Cyber Threats to Libraries and the Implications for the Actualisation of the Sustainable Development Goals: A Narrative Review

Magnus Osahon Igbinovia
https://orcid.org/0000-0001-9104-2991
David Umahi Federal University of Health Sciences, Nigeria
Infor.migbinovia@gmail.com

Kingsley Efe Osawaru
https://orcid.org/0009-0004-0669-7862
Securi Group Limited, Scotland
osawarukingsleyefe@gmail.com

Emmanuel Nassar Onaivi
https://orcid.org/0009-0001-1255-441X
University of Wisconsin Milwaukee, United States
enonaivi@uwm.edu

Esther Oluwayinka Baipe
https://orcid.org/0000-0001-7872-3645
University of Medical Sciences, Nigeria
solankeyinka@gmail.com

Juliana O. Akidi
https://orcid.org/0000-0002-0468-7351
Alex Ekwueme Federal University, Nigeria
obyakidij@yahoo.co.uk

Afebuameh James Aiyebelehin
https://orcid.org/0000-0002-8092-9949
Ambrose Alli University, Nigeria
jamesaferich@gmail.com

Abstract

The article explored cyber threats to libraries and what they imply for the actualisation of the United Nations' sustainability agenda. To achieve this, the article examined how information acts as the connector between libraries and the sustainable development goals (SDGs). It examined the possible causes of cyber threats to libraries and the implications for SDGs. It investigated measures required to address cyber threats in libraries for the realisation of SDGs. A qualitative narrative review approach was adopted to collect and analyse literature from two major databases (EBSCOhost and ProQuest), complemented by Google Scholar. The findings revealed that libraries provide access to information which is a significant factor in actualising significant targets within the development framework. The findings also revealed possible causes of cyber threats to libraries. Cyber literacy, advocacy, the development/adoption of a cybersecurity policy, and adherence to cybersecurity measures were

UNISA university of south africa PRESS
Southern African Journal of Security
#19016 | 18 pages
https://doi.org/10.25159/3005-4222/19016
ISSN 3005-4222 (Online)

identified as ways of addressing cyber threats in libraries that threaten the actualisation of SDGs. The article reinforced the need for concerted efforts towards curtailing the menace of cyber-attacks in libraries for sustained information access and the realisation of the SDGs.

Keywords: access to information; cyber-attack; cybersecurity; cyber threats; libraries; sustainable development goals (SDGs)

Introduction

The United Nations' sustainable development goals (SDGs) are a universal call to action and a development framework that stimulate progress across nations within a timeframe (2015–2030). This timeframe adds urgency to the actualisation of the SDGs, demanding that all stakeholders play their part in transforming our world. It also has implications for keeping track of progress using critical success indicators at national and subnational levels.

The International Federation of Library Association and Institutions (IFLA) established herself (on behalf of the global library community) as a major stakeholder in the global development agenda. As a strategic move, prior to the adoption of the SDGs, the Lyon declaration was launched by IFLA on 18 August 2014 as an advocacy tool for the recognition of access to information in the development framework. In session 105 of the IFLA 2015 conference, there was a discussion on how libraries can contribute to sustainable development. Consequently, IFLA advocated that sustainable development can be powered by equitable access to information, which libraries provide.

To ensure equitable access to information, libraries must acquire and maintain digital collections that are accessible and available to meet the dynamic needs of their users. With digital resources, libraries are able to effectively bridge the digital divide and enhance equal participation in global development. However, the sustainability of these digital resources and information systems are endangered by cyber threats that could make them unavailable and inaccessible to those who need them. Oguedoihu and Adinchezor (2022) highlighted the dangers of these threats to the sustainability of information service provision. Aregbesola and Nwaolise (2023) reported that these threats could hinder the availability of digital resources if not prevented. Thus, cyber threats may compromise libraries' ability to contribute significantly to the actualisation of the SDGs by hindering access to information.

Although there seems to be an increase in cyber threats to libraries occasioned by the fluidity in digital information ecosystems, not much investigation has been carried out to examine how these threats compromises libraries' ability to contribute to the SDGs, as a development stakeholder. Some studies that have examined cybersecurity issues in libraries, while others have examined libraries' contribution to the SDGs. There is, however, a gap in the literature on how cybersecurity issues like cyber threats can hinder the potential of libraries to contribute to the SDGs. This review therefore synthesises

available literature that connects libraries, cyber threats and the actualisation of the SDGs. This will provide a conceptual understanding of the impact of cyber threats on libraries in relation to the actualisation of the SDGs.

