirical evidence supports this multidimensional interpretation. Osayande et

al. (2024) examined CCTV, RFID, biometrics and electronic security gates in selected university libraries, while Njoku et al. (2023) demonstrated that institutional repositories require deliberate cybersecurity and risk-management measures.

Three established information security principles confidentiality, integrity and availability are particularly applicable to the digital academic library. Confidentiality concerns preventing unauthorised disclosure of protected information; integrity requires maintaining the accuracy and reliability of information and systems; and availability means ensuring that authorised users can access information and services when required.

Security should nevertheless not be equated with maximum restriction. Academic libraries exist principally to facilitate access to information. Effective security management therefore requires a balance between protection and accessibility. Academic-library security should aim for secure access rather than restricted access.

The Changing Security Environment of Nigerian Academic Libraries

1. Coexistence of Print and Digital Collections

Nigerian academic libraries increasingly maintain hybrid collections consisting of books, journals, theses, dissertations and special collections alongside electronic databases, institutional repositories, e-books and digitised resources. This creates parallel security requirements.

Ezema and Eze (2024) investigated institutional repositories in 23 universities in South-East Nigeria and found that only 26% had fully implemented institutional repositories. Inadequate ICT infrastructure and shortage of skilled personnel were among the principal challenges. Although their study primarily addressed repository implementation and institutional visibility, its findings have security implications because sustainable digital collections depend on reliable infrastructure and appropriately skilled personnel.

International evidence points in the same direction. Asim et al. (2022) found that Pakistani university libraries were combining conventional library operations with RFID tags, smart doors, automated fire alarms and card-recognition technologies. This implies that security planning can no longer separate the traditional library from the digital library; both form a single institutional information environment that requires integrated protection.

2. Increasing Dependence on ICT

Library-management systems, institutional repositories, electronic databases, computers, servers, wireless networks and digitisation equipment have become central to academic-library service delivery. Njoku et al. (2023) investigated cybersecurity in Nigerian institutional repositories using a sample of 88 librarians and ICT personnel, of whom 62 responded (70.4%). The study identified risks associated with viruses and cyberattacks and emphasized their implications for the confidentiality, integrity and availability of digital resources.

Increasing dependence on technology means that failure or compromise of a server or network may disrupt access to far more information than the loss of a single printed resource. Digital resilience should therefore become an explicit library-management responsibility.

3. Expansion of Library Spaces and Services

Contemporary academic libraries provide reading spaces, postgraduate facilities, collaborative-learning areas, computer laboratories, electronic-resource centres and sometimes extended opening hours. Different spaces have different risk profiles. A general reading area, for example, requires different security controls from a server room or special-collections section. Academic libraries should therefore adopt security zoning, matching controls to the sensitivity of particular spaces, collections and systems.

Security Threats in Academic Libraries

1. Theft and Unauthorised Removal

Theft remains one of the most persistent threats to academic-library collections. Osayande et al. (2024) found substantial losses from theft, mutilation, and vandalism in selected Nigerian university libraries. Comparable findings have been reported elsewhere in Africa. Ameyaw, Amoah and Frempong-Kore (2024), studying the Walton Whaley Library of Valley View University in Ghana, linked theft and mutilation to weak security arrangements, inadequate staffing, and the absence of CCTV surveillance.

The Nigerian and Ghanaian evidence suggests that theft should not be interpreted as individual misconduct alone. Security-system deficiencies, inadequate surveillance, insufficient copies of high-demand resources and weaknesses in service design may create conditions that facilitate collection abuse.

2. Mutilation and Vandalism

Mutilation includes tearing pages, removing illustrations or chapters, writing on resources and deliberately damaging library materials. Vandalism extends to furniture, equipment and facilities. The continuing losses identified by Osayande et al. (2024) indicate that expanding electronic resources has not eliminated physical collection abuse.

Libraries should therefore address mutilation through both deterrence and service improvement. CCTV, security gates and staff surveillance may deter misconduct, but adequate collections, accessible electronic alternatives, scanning or reprographic services, and user education may reduce pressures contributing to inappropriate behaviour.

