Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.3456/cal/215900

Building a resilient data ecosystem in higher education – a strategic approach to information management in cyberspace

Monika NOWIKOWSKA
Akademia Sztuki Wojennej
ORCID: 0000-0001-5166-8375
E-mail: m.nowikowska@akademia.mil.pl

Abstract

The article presents the importance of creating a secure and resilient data ecosystem at universities in the context of growing cyber threats. The Author analyzes ways of managing information and indicates how academic institutions can develop strategies to strengthen data protection and effective use.

The subject of the article is the construction and management of a data ecosystem in higher education, with particular emphasis on information security in the digital environment.

The following methods were used in the study: analysis of literature on cybersecurity, review of academic data management practices, case studies of universities using modern information protection models.

Key elements of a resilient data ecosystem were identified: integration of IT systems, security policies, user education, monitoring of cyber events, and continuous improvement of procedures. It was emphasized that institutions using a strategic approach achieve a higher level of stability and security.

Effective data management in higher education requires a holistic strategy that encompasses technology, organization, and security culture. Universities should invest in the development of digital competencies, protection systems, and incident response procedures to ensure lasting resilience in cyberspace.

Keywords

cyberspace, data ecosystem, higher education, information management

This article was written as part of an international project "Research Universities" (Res-Uni), funded under the Erasmus+ Key Action 2 - Capacity Building in the Field of Higher Education (CBHE).

Project number: 101179358 Erasmus+ Key Action 2 - Capacity Building in the Field of Higher Education.

General remarks

The dynamic development of digital technologies has made data one of the most valuable resources for many institutions. It is widely accepted that all information is a strategic commodity and must be protected against unauthorised disclosure[1]. Data and information are also a fundamental resource for higher education. Universities and colleges collect and process ever-increasing volumes of information, ranging from administrative and financial data, through research results and laboratory data, to the personal data of students and staff[2]. In this context, a key challenge is to build a resilient data ecosystem that combines security, accessibility, quality and regulatory compliance in an environment full of cyber threats[3]. Modern universities operate in a highly computerised environment, where data flow is the basis for the implementation of their teaching, research and administrative missions. Data has become the fuel for decision-making processes, a tool for assessing the quality of education, an element of building scientific prestige and a resource with commercialisation potential[4]. At the same time, the growing complexity of IT systems and the intensification of cyber threats mean that the traditional approach to security is proving insufficient. It is becoming necessary to build a resilient data ecosystem – one that is multidimensional, flexible and based on continuous adaptation.

The subject of consideration is the data ecosystem in universities – what is it and why does it require special protection? The key pillars of building a resilient data ecosystem were also analysed. In order to formulate the direction of the analysis and define the field of research, the following research questions were posed at the beginning of the article. How can universities build a resilient and secure data ecosystem that will enable effective information management in the face of a growing number of threats in cyberspace? Specific questions include: what elements make up the data ecosystem in higher education and which of them are crucial for its resilience? What are the most common cyber threats targeting academic institutions? What strategies and tools can be used to improve information security at universities? What role do management procedures, security policies and cyber hygiene culture play in building institutional resilience? How can cloud solutions, automation and artificial intelligence support data management? Finally, what practical implementation models can be used to develop the digital resilience of universities? Asking these questions organises the course of further consideration and allows the analysis to focus on the key aspects of the problem.

The article adopts a qualitative research approach based on the analysis of source materials, case studies and a comparison of solutions used in various higher education institutions. The methodology included the following elements:

[1] K. Chałubińska-Jentkiewicz, M. Nowikowska, Ochrona informacji w cyberprzestrzeni, Warsaw 2021, p. 19.
[2] J. Taczkowska-Olszewska, Pojęcie i rodzaje danych osobowych [in:] J. Taczkowska-Olszewska, M. Nowikowska, Prawo do informacji publicznej. Informacje niejawne. Ochrona danych osobowych, Warsaw 2019, p. 245.
[3] K. Chałubińska-Jentkiewicz, M. Nowikowska, Ochrona danych osobowych w cyberprzestrzeni, Warsaw 2021, p. 50.
[4] See A. Stępień-Banach, Ochrona danych osobowych w szkołach wyższych [in:] D. Wociór (ed.), Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego, Warsaw 2016, pp. 271-280.

a review of the literature on the subject, a comparative analysis, case studies and a synthesis of conclusions and recommendations. An analysis of available scientific sources, industry reports and standards for information security and data management (e.g. ISO/IEC 27001, GDPR[5]) was carried out. The aim of the review was to determine the current state of knowledge and identify research gaps in the field of digital resilience of universities. Examples of cyber attacks on academic institutions were taken into account. Case studies illustrate the practical application of theory and assess the effectiveness of solutions in real-world conditions. Based on literature analysis, comparisons and case studies, a set of conclusions and strategic recommendations for higher education institutions was developed. The synthesis provides the basis for proposing a model for building a resilient data ecosystem.