Research Objectives

The article theoretically examines cyber threats in libraries and their implication for the actualisation of the SDGs. Specifically, the study examined literature on the following:
(1) Information as the connector between libraries and the SDGs
(2) Possible causes of cyber threats to libraries
(3) Implications of cyber-attacks on libraries in relation to the realisation of the SDGs
(4) Addressing cyber threats in libraries in relation to the realisation of the SDGs

Methodology

The study adopted a qualitative narrative review approach to collect and synthesise existing literature on the concept under investigation. This approach was used to examine cyber threats in libraries and what they imply for the actualisation of the global development agenda. The method was necessary to explore existing knowledge around the theme of this study, providing understanding to the theme based on synthesised literature without losing the voice of the authors. This approach aligns with that used in previous studies (e.g., Echedom and Okuonghae 2021). To achieve the objectives of the study, literature around the theme was retrieved using the search string: Cybersecurity OR cyber-attack OR cyber threat AND librar* AND SDGs. To retrieve literature that would be relevant to the review, two databases were used as information source for the study, namely EBSCOhost (academic complete) and ProQuest, complemented by Google Scholar. These databases were selected because of their multidisciplinary nature, given the nature of this study. To access grey literature that is relevant to the study, the authors also consulted organisational and professional websites.

In terms of inclusion criteria, the study considered literature published in English between 2015 and 2025. The source type for inclusion in the study was scholarly journals with the exception of grey literature from organisational and professional websites. Additionally, the search result was filtered by relevance rather than recency. The authors selected relevant literature within a two-week period and conducted the review and reporting of the literature between November 2024 and January 2025, adhering to the highest ethical standards.

Results

The review of the selected literature presented interesting findings that serve as conceptual evidence on how cyber threats to libraries can hinder libraries' contribution to the actualisation of the SDGs. By synthesising insights from 32 studies, the findings of the article are provided in accordance with the research objectives. These objectives reflect the themes within which discussions were made. Table 1 provides a thematic

summary of findings from the reviewed literature in accordance with the objectives of the article.

Table 1: Thematic summary of findings

Themes (Research Objectives)	Some Key Citations	Pertinent Findings
Information as the connector between libraries and SDGs	IFLA (2015); Igbinovia (2016, 2017); Alex-Nmecha, Horsfall, and Igbinovia (2017); Idiegbeyan-Ose et al. (2018); Igbinovia and Odelami (2019).	The access to information provided by libraries is an enabler of the actualisation of the SDGs. Information services across various domains address critical goals and targets within the development framework. Information services provision positions libraries as a critical actor or stakeholder in achieving the SDGs. Therefore, libraries' level of contribution to the agenda is a function of the access to information resources and information services they provide.
Possible causes of cyber threats to libraries	Ajie (2019); Luft (2020); Li and Liu (2021); Sanders and Scanlon (2021); Holt et al. (2021); Igbinovia and Aiyebelehin (2023); Kont (2023); Oyedokun (2024); Al-Hosani (2024); Soni and Soni (2025); Hakami (2025).	The possible causes of cyber threats to libraries which could potentially lead to cyber-attacks are the high monetisation of information resources and radical ideologies (hacktivism) that are either politically, religiously, or culturally motivated. Also, the lack (or poor implementation) of a cybersecurity policy, poor cyber literacy, and unethical cyber practices may result in cyber threats to libraries.
Implications of cyber-attacks in libraries for the realisation of the SDGs	Igbinovia (2017); Li and Liu (2021); Shandler and Gomez (2022); Stokes (2022); Aregbesola and Nwaolise (2023); The British Library (2024); Akor et al. (2024); Mohamed and Abuobied (2024).	Cyber-attacks on libraries' information systems create a disruption in information service delivery. This causes temporary or permanent loss of access to information. Lack of access to medical or health information, business information, and agricultural information may have critical implications for people, and in a broader sense affects sustainable development. Cyber-attacks on information systems will disrupt libraries' provision of Internet access which facilitates social and economic development. Such attacks could also potentially damage the reputation of the library which affects users' return-intention, invariably hindering the personal growth and development accrued from library usage.

		Cyber-attacks also hinder libraries' propensity to provide research services, and research activities are linked to the actualisation of sustainable development.
Addressing cyber threats in libraries for the realisation of the SDGs	Wojcicki (2019); Igbinovia and Ishola (2023); Lillian (2024); Bellini and Tammaro (2024).	The studies provided some measures that can address cyber threats in order to optimise libraries' contribution to the realisation of the SDGs, including developing the cyber literacy of library personnel and users, which equips them with the ability to safely navigate the cyber space. Also, sustained and targeted advocacy that reforms people's perception and attitude towards the library could prevent cyber-attacks. Developing or adopting a cybersecurity policy will significantly address cyber threats in libraries. Moreover, cyber threats against libraries can be addressed by adhering to cybersecurity measures/practices.

Discussion of Findings

The literature selected for the article were reviewed and presented in this section in line with the specific objectives guiding the article. In critically analysing the literature, authorial voice was introduced to bring a unique perspective to the study in a way that contributes to knowledge, particularly in the field of librarianship. The authors provided objective interpretations to the findings in the literature as presented subsequently.

Libraries and SDGs: Information as the Connector

Libraries have a historic role of providing access to information for societal transformation. They provide access to information resources and services that meet the varied needs of users. The accessibility (which libraries provide) and utilisation of information serve as critical factors for achieving sustainable development (Igbinovia 2016). This is why information is pronounced across the goals and indicators within the framework. For instance, SDGs 2c, 3.7, 5.6.2, 9.c, 12.8, and 16.10 show some of the targets that specifically focus on access to information as enablers of realising the SDGs. This implies that adequate information access is germane to the realisation of the SDGs.