3. Non-return and Misuse of Borrowed Resources

Not all collection loss involves deliberate theft. Materials may remain overdue for extended periods, circulation transactions may be incorrectly recorded, and borrowing privileges may be abused. Automated circulation systems can improve accountability through transaction histories, authentication and reminders. However, technology must operate within clear lending policies and accurate user databases. Technology should support management processes rather than substitute for them.

4. Theft and Damage of ICT Equipment

Computers, servers, scanners, routers, storage devices, surveillance equipment and other technologies represent substantial investments. The increasing technological nature of Nigerian academic libraries means security must cover equipment as well as information resources. Asset tagging, inventory control, CCTV, restricted access to equipment rooms and documented responsibility for movable equipment should consequently form part of security management.

5. Unauthorised Physical Access

Server rooms, archives, staff offices, special collections and technical-service areas require controlled access. Traditional keys may remain appropriate in some environments, while smart cards, electronic access systems or biometrics may be justified for higher-risk locations. Internationally, Asim et al. (2022) found smart security doors and card-recognition systems among technologies already being implemented in Pakistani university libraries. Access controls should follow the principle of proportionality: security measures should correspond to the sensitivity and value of the resources being protected.

6. Fire, Electrical and Environmental Threats

Security threats are not exclusively intentional. Fire, flooding, roof leakage, electrical surges, excessive humidity and other environmental conditions can cause extensive losses. Fatade et al. (2023) identified fire as a major disaster threat confronting two academic libraries in South-West Nigeria and recommended disaster-response teams.

Fire detectors, appropriate extinguishers, electrical protection, emergency exits,

environmental monitoring and disaster-response procedures should therefore be considered security controls. For Nigerian academic libraries, power resilience deserves particular attention because electrical interruptions can simultaneously disrupt surveillance cameras, access-control systems, servers and digital services.

7. Cybersecurity Threats

Cybersecurity is now inseparable from academic-library security. Njoku et al. (2023) identified cybersecurity risks confronting Nigerian institutional repositories and emphasised the need to protect digital scholarly records against viruses and cyberattacks.

The problem has a significant human dimension. Kavak (2024), surveying 136 personnel working in academic libraries in Türkiye, found that information-security awareness had a positive and statistically significant effect on security compliance. Together, the Nigerian and Turkish evidence demonstrates that cybersecurity requires two complementary dimensions: technical security controls and human security behaviour.

8. Personal Data and Privacy

Academic libraries increasingly process user-registration details, circulation records, electronic authentication information, surveillance footage and potentially biometric data. Privacy therefore constitutes an important dimension of library security.

Asher et al. (2022), based on approximately 2,200 student responses across eight higher-education institutions in the United States, found generally high trust in libraries but also clear privacy concerns. Students viewed librarian access to and sharing of personally identifiable information as potentially violating privacy, while many were unaware of the data and analytics practices libraries undertake.

This has significant implications for Nigerian libraries. CCTV, biometrics, electronic-resource authentication, and learning analytics may enhance management or security but also create personal information that requires protection. Nigeria's Data Protection Act 2023 further strengthens the need for responsible personal-data governance. Security measures should protect library users without turning the security system itself into an unnecessary privacy risk.

Electronic and Technological Library Security Systems

1. Closed-Circuit Television

CCTV is among the most visible electronic security technologies used in academic libraries. Cameras can monitor entrances, exits, reading areas, shelving zones and other vulnerable locations. Osayande et al. (2024) found CCTV to be the best-conditioned electronic security technology among those examined in four South-West Nigerian university libraries, followed by electronic security gates and RFID, while biometric systems were comparatively weak.

CCTV, however, should not be equated with security simply because cameras are installed. Its effectiveness depends on camera positioning, image quality, recording and storage capacity, power reliability, monitoring arrangements, maintenance and procedures for responding to incidents. Privacy must also be considered because surveillance footage constitutes information about identifiable persons.

2. Electronic Security Gates

Electronic security gates can detect improperly issued tagged resources at library exits. Osayande et al. (2024) found electronic security gates to be among the better-performing electronic security systems in the university libraries investigated. Their effectiveness nevertheless depends on consistent tagging, functioning sensors and appropriate staff response.

3. Radio-Frequency Identification

RFID is particularly relevant because it can integrate identification, circulation, stock management, and security. Nigerian evidence indicates increasing adoption, although condition and utilisation vary across institutions. International evidence

demonstrates its wider potential. Asim et al. (2022) found RFID tags being used in Pakistani university libraries for security as well as self-check-in and self-check-out services. RFID should therefore be understood as an integrated identification, circulation, inventory, self-service and security system.

