International Federation of Library Associations and Institutions

IFLA Statement on Cybersecurity

Approved by the IFLA Governing Board, February 2022

This IFLA policy statement, aimed at libraries, library associations and library educators, and governments (including intergovernmental organisations), looks to explain the concept of cybersecurity in the context of the work of libraries, and make recommendations for improvements.

Libraries act as a gateway information provider, and public libraries in particular increasingly play a role in levelling inequity of access to information. In carrying out this mission, libraries increasingly rely on digital technologies, both in order to provide access to information, and to ensure their own effective operation.

In doing do, they are faced with the fact that such systems can be vulnerable to attack, creating risks for institutions, staff and users alike. Cybersecurity is therefore an essential element in the work of libraries, in order to protect both library clients and library staff while providing access to information for the community.

As such, there is a growing need to consider how libraries can approach questions around cybersecurity in a way that upholds key values around intellectual freedom.[1]

Cybersecurity, and Why it Matters in Libraries

Definitions of cybersecurity focus on the protection of networks, devices and data from unauthorised access and/or use. Closely connected to this are efforts to ensure the confidentiality, integrity and availability of information.[2] Some site this within the wider concept of Digital Security, which goes beyond the technical and/or criminal in order to consider economic and social aspects also.[3]

---

[1] This includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers (including the freedom to read, and wider freedom of access to information and freedom of expression). See in particular the IFLA Statements on Privacy in the Library Environment (2014): https://www.ifla.org/wp-content/uploads/2019/05/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf, and Statement on Libraries and Intellectual Freedom (1999): https://repository.ifla.org/handle/123456789/1424

[2] See the US Cybersecurity and Infrastructure Security Agency https://us-cert.cisa.gov/ncas/tips/ST04-001, UK National Cyber Security Centre: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security, ENISA: https://www.enisa.europa.eu/publications/definition-of-cybersecurity .

[3] OECD: https://www.oecd.org/digital/ieconomy/digital-security/

Standards around cybersecurity centre on the components of information systems:

- The critical applications
- The servers and installations supporting the applications (data centres, etc.)
- The security around the networks supporting the systems
- The security around software development, change control and deployment
- The "end user" or client environment

These are all relevant for libraries in their efforts to ensure cybersecurity, although not all libraries have the same level of control over the different components of the systems that they use. Situated in many different institutional contexts, the cybersecurity policies of the library will often be determined by the overarching policies of the governing institution.

For example, libraries may have little agency in the management of the infrastructure on which they operate, but are typically involved in the end user or client environment, and have a critical role in selection, administration, education and management of the library systems and services provided.

Areas for Library Engagement or Advocacy

Whether it is through their actions, or through influencing the actions of others, libraries will want to promote cybersecurity in the following areas:
(1) Protecting library systems from cyber security risks and threats in order to enable ongoing service provision
(2) Ensuring the protection of library users from internet-based threats while using library systems
(3) Protecting the privacy of user information

Many libraries, in providing access to the internet, will also have a legal or other obligation to ensure that this access is not used to harm others. As such, libraries may also need to take steps to ensure that users themselves do not engage in cybercrime activities using library systems or resources and comply with the institutions' acceptable use policy.

More positively, given that users may well use the internet and other information systems outside of the library, there can also be an opportunity to promote behaviours and protocols for the safe use of services through digital literacy programmes.[4]

[4] For example, the UK's Internet Safety Strategy highlights the importance of education: https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper

Finding the Balance

Promoting cybersecurity is not uncontroversial of course. Efforts to identify potential risks can come into conflict with efforts to ensure the privacy of library users and others.

For example, libraries may be obliged to implement technologies for the enforcement of acceptable use policies or be subject – along with internet users more broadly – to surveillance by security authorities. In such cases, it is important to be transparent about the rules and tools that are in place, in order to give users a reasonable choice.

