PRZEGLĄD BIBLIOTECZNY 2025
e-ISSN 2545-2487

GRZEGORZ GMITEREK
Faculty of Journalism, Information and Book Studies
University of Warsaw
e-mail: ggmiterek@uw.edu.pl
ORCID 0000-0002-5692-1824

DIGITAL SECURITY IN LIBRARIES. CHALLENGES, THREATS, AND DATA PROTECTION IN THE DIGITAL AGE

Dr hab. Grzegorz Gmiterek is an Associate Professor at the Faculty of Journalism, Information and Book Studies of the University of Warsaw. His research interests focus on issues related to the use of new technologies in cultural and scientific institutions (especially Web 2.0 tools and services as well as mobile devices and applications). Scholar Of the Historical and Literary Society in Paris in Dr. Maria Zdziarska-Zaleska's name. Participant of the US Department of State's International Visitor Leadership Program "Library & Information Science". Author of several dozen of scientific publications, including the following books: *Library in social network. Library 2.0* (Warsaw 2011), for which he was granted the Scientific Award of SBP in the name of Adam Łysakowski and the CLIO Award Of the Faculty of History of the University of Warsaw, co-author of the book *Mobile applications in libraries and beyond* published in 2017 (distinction of the Rector of the Warsaw Technical University for the publication academic studies in the field of technical sciences and sciences during the Academic and Scientific Book Fair in the ACADEMIA contest) and the author of the book *Mobile applications in information systems. Theory and practice* (Warsaw 2020), for which he received the 2020 Science Award of SBP in the name of Adam Łysakowski (category: Works of theoretical, methodological, source character).

KEYWORDS: Cybersecurity. Libraries.

ABSTRACT: **Purpose of the article** – Analysis of selected challenges and threats related to cybersecurity in Polish and international libraries and proposals for solutions to enhance data and user protection. **Research methods** – The research utilized the analysis and critique of scientific literature and source materials available online, including recent publications, reports, press articles, and industry sources. Artificial intelligence tools such as Scopus AI, SciSpace, Scite, Primo AI Search Assistant and the Perplexity search engine were also used to obtain current data on cyberattack incidents. **Key findings** – Due to digitization and access to a variety of IT tools, libraries are becoming increasingly vulnerable to cyberattacks. These attacks can lead to data loss, violations of user privacy, service disruptions, and financial and reputational damage. **Conclusions** – Cybersecurity in libraries requires a comprehensive approach encompassing technologies, procedures, and education. Only such comprehensive measures will minimize threats, protect user data, and ensure the continued operation of libraries in the digital era.

INTRODUCTION

In the modern world, libraries play a key role, providing access to information and knowledge increasingly through modern and interactive technologies. Undoubtedly, however, with the development of digital services, new threats related to data security and user privacy are emerging. Furthermore, for a long time, these institutions were perceived as safe places, virtually immune to digital threats, to which the business sector, public administration, and financial institutions were more vulnerable. Yet recent years have seen changes that are clearly related to the rapid digitization of library services, which consequently makes libraries also targets for cyberattacks. Regardless of the type of library, these institutions use integrated library systems or library service platforms, provide e-documents and databases, increasingly conduct user registration and services online, provide computers and other digital devices and Wi-Fi connections in their buildings, and, to a greater or lesser extent (depending on the institution), engage with social media. The above-mentioned aspects of library operations are just a few examples related to the potential emergence or increase of digital threats in libraries.

RESEARCH OBJECTIVES AND METHODS

In this article, I analyze selected cybersecurity challenges in Polish and international libraries and propose solutions to enhance the protection of information and users, with particular emphasis on data processed in library systems. The aim of my analysis is to identify and characterize

cyberthreats and cyberattacks that have occurred in libraries both in Poland and internationally. Based on the experiences of these institutions, I also present measures enabling the effective protection of digital collections and user data. Furthermore, I highlight the challenges libraries face in implementing effective cybersecurity solutions.

During my research, I utilized the method of literature analysis and critique. The topic of cybersecurity in libraries is already present in the literature. However, it is worth noting that the most numerous attacks on these institutions have occurred in recent years, and not all of them have been described in scholarly publications to date. This is particularly true of attacks on Polish libraries. I will only mention here that the last case I analyzed occurred in July 2025, during the writing of this text. Therefore, important sources of information for me included library websites, their fan pages on social media, and articles in news outlets and in local and national press. I conducted my primary literature searches using the Primo Library Discovery Service available at the University of Warsaw Library. I was particularly interested in publications from the last few years, which are current enough to describe the threats we are constantly facing. While searching for information about publications, I also used tools with artificial intelligence components: Scopus AI, Primo AI Search Assistant, SciSpace, and Scite. I also conducted a supplementary search using Google Scholar. To identify information about cybercriminal attacks on Polish libraries, I used the Google search engine and the news aggregator Google News. The Perplexity search engine, based on generative artificial intelligence, also proved useful in searching for such information. I should emphasize that each piece of information about a hacker attack obtained this way[1] was then verified in other online sources (e.g. on the website of a given library).