The library is one of the principal actors in the actualisation of the SDGs. It also stands out as a strategic partner since the actualisation of the goals is dependent largely on the availability and use of information. Earlier on, the United Nations Development Group noted that genuine participation and access to information are the foundations of empowerment and development (IFLA 2015). IFLA further noted that in Moldova, for example, libraries are contributing to Open Government Partnership (OGP) action

plans, a platform between government, civil society, and business to drive commitments to open government and accountability. Librarians attend civil society meetings to help develop the country's national action plan through quality information, and to include the role of libraries as a supporter of access to information.

Libraries have become long-standing development partners that provide cost effective alternatives to accessing quality information. As noted in the IFLA report (2015), many countries have designated libraries as UN depositories, making them an important venue for information about the UN and the SDGs. In fact, "libraries support many aspects of The UN 2030 Agenda's vision and the SDGs. Libraries are key public institutions that have a vital role to play in development at every level of society" (IFLA 2015, 3). By reason of their primary goal, libraries have the mandate to provide access to basic information on education, health, agriculture, and social and civic issues, as well as provide capacity building that will be required for sustainable development. Through extension services, libraries take agricultural and health-related information to rural dwellers (Idiegbeyan-Ose et al. 2018). They provide SMEs with business information for economic revamp (Igbinovia and Odelami 2019). Through the provision of the political information required to enhance political participation and democratic governance (Alex-Nmecha, Horsfall, and Igbinovia 2017), libraries are building strong institutions and inclusive societies in line with the sustainable development framework.

Access to information provided by libraries is, therefore, a significant factor in actualising significant targets within the development framework. Therefore, it is safe to say that librarians as information professionals are well positioned to foster the attainment of the SDGs through quality information service delivery. The information services that libraries provide in response to achieving sustainable development cut across various sectors of society. As such, libraries provide information required to make informed health decisions, increase agricultural production, enhances functional and financial literacies among business owners, improve political participation for good governance, and provide information on legal issues that support justice and human rights. These capabilities strengthen libraries' capacity as information hubs that support the actualisation of the SDGs. In providing information services to individuals, groups, and communities, libraries manage the data of their users and personnel, as well as house a myriad of electronic information resources in the form of databases and offline records. These require safeguarding against cyber threats for the continuous functioning of the library system for effective information service delivery.

Possible Causes of Cyber Threat to Libraries

The rapid expansion of new technologies into every sector has contributed to the proliferation of alternative models of education, learning, and skill signalling in global labour markets (Goger, Parco, and Vegas 2022). This reality has forced libraries of all types to deliberately incorporate digital technologies into their service system. This transformation of conventional libraries into digital and virtual libraries has exposed their information system to threats that could undermine their objectives (centred on

information service delivery). These threats, which can also be called cybersecurity threats, cut across cyber cracking, data breaches, spyware, denial of service (DoS) attacks, malware, phishing, and pharming (social engineering).

These threats negate the core principles of librarianship as enshrined in the IFLA code of ethics which are access to information, privacy, confidentiality, integrity, and responsibility towards individuals and society. Some possible causes of cyber threats, reflected in cyber intrusions and subsequent attacks, on library's information system include the following:

High Monetisation of Information Resources

Although there are justifications for the commodification of information, it becomes problematic when the cost is far beyond people's ability to afford it. The condition of paying a specified amount of money as a condition to access scholarly literature online is considered to be commodification of information resources, and it is a barrier to information access (Igbinovia and Malgwi 2025). As such, one of the problems with the monetisation of information resources is limited access to knowledge and information especially by those in the disadvantaged socio-economic group (Igbinovia and Aiyebelehin 2023). Barriers to access to information due to information resources monetisation creates a divide along economic lines, which implies that those below a certain economic level are deprived of access to the information required for personal progress and social and economic development. This supports the assertion of Sanders and Scanlon (2021) that people below a certain economic threshold are more likely to lack access to information and information infrastructure. Information resources that are monetised often include fee-based or subscription-based information resources like journals, books, and electronic information resources (Olaseigbe et al. 2024). People who are unable to pay the necessary fees are often deprived of such information.

Information deprivation makes people seek alternate and (sometimes) illegal means of information access. As such, information seekers explore unauthorised shadow libraries like Sci-Hub, Library Genesis (LibGen), and Z-Library, which provide "black open access," that is, illegal or unsanctioned free access to paywalled or copyrighted information resources without appropriate permission (Soni and Soni 2025). The authors noted that this "black open access" poses a threat to the information ecosystem. Also, when information seekers are unable to pay the required fee to access monetised information, they may resort to illegal access through activities like hacking, which is a cyber-attack against libraries (Igbinovia and Ishola 2023). This is usually obtainable when people are looking for ways to circumvent paying for information access (Shah 2022). By implication, when the cost required to access information resources is beyond the ability of information seekers to pay, they explore illegal means like hacking and exploring "black open access" options which could pose cyber threats to libraries and information systems.

