Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

Refocusing on Information Security Necessities for the Emerging Library Systems: A Conceptual Review

Inemesit Udom Udoh, CLN, MNLA
University Library
Akwa Ibom State University, Ikot Akapden
Akwa Ibom State, Nigeria
Email: inemuddarlingdesmart@gmail.com; inemesitudoh@aksu.edu.ng
ORCID No.: https://orcids.org/0000-0003-0230-3817
Phone no.: +234(0)8084872570

Abstract
This paper examined the necessities for information security for the emerging library systems. It adopted a conceptual research approach. Through the study, it has been established that information security is a basic strategic requirement for ensuring that emerging library systems are protected and safeguarded against unauthorize persons or systems that intentionally or unintentionally attempt to damage, steal, destroy, hack, disrupt or subvert information and information assets in any formats and media. It revealed that information security is the foundation through which emerging library systems can sustainably fulfill their mission, vision and objectives by safeguarding the confidentiality, integrity, availability, authenticity, accountability, reliability and utility of information. It indicated that information security in the emerging library systems is achieved through the integration of people, processes and technologies such as artificial intelligence technologies, blockchain technologies, etc. It requires various fundamental competencies such as IT skills, environmental scanning skills, communication skills, collaboration skills, etc. The paper showed that gross inadequate funding, which has inherent multiplier effects on the capability to employ skilled staff, train existing staff, acquire relevant technological facilities, provide state-of-the-art security gadgets, etc., are the major challenges facing information security in the emerging library systems. It however, suggested adequate funding to help in acquiring and installing necessary state-of-the-art security gadgets while supporting regular training of library staff to take adequate precaution against unauthorized access, theft, hackers, hardware and software viruses, etc., in the emerging library systems.

Keywords: Information, Security, Information Security, Emerging Library Systems

Introduction

Information security is the essence of every information management system, including the libraries. It ensures the integrity, authenticity, confidentiality, availability, accessibility, and useability of information for various purposes, especially in the new world that is characterized by a rapid pace of technological advancement and integration of technologies into the library systems. The massive integration of innovative technologies such as artificial intelligence (AI) technologies, blockchain technologies, cloud-computing technologies, biometric authentication technologies, Internet of Things (IoT) and other emerging technologies has challenged the entire library systems, requiring a different understanding and

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

implementation of new information security procedures by librarians. In fact, by integrating emerging technologies into their systems, libraries can strengthen their information security posture, improve threat detection and response capabilities, as well as enhance the overall security and management of information assets in both print and digital formats (Holland, 2020).

According to Udoh (2024), information is life, and the need for effective information security cannot be overemphasized. Information serves as the sustainer of meaningful living, as well as successful professional, official and private engagements. It accelerates development and shapes decision making. It affects the entire economic, social, political, cultural, religious and educational wellbeing of the people and nations (Amadi et al., 2020). On the contrary, any information whether in print or electronic media, which its security is tampered with by hackers, attackers, manipulators, terrorists or any rival groups or systems, could become a source of threat to life and a potential barrier to the attainment of individuals' and societal growth.

From the above standpoints, the necessities for information security in the emerging library systems cannot be underestimated. This is because information security is regarded as a fundamental issue that affects all facets of life. It is particularly essential in protecting the large amount of information, information sources and information resources in the emerging library systems for dependable and reliable information services delivery. Information security helps to safeguard the ever-changing environment within which information is provided and utilized. It is a compelling issue that deserves greater attention by all libraries, librarians and library management.

To reiterate the obvious, apart from the security of life and tangible properties which is of global concern, security of information, information assets and information system has become a big challenge to all libraries from America to Asia, from Africa to Europe, and from Australia and Antarctica. The effects of information security span across all libraries in developed and developing countries. In fact, emerging library systems are more vulnerable to series of security threats than ever before. This occurs due to emerging technologies, technical threats to hardware and software devices, human attitude and activities, as well as the physical environments which the libraries exist. This justifies the attempts by various countries and organizations to develop information security policy framework in order to protect critical information infrastructures as essential requirements to each nation's security and economic well-being (Commonwealth of Australia, 2025). It is also worthy to note that information security is necessary in the emerging library systems to protect information at the various stages of the information management lifecycles, as well as protect personal and professional information of the libraries, librarians and library users.

Therefore, based on the above background, this paper conceptually examined the necessities for information security in the emerging library systems with the following specific objectives:

- Overview and meaning of information security;
- Delineation of emerging library systems;

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

- Elements of information security in the emerging library systems;
- Types or forms of information security in the emerging library systems;
- Information security tools in the emerging library systems;
- Necessities for information security in the emerging library systems;
- Competencies for information security in the emerging library systems;
- Information security policy structures and statements for the emerging library systems;
- Challenges associated with information security issues in the emerging library systems, and
- Strategies for dealing with information security issues in the emerging library systems.

Overview and Meaning of Information Security

Information security has to do with a wide range of activities aimed at protecting information, information assets and information systems from unauthorized persons or institutions. According to Udoh (2024), information security concerns with a broad spectrum of actions, activities, processes, behaviours and attitude of ensuring or guaranteeing the safety of information and information tools against any form of threats, attacks or damage. It is defined as the process of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction with the purpose of providing the integrity, confidentiality and availability of information (E-Government Act of 2002, as cited in Shivarama & Dawar (2016). Similarly, Ngwum et al (2020) conceived information security as the protection of information, information facilities and the systems that store, use and transmit information from a wide range of threats in order to preserve the value of information for an organization. It involves deliberate management activities of defining the security controls to protect information assets.

Information security is also conceived as an act of preventing crime or unauthorized removal or loss of information materials or attack from information systems and associated tools from intruders, cybercriminals or thieves. It embeds the overall strategies, policies, programmes, and procedures deployed to mitigate risk and ensure access to a particular information and information resources in the libraries (Oluwabunmi & Ezinwanyi, 2022). Information security issues become prominent due to threats and attacks to information and the privacy of individuals, groups of individuals and organizations providing information and/or utilizing information. It is necessitated by the need to prevent adverse consequences from the intentional and unwarranted actions of information users, hackers, terrorists and other unscrupulous elements (Marett & Barnett, 2021).

Information security issues focus on detecting, identifying and preventing unauthorized acts of information and computer users as well as ensure information and data confidentiality (Smith, as cited in Zia et al., 2020). Information security covers information security policy, risk analysis, risk management, and disaster recovery in the library systems. This involves full integration of people, processes and technologies like artificial intelligence (AI) in the prevention of security threats and breaches of information and information systems. For instance, AI facilitates information security by enhancing the efficiency of threat detection

and response, as well as providing a proactive approach to safeguarding sensitive data (Akor et al., 2024; Mensa et al., 2023; Ayobami, 2024). Information security also enhances the provision of safety and secured information facilities for the library systems, including library staff, library resources, equipment and library patrons against theft, mutilation and threats.