The selected research methods enabled a comprehensive view of the problem from a theoretical and practical perspective. The qualitative approach was appropriate due to the complexity of the phenomenon and the diversity of factors affecting the cybersecurity of universities. The use of case studies and comparative analysis allowed for the identification of effective solutions.

Resilient data ecosystem in higher education

The data ecosystem in higher education is a set of processes, tools, digital resources and people who create, store and use information for teaching, research and institutional management purposes. Its resilience means the ability to ensure continuity of operation in the face of cyber attacks and failures[6], to secure the confidentiality, integrity and availability of data[7], to effectively manage the information lifecycle (from acquisition to archiving)[8], to prevent data leaks and misuse[9], and to scale solutions as the infrastructure and needs of the university develop.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) (OJ EU L 119 of 2016).

[6] P. Zaskórki, J. Woźniak, Sprawność informacyjna a odporność na ryzyko utraty ciągłości działania współczesnej organizacji, „Studia i Prace. Kolegium Zarządzania i Finansów" 2024, Zeszyt Naukowy 199, p. 55.

[7] J. Łuczak, M. Tyburski, Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Poznań 2009, p. 12.

[8] For more details, see: K. Chałubińska-Jentkiewicz, M. Nowikowska, Ochrona informacji w cyberprzestrzeni, p. 21; R. Kowal, Zarządzanie cyklem życia aplikacji – na przykładzie Sap Solution Manager, „Studia Ekonomiczne" 2013, vol. 128, p. 41; P. Królas, Identyfikacja ryzyka związanego z krótkim cyklem życia okazji – studium przypadku, „Zeszyty Naukowe Politechniki Poznańskiej" 2019, no. 80, p. 150.

[9] A. Opalska-Kasprzak, W.A. Kasprzak, Inżynieria społeczna jako narzędzie cyberprzestępcy - analiza kryminologiczna i kryminalistyczna, „Przegląd Policyjny" 2021, no. 4(144), p. 190; J. Kwaśnik, Wpływ ataków socjotechnicznych na konstrukcję i kształt polityki bezpieczeństwa, [in:] M. Górka (ed.), Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa, Warsaw 2017, p. 40.

In an era of increasingly frequent ransomware attacks[10], phishing[11] and information manipulation, digital resilience is becoming a strategic management priority[12]. It should be emphasised that digital resilience is still a new and very broad term. Its significance for businesses is still evolving, and understanding digital resilience is followed by cloud resilience. It is commonly pointed out that digital resilience can be considered from the perspective of four key aspects: 1) cybersecurity, 2) IT system architecture, 3) risk and business continuity management, and 4) cost efficiency. The first element, cybersecurity, is the foundation of resilience in terms of prevention, detection and response to cyber threats. The next element is IT system architecture, ranging from infrastructure to the architecture of specific solutions and the manufacturing processes of designing and building technological solutions. The third aspect is risk and business continuity management, not only in terms of critical architecture, but also individual solutions. Finally, the fourth important area of resilience is cost efficiency, which allows for the management of the risk of uncontrolled increases in technology costs[13] .

To summarise the above, it can be said that a data ecosystem is a dynamically interacting set of information resources (personal, research, teaching and administrative data), technological tools (e-learning platforms, cloud, repositories), procedures and regulations (security policies, GDPR, data licensing), users (students, teachers, IT department, external stakeholders), and finally security infrastructure (firewalls, backup systems, SOC). Unlike the business sector, the university ecosystem is particularly open and dispersed, which increases the potential for cooperation, but also vulnerability to incidents. Freedom of research and scientific data exchange require a balance between openness and control.

The key pillars of building a resilient data ecosystem include cybersecurity, data management, cloud infrastructure, organisational resilience and a culture of cyber hygiene.

---

[10] Ransomware is a popular method of fraud used by cybercriminals to convince victims to click on a link pretending to be correspondence from a trusted institution, e.g. an office or company. Ransomware is malicious software (malware) that blocks access to data or an entire computer system by encrypting files and demanding a ransom in exchange for the key to decrypt them, often in cryptocurrencies, which poses a serious threat to individual users and businesses. It usually works through malicious emails with attachments or links, and after infection, it encrypts files, demanding payment for their unlocking, often threatening to make them public. F. Radoniewicz, Ransomware [in:] K. Chałubińska-Jentkiewicz (ed.), Leksykon cyberbezpieczeństwa, Warsaw 2024, p. 215; Ch. Hadnagy, Social Engineering: The Art of Human Hacking, New Jersey 2010, pp. 106-107.

