Education Reform and Development, 2024, Volume 6, Issue 11
https://ojs.bbwpublisher.com/index.php/ERD
Online ISSN: 2652-5372
Print ISSN: 2652-5364

Research on Archival Data Security Governance Under the Background of Digital Transformation

Dan Shi*

GongQing Institute of Science and Technology, Jiujiang 332020, China

Corresponding author: Dan Shi, m15230863729@163.com

Abstract: With the rapid development of technologies such as big data, artificial intelligence, cloud computing and blockchain, archive security governance has become an important issue in archive management and information construction. Based on summarizing the current situation of archives security management theory and practice at home and abroad, this paper discusses the challenges it faces and analyzes the future management trend. The aim is to provide theoretical data analysis references and practical guidance for constructing a perfect and efficient file security governance system.

Keywords: Digitization; Archives; Security governance

Online publication: November 22, 2024

1. Introduction

Under the background of digital transformation, the importance of archival data security governance has become increasingly prominent [1]. As an important carrier to recording history and inheriting culture, the security of archives is directly related to the interests of the country, all units, and even individuals. With the rapid development of information technology, the scale, type and complexity of archival data are increasing, which puts forward higher requirements for archival security management [2]. Therefore, in-depth research on the status quo, challenges and future trends of archival security governance has important theoretical significance and practical role.

2. The impact of digital transformation on archival data security

2.1. The surge in data volume brings storage challenges

According to IDC (Data Center), the global data volume will grow at a rate of about 40% every year. The explosive growth of archival data poses a serious challenge to traditional data storage models, which in turn threatens the security of data and its storage. Among them, the primary problem is the lack of data storage space, the limited capacity of traditional storage media and the high expansion cost. Of course, many units turn to cloud storage, cloud storage also with its elastic expansion and demand characteristics, effectively

alleviates the problem of storage space shortage, but also in the perspective of archival data security governance practices to promote the development of digitization, networking and intelligent process [3]. Nex, the second biggest problem is that the surge in the number of data has also increased the difficulty of storage management, and many units have begun to introduce new technologies such as big data technology and artificial intelligence algorithms to build a new storage architecture to achieve centralized data management and intelligent analysis [4].

2.2. Security risks during data transmission and sharing

In terms of data transmission, with the explosion of data quantity, data is also faced with many security risks in the process of cross-platform and trans-regional transmission, mainly including data interception, tampering and forgery. For example, in the process of unencrypted data transmission, hackers may use network monitoring technology to intercept sensitive data and then make illegal use of it [5]. In addition, the data may also be subject to man-in-the-middle attacks during transmission, where the attackers alter or falsify the transmitted data by posing as a legitimate communication party, resulting in data distortion or misleading the recipient. To deal with these risks, the adoption of advanced encryption technology is key. For example, SSL/TLS protocol is used to encrypt data transmission, which can ensure the confidentiality and integrity of data during transmission [6,7].

2.3. Uncertainty caused by the application of new technologies

New technologies such as cloud computing, big data, artificial intelligence and blockchain are being integrated into the field of archival data security governance at an unprecedented speed [8]. However, the application also brings many uncertainties. Take cloud computing as an example, its powerful data storage and processing capabilities provide new solutions for file data security, but the openness of the operating environment on which cloud computing is based also increases the risk of data leakage or loss. According to Gartner's prediction of the future development trend of cloud computing in the field of IT infrastructure, by 2025, more than 80% of enterprises and organizations will prioritize the adoption of the multi-cloud or hybrid cloud strategy, which means that archive data will flow between multiple cloud service providers, and the virtualization characteristics of cloud computing make data boundaries blurred. Traditional security protection methods are difficult to directly apply to the cloud environment, further exacerbating the uncertainty of data security [9].

In addition, the wide application of big data technology, although it provides the possibility of deep mining and value discovery of archival data but also brings the challenge of data privacy protection. The centralized processing and analysis of big data makes it easier for sensitive information to be exposed and abused. For example, in the field of medical archives, the application of big data technology can help doctors diagnose diseases more accurately, but patients' personal information and medical records may also be exposed to the risk of leakage or abuse as a result. Therefore, when introducing new technologies such as artificial intelligence, it is necessary to fully consider the uncertainties they may bring and take appropriate measures to prevent them.

3. Analysis of the research status of archival data security governance

3.1. Research status of security governance at home and abroad

Foreign research on archival data governance mainly includes digital archival management, archival data

security, archival data sharing, and archival data standardization. On the whole, foreign countries pay attention to the improvement of the legal framework and the guidance of technological innovation. For example, the European Union, through the General Data Protection Regulation (GDPR) and other legal frameworks, has made strict regulations on personal data protection, emphasizing the rights of data subjects and the responsibilities of data controllers, and implementing a refined data classification and grading system. At the same time, advanced encryption technologies, such as end-to-end encryption and homomorphic encryption, are widely used in cloud computing services to ensure the confidentiality and security of user data during transmission and storage [10].