In summary, information security primarily aims at ensuring that the library systems are protected against any unauthorize person or system that may intentionally or unintentionally damage, mutilate, deface, destroy or disrupt information assets in all formats and media. It helps in safeguarding the confidentiality, integrity, availability, accountability, authenticity and reliability of information. It is accomplished through formulation and implementation of necessary policies that deal with information privacy, physical security equipment and computer procedures. It also involves training of staff to acquire information security management skills and competencies to be able to safeguard information resources and assigning staff to take responsibility for information security tasks. Information security in the new world library systems involve taking precaution against theft, attackers, hackers, malware infection, virus and stealing of information resources, equipment and other associated facilities while ensuring effective access to information by monitoring different types of access to information and information systems.

Emerging Library Systems: A Delineation

The concept of emerging library systems is akin to a library system that is transformed by the adoption of innovative and digital technologies for enhanced library operations and services. It can be construed as analogous to a smart library system, which is characterized by automation, digital resources, user-center services, open access to research materials and collaboration for enhanced flexibility, adaptability, and extendibility of library resources and services. Emerging library systems are library systems where the Internet and other information and communication technologies (ICTs) such as artificial intelligence and machine learning technologies, radio frequency identification (RFID) facilities, Internet-of things (IoTs), integrated library management system (ILMS), federated search and discovery tools, Web-OPAC, digital software like Dspace, E-print, Koha, etc., content management software (Mensa et al., 2023; Nahak & Padhi, 2019; Orji & Anyira, 2021), are integrated to manage and deliver effective digital information resources and services to a more diversified groups of users. They provide interactive, innovative, creative, transformative and cross-border services to users.

Emerging library systems are converting from conventional to hybrid systems, providing access to a variety of digital information resources. This implies that users can plug into the library's computers, connect to the library's Wi-Fi network, upload and download content of e-books, e-journals, e-newspapers, e-databases, digital audio and visual books for their information, educational, research and recreational needs. They provide access to e-theses, e-dissertations, e-reports, e-government publications, e-conference proceedings, as well as facilitate users' possibility of sharing information from social media handles such as LinkedIn, Facebook, Instagram, X (formerly Twitter), YouTube, ResearchGate, Academia, etc. Emerging libraries are platforms for innovation and creativity in information services delivery (Akpan-Atata et al., 2014).

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

Emerging library systems are practically libraries that are changing their mode of information gathering, cataloguing and classification, information retrieval, and dissemination. For instance, increased connectivity has brought about rapid pace of circulation services through automated check-out and check-in system, open access software, and electronic security system (Agboke & Oladokun, 2024). This helps in lending services, return, renewal, reservation and automatic reminders, while enhancing user experiences and operational efficiency (Akawu et al., 2024). Also, Open Access software as a characteristic of the emerging library systems helps in making information available to scholars, researchers or faculty members free of charge or at a minimal cost. This is just as the use of electronic security systems such as electrical gadgets, terminals, and circuits help in protecting and securing library collections from theft, mutilation, damage, and sudden disappearance (Song et al., 2018).

In a nutshell, emerging library systems are libraries that leverage on emerging technologies to provide remote control of library resources, services and facilities, including automatic doors, lighting, self-service kiosks and public computers. They have a structure and framework that allow extension of library opening hours, so that patrons can access, retrieve and utilize the resources and services of the library at all times (Leicestershire County Council, 2021). This however, requires great attention to information security in order to ensure that the resources and services that are more prone to security threats are protected against intruders and attackers.

Elements of Information Security for the Emerging Library Systems

Information security is an embodiment of various integrated, interrelated and interwoven components or elements. These components, according to Lima et al. (2017); as well as Shivarama and Dawar (2016), are confidentiality, integrity, and availability. Similarly, Parker, as cited in Goldstein et al. (2007) identify six elements of information security, which include confidentiality, possession/control, integrity, authenticity, availability and utility. The authors further opined that these elements contribute to the preservation and protection of information against threats, breaches, and disruption, as well as facilitate appropriate information access and dissemination. This implies that library systems should accord necessary consideration to information security in order not to compromise the integrity of the information and the goals of information utilization.

In this work, the elements considered essential in information security in the new world library systems are:

- Data privacy/security
- Personal information
- Information/technology protection
- Online information
- Antivirus software systems
- Confidentiality
- Possession/control
- Integrity
- Authenticity

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

- Availability
- Accessibility
- Utility/Satisfaction
- Auditability/accountability

These components are regarded in this work as embedded components of information security/safety net for the library systems. They are briefly discussed for better understanding as follows:

- **Data Privacy/Security:** Effective information security begins with effective data security which lies in ensuring the privacy of data. Data are the raw facts, opinions or materials through which information is generated and disseminated before it could be considered for security. According to the United Nations Development Group (UNDG, 2017), privacy is defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other individuals. Data privacy represents an individual's right to be let alone (Warren & Brandeis, as cited in Guarda, 2008). Privacy is being free from outside interference, not having uninvited intrusion (Yusuf & Awoyemi, 2022). It has to do with individuals' or institutions' right to keep their personal and private data secret from intruders, hackers, interrupters, attackers, rivals or saboteurs. In the context of library systems, data privacy refers to how they use personal or private data of users, library staff, faculty members, and management from unauthorized persons (Udoh, 2024). It implies processing personal/private data in an ethical and legal manner (PricewaterhouseCoopers - PwC, 2020). It forbids or restricts library systems from bombarding patrons with unwanted SMS or other unnecessary messages or sharing personal data of patrons with third parties without their consent. Data privacy is necessary due to the fact that data theft and unauthorized access to personal/private data of users has the potential of causing severe economic, moral, reputational and personality damages which could result in loss, frustration, depression and even suicide of the affected library patrons.
- **Personal Information/Data:** Personal information/data is another important component of information security in libraries. It is defined as information that relates to an identifiable person, either directly or indirectly (PwC, 2020). Personal information/data could be a person's name, gender, age, date of birth, origin, family history, economic and educational status, health status, beliefs, sexual orientation, political affiliation, ID number, email address, mobile phone number, or digital identifier such as IP address, username or location data such as GPS coordinates. In the libraries, personal information/data of users could be registration number, academic department, course of study, level, or other vital information of the students or the staff ID number, salary grade level, position, etc., in the case of academic and non-academic staff. This information, if disclosed to an unauthorized person could become a serious source of security threat to the affected person. Thus, libraries are duty bound to safeguard the personal information/data of library patrons in order to prevent disruption, data theft and security breaches.

