Scientific and Social Research, 2024, Volume 6, Issue 5
https://ojs.bbwpublisher.com/index.php/SSR

Research on Information Data Security of University Archives

Min Feng*

Archives of Sichuan Normal University, Chengdu 610101, Sichuan Province, China

Corresponding author: Min Feng, csdfm20120126@163.com

Copyright: © 2024 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: Under the background of the rapid development of information technology, the information technology of university archives has become an important part of the modernization of education management. However, in this process, the problem of data security has become increasingly prominent, which has become a major obstacle restricting the in-depth development of university archives informatization. In the face of security threats such as data leakage and network attacks, this paper proposes a series of systematic protection countermeasures, aiming at providing a safe and reliable data environment for university archive informatization, ensuring the integrity and availability of information resources, and thus promoting the improvement of university management efficiency and the optimal allocation of education resources.

Keywords: Universities; File informatization; Data security issues

Online publication: June 7, 2024

1. Introduction

With the advent of the digital age, the information construction of university archives has made remarkable progress. Many higher education institutions have begun to manage and store archival materials through the use of advanced information technologies, such as cloud storage services, blockchain technology, and big data analytics, which not only improve the efficiency of archival retrieval but also enhance the ability to share information. However, this rapid development has also brought new challenges to information security management. The security and privacy protection of archival information have become the key issues that hinder further development, which requires universities to pay more attention to the comprehensive protection strategy of data security while promoting information archive construction.

2. The importance of university archives information data security

2.1. Impact of data security on university archives informatization

The importance of data security in the information of university archives cannot be ignored, which is directly related to the reliability of educational resources and the stability of university operations. With the acceleration of the pace of informatization, a large number of sensitive information and important data are stored electronically, and if security measures are not in place, it is easy to cause data leakage or loss, thus affecting the reputation and education quality of colleges and universities [1]. Data security is not only a technical issue but also a major management challenge that requires fundamental protection of data integrity, availability, and confidentiality.

The lack of data security can lead to a crisis of trust in the management process of educational institutions. Once the archival data of educational institutions is accessed without authorization or maliciously tampered with, not just the privacy rights of individuals are damaged, but also the credibility of the entire institution will be questioned [2]. For example, the leakage of students' personal information not only infringes on personal privacy but also may lead to a series of social problems such as fraud. In addition, weak data security can also make it difficult for colleges and universities to effectively recover critical data in the face of natural disasters or technical failures, increasing uncertainty in the operation of educational institutions. The strengthening of data security helps improve the scientific university management and the accuracy of decision-making. Under the background of archival informatization, relying on stable and secure data storage and processing systems, colleges and universities can more accurately manage student information, analyze scientific research data, and allocate educational resources. This efficient and secure information processing method not only improves the quality of education and management efficiency but also provides a reliable data guarantee for academic research. For example, by ensuring the security of research data, universities can promote the in-depth development of scientific research projects and enhance the innovation and practicality of research results on the premise of maintaining the authenticity of data [3].

2.2. Necessity of strengthening data security management

It is necessary to strengthen the data security management for the information of university archives. In the digital era, university archives contain a large amount of sensitive personal information and important academic research data, and the security of these data is directly related to the reputation and academic integrity of the university [4]. If the data management is lax, it may lead to the leak of information, which not only damages the privacy of individuals but also may lead to legal liability and bring unforeseeable negative effects to the school. Therefore, strengthening data security management to ensure the confidentiality, integrity, and availability of data is a basic requirement for maintaining the school's reputation and legal compliance. In addition, with the rapid development of science and technology and the increasingly complex network environment, all kinds of new network threats continue to emerge, and the security threats faced by university data are also increasing. Whether it is an internal operational error or an external malicious attack, it can lead to a serious data security incident and affect the normal operation of the school. Therefore, strengthening data security management is crucial to prevent and mitigate these risks, which can improve the ability of universities to resist security threats and ensure the smooth progress of teaching and research [5]. To sum up, from the perspective of protecting the core interests of colleges and universities and adapting to technological development, the necessity of strengthening data security management is obvious, and it is an important part of the informatization strategy of colleges and universities that cannot be ignored.

3. Security risks faced by informatization data of university archives

3.1. Data leakage caused by human error

In the process of university archives informatization, human error is an important factor leading to data leakage. Due to improper operation, misoperation, or neglect of data security awareness, employees may inadvertently trigger illegal data leakage, bringing incalculable losses to the school [6]. For example, an employee may choose the wrong command or option when handling sensitive data because he or she is unfamiliar with the operational process, resulting in the data being mistakenly deleted or leaked. In addition, the use of unofficial data processing software or tools may also give rise to security vulnerabilities, exposing the data to the risk of unauthorized access. This type of data breach not only involves a violation of an individual's right to privacy but can also result in a school facing legal action or having its reputation damaged. The problem of data leakage caused by human error reflects the inadequacies in personnel training and security culture construction. The lack of continuous and effective data security training for employees will prevent employees from correctly judging and acting when faced with complex data operations. Even experienced technicians can make fatal mistakes in a state of fatigue or stress [7]. Moreover, if colleges and universities fail to establish a culture that encourages employees to report potential security risks and errors, employees may conceal errors for fear of being blamed, further exacerbating the consequences of a data breach.