CYBERSECURITY – CHALLENGES AND THREATS FOR LIBRARIES

Advances in the application of information technologies in libraries, and with them the use of these technologies in almost every area of library operations, are leading to the emergence of a number of new challenges and threats in cyberspace. In the literature, the term "cyberspace" is defined in various contexts, often depending on needs. Robert Janczewski

[1] In this article, the term "hacker" is associated with negative connotations, particularly in relation to the examples of criminal activities cited in the text, such as cyberattacks, aimed at gaining unauthorized access to computer systems, networks, or data in order to cause harm. However, it is important to emphasize that hacker culture encompasses a diverse set of values, practices, and beliefs that have evolved over time, reflecting both positive and negative aspects. In a positive context, a central element of this culture is the hacker ethic, which promotes ideals such as openness, collaboration, and the free exchange of information (Castellanos-Rivadeneira & Valerio-Ureña, 2020, pp. 134).

rightly points out that "different areas of human activity use this concept in various meanings" (Janczewski, 2022, p. 141). For the purposes of this article, I adopt the definition of "cyberspace" provided by Janusz Wasilewski, citing the US Department of Defense. According to this definition, cyberspace is "a global domain of the information environment consisting of interdependent networks created by information technology (IT) infrastructure and the data contained within them, including the Internet, telecommunications networks, computer systems, and the processors and controllers embedded within them" (Wasilewski, 2013, p. 227).

Cyberspace undoubtedly creates opportunities for criminal activities and attacks targeting public institutions such as museums, archives, and libraries. According to the definition provided in 2024 by Małgorzata Michałowska and Ewa Hassa, the term "cybersecurity" means "the resilience of information systems to activities that violate the confidentiality, integrity, availability, and authenticity of processed data or related services offered by these systems" (Michałowska, & Hassa, 2024, p. 101). It is worth noting that the "GDPR Guide for Libraries", published by the Association of Polish Librarians, also refers to cybersecurity as a concept encompassing "solutions for IT security, including the security of personal data in cyberspace". And further: "it also encompasses infrastructure security, from individual computer or telephone equipment to the overall ICT infrastructure, including critical infrastructure" (GDPR Guide for Libraries, 2020, p. 126). It is probably no wonder that cybersecurity in libraries is a crucial issue today. This is, of course, primarily related to these institutions' management of sensitive user data, but also to the integrity of library resources and services.

What threats do libraries face in the context of their cyberspace operations? The answer to this question is not at all simple. Different threats can have different consequences for the operations of these institutions. Understanding them is crucial for implementing effective security measures. Furthermore, these threats are evolving with the increasing integration of advanced technologies and the digital transformation of library services. Among the typical examples of security vulnerabilities cited in the literature are distributed denial-of-service (DDoS)[2], malware[3],

[2] DDoS (distributed denial of service) – "an attack on a computer system or network service in order to prevent it from functioning by occupying all available resources, carried out simultaneously from multiple computers". [In:] Pohoska, K. (2025, March 3). Cyberprzestępczość – prognozy na 2025 rok. *Stołeczny Magazyn Policyjny*, Retrieved August 12, 2025, from https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html.

[3] Malware – "Installation of malicious software that can disrupt library operations or compromise data security" (Saha, 2024).

ransomware[4], phishing[5], SQL injection attack[6], session hijacking and Man-in-the-Middle attacks,[7] and cross-site scripting (XSS)[8] (See Humayun, et al., 2020, pp. 3173 ; Oladokun, et al., 2024).

Among the most common hacker attacks on libraries are malware infections (including viruses, worms, and Trojans), which can corrupt data, disrupt library services, systems, and networks, and violate user privacy. Malware infections can result from accidental or inadvertent downloads of infected files, library staff visiting infected websites, or opening malicious email attachments (Akor et al., 2024). Ransomware appears to be the most dangerous type of attack, which encrypts files and locks the system, often resulting in inaccessibility of data and services, often until a ransom is paid. This type of attack can also result in data loss for the library and a violation of user privacy. The proliferation of ransomware-as-a-service (RaaS) platforms has made ransomware attacks more accessible to cybercriminals, increasing the risk to libraries (Akor et al., 2024).

A significant aspect of hacker attacks is, of course, the compromise of data, often sensitive, concerning both users and library employees and collaborators. For example, unauthorized access to institutional databases can result in the disclosure of ID numbers, passport data, information about users' place of residence, their telephone numbers, etc. (Rahim, et al., 2024). Internal library documents (e.g., contracts, invoices) are also at risk of disclosure. Such actions can damage the library's reputation and entail legal and financial consequences.

It's also worth at least mentioning "brute force" attacks, which involve repeated attempts to gain unauthorized access to library systems by guessing passwords. Such attacks can also lead to unauthorized access to sensitive data and disruption of library services (Putri, et al., 2024,

[4] Ransomware – "a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files" (Corrado, 2024).

[5] Phishing – "a method of fraud in which a criminal impersonates another person or institution in order to obtain confidential information (e.g. login details, credit card details), infect a computer with malware, or persuade the victim to take specific actions". (Akademia NASK, n.d.).

[6] SQL Injection attack – "In this attack, an input string is injected through the application to change or manipulate the SQL statement to the attacker's advantage. This attack harms the database in several ways, including unauthorized access and manipulation of the database, and disclosure of sensitive data". (Humayun, et al., 2020, pp. 3173).

[7] "Man-In-The-Middle (MITM, also abbreviated in the literature as MIM, MitM, MiM or MITMA) is an attack where an unauthorized third party secretly gains control of the communication channel between multiple endpoints. The MITM attacker can interrupt, manipulate or even replace the target victims' communication traffic. Further, victims are not aware of the intruder, thus believing that the communication channel is safe and protected". (Humayun, et al., 2020, pp. 3173).

[8] "Cross-Site Scripting (XSS): In this type of attack, a malicious attacker tries to run a JavaScript code in the client's browser in order to steal the client's sensitive data. It is a commonly used vulnerability found in recent websites". (Humayun, et al., 2020, pp. 3173).

pp. 266). They involve access to databases and administrator accounts, as well as the ability to manage social media fan pages.