In China, a governance system with Chinese characteristics has been formed in terms of archival data security governance. For example, in recent years, the National Archives Administration has actively promoted the construction of archival informatization and digitization and issued several policy documents on archival data security, such as the "Security Management Standards for Archival Digitization Outsourcing," which specify the security requirements of archival data in the whole life cycle of generation, collection, processing, storage, retrieval, utilization and protection (including privacy protection). At the same time, it has continuously improved laws and regulations in combination with practice, such as the Network Security Law and the Data Security Law, etc., and built a multi-level and three-dimensional protection network. The specific measures mainly include: Establishing a data classification and classification system, and clarifying the protection requirements of different levels of data; Implementing data encryption, access control, audit trail, and other technical means to ensure the confidentiality, integrity and security of data in the process of storage, transmission and processing; And establish an emergency response mechanism to deal with potential security threats and emergencies [11].

At home and abroad, there are different strategies for archival data security governance, which comprehensively reflect the wisdom of data security governance under different cultural, legal and technical backgrounds. In the future, with the in-depth development of digital transformation, exchanges and cooperation at home and abroad in archival data security governance will become increasingly frequent, and jointly promote the improvement of global archival data security governance.

3.2. Existing problems and deficiencies in security governance

In the practice of archival data security governance, the problems and deficiencies facing urgent attention, mainly include the following points:

(1) The primary problem lies in the ambiguity of the implementation of the classification and hierarchical protection of archival data, which may lead to the failure of adequate protection of key sensitive data [12]. The lack in encryption and protection technology is also a significant weakness in the current governance system. As hacker attack methods continue to evolve and upgrade, traditional encryption technologies are no longer able to defend against increasingly sophisticated security threats. According to a report released by cyber security giant McAfee, the economic loss caused by encryption breaches runs into billions of dollars every year. To this end, it is important to actively introduce and apply advanced encryption and protection technologies, such as quantum encryption and zero-trust networks, to build a more stable security line of archival data. At the same time, strengthening the construction of network security protection systems, including the deployment of efficient firewalls, intrusion detection systems, etc., is also an indispensable link.

(2) The absence or imperfection of a data backup and recovery mechanism is another major problem in

the current archival data security governance [13]. If a perfect data backup and recovery mechanism is not established, once the data is lost or damaged and other emergency situations, it may bring immeasurable losses. Therefore, establishing a sound data backup and recovery mechanism to ensure the recoverability and integrity of data is an important part of ensuring the security of archival data.

(3) The lack of personnel training and awareness is also a major challenge in the current archival data security governance. As Microsoft founder Bill Gates has emphasized, "Technologies are just tools. It's how we use them that matters." However, in reality, many enterprises and organizations in the process of promoting digital transformation, often neglect the importance of personnel training and awareness raising, resulting in employees' insufficient understanding of data security or related operational behaviors. Therefore, personnel training and awareness promotion work must be strengthened, improving the level of understanding and attention of employees to data security, and lay a solid foundation for improving the security of archival data [14].

4. The archival data security governance strategy under the background of digital transformation

4.1. Scientifically classify data and strengthen protection

In the age of information explosion, data has become one of the most valuable assets of enterprises. In order to ensure the safe and effective use of data, we need to scientifically classify data, constantly strengthen protection, and build a comprehensive and multi-level data security system.

Data classification is the cornerstone of data management. Careful classification can clearly understand the value, sensitivity and potential risks of each type of data. According to the requirements of data privacy and protection level, it can be classified into public data, internal data, sensitive data, etc. Open data is information that can be shared without restriction, such as company profiles, product descriptions, etc., without special protection measures. Internal data is limited to internal employee access data, such as employee files, project progress, etc., needs to set appropriate control measures. Sensitive data includes highly sensitive information such as customer information, trade secrets, and state secrets, which must be protected by high-intensity encryption measures.

Based on data classification and importance, different protection levels should be divided according to the actual situation, and corresponding strengthening measures should be taken to improve security by technical means, such as encryption and firewalls. At the same time, a management system should be established to clarify permissions and responsibilities. Technologies such as cloud computing and big data have brought new challenges and opportunities. They can build an efficient and intelligent data security protection system, realize rapid data backup and recovery, detect security threats on time, and facilitate the whole process of protection before, during, and after the event.

4.2. Establishing a proper data backup and recovery mechanism

Reasonable construction of data backup and recovery mechanisms is an indispensable part of ensuring the security of file data, which needs to start from multiple dimensions. First of all, it is important to implement a combination of regular and irregular backup strategies to ensure comprehensive coverage and timely updates of data. At the same time, cloud storage technology should be used to realize remote backup to further enhance the disaster resistance of data. Second, a process for quick response and efficient recovery should be

established. This includes making detailed recovery plans, conducting regular recovery drills, and optimizing recovery time objectives (RTO) and recovery point objectives (RPO).