Radical Ideology

Radical ideologies may spur attacks on information systems and institutions like libraries. Radical ideologies or extremism provide the impetus for a variety of nefarious online activities like cyber-attacks (Al Hosani 2024). Therefore, ideologically driven hacktivism or cyber-terrorism, which can be politically, religiously, or culturally motivated, impede access to information. Hacktivists or cyber-terrorists attack information systems based on their ideologies, destroying these systems with unauthorised access, malicious code, and other cyber-attacks (Laitala 2012). There is a gradual increase in extremist-related (or ideology-based) cyber-attacks (Holt et al. 2021). Politically motivated actors (hacktivism) have attacked popular web pages or email hosts to announce political message which lead to restrictive access to information via those web pages (Li and Liu 2021). Although ideologically motivated violence is relatively rare, it is a proven cause of cyber threats targeting educational institutions, including libraries and information centers.

Lack of (or Poor Implementation of) Cybersecurity Policies

A cybersecurity policy provides the technical mechanisms with which to combat threats to information systems or infrastructure in libraries (Ajie 2019). This implies that developing and implementing a cybersecurity policy is a strategy to safeguard library information systems. Conversely, the lack of such a policy is a probable cause of cyber threats to libraries. Unfortunately, there is evidence that most libraries lack a cybersecurity policy to deal with the evolving cyber threats they face (Luft 2020). This lack of a cybersecurity policy connotes a lack of standards and regulatory framework or blueprint for addressing cybersecurity issues. Where cybersecurity policies do not exist, libraries will lack clear mechanisms and structures for safeguarding personal data, information resources, and systems. The absence or poor implementation of cybersecurity policies means that libraries are unprepared to tackle cyber threats, thus deepening the vulnerability of their information systems.

Cybersecurity policies provide the guidelines, procedures, and responsibilities for cybersecurity practices in libraries (Ibraheem et al. 2025). Such policies are critical in ensuring that users' privacy is protected and that libraries align with relevant data protection regulations (Saha 2024). Such policies also dictate the appropriate cyber behaviour of various actors in ensuring safety in the cyber space, and create security awareness among relevant stakeholders. This type of awareness moulds stakeholders' perception of and behaviour towards cybersecurity threats, policy compliance, and training (Igbinovia and Oladokun 2024). Where such policies do not exist, actors or stakeholders may be uninformed or unaware of cybersecurity measures relevant to safeguard the information systems in libraries, and they may display cyber behaviour that can compromise the cybersecurity of libraries. Consequently, there has been advocacy for library management to develop a cybersecurity policy to guide the cyber ethics of library personnel and users (Igbinovia and Ishola 2023). Therefore, the lack of

or poor implementation of a cybersecurity policy exposes libraries to cyber threats and attacks.

Poor Cyber Literacy

Cyber literacy is the ability or competency required to safely and ethically navigate the cyber space. Kont (2023) referred to it as the ability to use computer technologies, with proper knowledge of the consequences of the action. Although this definition did not specify the context in which these technologies are used, which is the cyber or online environment, it implies that lack of such ability portends adverse consequences like cyber threats. Poor cyber literacy thus implies an inability to ethically use digital technologies (hardware and software) in the cyber space, detect cyber threats and address them. This inability among library personnel exposes the library's information system to cyber-attacks and makes them vulnerable to cyber harm. This suggests that poor cyber literacy among library personnel may expose libraries and their information systems to cyber-attacks. Unfortunately, there seems to be poor cyber literacy among librarians (Hakami 2025) who should be educating users on various literacies, including cyber literacy. Poor cyber literacy hinders library personnel's ability to navigate through the cyber space, observing cybersecurity measures and aligning with best practices in ensuring the safety of the library's information systems.

Unethical Cyber Practices

Cybersecurity threats can be caused by failure to adhere to cyber ethics which reflects the rightness and wrongness in cyber practices. Cyber ethics are critical measures and practices that help keep data, networks, and information safe from cyber threats (Igbinovia and Ishola 2023). Library personnel and users are often not conscious of using information systems in a way that is morally acceptable. In some cases, library personnel may deliberately or inadvertently engage in unethical cyber practices (Hakami 2025) which could cause cyber threats to libraries. Some of these unethical cyber practices or behaviour include sharing users' credentials with unauthorised persons, unauthorised data copying, poor password management, shoulder surfing (Igbinovia and Ishola 2023), intentionally bypassing security measures or protocols (Aregbesola and Nwaolise 2023), data misappropriation, and malware injection (Oyedokun 2024). Oyedokun further stressed that these unethical practices undermine libraries' ability to contribute to the realisation of the SDGs. These unethical cyber practices expose information systems to cyber threats that can potentially harm the systems, restricting access to information. This reinforces the need for ethical cyber practices among library professionals as a way of safeguarding information systems for continuous information access.