[11] Phishing is a method of cyberattack – fraud – which involves impersonating a trusted person, organisation or institution (banks, companies, portals) in order to obtain confidential data (passwords, credit card details, personal identification numbers) or infect a computer with malware, most often using fake emails, text messages or instant messages containing links to fake websites. The aim of such actions is to persuade the victim to take a specific action. Fraudsters impersonate well-known institutions and send fake emails containing links to click on or encouraging the recipient to open them. J. Jancelewicz, J. Jancelewicz, Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych, „Trzeci Sektor" 2022, no. 3–4, pp. 59-60; F. Radoniewicz, Phishing, [in:] K. Chałubińska-Jentkiewicz (ed.), Leksykon cyberbezpieczeństwa, Warsaw 2024, pp. 198-199.

[12] A. Połowin, Cyberzagrożenia w internecie – analiza przypadków. „Cybersecurity and Law" 2024, no. 2(12), p. 117 et seq.

[13] A. Jadczak, Budowanie odporności cyfrowej w chmurze to proces ciągły, https://itwiz.pl/budowanie-odpornosci-cyfrowej-w-chmurze-to-proces-ciagly/ [access: 1.12.2025].

It should be emphasised that cybersecurity and technical resilience are the foundation for building a resilient data ecosystem in higher education. The literature on the subject indicates that the concept of cybersecurity can refer to a strictly defined area of activities related to information security (network content), communication security (transmission), and the security of networks enabling communication. The definition of cybersecurity requires the inclusion of many already defined phenomena. Such auxiliary concepts in defining cybersecurity are: information security, cybercrime[14]. Within the first pillar – cybersecurity – it is important for higher education institutions to implement, among other things, security policies compliant with standards (e.g. ISO 27001), network segmentation and access control, data encryption and the use of advanced threat detection systems (e.g. SOC)[15] .

Building a resilient ecosystem requires layered protection that includes prevention, detection, response, and recovery. Prevention boils down to measures such as using strong passwords, encryption, and multi-factor authentication. MFA is a method of securing account access that requires at least two different forms of identification, not just a password. This increases security because even if one password is stolen, the hacker will not be able to gain access without the second factor, such as a code from a mobile application or a hardware key. Detection includes log monitoring, SIEM systems[16] (modern IT security management tools), and behavioural analysis[17]. Response includes incident

[14] K. Chałubińska-Jentkiewicz, Cyberbezpieczeństwo – zagadnienia definicyjne, „Cybersecurity and Law" 2019, no. 2(2), p. 13.

[15] A. Ferens, Cyberbezpieczeństwo i cyberryzyko w raportach zintegrowanych i sprawozdaniach zarządu operatorów usług kluczowych, „Zeszyty Teoretyczne Rachunkowości" 2021, vol. 45, no. 2, p. 46.

[16] SIEM, or Security Information and Event Management, is an advanced IT security management tool that enables organisations to monitor and analyse. The system acts as a central point for collecting data from various sources, such as servers, network devices, applications and security systems. This provides a comprehensive picture of what is happening in the IT environment. One of the key functions of SIEM is to analyse vast amounts of data to detect anomalies and potential threats. It uses advanced algorithms to correlate seemingly unrelated events and identify patterns that indicate security incidents, such as intrusion attempts or privilege abuse. SIEM operates in real time, which means that IT administrators can respond quickly to emerging threats, minimising their impact on the organisation. In addition to monitoring and analysis, SIEM also serves as a reporting tool, providing detailed data on security status, threat trends and compliance with regulations such as GDPR. This helps organisations meet audit requirements and make strategic decisions about IT security. SIEM is therefore a tool for organisations that need a centralised system for large-scale security monitoring and analysis. M. Fusiek, Co wybrać: SOAR czy SIEM? Rola SIEM i SOAR w nowoczesnym zarządzaniu bezpieczeństwem IT, https://arkanet.pl/baza-wiedzy/co-wybrac-soar-czy-siem-rola-siem-i-soar-w-nowoczesnym-zarzadzaniu-bezpieczenstw emit/?c=knowledgebase&gad_source=1&gad_campaignid=23150664929&gbraid=0AAAApZg DPGR7yGVH37hSfEswCLmEsWGf&gclid=Cj0KCQiA6NTJBhDEARIsAB7QHD0HHJazeotO9D npEb7rYlKAe_Z6KxpOh10chv5SPiQF2I1M03Xq_IUaAiOoEALw_wcB [access: 1.12.2025].

[17] UBA (User Behaviour Analytics) is a tool that can be used to increase cybersecurity. It is used in larger corporations to identify unusual activities undertaken by system users. Traditional software will not detect a compromised account or an attempt to steal data by an employee, unlike UBA. This type of software constantly monitors user activity, recording not only the websites visited, but also the time the password is entered, what files are viewed, how the mouse and keyboard are used, and what applications the user uses. This type of software can also track where the user accesses the system from, what IP address they use, and what devices they use. The main difference between UBA and traditional security methods is the focus on user behaviour, rather than just signature-based security or known threats. UBA solutions analyse user behaviour in the context of security, detect anomalies and proactively identify threats, even those previously unknown. This type of software can cause problems, including overly strict attack

response procedures and CSIRT teams[18]. Recovery, on the other hand, involves backups and business continuity plans (BCP). Infrastructure should be designed according to the "security by design" principle, taking security into account from the planning stage[19]. Paweł Kostkiewicz points out that *"security by design"* means creating software and IT equipment, network infrastructure and digital services that are secure from the ground up. Security-by-design is an approach that aims to increase the cyber resilience of public institutions and improve trust between organisations. "Both approaches can be seen – together – as a synergistic, self-reinforcing mechanism covering supply (the manufacturer/supplier perspective) and demand (the user/purchaser perspective)"[20].