Of course, in other ways, the goals of cybersecurity strategies and privacy can also fit together. For example, the risk of losing personal data through cyber attacks can be minimised if libraries are not storing unnecessary personal data in the first place, and are ensuring that this is properly encrypted.

Recommendations

IFLA therefore makes the following recommendations.

Where they have (partial or full) responsibility for their own information systems, libraries should:

- Implement policies on minimising data gathering and retention, including the deletion of usage history after defined periods of time.
- Use available tools to protect users while they are using library systems, including standard measures for information security, encrypted web services, effective password and web session controls, or applying the principle of least privilege,[5] while at the same time ensuring maximum privacy.
- Implement end-point security controls on all library workstations and servers.[6]
- Where tools are implemented to monitor for inappropriate use or inadvertent threats, to do so in a way that provides maximum transparency and respect for privacy.

[5] https://en.wikipedia.org/wiki/Principle_of_least_privilege

[6] A number of ISO Standards cover questions around cybersecurity. However, these standards are not available open access, and so cannot be endorsed by IFLA as models for the global library field. Examples include ISO 27001 - Information Security Management System – Requirements, www.iso.org/isoiec-27001-information-security.html; ISO 27002 - Code of Practice for Information Security Management, https://www.iso.org/standard/54533.html; ISO 27032 - Information technology - Security techniques - Guidelines for cybersecurity, https://www.iso.org/standard/44375.html

Where they are part of a wider institution (and so do not have control over key components of information systems) or rely on third party vendors:

- Advocate for effective cybersecurity measures by host institutions, which also uphold principles of privacy. This can include promoting privacy-friendly practices around data collection and retention.
- Encourage third-party vendors to libraries to implement meaningful cybersecurity themselves, in order to ensure that library users do not face any unacceptable risks when using their services.

All libraries should:

- Either alone, or in partnership with a host institution as appropriate:
    - Develop and publish acceptable use policies for internet use and use of other information systems.
    - Develop and publish privacy policies, defining where and what information is collected and how it is used, and what happens in case of a breach.
    - Develop and publish a cybersecurity and information security policy that defines the principles and practices used to protect library systems and provide resilience and recovery in case of failure. This should be informed by the institutional policies and procedures in this area.
    - Ensure that all library personnel understand and are able to implement the cybersecurity fundamentals (e.g. good password practices, etc.) relevant for their respective tasks.
- Explore the potential to build digital literacy among users, including understanding of how to avoid threats to cybersecurity.

Library associations and other support organisations should:

- Provide updates and information as appropriate about cybersecurity in the work of libraries, and where possible, offer training or links to other resources.
- Consider working with others engaged in helping to keep people safe online.

Governments should:

- Ensure that libraries have the resources and training to be able to maximise cybersecurity, as well as invest in digital literacy programming (including through libraries) in order to promote online safety.[7]
- Ensure that wider cybersecurity policies combine effectiveness with respect for human rights, including privacy.

[7] K. M. Caramancion, "An Exploration of Disinformation as a Cybersecurity Threat," *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, San Jose, CA, USA, 2020, pp. 440-444, doi: 10.1109/ICICT50521.2020.00076

Annex: ISO Standards

The ISO standards provide a general set of standards for cyber- and information security in any organisation. This should form a baseline for Information Technology practices for the technical aspects of cybersecurity in the library.

ISO/IEC 27001 (Information Security Management System - Requirements) specifies the requirements for a well-defined Information Security Management System (ISMS) within an organisation. This looks at the systematic processes for security management.[i]

ISO/IEC 27002 (Code of Practice for Information Security Management) contains guidelines and best practices recommendations for 10 key security areas: security policy; organisation of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; and compliance. This is typically in the domain of the Information Systems management of security in the Information Technology architecture.[ii]

ISO/IEC 27032 (Information technology - Security techniques - Guidelines for cybersecurity) expands on the baseline practices for cyber security.[iii]

---

[i] https://www.iso.org/standard/54534.html
[ii] https://www.iso.org/standard/54533.html
[iii] https://www.iso.org/standard/44375.html