Implications of Cyber-Attacks on Libraries for the Realisation of the SDGs

A critical effect of cyber-attacks on libraries is the temporary or permanent disruption of libraries' information systems, which derails the library from providing access to information. This contradicts SDG 16.10 which mandates public access to information. According to Li and Liu (2021), a cyber-attack is an intentional attempt to disrupt the services of an information system that impedes access to information. One such type of attack is DoS, which deprives system users of access to information contained in an information system. Attacks on information systems also create disruptions in information service delivery (Akor et al. 2024; Mohamed and Abuobied 2024), making it difficult for people to have timely access to market information (SDG 2c), health information (SDG 3.7), information for sustainable consumption and production (SDG 12.8), scientific information (SDG 14.5), and information for peaceful and inclusive living (SDG 16.10). For instance, the cyber-attack on the University of Vermont Medical Center disrupted their service delivery and resulted in loss of access to medical information required for health sustainability (Stokes 2022).

Cyber-attacks on libraries' information system may hinder people's access to technological infrastructure and Internet facilities in the libraries which impedes SDG 9c on access to information and communications technology and to the Internet. Libraries are a major provider of access to digital technologies and Internet access in countries of the Global South (Igbinovia and Aiyebelehin 2023) and Global North (Kinney 2010). However, with cyber-attacks, libraries would lack the ability to provide Internet access, invariably affecting their contribution to the actualisation of the global development agenda.

Moreover, cyber-attacks which lead to theft of users' personal data causes distrust with adverse effect on people's intention to return to the library, invariably hindering their personal growth and development which is the broad objective of the development agenda. Shandler and Gomez (2022) affirmed the notion that a cyber-attack on an institution diminishes public trust in the institution. Aregbesola and Nwaolise (2023) referred to this as reputational damage capable of tarnishing the library's image, making it less attractive to current and prospective users. This mistrust and lack of confidence in libraries affects users' willingness to use them, thus depriving them of the growth and development that comes with access to and utilisation of information and knowledge.

Cyber-attacks on libraries destroy scholarly materials that drive research and innovation, making them inaccessible for consumption and subsequent developmental actions. Libraries manage research data which are used for developmental projections; this research data can be destroyed by cyber-attacks. The cyber-attack on the British Library provides a case study of how research services can become inaccessible to library users due to malicious cyber-attacks (The British Library 2024). Igbinovia (2017) revealed how research serves as a means to realising the SDGs, and what this

implies for libraries and library professionals. Consequently, the disruption of research services and access to scholarly materials caused by cyber-attacks would have an adverse effect on the actualisation of sustainable development. Precisely put, cyber-attacks distort the delivery of research services in libraries which are enablers of the realisation of the SDGs.

Addressing Cyber Threats in Libraries for the Realisation of the SDGs

Libraries, being a central hub for information, play a crucial role in the actualisation of the SDGs (Alex-Nmecha and Igbinovia 2020; Igbinovia 2016, 2017; Igbinovia et al. 2018; Igbinovia and Aiyebelehin 2023). Consequently, strengthening cybersecurity in libraries by addressing cyber threats capable of compromising the sustainability of information resources and information systems becomes critical to the realisation of the SDGs. Some of the measures by which cyber threats in libraries can be addressed are discussed below.

Cyber Literacy

Library personnel and users need to be equipped with the ability to safely navigate the cyber space, observe cybersecurity measures, and address cyber threats when they occur. Thus, there is a need to include cybersecurity in library school curriculums to prepare professionals ahead of practice in a complex digital environment (Igbinovia and Ishola 2023). Also, educational institutions can include cybersecurity courses into their curriculums. Bellini and Tammaro (2024) noted that such training brings about familiarity with cybersecurity practices. IFLA issues a statement on digital literacy in which recommendations were made on the role of key stakeholders in building digital literacy as well as expectations from the library community (IFLA 2017). This statement can be applied in building capacity for cyber literacy among library professionals.

Advocacy

Sustained and targeted campaigns and enlightenment can be used to build relationships with people and reform their perception and attitude towards libraries and other information centres (Ezeala and Hundu 2019), in order to mitigate possible cyber-attacks based on extreme political, cultural, and religious ideologies. Advocacy can also be applied in getting funders to subsidise the cost of accessing scholarly materials especially in the Global South which is characterised by poor economic conditions. The goal is to uphold the underlying principles of open knowledge, which makes information freely accessible to everyone, consequently discouraging illegal access to information systems.

Development/Adoption of Cybersecurity Policies in Libraries

Cybersecurity policies in libraries are required to safeguard personal data, information resources and management. Such policies ensure the confidentiality, integrity, and availability of information and information systems. While cyber threats significantly

threaten data integrity and confidentiality (Oyedokun 2024), cybersecurity policies can be used to combat cyber threats, and become a line of defence against cybercriminals (Wojcicki 2019). Such policies are often dynamic to allow vital alterations or periodic updates based on the changes in cybersecurity projections and risk assessment of the library. The IFLA Statement on Cybersecurity that was approved by the governing board in 2022 should guide libraries in developing a cybersecurity policy.

Cybersecurity Measures

Library personnel and users are required to adhere to cyber ethics, be conscious of cybersecurity issues, and keenly observe cybersecurity measures to protect their data and the overall information systems. Lillian (2024) underscored the relevance of data protection through ethical cybersecurity practices. Some of the practices or measures that can help strengthen cybersecurity in libraries are:

- Use of biometric technologies for identity authentication: The adoption of fingerprint, facial recognition, voice analysis, hand geometry, and vein or vascular pattern recognition (VPR) would further strengthen information security measures in libraries.