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

- **Information/technology protection:** The essence of information security is to protect information, information resources, associated technologies and information systems. According to Mandarino, as cited in Lima et al. (2017), information and associated technologies are the main focus of information security attention. Thus, protecting information and associated technologies is fundamental in effective information security in libraries. This is because without the protection of information and technologies against threats and intrusion, the essence of information security will be defeated.
- **Online information:** Online information refers to all information sources such as e-books, e-journals, e-newspapers, e-magazines, e-dictionaries, e-encyclopedias, real-time databases, etc., accessible online or offline via internet-mediated computer systems or associated computer tools like CD-ROMs, bibliographic databases, among others. These categories of information are highly threatened by computer viruses and technological obsolescence. They have various regulations and need for preservation and security due to their formats, contents and cost than even the printed information. Online information also comes at the expense of higher risks with websites frequently disappearing and digital media becoming easily obsolete. There is equally the issue of abuse of privacy of the information. In sum, online information as a component of information security in libraries involve issues relating to intellectual property rights, licensing and legal issues, information commodification, among other factors.
- **Antivirus software systems:** Computer viruses constitute serious threats to information and information systems thereby necessitating information security in the new world library systems. According to Kanona and Baddar (2017), computer virus is piece of computer code or programme that attaches itself to a programme or file and spread from computer to computer, manifesting mildly bothersome effects to the downright destructive effects. Computer viruses are also programmes that infect other computer programmes by modifying them in such a way that cause damage to hardware, software, files, or information. They could gain access to computers or information systems through internet connection or other transmission media such as CD-ROMs or any other removable disks. Meanwhile, the presence of computer viruses that threatens information and information systems in the libraries necessitate the use of antivirus software systems. Thus, antivirus software consists of computer programmes that attempt to identify, thwart and eliminate computer viruses and other malicious software or malware (Kanona & Baddar, 2017). Choudhary et al. (2013) define antivirus software as a set of programmes that is used to analyse information and if infected files are found, it disinfects them. Antivirus software scans files or computer's memory for certain patterns and may indicate an infection in the systems. Antivirus software systems are basic component or requirements for information security in the new world library systems. They help to improve information and information systems' security by decreasing the possibility of infection and virus attack using a firewall to keep information systems up-to-date for the safety of information, information resources and associated technologies in the library systems.
- **Confidentiality:** Confidentiality of information is a vital element of information security in the library systems. It seeks to ensure that information is accessible only to

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

duly authorized persons such as registered library users or management (Udoh, 2024). In other word, it protects information against unauthorized access (Lima et al., 2017). The American Library Association (2019), Article III of the *Code of Ethics of the American Library Association* asserts that confidentiality extends to information sought or received and resources consulted, borrowed, acquired or transmitted, including, but not limited to, reference questions and interviews, circulation records, digital transactions and queries, as well as records regarding the use of library resources, services, programmes, or facilities. Protection of users' privacy and confidentiality of information are fundamental parts of the mission and the ethical practices of emerging libraries. Confidentiality of information aims at protecting information from the view, being seen or copied by unauthorized persons.

- **Possession/control:** Possession as component of information security in libraries has to do with securing the ownership of information, information resources and information tools. In the context of brick and wall libraries, it could involves putting ownership stamp and accession numbers on information resources and other unique signages on information tools for easy identification and tracking. For digital/online information, it could indicate using password, encryption, keywords, biometrics, firewalls, etc., to secure access and use while preventing unauthorized intrusion. On the other hand, control entails describing rules to regulate how library users, staff and others are allowed access, retrieval, downloading, sharing and use of information, information resources and information systems. Control checkmates and curtails theft, mutilation, loss, misplacement, mis-shelving, unauthorize borrowing and other unwanted users' behaviours in the libraries. In this wise, possession and control are essential elements of information security in libraries.
- **Integrity:** According to Shivarama and Dawar (2016), integrity means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. Lima et al. (2017) affirm that integrity as a component of information security refers to the inability to change information on the network. It aims at safeguarding the data and information, thus ensuring the veracity, accuracy and authenticity of the information, as well as its processing methods. The loss of integrity of information occurs when lacking due security and the modification of an important topic occurs, which can be altered by the most surprising motives, even intentionally. From this light, ensuring that the integrity of information in content, motive, originality and context remain intact is the goal of information security in libraries. It implies that protecting the integrity of information mean safeguarding and protecting the integrity of the information source(s), information users and the libraries, at large.
- **Authenticity:** This means the verifiability of information to ensure that the information, information sources, information processing methods, channels of information dissemination, information users, etc., are actually what they claim to be. Authenticity of information implies that the q*uality of information is what it purports to be and that it is free from tampering, mutilation, or corruption (*Lima et al., 2017*).* As a component of information security in libraries, authenticity is the process of ensuring that information received is the same information that was sent and has not

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

been tampered with or altered. It helps in checking and curtailing misleading, false, or misrepresented information when dealing with both print and digital information. Haider and Koronios, as cited in Udoh (2024) opined that authenticity of information as a component of information security deals with a variety of criteria such as authorship, purpose, authority, origin, scope, and paper quality of documents. Richmond, cited in Udoh (2024) suggested that the authenticity of digital/online information aims at securing information by focusing on content, credibility, critical thinking, copyright, citation, continuity, censorship, connectivity, comparability, and context of the information. It is therefore, necessary to note that the authenticity of print and digital information can be established by judging the information for its accuracy, authority, currency, coverage and objectivity.

- **Availability:** As a common component of information security in libraries, availability seeks to ensure that data, information, information resources and information systems are always and fully available whenever requested. In other word, this component focuses on the assurance that authorized persons such as registered library users (students, members of staff, especially faculty members) can access the information in the libraries when they need to, at the right times, in the right place and in the right ways. The absence of availability occurs when the information is deleted, becomes inaccessible to authorized users to consult, or in a bad physical condition that it cannot be used by users. Availability of information is vital to libraries and librarians because if information sought for is not available, it will impinge on the realization of the mission, vision and objectives of the libraries.
- **Accessibility:** Accessibility as a component of information security in the new world library systems is based on the premise that if information is not accessible to users, the essence of acquiring and processing that information is defeated. Thus, information in the library systems is secured, protected, and safeguarded in order to enhance access to authorized users for their educational, teaching, research, cultural and recreational purposes. In other words, accessible information is that information which is able to be read or received and understood by the individual or group for which it is intended. This implies that information in the library systems should be protected from hackers, intruders, terrorists, and other saboteurs in order to be accessed (read, received, and understood) by users. However, accessibility of information can be achieved through various access tools such as manual library catalogue or machine-readable catalogue (MARC) like online public access catalogues (OPACs), indexes, abstract, bibliographies, Internet search engines, databases etc., (Igere, 2022; Nnadozie et al., 2024; Sood, 2023; Udoh et al., 2020). Accessibility of information can also be achieved through access control techniques such as discretionary access or mandatory access. Discretionary access is an access policy determined by the libraries as the owner of the information and information resources. Under this method, the libraries decide who is allowed access to the information, information resources and information system. On the other hand, mandatory access is a multilevel information system with highly sensitive information such as classified government and military information. Mandatory information

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

access policy is an access policy that access to information is determined by the system through an interaction between subjects and objects.

- **Utility/Satisfaction:** Utility of information is simply the usefulness of information to a user. Utility is used to determine the worth, value or useability of something such as information. It is the total satisfaction, enjoyment or benefit derived from consuming or utilizing a particular piece of information or information resources. In other word, information yields utility to the extent to which it is useful and useable for satisfying a user's information need. As a component of information security in the library systems, utility represents and emphasizes the need to secure, protect, and safeguard information in order to ensure the worth, value, usefulness, and utilization of information, information resources or information system for the satisfaction of the users. Therefore, though the utility and satisfaction of information varies from person to person depending on their information needs, it is very essential that libraries strive to preserve, protect, safeguard, and prevent any form of threat, attack or intrusion to information in order to maintain or sustain the usefulness and benefit of information to users.
- **Auditability/accountability:** Information auditability/accountability or simply "information audit" is a very important information security element in the new world library system. According to Sharma and Singh (2012), information auditability is a process as well as an analysis of information for the accuracy, suitability and validity. It represents a systematic, deliberate and conscious process through which the library systems understand the constituents of their information assets, information environment, information flow, information use and information gaps in order to connects with its missions, goals and objectives. Frost and Choo (2017) posited that information accountability embraces all the methods and tools needed to catalogue, model, evaluate, quality-control, and analyse a library's information assets and information management system. Information auditability/accountability is a risk mitigation exercise and quality improvement process (Lateef & Omotayo, 2019). It helps in the identification, storage, protection and evaluation of information and information resources in the library systems as well as how the information is processed, assessed and where there are areas of risks, put procedures in place for improving the information security system. It facilitates the process of creating awareness on the importance of information security in order to monitor conformity with information related standards, legislations, policies and guidelines.