The second pillar, data and data quality management and data lifecycle, includes, among other things, cataloguing and classifying information, monitoring quality, and auditing data and data processing. As part of building a resilient ecosystem, universities should create data catalogues and repositories with metadata descriptions. Data classification systems based on sensitivity are also an important element. Universities should also have data retention and access control procedures in place. Effective data lifecycle management increases process transparency and supports decision-making analytics. The final element is planning and conducting data quality and integrity audits[21]. Data quality and integrity audits are assessment processes that check whether data is accurate, consistent, complete and protected from unauthorised changes (integrity), as well as whether it is useful and effective in the company's operations (quality), which is crucial for reliable business decisions and regulatory compliance. These audits detect problems such as inconsistencies, validation errors, and lack of change tracking, and also help monetise data and improve data management[22].

The third pillar is cloud and hybrid infrastructure. Cloud computing is a model that guarantees ubiquitous, convenient, fast and on-demand access to shared computing resources (servers, storage, applications, services) via a network[23]. The literature on the subject emphasises that these resources are provided and released with minimal management and interference from the provider[24]. Computers are no longer data carriers. Data is transferred to virtual external storage. It should be emphasised that cloud computing is similar to outsourcing. It involves the use of third-party computer programs, infrastructure

---

detection sensitivity settings, which can result in a large number of false positives, denying users access to the system. Systems of this type process huge amounts of data on user behaviour and habits, generating ethical problems. P. Zaborowski, M. Kozłowski, Zastosowanie sztucznej inteligencji w rozwiązaniach cyberbezpieczeństwa, „Cybersecurity and Law" 2025, no. 1(13), p. 130.

[18] M. Nowikowska, The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland [in:] K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cybersecurity in Poland, Legal aspects, Springer Cham 2022, p. 224.

[19] For more details, see: P. Kostkiewicz, „Security-by-design" – bezpieczeństwo systemowe ICT – w przepisach, normach i praktyce, „Przegląd telekomunikacyjny" 2025, no. 4, pp. 42-53.

[20] Ibid., p. 42.

[21] M. Nowikowska, Zasada rozliczalności i przejrzystości – rozwiązania w zakresie niezależnego audytu w świetle postanowień aktu o usługach cyfrowych, „Europejski Przegląd Sądowy" 2025, no. 3, p. 37 et seq.

[22] Ibid., p. 41.

[23] M. Nowikowska, Procesowa kontrola danych informatycznych w chmurze obliczeniowej, „Cybersecurity and Law" 2023, no. 1(9), p. 169.

[24] J. Wrona, Z. Zawadzka, Cyberbezpieczeństwo w prawie własności intelektualnej [in:] C. Banasiński (ed.), Cyberbezpieczeństwo. Zarys wykładu, Warsaw 2018, pp. 377-378.

and programming tools hosted by the provider to create your own applications[25]. The cloud enables scalability and cost reduction, but requires a shared responsibility model, secure access (MFA, VPN), disaster recovery plans and offline backups. Moving data to the cloud enables scalability[26], but requires a well-thought-out responsibility model.

A private cloud is an infrastructure created exclusively for the needs of a single organisation. It may be physically located at the company's headquarters or managed by an external operator, but only selected users have access to it. This model ensures maximum control over data, complete security and the ability to adapt systems to specific legal, industry or technological requirements. It is created for the needs of a specific (single) organisation and is not accessible to other entities[27].

Public cloud – available to all interested recipients. It is a solution in which IT resources, such as servers, disk space, computing power or applications, are made available by external providers via the Internet. These services operate in data centres belonging to companies such as Amazon Web Services, Microsoft Azure and Google Cloud Platform[28].

A hybrid cloud is a model that combines elements of public and private clouds, enabling the seamless transfer of data and applications between environments depending on business needs. In practice, this means that sensitive data or key systems can operate in a private environment, while seasonal workloads and less critical processes can operate in a public environment. This approach offers great flexibility, allows for cost and performance optimisation, and at the same time enables compliance with security and regulatory requirements[29].