In addition, data backup and recovery mechanisms need to be coordinated with the overall security strategy. By integrating security measures such as identity authentication and access control, it ensures that only authorized people can access the backup data. At the same time, encryption technology is used to protect the backup data to prevent it from being stolen or tampered with during transmission and storage. Implementing a scientific backup strategy, establishing an efficient recovery process, and strengthening security measures can effectively deal with the data challenges brought by digital transformation and ensure the security and integrity of archival data.

4.3. Strengthen personnel training and enhance security awareness

The core of archival data security governance lies not only in the technical level of protection but also in the key link of personnel training and awareness promotion. According to the Global Data Breach Survey Report 2022, more than 50 percent of data breaches are caused by internal personnel's negligence or improper operations. To effectively raise awareness of data security among archivists, enterprises should implement regular training programs covering the latest data security regulations, policy interpretations, security practices, and typical case analyses. For example, practical drills of "simulated hacking attacks" can be introduced to allow employees to experience the consequences of data breaches firsthand, to deeply understand the importance of data security. At the same time, interesting activities such as the "Security Awareness Challenge" can be introduced to stimulate employees' enthusiasm to participate, and the knowledge of data security can be internalized and externalized in practice [15].

In terms of training methods, digital means, such as online learning platforms and short video tutorials, should be made full use of to ensure the timeliness and coverage of training content. In addition, a "tutorial system" should be established, with experienced veteran employees or external experts acting as mentors to give one-on-one guidance to new employees to help them quickly master data security knowledge and governance skills. This kind of "mentoring" approach not only helps improve the training effect but also forms a good learning atmosphere within the enterprise.

5. Conclusion

Archival data security management is not an overnight task, but a systematic project that requires continuous investment and fine management. It not only requires the technical level of innovation and reinforcement but also needs the system manpower and material resources of multiple guarantees. In this context, it is particularly important to build a comprehensive, efficient, and flexible archival data security governance system. Only by adhering to the strategic policy of attaching equal importance to technological innovation and system construction, personnel training, and team building in parallel, internal management and external cooperation, can build an indestructible archival data security defense line and provide a strong guarantee for the construction and long-term development of the archival security governance system.

Funding

Archival Science and Technology Project Plan of Jiangxi Province in 2024, "Research on the Theory and

Application of Archival Security Governance Based on Big Data" (Project No.: 2024—jd—006)

Disclosure statement

The authors declare no conflict of interest.

References

[1] Jin B, Yang P, 2022, Construction of a Maturity Model for Archival Data Security Governance Capabilities in the Era of Big Data. Archives Science Newsletter, 2022(1): 29–36.

[2] Zhou L, He X, 2023, Construction and Operation Mechanism of Archival Data Security Governance Model. Archives and Construction, 2023(11): 16–20.

[3] Teng Z, Yu Y, Zhou H, 2023, Analysis of Data Security Technology Based on Cloud Storage. Network Security Technology and Applications, 2023(12): 61–62.

[4] Liu J, Zhengwei Y, Wang Y, 2023, Challenges of Data Integrity Verification in Mobile Cloud Storage Outsourcing Algorithms. Journal of Chengdu University: Natural Science Edition, 42(1): 35–39.

[5] Su J, Du N, 2024, Review of Foreign Research on Privacy Risk Control in Open Sharing of Public Data Resources. Modern Intelligence, 44(3): 164–177.

[6] Zhou W, Zhang D, Bi M, et al., 2022, Design of Chip Testing Software Platform Based on SSL/TLS Protocol. Journal of Tianjin University of Technology, 37(3): 43–48.

[7] Yao Q, 2023, Analysis of Computer Network Application Security. Network Security Technology and Applications, 2023(5): 169–171.

[8] Chen X, 2024, Archive Data Security Governance in the Era of Big Data. Network Security Technology and Applications, 2024(6): 70–72.

[9] Ding H, He W, Yan H, 2024, Research on Development of Graphical Analysis System for Electronic Archives Data in Cloud Environment. China Archives, 2024(6): 64–66.

[10] Li Y, 2024, Foreign Experience and Enlightenment in Archival Data Security Governance. Archive Memory, 2024(1): 52–54.

[11] Feng Z, Wang X, 2024, A Review of Research on Archival Data Governance in My Country. Journal of Archives, 2024(2): 13–24.

[12] Chen X, He X, 2023, Research on Key Technologies of Big Data Security and Privacy Protection. Software, 44(10): 50–52 + 73.

[13] Chen Z, Zhang Y, Guo M, et al., 2024, Analysis of Data Protection Countermeasures in the Era of Big Data. Network Security Technology and Applications, 2024(3): 54–56.

[14] Jing X, 2024, Analysis on Improving the Quality and Efficiency of Archives Management in the Era of Big Data. Lantai Inner and Outer, 2024(22): 31–33.

[15] Pang H, 2024, Research on the Problems Faced by the Digitalization Development of University Personnel Archives and Countermeasures. Lantai Inner and Outer, 2024(22): 13–15.