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

The embedded components of information security for the emerging library systems are presented for easy understanding of their relationship in figure 1 below:

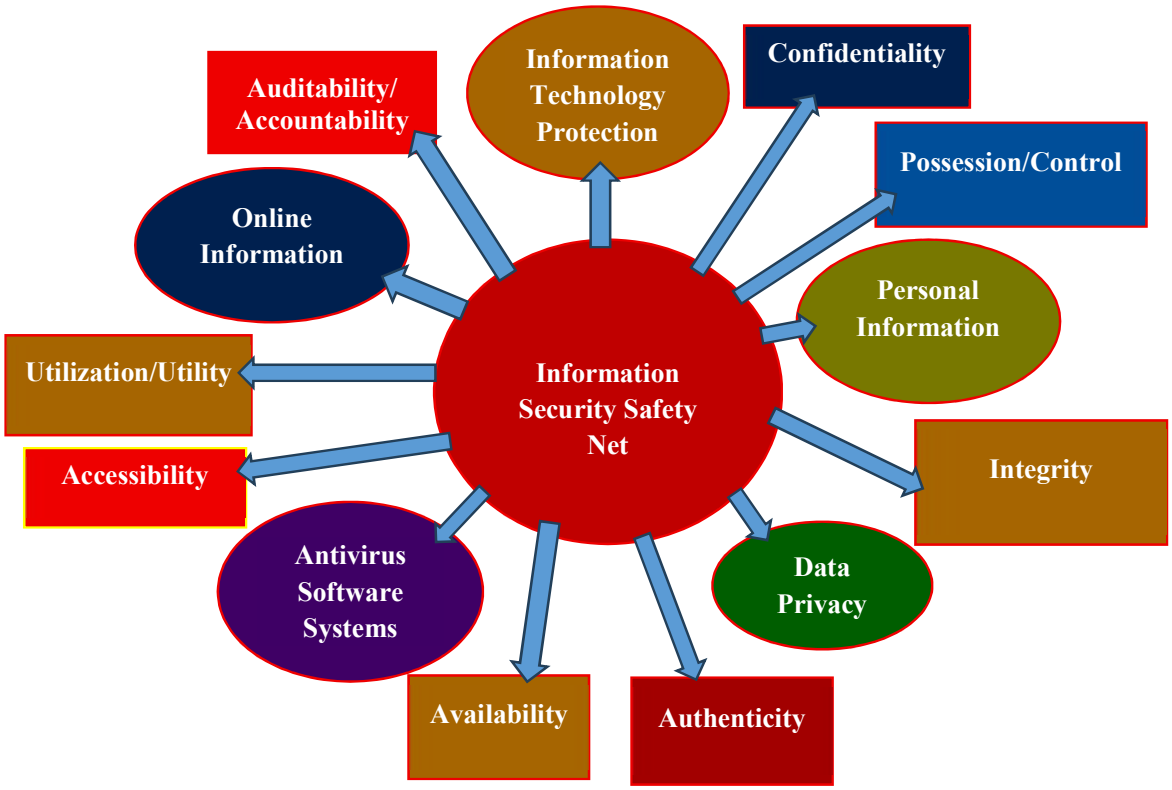


Figure 1: ***Embedded Components of Information Security Safety Net as Modified by Inemesit U. Udoh (2025)***

Types of Information Security in the Emerging Library Systems

As already discussed, information security is essential in the emerging library systems, covering a variety of activities that are grouped based on the nature of threats and their implications on the broad information spectrum. However, Teradata (2025) categorized information security that can be implemented in the emerging library systems into three main types, namely; cybersecurity, application security, and operational security.

1. **Cybersecurity:** Cybersecurity refers to the protection of computer systems and networks from theft, damage, or unauthorized access to hardware, software, and data (Teradata, 2025). It is defined as the protection of the cyberspace or digital library systems against any form of intrusion or unauthorized access. According to Fadehan and Okiki (2023), cybersecurity is the practice of safeguarding computers, servers, mobile devices, electronic systems, networks and data from unauthorised access, theft and damage. Cybersecurity is necessary as a type of information security in the emerging library system due to the fact that cybersecurity breaches can have far-reaching consequences, including reputational damage, financial losses, legal

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

liabilities, and intellectual property theft (Oladokun et al., 2024). It helps in protecting and sustaining quality library services by preventing disruption, loss of critical data, and exposure users' privacy. It involves network security, endpoint security, cloud security and Internet of Things (IoTs) security.

- **Network security:** This focuses on protecting the integrity and usability of network and data in the library systems. Network security ensures the sustainability of library network systems for efficiency operation by protecting library server from attacks and intrusions.
- **Endpoint security:** This concerns with securing end-user devices such as computers and mobile devices in the library systems. It helps in protecting computers against viruses, malware infection, etc.
- **Cloud security:** This is addressing the cybersecurity threats to cloud computing environments of the library systems. It ensures that the cloud-computing environment is secured against attacks, software theft, intrusion and damage.
- **Internet of things (IoT) security:** This deals with the protection of interconnected devices against hacking, internet libel, cyberbullying, online harassment, etc.

2. **Application (Apps) security:** This type of information security involves taking measures to improve the security of applications by identifying, fixing, and preventing security vulnerabilities (Teradata, 2025). It is central in protecting software applications from external threats such as malware attacks by ensuring that applications are built and maintained with security in mind from the outset. In the emerging library systems, application security refers to all measures taking into consideration to enhance the security of library application software including installation of antivirus systems and server backups for improved sustainable services delivery. It also includes secure coding practices, vulnerability scanning, code review, and application firewalls.
3. **Operational security (OpSec):** This type of information security in a library system has to do with the protection of critical data and information through processes and decisions for handling and protecting data and information assets. It involves developing and implementing policies for data encryption, access control, and user authentication, as well as physical security measures to protect hardware infrastructures and procedures for disaster recovery (Teradata, 2025). It strictly aimed at ensuring that only authorized users can access sensitive information, while enhancing continuity planning in the event of a security breach or failure in the library systems.

Necessities for Information Security in the Emerging Library Systems

The need for information security in the emerging library systems can be compared to the need for blood for human survival. Information security is primarily aimed at guaranteeing the availability and access to information. It serves as a necessity in the emerging library systems because of advancement in technological tools, constant technological obsolescence, pervasive preference for electronic information resources, and the vulnerability of libraries to security threats. Information security is also necessary due to human factors, natural disasters, computer and Internet viruses, hacking, theft, mutilation, illegal borrowing of books,

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

defacement, and other threats facing libraries in the modern times. It ensures that the integrity, authenticity, availability and utility of information are guaranteed.