It is worth emphasizing that information about hacker attacks doesn't always have to be publicly disclosed by libraries. In Poland, for example, there's no clear legal provision obliging these institutions to report all cybersecurity incidents. However, attacks that may result in a breach of access to library users' personal data should be reported to the President of the Personal Data Protection Office (UODO) within 72 hours, and information about such an incident should be provided to data subjects if there is a risk of their rights or freedoms being violated (GDPR Guide for Libraries, 2020, p. 138). In short, reporting incidents that threaten users' personal data should occur if there is a risk of a breach, while other cyberattacks don't always have to be publicly disclosed. The decision in such cases rests with the institution.

As a side note to these considerations, it is also worth addressing the use of data processing tools by libraries, particularly those based on generative artificial intelligence. This refers to data on reading preferences, which, during a user's search and selection process, could theoretically constitute sensitive data. The situation is similar, albeit in a much more advanced way, to that of readership statistics. Regarding the latter, Zofia Lipińska's words are interesting: "However, libraries should proceed with extreme caution in this area – maintaining statistics based on the Public Statistics Act of 29 June 1995 is one thing, but creating, for example, reader profiles for users of a specific library may be considered an abuse of statutory authority. Therefore, if a library engages in such practices or uses computer programs that recommend books based on reading history, it is worth obtaining appropriate consent, as these activities may be considered reader profiling". (Lipińska, n.d.). The aspect of library user profiling (including forecasting their needs and interests, and utilizing recommendation systems that suggest books, articles, and other resources tailored to individual users), especially with the active use of generative artificial intelligence, is clearly related to the issue of library user safety. I have no doubt that in an era of increasingly widespread use of these tools, which often operate on large data sets, a responsible and transparent approach to collecting and processing user information is essential. Lack of appropriate security measures, especially user consent, can lead to privacy violations and, consequently, a loss of trust on their part. Therefore, libraries should not only ensure the technical security of their systems but also scrupulously adhere to the privacy policies regarding their employees and users, particularly those related to profiling and the processing of sensitive data. The characteristics concerning privacy protection can be found, among others, in the "GDPR Guide for Libraries" published by the Publishing House of the Polish Librarians Association. Such protection

consists in "protecting the ability of an individual or group of people to maintain the privacy of their data, personal habits and behaviors that are not publicly disclosed" (GDPR Guide for Libraries, p. 126).

THE LIBRARY AS A TARGET FOR CYBERCRIMINALS

Returning to the main topic of this article, recent years have seen a number of cyberattacks on libraries, affecting institutions both in Poland and around the world. An example is the attack on the website of the University of Warmia and Mazury Library in Olsztyn. In January 2016, a hacker blocked access to the homepage and posted an image of the "Quran" ("Haker zablokował stronę biblioteki UWM", 2016). After entering the library's address in a search engine, a message appeared stating that the website had been hacked: "HaCked By Fr13nds Team [#OP_WorlD]" ("Atak hakerów na serwery UWM…", 2016). The library website was unavailable for approximately 10 hours. In this case, no user personal data was leaked. An employee from the library's computerization department admitted in an interview with Radio Olsztyn that hackers managed to find a bug on the website and ruthlessly exploited it. The primary problem, it seems, was the use of publicly available ready-made solutions. The employee admitted to a journalist: "Sometimes I use ready-made solutions that are made available. Unfortunately, they simply hacked through one of the plugins" ("Atak hakerów na serwery UWM…", 2016). The simplest solution to avoid this problem would be to avoid using unverified, publicly available solutions and to regularly update and audit the library's software.

In January 2019, the Central Military Library (CBW) reported that the Ministry of National Defense's Computer Incident Response System Support Center had observed phishing attacks targeting library users. The senders of the messages impersonated CBW employees and informed them of the need to return books from a list, which included a link. Clicking the link downloaded malware. The library stated on its website that such messages should be deleted without clicking the link. It also presented detailed characteristics of phishing emails in an exemplary manner. This message was supplemented by a screenshot of a sample fake email, allegedly sent by the Central Military Library. In reporting the attack, the library assured users that their data was secure and had not been disclosed. Users were also instructed to exercise extreme caution when using email (Central Military Library, 2019).

Another example from Poland: On the night of January 5-6, 2024, an attack was carried out on the Data Processing Center of the University of Zielona Góra. As a result, the library system and the Zielona Góra Digital

Library, among others, were blocked. A spokeswoman for the University of Zielona Góra reported that as a result of the hacking attack, the ability to read virtual machine files containing personal data of employees and students was temporarily blocked (Łukasiewicz, 2024). The Akira group was behind the attack, and the ransom demanded was $750,000. The university did not pay it (May, 2024). According to Katarzyna Doszczak from the University of Zielona Góra press office, the university fell victim to a ransomware attack (May, 2024). To be more precise, according to the European Cybersecurity Agency (ENISA), ransomware has been the most devastating type of cyberattack in the last decade (Knowledge Base. Service of the Republic of Poland, 2022). Małgorzata Poniatowska-Jaksch noted that in 2024, cybercriminals using this type of solution increasingly used services available on the dark web instead of their own programs (Poniatowska-Jaksch, 2024, p. 7). It is worth noting that in the case of the University of Zielona Góra, administrators managed to recover the university's IT systems, which have an IT resource monitoring system in place (May, 2024). However, it took ten days for all digital services to be restored (University of Zielona Góra. Computer Center, 2024).