4. Access-Control and Biometric Systems

Electronic cards and biometric technologies can strengthen access control to restricted facilities. Osayande et al. (2024), however, found biometric systems to be comparatively poorly developed among the electronic security technologies examined. Biometric implementation should be approached cautiously because biometric identifiers are sensitive information. Libraries should establish clear purposes, access restrictions, retention rules and safeguards before deploying such systems.

5. Fire and Environmental Systems

Automatic fire alarms, smoke detectors, fire extinguishers, water sensors and environmental monitoring systems should be treated as part of security infrastructure. Internationally, Asim et al. (2022) found automatic fire alarms among IoT-enabled technologies already implemented in Pakistani university libraries. Nigerian evidence identifying fire as an important disaster threat reinforces the relevance of such systems.

6. Network and Cybersecurity Technologies

Digital security controls include firewalls, endpoint protection, anti-malware systems, encryption, secure authentication, software patching, access logging, network segmentation and backup. Njoku et al.'s (2023) evidence on Nigerian institutional repositories directly justifies incorporating these controls into academic-library security planning. Cybersecurity is now part of library security rather than an unrelated technical responsibility.

Library Security Management: Beyond Security Equipment

1. Security Governance and Policy

Governance establishes who is responsible for security, what assets should be protected, what level of risk is acceptable and how security performance will be monitored. Kavak's (2024) study of academic-library personnel in Türkiye found that information-security awareness significantly influenced security compliance. Asim et al. (2022) identified the absence of policy and strategic plans as one of the challenges affecting implementation of IoT technologies in Pakistani university libraries.

Every Nigerian academic library should therefore operate under a written, institutionally approved security policy covering physical collections, digital resources, facilities, surveillance, ICT, personal data, emergency response, incident reporting, and recovery.

2. Security Risk Assessment

Security investment should be based on risk rather than technological fashion. A systematic process should examine assets, threats, vulnerabilities, likelihood, impact, existing controls, residual risk and additional treatment. The cybersecurity risks identified by Njoku et al. (2023) and the disaster threats reported by Fatade et al. (2023) illustrate why academic libraries require a broad risk assessment that encompasses both physical and digital environments. Libraries should maintain a risk register that identifies high-priority risks, responsible officers, existing controls, and treatment requirements.

3. Assignment of Responsibility

Security should be understood as a shared institutional responsibility. The University Librarian should provide strategic leadership, but librarians, systems librarians, ICT personnel, university security officers, facility managers and senior university administrators have complementary responsibilities. Cybersecurity particularly requires close cooperation between the library and institutional ICT departments, while

disaster preparedness requires coordination with facilities departments, security units, fire services and university administration.

4. Security Financing

Modern security systems require initial and recurrent expenditure. Asim et al. (2022) identified budgetary constraints as a major obstacle to implementing IoT technologies in university libraries. Nigerian evidence of uneven electronic-security deployment likewise suggests that technology acquisition cannot be separated from institutional capacity. Security budgeting should include acquisition, installation, software licenses, electricity, replacement components, storage, technical support, staff development and preventive maintenance.

5. Preventive Maintenance

A non-functional CCTV camera provides no surveillance. A damaged RFID gate offers little protection. An untested fire alarm may create false confidence. Academic libraries should maintain equipment registers documenting installation dates, maintenance history, faults, repairs, replacement schedules and responsible officers. Libraries should treat maintenance as a security investment rather than an optional technical expense.

6. Incident Reporting and Documentation

Security incidents should generate organisational learning. Libraries should maintain structured incident registers containing the date, location, nature of the incident, asset affected, immediate response, persons notified, investigation, outcome, and corrective action. Over time, such records can reveal patterns that individual recollections cannot.

Human Factors and Security Culture

1. Staff Training

Security effectiveness depends substantially on human behaviour. Kavak (2024) found moderate levels of security awareness and compliance among academic-library employees in Türkiye and demonstrated a significant positive influence of awareness on compliance. Security training in Nigerian academic libraries should cover suspicious behaviour, alarm response, phishing, password security, data protection, emergency evacuation, fire response, incident reporting and appropriate use of institutional systems.