However, from the above general analysis, the following are considered as the specific necessities for information security in the emerging library systems.

i. Information security helps in safeguarding and protecting investments in the computerization of emerging library systems.
ii. It ensures that the library systems are predictably and reasonably dependable amidst all sorts of malicious, intentional and unintentional intrusions, attacks, threats and risks.
iii. It serves as a tool in minimizing the risk of damage, theft, subversion, intrusion or sabotage in the emerging library systems.
iv. It protects information, information resources and information systems in the libraries from loss, misuse, unauthorized access, modifications, disclosure or destruction.
v. It safeguards users' personal information and privacy from theft, misuse and hackers.
vi. It safeguards critical research data, personal information of researchers, library staff and library patrons and other sensitive information in the libraries from criminals and terrorists.
vii. It mitigates the libraries from financial, economic, productivity, reputational and legal risks that can threaten their corporate existence.
viii. It prevents information leakages that can compromise research grants from various organizations as well as the reliability of university's information security system.
ix. It serves as effective measures to enhance trust, confident and stability in the library systems as fiduciary institutions.
x. Information security is a strategy for protecting digital information assets against cybercriminals that may come in the form of hacking, inserting viruses or worms in the systems, data loss, server damage, stopping of user services, denial of access to website and portal, as well as publishing illegal and unethical contents on the library webpages.
xi. Information security equally protects libraries against critical data exposure and vandalism which may cause the library systems breach of trust among users.

Information Security Tools in the Emerging Library Systems

The task of effective information security in the emerging library systems is considered within a clear understanding of what constitute information security tools as well as sources of threat to information security. In other words, understanding information security tools is pertinent in the sense that without streamlining the tools, information security in the emerging library systems will be discussed amiss. Thus, this section examines information security tools under three basic umbrellas such as people, finance, processes and technology.

- **People**

People are fundamental in successful information security and at the same time, the biggest sources of threats to information and information systems in the libraries. According to

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

Oluwabunmi and Ezinwanyi (2022), people are the main issue in the human aspects of information security due to their direct contact with information. People constitute the entire workforce and stakeholders in the library systems. They include library employees, members of the library management team, library patrons and experts in various areas who are engaged by the libraries from time-to-time to perform certain tasks. They have the potentials to make or mar the entire library information security systems. Studies show that human errors are the most highly ranked information security threats (Ajie, 2019). The author further reported that instances of poor information security practices due to human errors, poor passwords selection, piggybacking, shoulder surfing, dumpster diving, installing unauthorized hardware and software, access by unauthorized users and social engineering, lack of discipline, carelessness or lack of knowledge among library staff and patrons such as the use of incorrect security features, inadequate backups, switching off computers when an error is displayed, files deletion, etc., can put the library systems at high security risk. These situations cumulatively could threaten the integrity, availability, accessibility, confidentiality, reliability and utility of information. However, when the people especially library staff, patrons and other stakeholders of the libraries are doing the right thing and take information security issues seriously, they can become effective instrument in building and safeguarding information and information tools in the libraries.

- **Finance**

Finance is a very vital tool in information security in the library systems. It is needed in every area of life, and quite crucial in information security planning and implementation. Finance is the lifeblood of successful information security in the library systems. Availability of funds facilitates the acquisition of information security equipment such as hardware and software facilities. Adequate finance enhances the hiring, training and retraining as well as retaining of skilled staff including professional security personnel. It helps in acquiring state-of-the-art security gadgets such as AI and ML tools, CCTV camaras, Radio Frequency Identification (RFID) systems, 3M Exit technologies, fire-fighting equipment, Knoppix security tools, Microsoft baseline security analyzer (MBSA), Symantech endpoint protection and relevant antivirus software systems. With adequate finance, emerging library systems can boost their information security systems whereas this can be very difficult, if not impossible in a situation where there is no finance to fight security threats and attacks.

- **Processes**

Information security in the emerging library systems is built on integrated processes. According to Shivarama and Dawar (2016), the processes are based on the information security standards of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly signed and published on 25th September 2013 as ISO/IEC JTC 1/SC 27. The processes are offshoot of the ISO's International Standard for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system of 2001 and 2005. It specifies the code of practice for information security management, referred to in this work as *"information security processes."* The processes include formulation of information security policy in libraries, organization of information security, asset management, human

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

resources security, physical and environmental security, communication and operations management, access control, information system acquisition, development and maintenance, information security incident management, business continuity management, and compliance. These processes are further enclosed in the definition of the scope of information security standards in libraries; how documents in the libraries are referenced; defining the organizational context and stakeholders on information security issues; information security leadership and high-level support for policy; planning an information security management system, risk assessment, risk treatment; supporting an information security management system; making an information security management system operational; reviewing the information security system's performance and taking corrective action. These processes are the keys to achieving information security in contemporary libraries.

- **Technology**

Technological mechanisms are crucial tools in information security in the emerging library systems. Several technologies are used to safeguard and protect the libraries and information integrity, confidentially and availability. Technological tools are put in place to protect, control and monitor libraries and information access as well as prevent unauthorized access to data that are transmitted over the library information systems. According to Zia et al (2020), technological tools are the foundation that all libraries must put in place as the main defensive system. Technological tools such as artificial intelligence (AI) and machine learning (ML) tools, blockchain, biometric authentication, and Internet of Things (IoTs) technologies are identified as crucial in mitigating information security threats and enhancing the functionality of the emerging library systems. Akor et al. (2024) posited that blockchain technologies are crucial for secure data transactions, while artificial intelligence helps is vital for predictive threat analysis. Particularly, blockchain technologies can be used to create immutable records of library transactions, access permissions, and digital assets, ensuring data and information integrity and transparency. Libraries can implement blockchain-based solutions for secure data storage, archival preservation, and intellectual property management. Blockchain-based access control mechanisms can also be relied upon for enforcement of granular permissions, secure authentication of users, and tracking of data access and usage in library system. Tella et al (2022) further remarked that by leveraging blockchain, libraries can enhance data security, streamline audit processes, and build trust with stakeholders. Biometric authentication technologies can be used to verify user's identity based on unique physiological or behavioural characteristics, such as fingerprints, facial features, etc. Also, IoT technologies enable aggregation and analysis of telemetry data from diverse IoT devices to identify potential security threats or anomalies in real time, and by so doing, help in prompt incident response and remediation actions to mitigate risks and minimize impact of information security threats (Zewdie & Girma, 2020).

Technologies are very vital in information security. These tools could also become sources of threats to information security in the library systems. For instance, Ajie (2019) opined that hardware technological tools such as computers, flash drives, hard disk, printers, scanners, computer networks, etc., are prone to series of security attacks such as natural disasters, humidity, theft, vandalism, malicious intrusion, defections, electromagnetic interference, maintenance errors, etc. On the other hand, software technological tools are threatened by

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

security loopholes due to improper design and management. They are usually exposed to security threats and attacks such as stealing or copying software from the Internet with viruses, worms and Trojan horses, as well as corruption by system, system failure, maintenance errors, cyber-terrorism, software piracy, unauthorized access, unauthorized changes to software settings, adware, spyware, hacking, password sniffing, weak passwords and abuse of computer access control. Network security threats like passwords cracking, Internet based attacks of internal network resources, damage to equipment due to inadequate power supply or lightning strike, transmission errors, and website defacement affect information security in the library systems. As a matter of fact, if the security of these technological tools is threatened or jeopardized, the security of information in the library systems will equally be threatened.