It is not just large institutions that are vulnerable to attacks. Smaller libraries, and even their branches, can also be targeted by cybercriminals. Take, for example, the case of a library in the Lublin Voivodeship. On February 9, 2019, the server of the Municipal Public Library in Kraśnik was attacked by hackers. According to media reports, an employee noticed a message in English on the server informing someone that the branch's database had been deleted. According to the Library's director, "There was also information that if we wanted to recover the database, we had to pay in Bitcoins" (Antoń-Jucha, 2019). Due to the risk of unauthorized access to users' personal data, the matter was reported to the Office for Personal Data Protection and to the police (Antoń-Jucha, 2019). In this institution's case, on March 28, 2019, a notice about the incident appeared on its main website, giving information about the risk of disclosing users' personal data (Krasnik Municipal Public Library, 2019). The library provided detailed information about the possible consequences of unauthorized use by criminals. It also assured users that the latest version of the library system, which uses encryption of stored personal data, had been installed, which is intended to prevent or significantly impede unauthorized access to sensitive resources in the future (Krasnik Municipal Public Library, 2019).

The latest example from Poland concerns a situation that occurred in July 2025. The Rudy Library is a branch of the Kuźnia Raciborska Municipal Public Library. Its Facebook fan page was attacked and its employees lost access. "Our previous account was hacked, and despite numerous attempts, we are unable to recover it. Over five years of work,

memories, events, photos, comments, and hearts... went up in smoke", we read on the Library's new fan page (Rudy Library, 2025). This example demonstrates that social media account takeovers can be caused by a hacker attack, which essentially results in the blocking of the fan page and the inability to access the institution's published content. In the case of the Rudy Library, despite numerous attempts the previous account could not be recovered. The institution launched a new fan page and appealed to the online community for help in rebuilding trust and reach, asking for likes and shares about the new page.

It is worth remembering that account takeovers by unauthorized individuals can not only lead to data loss but can also expose libraries to other problems (e.g., impersonation of the institution, sending spam and other content, accessing sensitive data). Therefore, it is essential to implement appropriate security measures, including strong and unique passwords and two-factor authentication. Librarians' awareness of online account security and mandatory cybersecurity training are crucial. Implementing at least a few basic rules significantly increases the security of library social media accounts and helps avoid many serious consequences for both the institution and its users.

To summarize the above, it is worth mentioning that the number of cyberattacks on various public institutions and companies is growing in Poland. In 2024, there was a 60% increase in security incidents (over 111,000 cases). This increase was particularly noticeable in the public sector (Jaśkowiak, 2025). It is also hard to disagree with the words of the creators of the website SecurityBsides that "more and more criminals will start using artificial intelligence, which will make attacks more complex and harder to detect. Therefore, organizations should invest in modern protection systems and intensify employee education in cybersecurity" (SecurityBsides, 2025). It is worth noting that the issue of cybercriminals' use of artificial intelligence was also recently addressed in an article in "Stołeczny Magazyn Policyjny" (Pohoska, 2025).

Of course, hacker attacks aren't limited to Polish libraries. Examples of such situations from abroad can be found in Edward M. Corrado's article (Corrado, 2024, p. 84). It is worth noting that recent years have seen a series of events that have significantly disrupted the functioning of these institutions in various countries. To further illustrate the scale of the threat, below are two of the most well-known incidents that have significantly impacted the perception of the world of libraries in the digital age. These examples also provide important lessons in the need to implement effective security measures and to be aware of the risks associated with cybersecurity, which is constantly evolving and requires constant monitoring and adaptation to new threats.

The Toronto Public Library (TPL) is one of the largest public libraries

in the world, with over four million visitors annually and 1.2 million cardholders (Wyganowski, 2024). The library has 100 branches. On October 28, 2023, a ransomware attack was launched against the institution (Enis, 2024). The attack was orchestrated by the cybercriminals Black Basta group. In 2023, this group was considered one of the most dangerous (Canadian Centre for Cyber Security, 2024, p. 22). "The group uses a double extortion tactic, encrypting the victim's data and servers, as well as ransoming their sensitive data on their public leak site" (Mafera, 2024, 115). Cybercriminals gained unauthorized access to the library network, encrypted network resources, and stole the personal data of users, staff, and volunteers (Wyganowski, 2024). Up to 900 GB of data, containing 780,000 files, is estimated to have been stolen (Bains, 2024). This data had been collected by the library since 1998 (Wyganowski, 2024). It is worth noting that there is no evidence that the stolen data was published online. Nor is there any basis to claim it was disseminated in any way.

The attack resulted in the shutdown of most of the library's and its branches' IT systems, including the main website, electronic catalogues, public computers, printers, and access to digital collections. "Although TPL managed to keep all of its 100 branches open and host programs throughout the ordeal, patrons were unable to access their library accounts online or use the library's computers for more than two months. And while TPL has also continued to manually check out print books and other physical materials, the library has been unable to process holds or check the materials back in when they are returned" (Enis, 2024). Following the recommendations of cybersecurity experts, the institution did not pay the ransom (reported by the Toronto Star to be as much as $10 million), notified the City of Toronto and its cybersecurity team, the Toronto Police, and the Royal Canadian Mounted Police (Enis, 2024). Corrective measures were also implemented, including modernizing technical security measures and restoring services (Bains, 2024). The attack became a symbol of the growing threat to public institutions from cybercrime, emphasizing both the importance of protecting IT infrastructure and the importance of transparently informing victims and the public about the impact of such incidents. It was also one of the most serious cyberattacks on a public institution in Canada and worldwide.