3.2. Threats to data security caused by network attacks

Network attacks have become a major hidden danger threatening the information data security of university archives. With the progress of technology, attack methods are increasingly diverse and complex. From simple viruses and trojans to advanced persistent threat (APT) attacks, various forms of network attacks are constantly evolving [8]. These attacks can result in sensitive data being stolen, tampered with, or deleted, and in severe cases can even bring down entire data systems. The anonymous and transnational nature of cyberattacks makes tracking and responding to them particularly complex, as attackers can easily pose a threat to university data security on a global scale, and victims often struggle to quickly and effectively identify and defend against these attacks.

In addition, the threat of cyber attacks on data security is not limited to technical damage but also affects the reputation of universities and the reliability of academic research. Once the data is attacked, not only the security of personal information is damaged, but also the research results and intellectual property rights of the school may be illegally stolen or leaked, thus affecting the authority and competitiveness of the school in the academic and research fields [9]. For example, the tampering of research data may lead to the distortion of research results and even trigger a crisis of trust in the scientific research field.

3.3. Risks of natural disasters and hardware failures

Natural disasters and hardware failures are non-negligible risk factors in the process of university archives informatization, which can pose a serious threat to data security [10]. Natural disasters such as earthquakes, floods, and fires may not only cause direct damage to physical equipment but also paralyze the entire data center, resulting in the loss of a large amount of important data. For example, a university located in an earthquake zone may face damage to its data center due to an earthquake, affecting its entire operations. In addition, hardware failure is also a problem to be underestimated, such as hard disk damage, server overheating, and so on, can occur without warning, resulting in data loss or corruption. The existence of these risks significantly increases the challenges universities face in managing and protecting data. In the face of these unpredictable natural disasters and hardware failures, colleges and universities can suffer even more from inadequate backup and recovery strategies. The irrecoverability of data has caused irreparable damage, especially in the academic research field, because once the original research data is lost, relevant research may need to start over, which not only affects the research progress but also may have a long-term impact on the accuracy of research results [11].

4. University archives information data security protection countermeasures

4.1. Improve the data security management system

Under the background of university archives informatization, it is particularly important to improve the data security management system. The data security management system is not only the defense line to ensure information security but also the cornerstone of the stable development of universities. A good management system can effectively standardize the data processing process, improve the transparency of data operations, and reduce the occurrence of human errors [12]. For example, having strict data access rules that ensure that only authorized personnel have access to sensitive or important data can greatly reduce the risk of data being accessed illegally or compromised.

In addition, the improvement of the data security management system should also include the periodic review and update of the data security policy. With the rapid development of information technology and the emergence of new security threats, the original security strategy may be difficult to cope with the new challenges. Therefore, regular reviews and updates of security policies will help universities find and patch security loopholes in time and strengthen data protection measures [13]. For example, new encryption technologies are introduced to improve the security of data during transmission and storage, and more advanced firewalls and intrusion detection systems are used to defend against external attacks.

Strengthening data security awareness education is also an indispensable part of improving the data security management system. Every university staff member should be responsible for data security. Through regular data security training, all employees' awareness of data security and ability to cope with data breach incidents are improved [14]. In addition, establishing a sound internal reporting process and encouraging employees to actively report security issues are also effective measures to improve the level of data security management across the organization. Through these comprehensive measures, a safe and efficient archival information environment can be built to provide solid support for the long-term development of colleges and universities.

4.2. Strengthen data backup and storage

Strengthening the capacity building of data backup and disaster recovery is the key link in the security strategy of university archives informatization. As universities increasingly rely on digital archives, ensuring data integrity and recoverability is critical. Proper data backup can provide an important safety net for universities in the face of data loss or system failure [15]. For example, regular full and incremental backups not only minimize the risk of data loss but also quickly restore data to its last safe state in the event of a data corruption or system attack.

In addition, the construction of disaster tolerance capacity is another important measure to ensure data continuity and business continuity in universities. Establishing and maintaining an effective disaster recovery plan means universities can quickly recover critical operations and data systems in the event of a natural disaster or other emergency. This includes but is not limited to, setting up off-site backups and establishing a disaster recovery center to ensure that the backup center can take over operations if the primary data center is unavailable [16]. By implementing these strategies, universities can maintain basic teaching and administrative activities even under extreme conditions, reducing the impact of disasters on academic and research efforts.

Strengthening the capacity building of data backup and disaster recovery requires universities to invest corresponding resources to upgrade technology and facilities. This includes not only the procurement of advanced backup hardware and software but also ongoing training and drills for relevant personnel to ensure that they can effectively execute backup and disaster recovery plans when needed. In addition, it is critical to regularly review and update backup and recovery processes to adapt to new technological developments and to respond to potential new threats [17]. Through the implementation of these measures, universities can ensure that their valuable academic resources and operational data are properly protected and managed at all times.