- Encryption: Libraries could use end-to-end encryption (E2EE) to ensure that only a designated communication party can access sensitive information, preventing intrusion from third parties.

- Regular audits and assessments of information systems: The periodic review and evaluation of the information system to detect its vulnerability and strengthen the system against attack can help to prevent cyber-attacks. This helps to monitor users' complaints with cybersecurity measures and assess the strengths and weaknesses of available security software.

- Restrictions on designated computers: Computers in the libraries that perform the function of a server or are used for administrative purposes should be restricted. Such restrictions should be enforced through various authentication methods. Also, usage of designated computers should be guided by a cybersecurity policy that determines the software that can be installed on it, networks and external systems that should be connected to it, and constantly monitored to identify breaches and leaks.

- Firewall protection to prevent outside attack: By restricting access, firewalls help to protect the information systems against cyber-attacks by conducting security checks and inspecting incoming and outgoing network traffic.

Implications for Policy, Practices, and Collaborations

Although the authors have provided insights on addressing cyber threats in libraries for the actualisation of the SDGs, there is a need to make some extrapolations on its implication for policy, practice, and possible collaborations. First, IFLA has undoubtedly played an enviable role in driving the global agenda for sustainable development. However, there is a need for the Association to "up the game" by moving beyond declarations to providing frameworks that can be adopted or adapted by libraries based on institutional peculiarities. IFLA can provide a global cybersecurity framework for libraries that will act as a conceptual foundation for taking action on digital and cybersecurity policies. IFLA can also provide cybersecurity toolkits for library personnel, library users, and, by extension, the general public.

Several studies (e.g., Aregbesola and Nwaolise 2023; Oyedokun 2024) have emphasised the necessity of cybersecurity policies and frameworks in addressing cyber threats. However, there is a need to develop and implement these cybersecurity policies and frameworks at national and subnational levels, taking into cognisance the peculiarity of institutions at these levels. This makes it easy for institutional adoption and implementation. This can be achieved through targeted advocacy at national and subnational levels. Stepping down policies and frameworks to national and subnational levels could give a general consciousness of cybersecurity, enabling adherence to cybersecurity measures. Moreover, vendors of information systems, library software, and databases should tighten the security of their products to address their vulnerability against possible attack. As such, cybersecurity requirements must be identified and included throughout the lifecycle of information systems.

There is a need to foster collaborations with stakeholders from the information technology (IT) sector in order to develop a cybersecurity workforce in libraries**.** Such collaboration and synergy is expected to strengthen information systems in libraries. This collaboration was buttressed by Bellini and Tammaro (2024) when they asserted that effective and reliable collaborations are essential in strengthening cybersecurity resilience for digital libraries. Also, Aregbesola and Nwaolise (2023) emphasised that such partnerships help libraries in the development and implementation of robust cybersecurity frameworks that are designed to meet the library's specific need(s). Libraries are therefore expected to engage in relevant collaborations to strengthen their workforce preparedness for cyber threats.

Conclusion

By providing access to information, libraries play a critical role in the actualisation of the SDGs, cutting across various targets and indicators of the framework. Access to information is the connector between libraries and the SDGs, implying that the extent to which libraries provide access to information across various sectors will determine their contribution to the actualisation of the development agenda. To provide better access to information, libraries are now embracing the digital model of service delivery

which involves the use of more robust information systems or infrastructure, inherently exposing the libraries to cyber threats. Libraries can also be exposed to cyber threats when people explore illegal access to fee-based information resources. Also, ideologies that are politically, religiously, or culturally motivated could trigger cyber-attacks on information systems and institutions. Lack of a cybersecurity policy, poor cyber literacy, and unethical cyber practices among actors are other possible causes of cyber threats to libraries.

When cyber threats are not addressed, they result in cyber-attacks on libraries which compromises the integrity of their information systems and negate their contribution to the achievement of the SDGs by hindering access to information and information systems. There is therefore a need for concerted efforts towards curtailing the menace of cyber-attacks in libraries through stringent cybersecurity measures. These include developing cyber literacy among library personnel, engaging in advocacy to inform people on the value of libraries, developing and implementing cybersecurity policies in libraries, and adherence to cybersecurity practices. These measures are expected to safeguard the libraries' information systems and protect data and information resources for sustained access to information in support of sustainable development.