It is worth noting that an attacked institution doesn't always refuse to pay the ransom. Cybersecurity experts have recommend against doing so, even if the costs of recovering data exceed the ransom. Individual countries are also implementing regulations addressing such situations. For example, according to the UK's national policy, formulated by the National Cyber Security Centre (NCSC), no payments should be made in the event of a ransomware attack (Mayard, 2024). It is also clear that paying a ransom encourages cybercriminals to launch further attacks (Breeding, 2024).

However, looking at the reality of educational institutions, it is apparent that there is no clear-cut approach to this problem. Natalie Schwartz, for example, writes that over half of universities (56% of 200 universities in 14 countries) that fell victim to ransomware attacks paid the ransom to recover lost data (Schwartz, 2023). The matter is not as straightforward as it might seem at first glance.

The second ransomware cyberattack I describe occurred at the British Library, interestingly also on October 28, 2023. This library is considered the largest in the world. This makes it even more difficult to imagine a situation where this institution loses its capacity to function and is unable to offer even its basic services. Cybercriminals working with the Rhysida group, previously known for attacks on government institutions and hospitals, among other things, hacked into the library's IT systems. The group stole (and destroyed) data, encrypted a significant portion of the servers, and blocked all users from accessing the library network. As part of their illegal activities, files from the finance, technology, and human resources departments were copied (Mayard, 2024). The cybercriminals demanded a ransom of 20 bitcoins—nearly £600,000 (Houghton, Winterburn & Ken Oakley, 2025). Following the British Library's refusal to pay, hackers published approximately 600 GB of stolen resources on the dark web, including user personal data and employee documents (Mayard, 2024).

As a result of the attack on the British Library, its services were unavailable. Marshall Breeding writes that "practically all parts of the BL's technology infrastructure were impacted, including the ILS, the catalog, the many systems supporting the library's massive digital collections, request and retrieval services, and even the Wi-Fi network" (Breeding, 2024). Moreover, library users did not have access to its physical collections. (Breeding, 2024). The library's website and staff email were also blocked (Fiscus, 2024). Restoring the library system to full functionality following such an attack was a difficult and lengthy process. Although backups of digital collections and metadata existed, the lack of a functioning infrastructure to restore this data posed a significant obstacle to recovery (Öykü, 2024). For example, access to the online catalog was restored only on January 15, 2024, but without the ability to order documents (Fiscus, 2024).

Following the attack, the British Library took steps to promote transparency, publishing a detailed incident report in 2024 (British Library, 2024) and collaborating with the UK National Cyber Security Centre (NCSC) and law enforcement agencies. A website was also created (www.bl.uk/about/cyber-attack), where users can find answers to frequently asked questions about the cyberattack. This includes information on the consequences of the leak of library users' personal data. In an official statement from the Information Commissioner's Office (ICO), published

on April 30, 2025, the British Library was described as an institution that was transparent about the attack and its effects. The library's willingness to share information about the system's weaknesses, remedial actions taken, and cooperation with the NCSC and law enforcement agencies to improve data security were also praised (Information Commissioner's Office, 2025).

POSSIBILITIES FOR COUNTERING CYBER THREATS

What cybersecurity strategies should libraries implement? There are at least several answers to this question. Without a doubt, digital transformation has improved the accessibility and comfort of library services. At the same time, it has increased the risk of various cyberattacks, including those aimed at exploiting security vulnerabilities in library systems and insufficient staff and user awareness. It is also important to remember that cyber threats in libraries are constantly evolving, requiring continuous adaptation and technological innovation in this area as well. As a result, libraries must face challenges related to data protection, IT infrastructure, and educating staff and users about digital security. Among other things, systematically updating security systems is essential. Libraries must also be ready to utilize advanced IT tools to detect and analyze threats in library systems. This also applies to the application of AI in libraries (e.g., as part of service automation and efficiency; personalized user service; more effective information search and resource discovery). Particularly in large libraries, additional tools for effective control and continuous monitoring of the increasingly complex digital library environment may also be necessary. This is especially important in the context of real-time threat detection and response. Importantly, tools are already available today that provide insight into data at all levels of the IT infrastructure. These solutions also utilize machine learning mechanisms, continuously monitoring and analyzing telemetry data from the network infrastructure. Examples of such tools can be found in the literature, including DarckTrace, Cisco Network Analytics, and IBM QRader (Ghazal, et al., 2022).

Importantly, artificial intelligence can pose additional challenges for libraries. One example is AI tools that process user data to further personalize services. Remember that to operate efficiently, AI tools often require access to vast amounts of data, which may contain sensitive information. Therefore, libraries should obtain users' (informed!) consent before automatically analyzing their activity in the library system and allow them to opt out or limit data processing and further sharing (Kavak, 2024, p. 46). The solution in this case may be adopting appropriate privacy

policies, implementing proven data management solutions, and regularly auditing AI systems (Kavak, 2024, p. 46).

To improve cybersecurity, libraries can also use blockchain technology and biometric authentication for access control. Blockchain can, among other things, help secure digital resource management and data transfer (Akor, et al., 2024). However, the potential uses of this technology are much broader. In his doctoral thesis, Piotr Dariusz Chmielewski aptly identifies potential areas for implementing this technology in academic libraries. These include: data storage; managing licensing agreements and digital rights; supporting scholarly communication and open science; metadata management; managing data, holdings, and collections; managing the loan process; user services; and organizing and certifying training (Chmielewski, 2023, pp. 137-149). It is clear, therefore, that all of these application areas are, to a greater or lesser extent, related to cybersecurity.