Therefore, to safeguard the integrity, confidentiality, availability, accessibility, utility and auditability of information and information systems, specific technological tools and antivirus software systems should be put in place in the emerging library systems.

Competencies for Dealing with Information Security in the Emerging Library Systems

Information security in the emerging library system is a very rigorous and demanding exercise. It is in fact, not an all-comers process. It requires the application of certain competencies, skills and attributes in the use of relevant technologies and systems as well as in dealing with various stakeholders in order to achieve success. Broadly, competencies in information security entails the knowledge, skills, ability and aptitude to implement technical and managerial measures such as formulation of policies, procedures, safeguards and countermeasures in using computer hardware, software, and internet while paying attention to human and environment factors to identifying and mitigating information security threats and disruption to information systems. Deducing from Obim and Akpokurerie (2023), competencies for information security may be conceived as the totality of skills and technological know-how required by an individual to effectively, proactively and adequately protect, prevent and secure information and information infrastructures and also the skills to professionally handle the incidents of information security attacks within the institutions to prevent further attacks or damage. It may also be considered as a combination of technical, managerial and soft skills (Commonwealth of Australia, 2025).

Thus, in this paper, the competencies for information security are summarized into the following:

i. **IT skills:** These are the ability to use computer hardware, software, internet, server, workstations and other associated technologies to ensure the protection, safeguard and preservation of information against hackers, intrusion, subversion, and unauthorized access. These skillsets include knowledge of network security and security technologies, including operating systems and databases; ability to know emerging threats and attack vectors, including vulnerabilities; ability to identify and respond to information security incidents; ability to guide or lead information security teams and make strategic decisions; as well as ability to plan and implement information security projects, including risk assessments and security audits (Commonwealth of Australia, 2025). IT skills help library systems

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

to prevent system failure, cyber-terrorism, software piracy, unauthorized changes to software settings, adware, spyware, and password sniffing in the libraries.

ii. **Environmental scanning skills:** These are the ability to examine the physical environments of the libraries to prevent physical attacks such as fire outbreak, floods, thunder strikes, theft, vandalism, power outage, equipment failure, etc. Environmental scanning skills help in preempting possible threats in order to take preventive measures.

iii. **Communication skills:** These are the ability to effectively communicate the need for information security measures in the libraries with all stakeholders. It helps in creating awareness and ensuring compliance with information security policies in the libraries. Communication skills facilitate the process of sharing the message, enlightening staff and users of the libraries about the importance of information security in the library systems.

iv. **Marketing and advocacy skills:** These are the ability to promote and advertise information security issues to attract stakeholders' support. It facilitates the process of canvassing, sensitizing and engaging library management and other parties to buy into the information security project in the libraries.

v. **Budgeting and financial management skills:** These are the ability to plan financial matters, source and raise funds, prudently allocate and utilize available funds, as well as account for the use of allocated funds. Budgeting and financial management skills are necessary in effective information security in a library system in the sense that other resources required for information security to revolve around funding and the use of funds.

vi. **Interpersonal relationship skills:** These are the ability to get all stakeholders in the library systems involved in the information security programme. It involves creative and friendly ways of interacting, socializing, discussing and reaching agreement with all library staff and other stakeholders so that everyone will feel a sense of being carried along in the information security projects.

vii. **Collaboration skills:** These are another set of skills required for information security in the emerging library systems. According to Amadi et al. (2024), collaboration skills provide the opportunity to partner, share or fine-tune thoughts, ideas and purposes in order to develop strategies and tactics for multidimensional thinking towards achieving common and uniform purpose. It helps in building and sustaining trust with various partners in achieving information security programmes.

Information Security Policies and Statements for the Emerging Library Systems

Information security in the emerging library systems can be effectively implemented if relevant policy guidelines and regulations are complied with to guide the processes. Nieles et al. (2017) defined information security policies as a set of formalized procedures, guidelines, roles, and responsibilities to which employees are required to adhere to in order to safeguard and use information, information resources and associated technologies properly in their organizations. Similarly, Ifinedo (2014) posited that information security policies are guidelines, requirements, and rules prescribed by organizations to checkmate employees' behaviours and attitude in order to enhance information security compliance. This implies that

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

when library employees are familiar with information security policies, adherence to information security issues become a norm while breaches, threats, intrusions, and attacks to information and information resources become easily detected, curtailed and/or surmountable.

However, as a global phenomenon, information security is regulated by various frameworks and policy statements. These include:

- International Standards for Information Security in Libraries (ISO 27001 and ISO 17799);
- IFLA Internet Manifest Guidelines' Acceptable Use Policy (AUP); Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems and Networks;
- Generally Accepted Information Security Practices (GAISP) of the Information Systems Security Association (ISSA);
- Payment Card Industry Data Security Standards; British Standard Institute-Information Technology Security Techniques;
- Nigeria's National Cybersecurity Policy;
- Freedom of Information Act (FOIA); and many other policy frameworks.

These policy documents are aimed at ensuring the integrity, confidentiality, availability, accessibility and utility of information in the libraries and other information-driven institutions. For instance, as mostly related to the library systems, the International Standards for Information Security in Libraries (ISO 27001 and ISO 17799) provides the framework for the control of information security policy, organization of information security, asset management, human resources security, physical and environmental security, communication and operations management, access control, information system acquisition, development and maintenance, information security incident management, business continuity management and compliance.

The IFLA Internet Manifest Guidelines' Acceptable Use Policy (AUP) focuses on ensuring that library Internet users are aware of what is and what is not acceptable use of library computers. It spells out the sanctions for breaching the policy. AUP holds that libraries should define the limit of available services as well as inform users of their responsibilities, including legal requirements and those defined by the libraries like the penalty for illegal use of equipment such as library computers to watch pornographic movies, carryout betting and gambling or access other computers without permission.

Equally, the Freedom of Information Act (FOIA) states the right to privacy, including the right to open inquiry without outsider's scrutiny as well as information sharing and the limit to such rights. These policy statements help the emerging library systems to effectively protect, safeguard and prevent the entire information value-chains from unscrupulous elements and unwanted actions.

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

Challenges Facing Librarians in Dealing Information Security Issues in the Emerging Library Systems

Information security in libraries is a huge task that requires lot of physical, human, monetary, material and technological resources. It also requires relevant skills in handling requisite facilities as well as in dealing with the human factors which have great effects on the success or failure of the entire information security activities.

However, the key challenge facing information security issues in the emerging library systems is gross inadequate funding of libraries. This singular challenge has over time proved to have inherent multiplier effects on the capability of the libraries to employ skilled staff, train available staff on information security issues, acquire relevant information technology facilities, provide constant power supply, and provide state-of-the-art security gadgets in libraries. This assessment clearly accentuates the position of Ifijeh and Yusuf (2020), as well as Udoh (2024), who pointedly identified unstable power supply, inadequate funds, inadequate ICT skills of librarians, poor technology infrastructure, and lack of management support for libraries as the challenges militating against information security in libraries.