2. User Security Education

Library users also form part of the security environment. Orientation programmes should explain responsible use of resources, borrowing requirements, prohibition of mutilation, protection of authentication credentials and reasons for particular access or surveillance measures. The objective should be to develop a culture of collective stewardship in which users recognise that damage to library resources affects the entire academic community.

3. Management Leadership and Security Culture

Security culture is unlikely to develop where management treats security as an occasional operational concern. University Librarians should integrate security into strategic planning, budgeting, management meetings, staff development and service evaluation. Significant incidents should result in formal review and corrective action rather than temporary responses.

Cybersecurity, Data Protection and Privacy Management

1. Authentication and Access Management

Digital-library systems should apply the principle of least privilege: users and employees should have only the access necessary for legitimate responsibilities. Sensitive systems should require strong authentication, and multi-factor authentication should be considered, particularly for administrator and remote-access accounts. Promptly modify or deactivate accounts for employees who leave or change responsibilities.

2. Backup and Recovery

Backups are fundamental to resilience. Digital collections may be damaged through malware, ransomware, equipment failure, accidental deletion, or other events. Libraries should maintain multiple backup copies and, where feasible, store copies in physically or logically separated locations. Ezema and Eze's (2024) findings concerning infrastructure and skills deficiencies in Nigerian institutional repositories reinforce the need to build resilience into digital-collection development from the beginning. Backup restoration should be periodically tested.

3. Software Updating and Vulnerability Management

Outdated software creates avoidable vulnerabilities. Operating systems, repository platforms, library-management software and security tools should be maintained through documented patching procedures. Unsupported applications should be upgraded, replaced or appropriately isolated. Where libraries lack sufficient cybersecurity expertise, they should manage this function jointly with institutional ICT departments.

4. Data Protection and Privacy

The expansion of surveillance, analytics and authentication technologies requires libraries to determine what personal information is collected, why it is needed, who has access, where it is stored, how long it is retained, with whom it is shared and how it is securely disposed of. Asher et al. (2022) found that students expressed considerable trust in libraries but were concerned about access to and sharing of personally identifiable information and frequently lacked awareness of library data practices. Effective security should protect both institutional resources and legitimate user privacy.

Disaster Preparedness, Response and Business Continuity

Disaster preparedness deserves explicit recognition within academic-library security because disasters may simultaneously affect buildings, collections, technology, personnel and services. Fatade et al. (2023), surveying 169 staff in two South-West Nigerian academic libraries, found hacking to be a major security threat, particularly for e-libraries, and fire among significant disaster risks. Their overall assessment of disaster preparedness and security management was positive, but they recommended establishing disaster-response teams.

Every academic library should develop a disaster and business-continuity plan specifying priority collections and systems, emergency contacts and responsibilities, evacuation arrangements, communication procedures, alternative service arrangements, data backup and restoration, salvage procedures, coordination with emergency services and procedures for returning to normal operations. Libraries should periodically test preparedness through drills or simulations.

Integrated Library Security Systems and Management Framework (ILSSMF)

1. Rationale

The evidence reviewed reveals a consistent pattern. Nigerian academic libraries continue to experience conventional threats involving theft, mutilation and vandalism. At the same time, electronic security systems are being introduced unevenly; digital collections generate cybersecurity risks; disaster threats remain relevant; and the growing use of surveillance and authentication technologies raises privacy considerations. International evidence further demonstrates that security effectiveness is influenced by policy, technical capacity, financing and staff awareness.

The literature therefore exposes an important management problem: security measures are frequently discussed as separate interventions. CCTV is discussed independently of cybersecurity, RFID independently of policy, disaster management independently of digital recovery, and user surveillance independently of privacy. This fragmentation motivates the

paper's principal conceptual contribution: the Integrated Library Security Systems and Management Framework (ILSSMF). The ILSSMF synthesizes contemporary security challenges and management requirements in the context of Nigerian academic libraries.

2. Architecture of the ILSSMF



Figure 1. Integrated Library Security Systems and Management Framework (ILSSMF)

Source: Author's conceptualisation (2026).