AI and blockchain are technologies that can significantly help prevent or mitigate cyberthreats. However, despite their enormous potential (including streamlining administrative processes and strengthening the resilience of library IT infrastructure), they also pose challenges related to their implementation. Importantly, integrating these technologies with library security systems requires meticulous planning, investment in staff training, and rigorous adherence to best practices in cybersecurity management (Akor et al., 2024). The role of educating library staff and users about cybersecurity threats is particularly important here. Training, lectures, tutorials, etc., are crucial for identifying potential threats in the future and for responding to them (Panda & Kaur, 2024).

Library directors and staff must make every effort to effectively secure the data they collect and manage. Conscious actions and technical measures are essential to increase security in the digital environment. Edward M. Corrado points to helpful documents in this regard created by government agencies in several countries, as well as commercial and non-profit organizations working in the field of cybersecurity. Based on these documents, Corrado formulated recommendations for libraries, which are presented in a concise form below:

1. Develop a comprehensive cybersecurity plan that includes risk mitigation strategies and cyber incident response procedures. This plan should define responsibilities for monitoring data security and address privacy, legal, and ethical aspects of security policies.

2. Provide periodic training for employees on protecting user data and confidential information, with a particular emphasis on recognizing threats and implementing cybersecurity best practices.

3. Prepare user briefings on protecting privacy and data confidentiality, including information about vendors collecting search histories. Highlight

the risks associated with using illegal sources, such as "shadow libraries", and the risk of credential theft.

4. Require employees to use strong passwords and multi-factor authentication.

5. Create an inventory of all digital resources and components of the library's technological infrastructure. This inventory should include information about the data stored in various systems and the potential consequences of data loss or security breaches.

6. Limit access to non-public data, especially user data. Only employees whose duties involve using such resources should have access. These employees should have received appropriate training in managing confidential data. Encryption is possible. The library should only collect data that is necessary.

7. Regularly backup data according to the 3-2-1 strategy, i.e., maintaining three copies on two different media, with one copy stored off-site, e.g., in the cloud.

8. Systematically update library system software to eliminate security gaps.

9. Assess technology and software used in libraries through the lens of cybersecurity, taking into account provisions in contracts with vendors, as well as audits and security certifications (e.g., ISO/IEC 27001). Employees should be familiar with the terms and conditions of use of systems, individual services, and resources, particularly regarding the storage by vendors of data and information about user activity (e.g., search history).

10. Consider the financial and staffing needs associated with maintaining cybersecurity. In the event of a cyberattack, the costs of restoring infrastructure operations may significantly exceed the costs of counteracting such an attack in advance (Corrado, 2024, pp. 87-92).

What other recommendations should be considered to protect libraries from cyberattacks? A British Library report published in March 2024 provides guidance. The report aims, among other things, to help other institutions implement appropriate procedures. It contains 16 key conclusions worth considering when planning digital security solutions for libraries. These include: increasing network monitoring capabilities; retaining on-call external security expertise; fully implementing multi-factor authentication; introducing policies to limit personal use of library IT; collaborating with other institutions in the industry and sharing information on cyber threats and cybersecurity best practices; implementing government standards; implementing network segmentation; and managing systems lifecycles to eliminate legacy technology (British Library, 2024).

The authors of the "GDPR Guide for Libraries", point out, among other things, the possibility of restricting external access to library equipment.

They also consider it good practice to separate the internal (library) network from external resources (GDPR Guide for Libraries, 2020, p. 127).

The authors also recommend restricting the connection of private media to library computers and disabling the autorun function for all media, as well as limiting the freedom to connect USB drives to computers (allowing only devices authenticated by an IT specialist). It is also important to scan external data media with antivirus software before each use and to destroy old devices, drives, etc., so as to prevent data recovery. Furthermore, they recommend regularly deleting unnecessary files/messages and protecting mobile devices used in the library (GDPR Guide for Libraries, 2020, p. 127).

CONCLUSIONS

Due to the increasing use of digital technologies and networked environments, libraries are highly vulnerable to various threats, including hacking. The threat of aggressive and destructive cyberattacks is greater than ever before. Cybercriminal groups can significantly disrupt the functioning of these institutions, endangering confidential data and undermining trust. Various forms of attacks can impact library operations in numerous ways, leading not only to service disruptions but also to privacy and data security breaches and damage to the institution's reputation. In a digital world where more and more resources and services are being made available online, libraries are becoming an attractive target for cybercriminals, requiring continuous improvement in data protection standards and IT systems. Only a comprehensive approach, combining modern technologies, appropriate procedures, and staff and user education, will effectively minimize risk and ensure secure access to information.

BIBLIOGRAPHY

Akor, S. O., Nongo, C., Udofot, C., & 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*, 2, https://doi.org/10.25159/3005-4222/16671.

Akademia NASK (n.d.). "Cyberlekcje. Phishing". Retrieved August 12, 2025, from https://tinyurl.com/2ux578ds.

Antoń-Jucha, A. (2019, February 28). "Atak hakerski na bibliotekę. Ktoś mógł uzyskać dostęp do danych osobowych". Retrieved August 12, 2025, from użytkownikówhttps://www.dziennikwschodni.pl/krasnik/atak-hakerski-na-biblioteke-ktos-mogl-uzyskac-do-danych-osobowych-uzytkownikow,n,1000238133.html.

"Atak hakerów na serwery UWM. Kłopoty ze stroną Biblioteki Uniwersyteckiej" (2016, January 21). Retrieved August 12, 2025, from https://student.wm.pl/330054,Atak-hakerow-na-serwery-UWM-Klopoty-ze-strona-Biblioteki-Uniwersyteckiej.html.

Bains, H. (2024, December 3). "MR23-00112: Toronto Public Library Closing Letter". Retrieved August 12, 2025 from https://tinyurl.com/3hmkftdz.