4.3. Improve the technical protection level of data security

Improving the level of data security technology protection is an important task that universities must face in the process of realizing archival informatization. With the increasingly complex and changing network environment, traditional security protection measures have made it difficult to cope with increasingly advanced and diversified security threats. Therefore, the use of advanced technical means, such as intrusion detection systems, firewalls, and encryption technology, has become an important means to maintain data integrity and confidentiality. By implementing these technologies, not only can unauthorized access be effectively prevented, but also timely detection and countermeasures can be taken when data is illegally tampered with or deleted [18].

Universities also need to focus on the full lifecycle management of data security. This involves every stage of data generation, storage, use, transmission to destruction, and strict security controls must be imposed at each stage. For example, data should be encrypted during transmission to prevent it from being intercepted or tampered with in transit. In addition, for sensitive data, technologies such as multi-factor authentication and behavior analysis should be used to identify and prevent abnormal access or operation behaviors [19]. This comprehensive technical protection not only enhances data security but also improves protection against insider threats.

With the development of technologies such as artificial intelligence and machine learning, universities should consider applying these new technologies to data security. Using AI for anomaly detection and response can provide a faster and more accurate response when data is compromised. In addition, machine learning technology can learn from and adapt to massive security events and continuously optimize security protection strategies to combat increasingly complex security attacks [20]. Through the application of these advanced technologies, the overall protection level of university data security can be significantly improved, and the security and efficiency of university information construction can be guaranteed.

5. Conclusion

To sum up, with the continuous progress of information technology, university archives informatization will usher in more opportunities and challenges for development. In this process, ensuring data security will become the key to improving education quality and academic research level. Universities need to establish awareness of data security and regard it as the top priority of information construction. By continuously optimizing the data security management system, strengthening technical protection, and improving the ability to cope with disasters, universities can better protect educational resources and ensure the continuity and stability of teaching and research activities. At the same time, universities should also strengthen cooperation with governments, enterprises, scientific research institutions, and other parties to jointly explore new models and new technologies of data security governance, and form a data security ecology of collaborative innovation and sharing and co-governance.

Disclosure statement

The author declares no conflict of interest.

References

[1] Deng LY, 2024, Research on the Security of University Archives Informatization Data. Journal of Lantai, 2024(07): 7–9.

[2] Li H, 2024, Big Data Enables Archive Management Innovation in Universities. Cultural Industry, 2024(07): 37–39.

[3] Yang BW, 2024, Research on University Archives Management from the Perspective of Information Security. Shaanxi Archives, 2024(01): 49–50.

[4] Tong YM, 2024, Research on the Importance and Path of the Construction of University Archives Information Security System. Lantai Inside-Out, 2024(05): 22–24.

[5] Zheng XX, 2024, Research on Digital Archive Information Security Protection Strategy in Universities. Office Automation, 2024(02): 58–60.

[6] Chen WL, 2023, Problems and Countermeasures of Digital Transformation of University Archives. Journal of Jinan Vocational College, 2023(06): 120–124.

[7] Wang WX, 2023, Research on Innovative Strategies of University Archives Management in the Era of Big Data. Journal of Lantai & Beyond, 2023(34): 25–27.

[8] Qin MJ, 2023, Research on University Archives Security Management System under the Background of Informatization. Office Business, 2023(15): 108–110.

[9] Zheng LC, 2023, Informatization Construction of Personnel File Management in Universities. Cultural Industry, 2023(12): 19–21.

[10] Li XY, 2023, Motivation, Influencing Factors and Optimization Strategies of Digitization of University Archives. Archives World, 2023(02): 19–24 + 61.

[11] Wang ZQ, 2022, Current Situation and Discussion on Information Construction of University Archives Management. Office Automation, 2022(24): 53–55.

[12] An F, 2022, Research on the Status Quo and Countermeasures of Information Management of University Archives. Yellow River Loess (Yellow Race), 2022(11): 47–49.

[13] Jia YW, 2022, Research on Security Management System of Digital Archives in Universities. Office Business, 2022(10): 176–177.

[14] Zhang J, 2022, Measures to Improve the Informatization Level of University Archives. Shandong Archives, 2022(02): 50.

[15] Qi HY, 2021, Research on Innovation of University Archives Management Model in the Era of Big Data. Shanxi Youth, 2021(22): 55–56.

[16] Yang L, 2021, Research on the Protection of University Archive Information Network Security. Journal of Lantai Internal and External, 2021(31): 7–9.

[17] Zhuo XL, 2021, Study on Archives Management in Universities in the Era of Big Data. Archives of Urban Construction, 2021(04): 74–75.

[18] Pan H, 2020, Analysis of the Application of University Archives Management Model in the Era of Big Data. Journal of Lantai & Beyond, 2020(20): 13–15.

[19] Xie H, 2020, Construction of University Archives Security Management Mechanism in Big Data Era. Journal of Heze University, 2020(03): 140–142.

[20] Fei ZQ, 2020, Research on Security of University Digital Archives in the Era of Big Data. Lantai World, 2020(01): 55–57.

Publisher’s note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.