Table 1. *Models for implementing and promoting cloud computing in higher education institutions*

Cloud model	Example data	Advantages	Risks
On-premise	HR and financial systems	full control	high infrastructure costs
Public cloud	e-learning, libraries	scalability and availability	risk of configuration errors
Hybrid cloud	combination of both	flexibility	management complexity

Source: *own study.*

The last pillar – organisational resilience (human factor) and cyber hygiene culture – includes, among other things, training for students and employees,

[25] M. Nowikowska, Procesowa kontrola danych..., p. 170; M. Nowikowska, Przetwarzanie informacji prawnie chronionej w chmurze obliczeniowej [in:] M. Karpiuk (ed.), Cyberbezpieczeństwo aspekty krajowe i międzynarodowe, Warsaw 2024, pp. 144-154.

[26] Scalable refers to computing resources that are flexibly allocated by the service provider regardless of the geographical location of the resources in response to changes in demand. M. Nowikowska, Procesowa kontrola danych..., p. 171.

[27] D. Dziembek, P. Bajdor, Wykorzystanie chmury obliczeniowej w przedsiębiorstwach – wstępne wyniki badań, „Studia Ekonomoczne. Zeszyty Naukowe" 2018, no. 368, p. 30.

[28] M. Fusiek, Hybrid cloud vs. public cloud vs. private cloud: which one should you choose for your company? https://arkanet.pl/baza-wiedzy/chmura-hybrydowa-vs-publiczna-vs-prywatna-czyli-co-wybrac-dla-swojej-firmy/ [accessed: 1 December 2025].

[29] D. Dziembek, P. Bajdor, op.cit., p. 30.

incident response procedures, building awareness of internal and external threats, creating data teams and information security inspectors, and security incident simulations. Even the best technology cannot protect an institution without aware users. A culture of security should be a natural part of a university's functioning, not a one-off project.

A strategic approach to information management in cyberspace

It should be emphasised that data resilience in higher education does not result solely from the technology in place. Strategic information management in cyberspace is also key. These activities include data management, security, legal compliance, scientific research and education. Universities are increasingly operating in a global knowledge exchange network, using cloud tools, e-learning platforms and data repositories. International cooperation increases innovation, but also exposes universities to cyber espionage targeting research projects, leaks of sensitive data, DDoS attacks paralysing university systems, and finally, disinformation and manipulation of public opinion. Therefore, the approach to information management should be continuously improved. The data management strategy should be part of the university's digitisation policy and include data resource management and open access.

Table 2. *Areas of a strategic approach to information management in cyberspace*

Area	Strategic actions
Data management	data retention policies, classification, version control
Security	incident response plan, penetration testing, threat analytics
Legal compliance	GDPR, licences, copyright
Scientific research	open repositories, protection of research results, fair data[30]
Education	cybersecurity training, good digital practices

Source: *own study.*

Information management in cyberspace is becoming one of the key elements of the functioning of modern organisations, both public and private[31]. Due to the growing amount of data, its volatility and the threats posed by cyberspace, it is necessary to implement a well-thought-out and long-term strategy that allows for the effective use and protection of information resources.

[30] The FAIR Data (Findable Accessible Interoperable Reusable) principles were formulated for the proper preparation and sharing of research data. FAIR Data describes what data should be like in order to make it accessible to both users and computer software that searches databases without human intervention. Research data stored in data repositories should meet four basic conditions: 1) Findable 2) Accessible 3) Interoperable 4) Reusable. All research data must be made available together with its metadata. The FAIR principles are still being developed and refined by the international GO FAIR initiative. https://www.go-fair.org/fair-principles/ [accessed: 01.12.2025].

[31] G. Gierszewska, Informacyjne podstawy strategicznego zarządzania przedsiębiorstwem „Problemy zarządzania" 2005, no. 1(7), p. 50.

A strategic approach to information management by universities means perceiving information not only as a resource supporting operational activities, but above all as an asset whose value determines competitive advantage[32] .

The first step in the strategic information management process is to identify information resources and classify them according to their importance, confidentiality and impact on the functioning of the university. This allows for the prioritisation of protective measures and the optimisation of security-related costs. Tools for monitoring data flow, integration and use for decision-making play a key role[33]. Strategic information management also includes the creation and implementation of security policies, incident response procedures and business continuity plans. In cyberspace, where threats evolve dynamically, organisations must not only protect their resources, but also build resilience and the ability to quickly return to full operational capacity after an attack[34] . An important element is user education, regular training in cyber hygiene and raising awareness of threats[35].

One of the goals of a strategic approach to information management is to ensure its availability and integrity in a way that supports the organisation's objectives. Tomasz Dutkiewicz and Henryk Spustek point out that from the point of view of a strategic approach to information management, three types of information can be distinguished: 1) information used to aid decision-making, 2) information ensuring adequate communication between the decision-maker and the executor, 3) information intended to meet other needs of its users at all levels of management. The above-mentioned types of information can be called decision-making information, relating to decision-making processes and team management[36].

A strategic approach to information management covers not only technical aspects, but also legal and organisational aspects, such as compliance with the GDPR, ISO/IEC 27001 standards and international cybersecurity standards. This enables the organisation to function effectively in the digital ecosystem, minimising the risks associated with cyber attacks and maximising the benefits of using information as a key strategic resource.

