International Journal of Education, Humanities and Social Sciences

Article

Research on Archive Information Security Issues in the Context of Digital Transformation

Boyang Yu [1,*]

[1] Beijing Union University, Beijing, China
* Correspondence: Boyang Yu, Beijing Union University, Beijing, China

Abstract: With the accelerated development of information technology, new technologies represented by cloud computing, big data, blockchain, and artificial intelligence have provided new technologies and assistance for various industries to transform and upgrade. Under the background of digital transformation, the digitalization construction of archives in China is flourishing. While strengthening the management of archive information and enhancing its value, it also poses new threats to archive information security. In recent years, the importance of archive information security has been increasing from all walks of life, and a series of beneficial explorations have been carried out. However, the issue of archive information security has not been fully resolved. Starting from the background of digital transformation, this article analyzes the security issues of archive information formed in the process of digitizing archives in China, and proposes corresponding response strategies, aiming to protect the security of digital archive information and promote the development of archive digitization. This article first summarizes the relevant literature on digital transformation and archive information security, laying a theoretical foundation for subsequent research activities; Subsequently, analyzing the current situation of digital archive information security management, it was found that digital archive information mainly faces security risks such as management loopholes leading to illegal information collection, technical risks leading to information leakage, and profit driven misuse of information; Further analyze these issues, understand their causes, and propose targeted response strategies such as strengthening archive security management through increased awareness, enhancing technical support through the introduction of artificial intelligence, promoting full process intelligence in archive work through increased funding, and enhancing digital archive security through strengthened supervision of the information security industry.

Keywords: digital transformation; archive information; safety problem

Published: 13 January 2025

1. Introduction

In recent years, new technologies represented by cloud computing, big data, blockchain, and artificial intelligence have not only changed people's lifestyles, but also provided important support for various fields to seek transformation and upgrading. Currently, "digital transformation" has become a hot topic of discussion and an important way for traditional industries to achieve innovative development, with archive management being one of them. In essence, the digital transformation of archives is a transformation of archive management concepts and methods supported by digital platforms, products, and technologies. It is the process of transforming archives and archive information into easily retrievable and usable information. Archives formed through information transformation carry richer information, more diverse storage forms, and higher management and usage efficiency. However, they also face unprecedented information security issues, such as hacker attacks on systems and information leaks. The exposure of these problems has sounded the alarm for archive management personnel. In the context of digital transformation, how to ensure the integrity, authenticity, and reliability of archival information, and avoid its damage, tampering, and leakage due to various accidents, is a key issue of concern for the archival academic community and even the entire society.

From a theoretical perspective, this study analyzes the issue of archive information security in the context of digital transformation and proposes corresponding solutions, enriching the research results in the fields of digital transformation and archive information security assurance, and providing reference for archive management and related research work. From a practical perspective, this study combines practical case studies to analyze the security issues of digital archive information, which helps archive management personnel identify the current archive information security problems; Propose feasible renovation strategies for digital archive information security issues, which can help archive management personnel fill the gaps in archive management work, optimize archive management models, and enhance archive information security.

2. Risk Analysis of Archive Information Security under the Background of Digital Transformation

2.1. Management Vulnerabilities Leading to Illegal Collection of Information

For digital archives, the more information they contain and the wider their coverage, the greater the security threats they usually face, and their security measures are also complex. Various functional departments and institutions need to coordinate and cooperate with each other to enhance their safety index through a scientific management system. In fact, based on the current practical situation, many units' digital archive information management systems are not yet complete, with some management loopholes, leading to the risk of digital archive information being leaked or missing due to illegal collection. Moreover, some management personnel lack awareness of archive information security risk management and are unable to keenly perceive the risks involved, leaving opportunities for illegal individuals to illegally collect information. In recent years, with the continuous popularization of network technology and the expansion and openness of cyberspace, the stored information has become more abundant, making it easier for people to access and use this information. Some criminals see the business opportunities behind archive information, illegally collect archive information, and obtain improper benefits, posing a huge threat to archive information security. The main reasons for the large-scale leakage of user information due to improper storage of user profile information by illegal elements include unauthorized collection of user information, illegal sale of user personal information, vulnerabilities in the network system itself, Trojan virus attacks, and the collection of non-essential personal information by operators, as shown in the following figure.