References

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

Akor, S. O., C. J. Nongo, C. O. Udofot, and B. D. Oladokun. 2024. "Cybersecurity Awareness: Leveraging Emerging Technologies in the Security and Management of Libraries in Higher Education Institutions." *Southern African Journal of Security* 2: 14 pages. https://doi.org/10.25159/3005-4222/16671

Alex-Nmecha, J. C., M. N. Horsfall, and M. O. Igbinovia. 2017. "Roles of Libraries in Ensuring Political Integration." *International Journal of Library and Information Science* 9 (9): 89–95. https://academicjournals.org/journal/IJLIS/article-full-text/7C1F64766237

Alex-Nmecha, J. C., and M. O. Igbinovia. 2020. "Achieving Sustainable Development Goals in Nigeria through Information Literacy: The Roles of Public Libraries." *Lagos Journal of Library and Information Science* 9 (1–2): 16–27. https://www.ajol.info/index.php/ljlis/article/view/199646

Al-Hosani, H. 2024. "Intellectual Security: Innovative Strategies to Combat Extremism in the Digital Era. Trends Research and Advisory." Trends Research & Advisory, 30 December. https://trendsresearch.org/insight/intellectual-security-innovative-strategies-to-combat-extremism-in-the-digital-era/

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

Bellini, E., and A. M. Tammaro. 2024. “Cybersecurity for Digital Libraries: An Interview with Emanuele Bellini.” *Digital Library Perspectives* 40 (2): 348–355. https://doi.org/10.1108/DLP-05-2024-147

The British Library. 2024. “Learning Lessons from the Cyber-Attack: British Library Cyber Incident Review.” The British Library, 8 March. https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf/

Echedom, A. U., and O. Okuonghae. 2021. “Transforming Academic Library Operations in Africa with Artificial Intelligence: Opportunities and Challenges: A Review Paper.” *New Review of Academic Librarianship* 27 (2): 243–255. https://doi.org/10.1080/13614533.2021.1906715

Ezeala, L. O., and J. T. Hundu. 2019. “Talking up Libraries −21st Century Library Advocacy.” *Journal of Applied Information Science and Technology* 12 (1): 23–28. https://www.jaistonline.org/12vol1/4.pdf

Goger, A., A. Parco, and E. Vegas. 2022. “Learning and Working in the Digital Age: Advancing Opportunities and Identifying the Risks.” Brookings, 17 May. https://www.brookings.edu/articles/learning-and-working-in-the-digital-age-advancing-opportunities-and-identifying-the-risks/

Hakami, A. A. 2025. “The Role of Public Librarians in Reducing Cybercrime: Literature Review.” *Public Library Quarterly*, 1–14. https://doi.org/10.1080/01616846.2025.2600686

Holt, T. J., M. Stonhouse, J. Freilich, and S. M. Chermak. 2021. “Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups.” *Terrorism and Political Violence* 33 (3): 527–548. https://doi.org/10.1080/09546553.2018.1551213

Ibraheem, I., A. A. Yusuf, B. L. Aremu, and M. T. Jidda. 2025. “Perspectives of Librarians on the Impact of Cyber Threats in the Management of Digital Libraries in Kwara State, Nigeria.” *FUDMA Journal of Sciences* 9 (12): 9–19. https://doi.org/10.33003/fjs-2025-0912-3990

Idiegbeyan-Ose, J., A. Owolabi, C. Segun-Adeniran, A. Aregbesola, S. E. Owolabi, and T. Eyiolorunshe. 2018. “Information Provision by Public Library to Agricultural Extension Agents in a Developing Country.” *Public Library Quarterly* 38 (1): 103–115. https://doi.org/10.1080/01616846.2018.1555412

IFLA. 2015. “Libraries and Implementation of the UN 2030 Agenda. IFLA Action for Development through Libraries Programme.” Accessed October 2015. https://www.ifla.org/wp-content/uploads/2019/05/assets/hq/topics/libraries-development/documents/libraries-un-2030-agenda-toolkit.pdf

IFLA. 2017. “IFLA Statement on Digital Literacy.” Accessed December 8, 2024. https://www.ifla.org/wpcontent/uploads/2019/05/assets/faife/statements/ifla_digital_literacy_statement.pdf

Igbinovia, M. O. 2016. “Libraries as Vehicles to Sustainable Developmental Goals: A Case Study from Nigeria.” *Library Hi Tech News* 33 (5): 16–17. https://doi.org/10.1108/LHTN-03-2016-0010

Igbinovia, M. O. 2017. “Librarians’ Involvement in Cross-Disciplinary Research and Its Implication to Sustainable Development Goals (SDGs).” *Library Review* 66 (4/5): 251–265. https://doi.org/10.1108/LR-09-2016-0078

Igbinovia, M. O., and A. J. Aiyebelehin. 2023. “Libraries as Facilitators of Digital Inclusion for Sustainable Development: The Nigerian Experience.” *Folia Toruniensia* 23: 53–73. https://doi.org/10.12775/FT.2023.003

Igbinovia, M. O., and B. C. Ishola. 2023. “Cyber Security in University Libraries and Implication for Library and Information Science Education in Nigeria.” *Digital Library Perspectives* 39 (3): 248–266. https://doi.org/10.1108/DLP-11-2022-0089

Igbinovia, M. O., and B. Odelami. 2019. “Influence of Information Availability and Use on Economic Integration of Small Scale Business Owners: The Role of Libraries.” *Library Philosophy and Practice (e-journal)* 3569. https://digitalcommons.unl.edu/libphilprac/3569

Igbinovia, M. O., and B. C. Ishola. 2023. “Cyber Security in University Libraries and Implication for Library and Information Science Education in Nigeria.” *Digital Library Perspectives* 39 (3): 248–266. https://doi.org/10.1108/DLP-11-2022-0089