The growing importance of information security in the academic environment

Universities are becoming an increasingly frequent target of cyberattacks. In addition to typical breaches such as personal data leaks, the following are particularly dangerous: ransomware blocking university systems, financial blackmail, theft of research results with high market value, state-sponsored APT attacks, manipulation and disinformation targeting the education sector[37]. The modern academic environment operates in conditions of intense information flow,

[32] K. Chałubińska-Jentkiewicz, M. Nowikowska, Ochrona informacji w cyberprzestrzeni, p. 19.
[33] G. Piechota, Strategia zarządzania informacją jako instrument ochrony przestrzeni informacyjnej państwa (*case study*: Ukraina), „Zarządzanie Mediami" 2022, t. 10, no. 2, p. 106.
[34] Ibid., p. 107.
[35] T. Dukiewicz, H. Spustek, Informacja w zarządzaniu strategicznym, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i zarządzanie" 2016, issue 92, no. 1955, p. 66.
[36] Ibidem, pp. 66-67.
[37] A. Pieczywok, Cyberprzestrzeń i dydaktyka cyfrowa na rzecz bezpieczeństwa człowieka, „Cybersecurity and Law" 2024, no. 2(12), p. 96.

globalisation and digitisation of educational and research processes. Universities process huge amounts of data. As a result, the importance of information security is growing, becoming one of the priorities of academic management.

One of the key areas is the protection of personal data subject to legal regulations, such as the GDPR. Universities must build systems that guarantee the confidentiality and availability of data while ensuring efficient communication and electronic handling of teaching processes[38]. The growing popularity of e- earning platforms, digital repositories and remote examination tools further increases the surface area for potential cyber attacks.

Scientific research is another sensitive area. Projects of strategic importance to the economy and industry, carried out in cooperation with external partners, require a high level of protection against cyber theft, industrial espionage and unauthorised disclosure of results. Leaks of such data can lead to financial losses, damage to the university's reputation, and threats to national or corporate technological advantage.

The growing importance of information security at universities also stems from the need to maintain public trust and meet the increasing requirements of grantors and international partners. Academic institutions are becoming an important part of the global information exchange space, which is why data and IT infrastructure protection is a prerequisite for their further development, innovation and competitiveness on the international stage[39].

Every year, there is an increasing number of cyberattacks targeting universities and research institutions. This is due to the fact that they store personal data, scientific research results, and often also information related to projects carried out for the military or industrial sector. Below are some examples of high-profile incidents from recent years.

Ransomware attack on Maastricht University (Netherlands) in 2019. Maastricht University fell victim to a cyberattack using ransomware. Most Windows-based devices were blocked. On 24 December 2019, a statement was published on the university's website stating that the institution had been hit by a serious cyberattack. According to the statement, the incident affected almost all Windows-based devices and made it very difficult to use email services[40] .

Data leaks of students and staff at the University of New Mexico (USA) in 2021. Hackers gained access to personal information such as social security numbers, financial data and students' educational status. It was necessary to inform thousands of people affected by the incident and offer them identity monitoring[41].

During the pandemic, many universities conducted biomedical research of great strategic value. The UK's National Cyber Security Centre reported attacks sponsored by third countries targeting universities and laboratories to obtain data

[38] Ibid., p. 97.

[39] I. Kulish, Problemy cyfryzacji w instytucjach szkolnictwa wyższego, „Nowoczesne Systemy Zarządzania" 2023, vol. 18, no. 3, p. 89.

[40] S. Palczewski, Uniwersytet w Maastricht ofiarą ransomware, https://cyberdefence24.pl/polityka-i-prawo/uniwersytet-w-maastricht-ofiara-ransomware

[41] Cyber Attacks Strike Multiple Schools and Universities in New Mexico, https://cyberpress.org/cyber-attacks-strike-multiple-schools-and-universities/ [access: 1.12.2025].

on vaccines and therapies. Attempt to steal COVID-19 vaccine research results (2020)[42] .

Attack on the Warsaw University of Technology (Poland) in 2022[43]. Information about students and academic staff at the Warsaw University of Technology was leaked from the university's systems. The scope of the data disclosed is very broad and concerns sensitive content. The incident led to the temporary shutdown of IT systems. It was necessary to conduct a post-breach analysis and restore services in emergency mode. Although no technical details were provided, the incident showed that Polish universities are also targets for cybercriminals.

The War Studies University in Warsaw (Poland) fell victim to a hacker attack by the CyberTriad group linked to Russia and possibly China. Data was stolen and computers were encrypted[44].

The above cases show that universities are not immune to cyber threats. On the contrary, they are becoming an attractive target every year due to their large data resources and often less restrictive security procedures than in the commercial sector. This highlights the need to invest in protection systems, security audits, staff training and the implementation of best practices in the field of cybersecurity.