3. Component One: Security Governance and Policy

Governance constitutes the foundation of ILSSMF because security requires institutional authority, responsibility and accountability. The component asks: Who is responsible? What is being protected? What risks are acceptable? What policies govern security decisions? How is compliance evaluated? Academic libraries should establish comprehensive security policies and, where appropriate, a Library Security Management Committee involving library management, institutional ICT, security, facilities and relevant administrative units.

4. Component Two: Risk Identification and Assessment

The second component establishes a systematic process for asset identification, threat identification, vulnerability assessment, likelihood and impact estimation, risk rating, and control selection. Assets include people, collections, facilities, equipment, systems and data. The different threats documented in Nigerian studies—from theft and fire to hacking and institutional-repository attacks—demonstrate why academic libraries need comprehensive risk registers rather than narrow theft-prevention plans.

5. Component Three: Physical and Environmental Protection

This component covers buildings, spaces, people and environmental hazards. Controls may include perimeter protection, lighting, controlled entrances and exits, CCTV, electronic access control, secure doors and windows, fire detection and suppression, electrical protection, environmental monitoring and secure equipment rooms. Physical security should operate through defense in depth, ensuring that the failure of one control does not eliminate protection entirely.

6. Component Four: Collection and Asset Protection

This component protects print collections, special materials and technological assets. Controls include ownership marking, barcoding, RFID, electronic security gates, controlled circulation, inventories, stock verification, restricted special collections, equipment tagging, asset registers and appropriate sanctions for deliberate violations. The continuing magnitude of theft, mutilation and vandalism reported in Nigerian libraries provides empirical justification for retaining collection protection as a distinct component even as libraries become increasingly digital.

7. Component Five: Digital, Cyber and Data Security

The fifth component protects institutional repositories, networks, library-management systems, digital collections and personal data. It incorporates secure authentication, multi-factor authentication where appropriate, access control, firewalls, endpoint protection, software patching, encryption, backups, access logging, vulnerability management, incident detection, data minimisation, privacy safeguards and secure data disposal.

8. Component Six: People, Security Culture and Partnerships

People implement, monitor, and use security technologies. This component therefore includes staff security awareness, specialist training, user education, professional ethics, clearly assigned responsibilities, internal communication, management commitment and interdepartmental partnerships. Libraries should establish working relationships with university ICT units, institutional security, facilities departments, data-protection functions, fire services and external emergency organisations where appropriate.

9. Component Seven: Incident Response, Recovery and Continuous Improvement

Absolute prevention is impossible. Security management must therefore include resilience. ILSSMF proposes the following incident cycle: DETECT → REPORT → CONTAIN → INVESTIGATE → RESPOND → RECOVER → DOCUMENT → REVIEW → IMPROVE. Significant incidents should result in post-incident reviews identifying what occurred, which controls succeeded or failed, and what corrective actions are required

10. Monitoring and Evaluation

Monitoring, evaluation, learning and improvement operate across every ILSSMF component. Possible performance indicators include the number of theft incidents, number of mutilated materials, value of lost assets, percentage of CCTV cameras operational, security-gate uptime, number and severity of cybersecurity incidents, percentage of critical systems patched, staff security-training coverage, successful backup-restoration rate, incident-response time, percentage of identified high risks treated and number of repeated incidents.

The framework can consequently be summarised as: GOVERN → ASSESS → PROTECT → SECURE → EDUCATE → DETECT → RESPOND → RECOVER → REVIEW → IMPROVE. The cycle repeats as the library's technologies, collections, users and risks change.

Challenges to Effective Security Management in Nigerian Academic Libraries

1. Inadequate Funding

Security systems require capital and recurrent expenditure. International evidence identifies budgetary limitations as a major barrier to emerging security technologies. Nigerian libraries operate within comparable resource constraints. Security investments should therefore be based on risk and lifecycle cost, not prestige or technological novelty.

2. Infrastructure Deficiencies

Ezema and Eze (2024) found inadequate ICT infrastructure among major constraints affecting institutional-repository implementation in South-East Nigerian universities. Weak electricity, networks and buildings can undermine sophisticated

security equipment. Supporting infrastructure should consequently be recognised as part of security investment.

3. Technical Skills Gaps

The shortage of skilled personnel identified in Nigerian institutional-repository environments has implications beyond repository implementation. Modern library security increasingly requires competencies in networking, cybersecurity, electronic surveillance, data protection and disaster recovery. Libraries require continuous staff development and institutional collaboration rather than expecting librarians to possess every specialist competency independently.