Igbinovia, M. O., and B. D. Oladokun. 2025. “Information Security in Libraries, Librarianship, and Information Science.” In *Encyclopedia of Libraries, Librarianship, and Information Science*, edited by D. Baker and L. Ellis, 401–411. Elsevier. https://doi.org/10.1016/b978-0-323-95689-5.00162-0

Igbinovia, M. O., and P. G. Malgwi. 2025. “Commodification of Information and Its Implication for Equitable Access to Information and Sustainable Development.” *Communicate*: *Journal of Library and Information Science* 27 (1): 21–38. https://www.cjolis.org/index.php/cjolis/article/view/146

Kinney, B. 2010. “The Internet, Public Libraries, and the Digital Divide.” *Public Library Quarterly* 29 (2): 104–161. https://doi.org/10.1080/01616841003779718

Kont, K.-R. 2023. “Cyber Literacy Skills of Estonians: Activities and Policies for Encouraging Knowledge-Based Cyber Security Attitudes.” *Information and Media* 96: 80–94. https://doi.org/10.15388/Im.2023.96.67

Laitala, N. 2012. “Hacktivism and Cyberterrorism: Human Rights Issues in State Responses.” MA thesis, Adam Mickiewicz University, Poznań. https://repository.gchumanrights.org/server/api/core/bitstreams/4d6739e8-1594-4461-9c0d-b30eee06b395/content

Li, Y., and Q. Liu. 2021. “A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments.” *Energy Reports* 7: 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lillian, N. R. 2024. “Strengthening Cybersecurity in Nigerian Libraries: Challenges, Mitigation Strategies, and Future Trends.” *Research Output Journal of Biological and Applied Science* 3 (2): 23–7. https://rojournals.org/strengthening-cybersecurity-in-nigerian-libraries-challenges-mitigation-strategies-and-future-trends/

Luft, P. J. 2020. “Proactive Management in Academic Libraries: Promoting Improved Communication and Inclusion of Academic Librarians and Archivists in Cybersecurity Policy Creation.” MA thesis, Columbus State University. https://csuepress.columbusstate.edu/theses_dissertations/421

Mohamed, N. N., and B. H. H. Abuobied. 2024. “Cybersecurity Challenges across Sustainable Development Goals: A Comprehensive Review.” *Sustainable Engineering and Innovation* 6 (1): 57–86. https://doi.org/10.37868/sei.v6i1.id207.

Oguedoihu, M. C., and I. P. Adinchezor. 2022. “Editorial.” *Ghana Library Journal* 27 (2): 139–292. https://doi.org/10.4314/glj.v27i2.0.

Olaseigbe, Y. F., O. S. Ozonuwe, A. T. Ogunojemite, R. A. Rotimi, A. O. Giwa, and A. A. Ogundana. 2025. “Self-Sustaining Library Services through Strategic Fee-Based Initiatives: A Road Map for Academic Library Administrators in Nigeria.” *Communicate: Journal of Library and Information Science* 26 (2): 160–170.

Oyedokun, T. T. 2024. “Digital Threats to Libraries and Their Impact on Sustainable Development Goals (SDGs).” *Thomas Adewumi University Journal of Innovation, Science and Technology* 1 (1): 1–21. https://journals.tau.edu.ng/index.php/tau-jist/issue/download/1/20?utm_source=chatgpt.com

Saha, R. 2024. “Data Privacy and Cyber Security in Digital Library Perspective: Safeguarding User Information.” *International Journal of Scientific Research in Engineering and Management* 8 (4): 1–5. https://doi.org/10.55041/ijsrem30761

Sanders, C. K., and E. Scanlon. 2021. “The Digital Divide Is a Human Rights Issue: Advancing Social Inclusion through Social Work Advocacy.” *Journal of Human Rights and Social Work* 6 (2): 130–143. https://doi.org/10.1007/s41134-020-00147-9

Shah, S. 2021. “Understanding the Effects of Online Paywalls on Information Access.” Honors Baccalaureate of Science, Oregon State University. Accessed December 8, 2024. https://ir.library.oregonstate.edu/concern/honors_college_theses/pg15bp10j

Shandler, R., and M. A. Gomez. 2022. “The Hidden Threat of Cyber-Attacks—Undermining Public Confidence in Government.” *Journal of Information Technology and Politics* 20 (4): 359–374. https://doi.org/10.1080/19331681.2022.2112796

Soni, A., and S. Soni. 2025. “Unveiling the Shadows: Exploring Shadow Libraries and Black Open Access in the Digital Age.” *Vidya - A Journal of Gujarat University* 4 (1): 29–33. https://doi.org/10.47413/svhb2k07

Stokes, A. M. 2022. “Disruption of Library Services Due to Hospital Cyberattack: A Case Study.” *Medical Reference Services Quarterly* 41 (2): 204–212. https://doi.org/10.1080/02763869.2022.2054198

Wojcicki, N. M. 2019. “Phishing Attacks: Preying on Human Psychology to Beat the System.” *World Libraries* 23 (1): 1–14. https://worldlibraries.dom.edu/index.php/worldlib/article/view/579/508