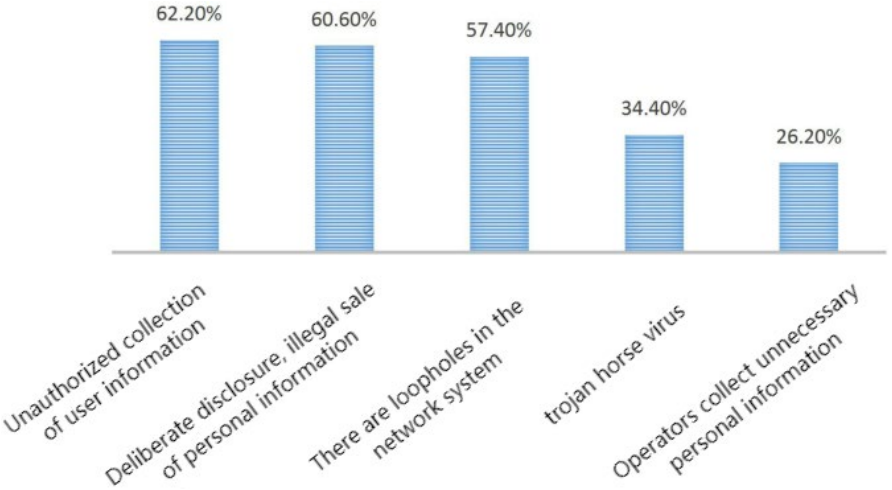

Figure 1. Main reasons for illegal information collection caused by management vulnerabilities.

2.2. Technical Risks Leading to Information Leakage

Cybersecurity and informatization are major strategic issues that are related to the work and life of the people, as well as the development and security of the country. In the context of the accelerated development of digitalization of archives and the comprehensive digitization of archive information, archive management personnel should fully realize that archive information is a strategic resource with enormous value, a big cake in the minds of some reactionary personnel, criminals, and network hackers, and its security is related to national security. According to the data released in the 18th Global Information Security Survey Report, criminal groups, internal employees, and hacker organizations are currently the most likely sources of attacks on digital archive information, accounting for 59%, 56%, and 54% of digital archive information security incidents, respectively. It can be seen that the problem of information leakage caused by technological risks has become an important issue that threatens the security of digital archive information and requires archive management personnel to pay attention to and study it. Especially for some consumer platforms, incidents of user profile information leakage due to technological risks are not uncommon, causing many troubles to users' normal life and work, and has become a major disaster area for illegal acquisition and sale of profile information in the online black market.

2.3. Interest Driven Misuse of Information

After obtaining digital archive information through improper means, criminals often analyze, process, and manipulate it for commercial purposes, forming images or data, and reuse these information resources. This phenomenon of improper use of information driven by interests can be mainly divided into two situations. One is direct improper use, that is, the owner of the archive information uses it privately, such as some apps collecting user archive information to understand their life needs, habits, and preferences, and then conducting precise marketing and personalized recommendations. Secondly, it is information transfer, which refers to the act of the owner of archival information illegally reselling it to third-party applications in order to obtain profits. Some criminals, out of consideration for market demand, economic interests, crime costs, and other factors, illegally obtain, collect, and trade digital archive information, and construct a black industry chain, which has already posed a huge threat to people's lives, social development, and national security. In response to related issues, the public security department has continuously increased its efforts to investigate and punish such illegal and criminal activities in recent years. However, due to the strong concealment and high difficulty of investigation of such illegal and criminal behaviors, as well as the incomplete relevant laws and regulations, and the lack of specific judicial interpretations of related criminal behaviors, judicial personnel still lack clear basis for conviction and sentencing, and cases of improper use of digital archive information driven by interests still occur from time to time.