In addition to the above, there is the problem of lack of clearly formulated information security policies in most libraries, and where there are policies, there is no meticulous implementation of the information security policies. Specifically, most library systems do not have functional closed-circuit-television (CCTV), and radio frequency identification (RFID) systems. There is apparent lack of dedicated information security librarians with adequate IT skills who should be responsible for ensuring the security of hardware and software systems against computer viruses, worms, malicious codes, hacking, and other sources of information security threats. This is also attributable to lack of training of library staff on specialized areas such as information security in the library systems.

As part of the inadequacies confronting information security in the library systems, there is an obvious inadequate security arrangement towards the protection and safeguard of library staff against physical attacks in the libraries. This manifests in the reoccurrence of verbal and physical abuse, and harassment of the library staff in most library settings.

Strategies for Dealing with Information Security Issues in the Emerging Library Systems

Securing information and information resources in the emerging library systems against attacks, threats, viruses, and intrusion require series of integrated, interrelated, deliberate and conscious actions and efforts. Fundamentally, it requires the provision of adequate funds to libraries order to accelerate the acquisition and installation of necessary state-of-the-art-security gadgets. It also requires administrative control measures such as formulation of information security policies, guidelines and standards. It is crucial to point out that staff training is a very fundamental responsibility of every library system. Well-trained, skilled, competent, and knowledgeable library staff are great assets for enhanced physical control measures such as the security of the physical environment, computing facilities, fire alarms, locks, security guards and devices. They play critical role in specifying staff duties for the use

of technical control measures like the use of software to monitor information in the library systems.

It is also suggested that the emerging library systems should adopt access control measures such as the use of password and authentication of data as well as use of malware scanners, firewalls, and anti-virus software to secure information in the library systems. This is because "strong to decipher password" and authentication of information can secure information against attacks or unauthorized access. Emerging library systems should pay serious attention to the formulation and enforcement of compliance to information security policies.

Particularly, emerging library systems should tighten physical security at their entrances, exit points and other strategic points. Suitable security measures such as the installation of artificial intelligence (AI) and machine learning (ML) technologies, blockchain technologies, biometric authentication technologies, and Internet of Things (IoTs) technologies, RFID, CCTV, 3M Exit technologies, etc., should be given considerable attention to enhance information security in the emerging library systems.

Conclusion

This work conceptually investigated the necessities for information security in the emerging library systems. Through this study, it has been established that information security is the basic strategic requirement of ensuring that the library systems are protected and safeguarded against any unauthorize person or system that intentionally or unintentionally attempt to damage, steal, destroy, disrupt or subvert information and information assets in any formats and media. It is equally seen as the foundation through which the emerging library systems can consistently and sustainably fulfill their mission, vision and objectives. Information security facilitates the possibility of safeguarding the confidentiality, integrity, availability, authenticity, accountability, reliability and utility of information. However, the study revealed that information security in the emerging library systems can be accomplished through integrated, conscious and concerted efforts that involved people, processes and technologies. It showed that the integration of people, money, processes and technologies require certain fundamental skills such as information technology (IT) skills, environmental scanning skills, communication skills, marketing skills, budgeting and financial management skills, interpersonal relationship skills and collaboration skills toward the formulation and implementation of necessary policies that deal with information privacy, physical security equipment and computer procedures, as well as staff training. In conclusion, the study indicated that information security helps in taking precaution against theft, hackers, hardware and software viruses, system failure, as well as unauthorized access and use, which are the main sources of information security threats in the emerging library systems.

References

Agboke, A. L. & Oladokun, B. D. (2024). Emerging technologies in academic libraries: prospects and challenges in Nigeria. *Communicate: Journal of Library and Information Science, 26*(2). https://www.cjolis.org

Ajie, I. (2019). A review of trends and issues of cybersecurity in academic libraries. *Library Philosophy and Practice (ejournal)*. 2523. https://digitalcommons.unl.edu/libphilprac/2523

Akawu, L., Abubakar, L., Adamu, M., & Mohammed, S. M. (2024). Evaluation of library management system in Nigerian federal university libraries. *Lapai Journal of Science and Technology, 10*(1), 72-92.

Akor, O. S., Nongo, C. J., Udofot, C. O. & Oladokun, B. D. (2024). Cybersecurity awareness: Leveraging emerging technologies in the security and management of libraries in higher education institutions. *Southern African Journal of Security,* 16671, 1-14. http://doi:10.25159/3005-4222/16671.

Amadi, E. C., Udoh, I. U. & Ukpong, C. A. (2024). Factoring in collaboration for quality services delivery in contemporary libraries. In F. E. Etim, I. I. Ekoja & F. A. Onifade (Eds.), *Contemporary practices for sustainable library and information services: A Festschrift in Honour of Professor Ahiaoma Ibegwam.* CELIMAT Publishers.

Amadi, E. C., Udoh, I. U. & Ekpenyong, G. E. (2020). Access to information in the attainment of sustainable development goals (SDGs) in federal university libraries in Nigeria. *Library Philosophy and Practice (e-journal).* 4005. https://digitalcommons.unl.edu/libphilprac/4005

American Library Association (2019). *Privacy: An interpretation of the library bill of rights*. https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Akpan-Atata, E. A., Oji, H. E. & Tom, E. S. (2014). Libraries as platforms for innovation and creativity in information delivery services in a depressed economy: An overview of Nigeria. *Asia Pacific Journal of Multidisciplinary Research, 2*(5), 125-131.

Ayobami, A. (2024). Leveraging AI for information and cybersecurity. https://www.isaca.org/resources/news-and-trends/industry-news/2024/leveraging-ai-for-information-and-cybersecurity

Choudhary, S., Saroha, R. & Beniwal, S. (2013). How Anti-virus Software Works? International Journal of Advanced Research in Computer Science and Software Engineering, 3, 4. https://www.ijarcsse.com

Commonwealth of Australia (2025). Information security manual: Guidelines for cybersecurity roles. https://www.cyber.gov.au/sites/default/files/2025-03/03.%20ISM%20-%20Guidelines%20for%20cybersecurity%20roles%20%28March%202025%29.pdf

E-Government Act (2002). *Public Law 107-347: Federal Information Security Management Act of 2002*. http://www.gpo.gov/fdsys/pkg/statute-116/pdf/statute-116-pg2899.pdf

Fadehan, O. & Okiki, O. (2023). Awareness, attitude and ethical concerns among faculty members in Nigerian universities on open educational resources (OERs). *Open Learning: The Journal of Open, Distance and e-Learning, 38*(4), 351–365. https://doi.org/10.1080/02680513.2023.2169122

Frost, R. B. & Choo, C. W. (2017). Revisiting the information audit: A systematic literature review and synthesis. *International Journal of Information Management, 37*(1): 1380–1390. http://dx.doi.org/10.1016/j.ijinfomgt.2016.10.001

Goldstein, N. C., Newmark, R., Burton, L., May, D., McMahon, J., Whitehead, C. D. & Ghatikar, G. (2007). Assessing security needs of the multifaceted relationships of energy and water providers. *Technical Report.* https://www.researchgate.net/publication/255201736

Guarda, P. (2008). Data protection, information privacy, and security measures: An essay on the European and the Italian legal frameworks.