4. Maintenance Problems

Acquiring equipment without maintaining it creates a false impression of security. Preventive maintenance contracts, technical audits, replacement schedules and recurrent budgets should therefore accompany electronic-security procurement.

5. Weak Security Culture

Employees and users may circumvent controls for convenience, disclose credentials, ignore alarms or fail to report suspicious incidents. The empirical association between awareness and security compliance illustrates why security culture should be deliberately developed.

6. Privacy and Ethical Concerns

Increasing surveillance may generate legitimate concerns about monitoring and personal-data processing. Evidence demonstrates that high levels of trust in libraries can coexist with concerns about access to and sharing of identifiable user information. Nigerian academic libraries should therefore pursue privacy-conscious security rather than assuming that more surveillance necessarily means better security.

7. Rapid Technological Change

IoT systems, artificial intelligence, cloud services, biometrics and interconnected devices continually change both library services and security risks. Technology implementation can outpace policy, infrastructure and technical capacity. Security policies must therefore be periodically reviewed rather than treated as permanent documents.

Implications for Academic Library Management

The evidence and arguments developed in this paper have several important implications. First, academic library strategic planning should explicitly incorporate security. It should not remain confined to circulation regulations or security personnel duties.

Second, University Librarians should treat security information as management information. Incident statistics, equipment status, cyber vulnerabilities, maintenance records and audit results should be periodically reviewed at management level.

Third, security investment should be risk-based rather than technology-driven. The most expensive technology is not necessarily the most appropriate security solution for every library.

Fourth, cybersecurity and privacy should be recognised as professional library-management issues. While technical implementation may be undertaken jointly with institutional ICT units, library management must understand the risks associated with the systems and information that support library services.

Fifth, disaster preparedness should be connected to business continuity. The critical question is not merely whether the library can respond to a fire, flood or cyberattack, but whether essential services can be restored within an acceptable period.

Sixth, security competencies should become part of continuing professional development for academic librarians. Finally, security requires institutional ownership. Protecting the academic library means protecting institutional research output, intellectual heritage, expensive technology, personal information and services central to the university's academic mission.

Recommendations

1. Develop comprehensive, institutionally approved security policies encompassing physical collections, facilities, technology, digital resources, cybersecurity, personal data, disaster management and service continuity.
2. Undertake periodic security-risk assessments and maintain formal risk registers.
3. Adopt layered security systems combining human, administrative, physical and technological controls according to identified risks.
4. Provide sustainable funding covering acquisition, maintenance, replacement, software, technical support, electricity and staff development.
5. Deploy CCTV, RFID, electronic security gates and access-control technologies according to institutional needs and capacity rather than technological fashion.
6. Strengthen cybersecurity through secure authentication, multi-factor authentication for privileged systems, software patching, endpoint protection, network controls, logging, backups and tested recovery procedures.
7. Align CCTV, biometric and other personal data processing with the requirements and principles of the Nigeria Data Protection Act 2023.
8. Institutionalise regular staff security, cybersecurity and privacy training.
9. Incorporate responsible use of resources and security awareness into library user education.
10. Establish preventive-maintenance schedules and operational testing for all security technologies.
11. Develop formal incident-reporting systems and conduct post-incident reviews.
12. Establish disaster-response and business-continuity plans and periodically test them.
13. Conduct regular physical, technological and procedural security audits.
14. Strengthen collaboration between university libraries, ICT directorates, institutional security departments, facilities units and data-protection personnel.
15. Adopt or adapt the proposed Integrated Library Security Systems and Management Framework (ILSSMF) as a systematic approach for integrating governance, risk, physical protection, collection security, cybersecurity, people, incident response and continuous improvement.

Conclusion

Library security in the twenty-first century extends considerably beyond preventing theft of books. Yet the empirical literature demonstrates that traditional threats have not disappeared. Nigerian academic libraries continue to experience theft, mutilation and vandalism even as they adopt CCTV, RFID, electronic security gates and other technologies.

At the same time, digital transformation has created additional vulnerabilities. Nigerian research on institutional repositories confirms risks from viruses and cyberattacks, while infrastructure and skills limitations complicate developing and protecting digital collections. Disaster-management evidence further demonstrates the relevance of fire, hacking and emergency preparedness.