Baza Wiedzy. Serwis Rzeczypospolitej Polskiej. (2022, October 24). "Ransomware – jedno z najpoważniejszych zagrożeń w cyberprzestrzeni". Retrieved August 12, 2025 from https://www.gov.pl/web/baza-wiedzy/ransomware--jedno-z-najpowazniejszych-zagrozen-w-cyberprzestrzeni.

Breeding, M. (2024). "Libraries Under Cyberattack". *Computers in Libraries*, vol. 44 No. 2 — March 2024. Retrieved August 12, 2025 from https://www.infotoday.com/cilmag/mar24/Breeding--Libraries-Under-Cyberattack.shtml.

British Library. (2024, March 8). "Learning lessons from the cyber-attack. British Library cyber incident review". Retrieved August 12, 2025 from https://cdn.sanity.io/files/v5dwkion/production/99206a2d1e9f07b35712b78f7d75fbb09560c08d.pdf.

Canadian Centre for Cyber Security. (2024). "National Cyber Threat Assessment 2025-2026". Retrieved August 12, 2025 from https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf.

Castellanos-Rivadeneira, J; Valerio-Ureña, G. (2020). "The Hacker Ethic and the Effective Use of ICTs in Alternative Economic Cultures: the case of Ik' ta K'op in Abasolo, Chiapas". *Development Studies Research*, 7, 1, pp. 131-140, https://doi.org/10.1080/21665095.2020.1816838.

Centralna Biblioteka Wojskowa. (2019, January 4). "Ostrzeżenie dla użytkowników Centralnej Biblioteki Wojskowej dotyczące wiadomości phishingowej. Ostrzeżenie przekazane przez zespół MIL-CERT". Retrieved August 12, 2025, from https://archiwum-cbw.wp.mil.pl/pl/1_311.html.

Chmielewski, P. D. (2023). *Obszary i potencjał zastosowania technologii blockchain w polskich bibliotekach akademickich*. Doctoral dissertation. Uniwersytet Mikołaja Kopernika w Toruniu. Wydział Filozofii i Nauk Społecznych. Instytut Badań Informacji i Komunikacji.

Corrado, E. M. (2024). "Cybersecurity and Libraries". *Technical Services Quarterly*, 41(1), 82–95. https://doi.org/10.1080/07317131.2023.2300530.

Czub-Kiełczewska, S., Wojciechowski, Ł. (Eds). (2020). *Poradnik RODO dla bibliotek.* Wydawnictwo Naukowe i Edukacyjne Stowarzyszenia Bibliotekarzy Polskich.

Enis, M. (2024, January 17). "Toronto Public Library Recovers from Ransomware Attack". Retrieved August 12, 2025, from https://www.libraryjournal.com/story/toronto-public-library-recovers-from-ransomware-attack.

Facebook Fanpage. Biblioteka Rudy. (2025, 9 July). Retrieved August 12, 2025, https://www.facebook.com/profile.php?id=61578147062312.

Fiscus, M. (2024). "Knowledge Held Hostage: What the British Library Ransomware Attack Can Teach Us". *College & Research Libraries*, 85(5), 628. doi:https://doi.org/10.5860/crl.85.5.628.

Ghazal, T. M., Hasan, M. K., Zitar, R. A., Al-Dmour, N. A., Al-Sit, W. T., & Islam, S. (2022). "Cybers Security Analysis and Measurement Tools Using Machine

Learning Approach". *2022 1st International Conference on AI in Cybersecurity, ICAIC 2022*. https://doi.org/10.1109/ICAIC53980.2022.9897045.

"Haker zablokował stronę biblioteki UWM" (2016, January 25). Retrieved August 12, 2025, from https://radioolsztyn.pl/haker-zablokowal-strone-biblioteki-uwm/01258151.

Houghton, F., Winterburn, M., & Oakley, K. (2025). "The 2023 Rhysida Ransomware Attack on the British Library: Prioritisation, Expertise, and Funding Issues". *Information Technology and Libraries*, 44(1). https://doi.org/10.5860/ital.v44i1.17112.

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study". *Arabian Journal for Science and Engineering*, 45, 3171–3189. https://doi.org/10.1007/s13369-019-04319-2.

Information Commissioner's Office. (2025, April 2025). Statement on British Library's 2023 ransomware attack. Retrieved August 12, 2025, from https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/04/statement-on-british-library-s-2023-ransomware-attack/.

Işık, Ö. (2024, September 30). "Full transparency: 10 lessons from the cyber-attack on the British Library". Retrieved August 12, 2025, from https://www.imd.org/ibyimd/technology/full-transparency-10-lessons-from-the-cyber-attack-on-the-british-library/.

Janczewski, R. (2022). "Cyberbezpieczeństwo w życiu społecznym". In: W M. Butrymowicz, J. Stala (Eds), *W służbie społeczeństwu. Polska w obronie praw człowieka na świecie i w kraju* (pp. 139-158). Uniwersytet Papieski Jana Pawła II w Krakowie. Wydawnictwo Naukowe.

Jaśkowiak, J. (2025). "Cyberzagrożenia w Polsce 2025: Najczęściej atakowana infrastruktura krytyczna". Retrieved August 12, 2025, from https://mikrokontroler.pl/2025/04/25/cyberzagrozenia-w-polsce-2025-najczesciej-atakowana-infrastruktura-krytyczna/.

Kavak, A. (2024). "Ethical considerations and privacy concerns in AI-enabled libraries". In: I. M. Khamis (Ed.), *Applications of Artificial Intelligence in Libraries* (pp. 45–76). https://doi.org/10.4018/979-8-3693-1573-6.ch003.