Holland, B. (2020). Emerging technology and today's libraries. *Emerging Trends and Impacts of the Internet of Things in Libraries,* 1–33. https://doi.org/10.4018/978-1-7998-4742-7.ch001

Ifijeh, G., & Yusuf, F. (2020). Covid-19 pandemic and the future of Nigeria's university system: The quest for libraries' relevance. *Journal of Academic Librarianship, 46*, 1-8. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7426696/

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, *51*(1), 69-79.

Igere, M. (2022). Relevance of library catalogue on usage of library resources among undergraduates of library and information science students in University of Benin, Nigeria. *Ilorin Varsity International Journal of Library and Information Science. 5(1). https://www.researchgate.net/publication/364356524*

Kanona, R. M. & Baddar, A. (2017). Viruses and antivirus. https://doi.10.13140/RG.2.2.15807.15522

Lateef, A. & Omotayo, F. O. (2019). Information audit as an important tool in organizational management: A review of literature. *Business Information Review, 36*(1), 15–22. https://doi:10.1177/0266382119831458

Leicestershire County Council (2021). Smart library. https://www.leicestershire.gov.uk/sites/default/files/field/pdf/2018/7/5/What-is-a-Smart-Library.pdf

Lima, J. S., de Araújo, A. R. S., Santos, F. E. P., Barbosa, L. G. M. & dos Santos, I. L (2017). Information security in academic libraries: The role of the librarians in planning and introducing new institutional policies. Digital Journal of Library and Information Science, 15(2), 389-419. https://dio.10.20396/rdbci.v0i0.8646416

Marett, K., & Barnett, T. (2021). Information security practices in small-to-medium sized businesses: A hotspot analysis. In *Research Anthology on Small Business Strategies for Success and Survival,* 576-596). IGI Global.

Mensa, C. P., Udoh, I. U. & Osiebe, P. O. (2023). Systematic analysis of adoption of innovative technologies in the provision of electronic information services in public university libraries in Akwa Ibom State, Nigeria. *Library Philosophy and Practice (e-journal).* 8080. https://digitalcommons.unl.edu/libphilprac/8080

Nahak, B. & Padhi, S. (2019). The role of smart library and smart librarian for e-library services. https://ir.inflibnet.ac.in/bitstream/1944/2338/1/10.pd

Ngwum, N. I., Raina, S., Aguon, S., Taylor, B. & Kaza, S. (2020). A model for security evaluation of digital libraries: A case study on a cybersecurity curriculum library. Journal of the Colloquium for Information Systems Security Education, 7(1). https://www.researchgate.net/publication/344357576

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security. *NIST special publication*, 800(12), 101.

Nnadozie, C. D., Udoh, U. I. & Osiebe, O, P. (2024). Descriptive analysis of the efficacy and applicability of library catalogue for information retrieval among undergraduate Students of Library and Information Science in University of Uyo, Akwa Ibom, State, Nigeria. *OMANARP International Journal of Art & Social Sciences, 1*, 52-63.

Obim, I. E. & Akpokurerie, A. O. (2023). Awareness of cybersecurity and its impact on information storage in the university libraries in south east Nigeria. *Information Technology and Librarianship*, 3(2).

Oladokun, B. D., Oloniruha, E. A., Mazah, D. & Okechukwu, O. C. (2024). Cybersecurity risks: A sine-qua-non for university libraries in Africa. *Southern African Journal of Security*, 15320, 1-14. https://doi.org/10.25159/3005-4222/15320

Oluwabunmi, M. T. & Ezinwanyi, M. (2022). Information security awareness and information security compliance in university libraries in South-West, Nigeria. *Library Philosophy and Practice (e-journal).* 7215. https://digitalcommons.unl.edu/libphilprac/7215

Orji, S. & Anyira, I. E. (2021). What is "smart" about smart libraries? *International Journal of Research in Library Science (IJRLS), 7*(4), 265-271. http://doi:10.26761/IJRLS.7.4.2021.1482

PricewaterhouseCoopers (PwC, 2020). Data privacy handbook: A starter guide to data privacy compliance. https://www.pwc.com/m1/en/services/assurance/risk-assurance/documents/data-privacy-handbook.pdf

Sharma, C. K. & Singh, A. K. (2012). An evaluative study of information audit and knowledge management audit. *Brazilian Journal of Information Science: Research Trends, 5*(1). 53-59. http://www2.marilia.Unesp.br/revistas/index.php/bjis/index

Shivarama, J. & Dawar, V. A. (2016). Digital information security for academic libraries: An overview. https://www.researchgate.net/publication/335389774

Song, U.S., Yusuf, Z.M. & Mairiga, H. M. (2018). Library electronic security systems and the challenges of theft and mutilation of library resources in academic libraries in Nigeria: A survey of academic libraries in Jigawa State. *International Journal of Applied Technologies in Library and Information Management, 4(*1), 10- 96-110.

Sood, S. P. (2023). Library catalogue: Definition, functions, importance and adjuncts. https://www.academia.edu/37018955/

Tella, A., Amuda, H. O. & Ajani, Y. A. (2022). Relevance of blockchain technology and the management of libraries and archives in the 4IR. *Digital Library Perspectives, 38*(4), 460–475. https://doi.org/10.1108/DLP-08-2021-0065

Teradata (2025). What is AI information security? https://www.teradata.com/insights/ai-and-machine-learning/what-is-ai-information-security#:~:text=AI%20information%20security%20refers%20to%20the%20use,detection%20and%20automate%20responses%20to%20security%20incidents.

Udoh, I. U. (2024). Information security: Imperatives and challenges for contemporary libraries. In F. E. Etim, I. I. Ekoja & F. A. Onifade (Eds.), *Contemporary practices for sustainable library and information services: A Festschrift in Honour of Professor Ahiaoma Ibegwam.* CELIMAT Publishers.

Jewel Journal of Librarianship
ISSN: 2141-3908 (Print); ISSN: 2736-0881 (Online)
https://www.jeweljournals.com/
Volume 20, Issue 2, 2025

Udoh, I. U., Okafor, V. N. & Ekpenyong, G. E. (2020). Strategic information access tools for dissemination of information in academic libraries in a digital era in Nigeria. *Library Philosophy and Practice (e-journal).* 4548. https://digitalcommons.unl.edu/libphiprac/4548

United Nations Development Group (UNDG, 2017). Data privacy, ethics and protection: Guidance note on big data for achievement of the 2030 agenda. https://www.unglobalpulse.org; https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

Yusuf, R. A. & Awoyemi, O. O. (2022). Cyber security and its implication on library users' privacy. Owena Journal of Library and Information Science (OJOLIS), 9(1). https://www.nigerianjournalsonline.com/index.php/OJOLIS/article/view/2698/2623

Zewdie, T. G. & Girma, A. (2020). IoT security and the role of AI/ML to combat emerging cyber threats in cloud computing environment. *Issues in Information Systems, 21*(4).

Zia, Y, Tehseen, S. & Kathane, R (2020). Information (ICT) security and libraries. *IP Indian Journal of Library Science and Information Technology, 5*(1), 43-45. http://doi.org/10.18231/j.ijlsit.2020.009