Universities can implement programmes to increase the resilience of the data ecosystem through: technologies and tools (anti-DDoS systems, next-generation firewalls), automatic vulnerability scanners and penetration tests. Within their organisations, universities can set up SOC/CSIRT units and conduct continuous monitoring of infrastructure and system logs. In the area of teaching and research methods, key activities include the inclusion of data security in study programmes and the development of laboratories simulating cyber attacks.

The above considerations lead to the conclusion that a university that invests in digital resilience builds a competitive advantage and an image of a trusted institution.

Conclusions and directions for development

Building a resilient data ecosystem is a long-term process that requires acombination of technology, procedures and competencies. The university of the future is a digitally aware organisation, open to development, but at the same time secure and resilient to disruptions in cyberspace. In the coming years, key activities for universities will include the integration of artificial intelligence in threat detection, the development of international standards for data sharing, and increased funding for academic cybersecurity.

---

[42] Polish Press Agency, United Kingdom: Record number of cyber attacks, targeting vaccine research, among other things https://www.wnp.pl/rynki/rynki-zagraniczne/w-brytania-rekordowa-liczba-cyberatakow-celem-m-in-badania-nad-szczepionka,506329.html [access: 1.12.2025].

[43] S. Palczewski, Wyciek danych z Politechniki Warszawskiej. Ucierpieć mogło nawet 5 tys. osób https://cyberdefence24.pl/polityka-i-prawo/wyciek-danych-z-politechniki-warszawskiej-ucierpiec-moglo-nawet-5-tys-osob [access: 1.12.2025].

[44] N. Bochyńska, Nowe szczegóły cyberataku na Akademię Sztuki Wojennej. Co wiemy?, https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-akademie-sztuki-wojennej-co-wiemy [access: 1.12.2025].

The above considerations lead to the conclusion that in order to build a resilient data ecosystem, higher education institutions should treat data as a strategic resource, equivalent to physical infrastructure. Secondly, it is very important to invest in modern cyber protection technologies and employee skills. Building a culture of digital awareness, in which every user is part of a protective shield, is the starting point for creating a resilient data ecosystem. Even the most advanced security technologies (e.g. encryption, network monitoring, antivirus systems) may prove insufficient if those using information resources are not sufficiently aware of the risks and do not follow proper cyber hygiene practices. According to many analyses, the greatest risk to data security stems not from system errors, but from careless actions or negligence on the part of users. In the academic environment, the human factor is particularly complex. It encompasses a variety of groups, from administrative staff to researchers, doctoral students and undergraduates. Each of these groups uses IT infrastructure in different ways, which can lead to different risks. Administrative staff process personal and financial data, researchers work on research projects of high intellectual value, while students usually have broad access to digital services. Building a resilient data ecosystem therefore requires investment not only in technology, but also in education and security culture. This includes regular training for employees, information campaigns targeting students, and the creation of clear data protection procedures. The introduction of strong password policies, mandatory two-factor authentication, and phishing tests can significantly increase an organisation's resilience. Building a culture of responsibility and incident reporting is also important. In summary, the human factor is the foundation of data ecosystem resilience in higher education. Even the best technical security measures will not be effective if system users do not understand the risks and do not follow appropriate practices. Universities that are able to create a culture of cybersecurity build the foundation for lasting data protection, increase public trust, and minimise the risk of serious information breaches.

Literature

Bochyńska N., Nowe szczegóły cyberataku na Akademię Sztuki Wojennej. Co wiemy?, https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-akademie-sztuki-wojennej-co-wiemy.

Chałubińska-Jentkiewicz K., Cyberbezpieczeństwo – zagadnienia definicyjne, „Cybersecurity and Law" 2019, no. 2(2).

Chałubińska-Jentkiewicz K., Nowikowska M., Ochrona danych osobowych w cyberprzestrzeni, Warsaw 2021.

Chałubińska-Jentkiewicz K., Nowikowska M., Ochrona informacji w cyberprzestrzeni, Warsaw 2021.

Dukiewicz T., Spustek H., Informacja w zarządzaniu strategicznym, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i zarządzanie" 2016, issue 92, no. 1955.

Dziembek D., Bajdor P., Wykorzystanie chmury obliczeniowej w przedsiębiorstwach – wstępne wyniki badań, „Studia Ekonomoczne. Zeszyty Naukowe" 2018, no. 368.

Ferens A., Cyberbezpieczeństwo i cyberryzyko w raportach zintegrowanych i sprawozdaniach zarządu operatorów usług kluczowych, „Zeszyty Teoretyczne Rachunkowości" 2021, vol. 45, no. 2.

Fusiek M., Co wybrać: SOAR czy SIEM? Rola SIEM i SOAR w nowoczesnym zarządzaniu bezpieczeństwem IT, https://arkanet.pl/baza-wiedzy/co-wybrac-soar-czy-siem-rola-siem-i-soar-w-nowoczesnym-zarzadzaniu-bezpieczenstwemit/.