Lipińska, Z. (n.d.). "RODO w bibliotece – na co jeszcze należy zwrócić uwagę?" Retrieved August 12, 2025, from https://www.biblioteki.gropius.com.pl/blog/rodo-w-bibliotece-na-co-jeszcze-nalezy-zwrocic-uwage.html.

Łukasiewicz, A. (2024, January 11). "Uniwersytet Zielonogórski o ataku hakerów: 'Nie ma dowodów na wyciek danych.'" Retrieved August 12, 2025, from https://zielonagora.wyborcza.pl/zielonagora/7,35182,30584000,uniwersytet-zielonogorski-o-ataku-hakerow-nie-ma-dowodow-na.html.

Mafera, J. (2024, August 31). "Black Basta Cybersecurity Advisory: Endpoint Protection for Healthcare". Retrieved August 12, 2025, from https://www.cyberdefensemagazine.com/black-basta-cybersecurity-advisory-endpoint-protection-for-healthcare/.

Maj, M. (2024, January 10). "[Aktualizacja] Uniwersytet Zielonogórski ofiarą ataku ransomware". Retrieved August 12, 2025, from https://niebezpiecznik.pl/post/uniwersytet-zielonogorski-ofiara-ataku-doszlo-do-zaszyfrowania-danych/.

Mayard, S. (2024, November 7). "The British Library Cyber Attack – One Year La-

ter". Retrieved August 12, 2025, from https://thegdprcomplianceconsultancy.co.uk/british-library-cyber-attack-one-year-later/.

Michałowska, M., & Hassa, E. (2022). "Cyberbezpieczeństwo a zarządzanie tożsamością w czasie pandemii – analiza przykładów zagrożeń". *Studia Administracji i Bezpieczeństwa*, 12(12), 99-118. https://doi.org/10.5604/01.3001.0015.9238.

Miejska Biblioteka Publiczna w Kraśniku (2019, March 28). "Aktualności". Retrieved August 12, 2025, from https://biblioteka.krasnik.pl/index.php/aktualnosci-gora?start=210.

Nurochman, A., Astuti, E. Y., & Widianingtias, S. (2024). "Analisis Keamanan Siber Sistem Informasi Perpustakaan di Perpustakaan Universitas Jenderal Soedirman". *BACA: Jurnal Dokumentasi Dan Informasi*, 45(1), 49–64. https://doi.org/10.55981/baca.2024.1237

Oladokun, B., Oloniruha, E., Mazah, D., & Okechukwu , O. (2024). "Cybersecurity Risks: A Sine Qua Non for University Libraries in Africa". *Southern African Journal of Security*, 2. https://doi.org/10.25159/3005-4222/15320.

Panda, S. & Kaur, N. (2024). "Cyber Sentinels: Exploring the Cybersecurity Awareness of Indian Library Professionals". In: I. Khamis (Ed.), *Applications of Artificial Intelligence in Libraries* (pp. 78-108). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-1573-6.ch004.

Pohoska, K. (2025, March 3). "Cyberprzestępczość – prognozy na 2025 rok", *Stołeczny Magazyn Policyjny*. Retrieved August 12, 2025, from https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html.

Poniatowska-Jaksch, M. (2024). "Ransomware w sektorze ochrony zdrowia – przyczyny, konsekwencje". *Kwartalnik Nauk O Przedsiębiorstwie*, *74*(4), 5–16. https://doi.org/10.33119/KNoP.2024.74.4.1

Putri, C. A., Anwar, R. K. , Amar, S. C. D. , & Rukmana, E. N. (2024). "Keamanan Informasi dan Privasi Pengguna dalam Layanan Perpustakaan Digital". *Media Pustakawan*, 31(3), 266–276. https://doi.org/10.37014/medpus.v31i3.5317.

Rahim, M. A. A. A., Mohamad, A. M., Kamaruddin, S. & Wan Rosli, W. R. (2024). "Data Leaks Through Public Digital Document Libraries: A Growing Concern in Relation to Personal Data Protection and Cyber Security Regulations", 2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS), Kuala Lumpur, Malaysia, 2024. https://doi:10.1109/NETAPPS63333.2024.10823567.

Saha, R. (2024). "Data Privacy and Cyber Security in Digital Library Perspective: Safe Guarding User Information". *International Journal of Scientific Research in Engineering & Management*, April 2024. https://doi:10.55041/IJSREM30761.

Schwartz, N. (2023, August 4). "Over half of higher ed. institutions hit by ransomware paid to get data back, survey finds". Retrieved August 12, 2025, from https://www.highereddive.com/news/higher-education-ransomware-paid-ransom-college/689929/.

SecurityBsides. (2025). "Ataki hakerskie w Polsce 2025 – przegląd zagrożeń i prognozy". Retrieved August 12, 2025, from https://securitybsides.pl/ataki-hakerskie-w-polsce-2025/.

Uniwersytet Zielonogórski. Centrum Komputerowe. (2024, January 7). "Aktualności. Uniwersytet Zielonogórski zaatakowany!" Retrieved August 12, 2025,

https://ck.uz.zgora.pl/aktualnosci/uniwersytet-zielonogorski-zaatakowany-15.html.

Wasilewski, J. (2013). "Zarys definicyjny cyberprzestrzeni". *Przegląd Bezpieczeństwa Wewnętrznego*, 5(9), 225–234.

Wyganowski, A. (2024). "Cyber risks, AI, impacts lessons learned from recent attacks". Retrieved August 12, 2025, from https://www.dri.ca/docs/2A-Cyber_Risks_AI_Impacts_and_Lessons_Learned_April_11_2024.pdf.