International evidence reinforces these concerns. University libraries elsewhere are implementing smart doors, RFID, automatic fire detection and other connected technologies, but financial constraints, inadequate policy and shortages of technical personnel can limit effective implementation. Information-security research also shows the importance of staff awareness and compliance, while privacy studies show that technological innovation can raise legitimate concerns about how libraries collect and use personal information.

These findings support the central proposition of this paper: effective academic-library security is an integrated management system, not a collection of security devices.

The proposed Integrated Library Security Systems and Management Framework (ILSSMF) responds to this need by connecting seven components: security governance and policy; risk identification and assessment; physical and environmental protection; collection and asset protection;

digital, cyber and data security; people, security culture and partnerships; and incident response, recovery and continuous improvement. Monitoring, evaluation, learning and improvement provide the feedback mechanisms linking these components.

The ILSSMF represents the author's conceptual contribution derived from the synthesis and interpretation of Nigerian and international evidence. It shifts academic-library security from reactive intervention to proactive risk management; from isolated technologies to integrated systems; from collection protection to total information-asset protection; and from individual responsibility to institutional governance and shared security culture.

Ultimately, security and access should not be viewed as opposing objectives. The purpose of library security is not to restrict legitimate access to knowledge but to ensure that people, collections, technologies and information remain sufficiently protected for access to be sustained. A secure academic library is therefore not simply one in which materials cannot be stolen; it is one that can protect its people and information assets, anticipate risks, withstand disruption, recover from incidents and continue providing trustworthy access to knowledge.

References

Asher, A. D., Briney, K. A., Jones, K. M. L., Regalado, M., Perry, M. R., Goben, A., Smale, M. A., & Salo, D. (2022). Questions of trust: A survey of student expectations and perspectives on library learning analytics. *The Library Quarterly*, *92(*2), 151–171. https://doi.org/10.1086/718605

Asim, M., Arif, M. S. K., Rafiq, M., & Ahmad, R. (2022). Applications of Internet of Things in university libraries of Pakistan: An empirical investigation. *The Journal of Academic Librarianship, 48*(6), 102613. https://doi.org/10.1016/j.acalib.2022.102613

Ezema, I. J., & Eze, J. U. (2024). Status and challenges of institutional repositories in university libraries in South-East Nigeria: Implications for visibility and ranking of Nigerian universities. *The Journal of Academic Librarianship, 50*(2), 102834. https://doi.org/10.1016/j.acalib.2023.102834

Fatade, A. T., Ajiboye, B. A., & Ogunjimi, M. S. I. (2023). Disaster preparedness and security management in two academic libraries in South-West Nigeria. *Gateway Information Journal, 24*(1 & 2), 46–61.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. Nigeria Data Protection Commission.

Kavak, A. (2024). Impact of information security awareness on information security compliance of academic library staff in Türkiye. *The Journal of Academic Librarianship, 50*(5), 102937. https://doi.org/10.1016/j.acalib.2024.102937

Njoku, I. S., Njoku, B. C., Chukwu, S. A. J., & Ravichandran, R. (2023). Fostering cybersecurity in institutional repositories: A case of Nigerian universities. *African Journal of Library, Archives and Information Science, 33*(1), 1–21.

Osayande, O., Mutula, S., & Izuagbe, R. (2024). A comparative study of electronic security systems of academic libraries in selected public and private universities in South-West, Nigeria. *Journal of Applied Information Science and Technology, 17*(2). 6-13

Ajala, I. O., & Oyeboade, S. A. (2008). Theft and mutilation of library materials in Nigerian academic libraries. *Library & Archival Security, 21*(1). 26-37

Ameyaw, S., Amoah, C. N. E., & Frempong-Kore, A. (2024). Who are the culprits? Evaluation of theft and mutilation of academic library materials: Experience from the Walton Whaley Library.

International Journal of Librarianship, 9(3), 47–74.

Maidabino, A. A., & Zainab, A. N. (2012). Assessment of theft and mutilation of information resources in selected academic libraries in Niger State. *Library Collections, Acquisitions, and Technical Services, 36*(3–4).

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29)*. U.S. Department of Commerce.