Fusiek M., Chmura hybrydowa vs. publiczna vs. prywatna, czyli co wybrać dla swojej firmy? https://arkanet.pl/baza-wiedzy/chmura-hybrydowa-vs-publiczna-vs-prywatna-czyli-co-wybrac-dla-swojej-firmy/.

Gierszewska G., Informacyjne podstawy strategicznego zarządzania przedsiębiorstwem „Problemy zarządzania" 2005, no. 1(7).

Hadnagy Ch., Social Engineering: The Art of Human Hacking, New Jersey 2010.

Jadczak A., Budowanie odporności cyfrowej w chmurze to proces ciągły, https://itwiz.pl/bud owanie-odpornosci-cyfrowej-w-chmurze-to-proces-ciagly/.

Jancelewicz J., Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych, „Trzeci Sektor" 2022, no. 3-4.

Kostkiewicz P., „Security-by-design" – bezpieczeństwo systemowe ICT – w przepisach, normach i praktyce, „Przegląd telekomunikacyjny" 2025, no. 4.

Kowal R., Zarządzanie cyklem życia aplikacji – na przykładzie Sap Solution Manager, „Studia Ekonomiczne" 2013, vol. 128.

Królas P., Identyfikacja ryzyka związanego z krótkim cyklem życia okazji – studium przypadku, „Zeszyty Naukowe Politechniki Poznańskiej" 2019, no. 80.

Kulish I., Problemy cyfryzacji w instytucjach szkolnictwa wyższego, „Nowoczesne Systemy Zarządzania" 2023, vol. 18, no. 3.

Kwaśnik J., Wpływ ataków socjotechnicznych na konstrukcję i kształt polityki bezpieczeństwa, [in:] M. Górka (ed.), Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa, Warsaw 2017.

Łuczak J., Tyburski M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Poznań 2009.

Nowikowska M., Procesowa kontrola danych informatycznych w chmurze obliczeniowej, „Cybersecurity and Law" 2023, no. 1(9).

Nowikowska M., Przetwarzanie informacji prawnie chronionej w chmurze obliczeniowej [in:] M. Karpiuk (ed.), Cyberbezpieczeństwo aspekty krajowe i międzynarodowe, Warsaw 2024.

Nowikowska M., The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland [in:] K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cybersecurity in Poland, Legal aspects, Springer Cham 2022.

Nowikowska M., Zasada rozliczalności i przejrzystości – rozwiązania w zakresie niezależnego audytu w świetle postanowień aktu o usługach cyfrowych, „Europejski Przegląd Sądowy" 2025, no. 3.

Opalska-Kasprzak A., Kasprzak W.A., Inżynieria społeczna jako narzędzie cyberprzestępcy - analiza kryminologiczna i kryminalistyczna, „Przegląd Policyjny" 2021, no. 4(144).

Palczewski S., Uniwersytet w Maastricht ofiarą ransomware, https://cyberdefence24.pl/polityka-i-prawo/uniwersytet-w-maastricht-ofiara-ransomware.

Piechota G., Strategia zarządzania informacją jako instrument ochrony przestrzeni informacyjnej państwa (*case study*: Ukraina), „Zarządzanie Mediami" 2022, t. 10, no. 2.

Pieczywok A., Cyberprzestrzeń i dydaktyka cyfrowa na rzecz bezpieczeństwa człowieka, „Cybersecurity and Law" 2024, no. 2(12).

Połowin A., Cyberzagrożenia w internecie – analiza przypadków. „Cybersecurity and Law" 2024, no. 2(12).

Radoniewicz F., Phishing, [in:] K. Chałubińska-Jentkiewicz (ed.), Leksykon cyberbezpieczeństwa, Warsaw 2024.

Radoniewicz F., Ransomware [in:] K. Chałubińska-Jentkiewicz (ed.), Leksykon cyberbezpieczeństwa, Warsaw 2024.

Stępień-Banach A., Ochrona danych osobowych w szkołach wyższych [in:] D. Wociór (ed.), Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego, Warsaw 2016.

Taczkowska-Olszewska J., Pojęcie i rodzaje danych osobowych [in:] J. Taczkowska-Olszewska, M. Nowikowska, Prawo do informacji publicznej. Informacje niejawne. Ochrona danych osobowych, Warsaw 2019.

Wrona J., Zawadzka Z., Cyberbezpieczeństwo w prawie własności intelektualnej [in:] C. Banasiński (ed.), Cyberbezpieczeństwo. Zarys wykładu, Warsaw 2018.

Zaborowski P., Kozłowski M., Zastosowanie sztucznej inteligencji w rozwiązaniach cyberbezpieczeństwa, „Cybersecurity and Law" 2025, no. 1(13).

Zaskórki P., Woźniak J., Sprawność informacyjna a odporność na ryzyko utraty ciągłości działania współczesnej organizacji, „Studia i Prace. Kolegium Zarządzania i Finansów" 2024, Zeszyt Naukowy 199.