3. Attribution of Archive Information Security Issues in the Context of Digital Transformation

3.1. Inadequate Policy Implementation and Lack of Awareness of Archive Information Security

Under the background of digital transformation, the full process of intelligent and digital development of archival work has accelerated, providing technical support for the use and utilization of archival information. In this process, the formulation and implementation of relevant policies play a crucial role. The lack of awareness of archive information security among archive management personnel, their lack of understanding and attention to relevant policies, has become an important reason for archive information security issues. For example, some archive management personnel have not carefully read and conducted in-depth research on the *14th Five Year Plan* for the development of the national archive industry. They lack direction in promoting digital archive construction through artificial intelligence and big data, and are at a loss in practical operations, resulting in slow progress in digital archive construction and many management and technical loopholes. The full process of intelligent and digital development in archive work is a complex and long-term process, involving multiple work links such as archive information collection, management, and use. Archive management personnel have insufficient understanding of relevant policies and inadequate implementation of relevant policies, which is an important factor affecting archive information security.

3.2. Insufficient Funding and Slow Progress in the Full Process of Intelligentization of Archival Work

The full process intelligence of archive work is one of the important achievements of digital transformation, as well as an important way to improve archive management efficiency and strengthen archive information security. In the field of information security, the application of this measure requires a large amount of financial support, and the insufficient investment in funds has affected the effective promotion of related work. For example, the use of artificial intelligence technology in archive information management highly relies on software and hardware devices, requiring a large number of advanced devices as support to achieve rapid and intelligent collection and storage of cross modal archive resources such as handwritten text, images, and photos; In the process of promoting the full intelligentization of archival work, a large number of advanced equipment introduced requires post maintenance to ensure normal functionality, which also requires a significant amount of funds. In fact, although the archives department has increased its investment in this area at present, there is still a certain gap between it and the actual demand.

4. Strategies for Addressing Archive Information Security Issues in the Context of Digital Transformation

4.1. Enhance Awareness and Strengthen Archive Security Management

The key to solving the problem of archive information security lies in “people”. Archive management personnel need to achieve a change in their thinking and enhance their awareness of archive information security. Especially for the leadership, it is important to understand the impact of digital transformation on archive security work, abandon outdated thinking, and prioritize archive security work. Specifically, the leadership needs to establish a global perspective and provide directional guidance for archive security work based on the overall development of the unit and the digital transformation of archives. At the same time, according to different types and types of archive information, formulate archive information security work plans and make detailed deployments to make archive management personnel aware of the importance of archive information security and the specific responsibilities they need to undertake. If necessary, the unit can establish a specialized inspection team for archive information security work, guide and supervise archive management personnel to conscientiously and strictly implement various archive information security policies, promote cooperation between different departments, jointly solve various problems faced in archive information security work, and ensure the efficient and smooth progress of related work. At the same time, the national level should also attach importance to the security of archival information, and formulate corresponding policies in conjunction with the background of digital transformation to strengthen the guidance of archival information security work at the policy level. For example, based on the in-depth application of artificial intelligence technology in the field of archive management, government departments can introduce relevant policies to strengthen the understanding of digital archive information security among archive management institutions and staff, and propose corresponding technical standards to guide their daily work, upgrade archive information collection and storage technology and management methods, and enhance archive information security.

4.2. Introducing Artificial Intelligence and Strengthening Technical Support

The development and application of artificial intelligence technology have effectively improved work efficiency in various fields and provided important technical support for the development of related work. The introduction of artificial intelligence should be emphasized in archive information management to enhance archive information security from a technical guarantee perspective. Firstly, by leveraging the advantages of modern artificial intelligence technology in data collection and processing, the process of collecting, managing, and using archival information can be optimized to avoid information input errors caused by manual operations, as well as information loss, damage, and leakage problems during the management and use of archival information. For example, artificial intelligence technology can be used to strengthen the control of archival information resources, increase the prevention of illegal access, and improve the integrity, reliability, and accuracy of digital archival information. Secondly, artificial intelligence technology should be utilized to strengthen personalized management of different types of digital archive information, and corresponding management systems and mechanisms should be established to meet the new changes and requirements of archive information security work. Furthermore, artificial intelligence technology should be utilized to enhance the standardization of archive information security work, such as achieving comprehensive and integrated archive induction through artificial intelligence technology, further clarifying the relationships between various archive management systems, and improving the security and stability of archive information storage.

4.3. Increase Capital Investment and Promote the Full Process Intelligence of Archival Work

To promote the full process intelligent development of archival work, sufficient funding is needed to support and solve the problem of insufficient investment. This is also the key to achieving intelligent archival management and improving the security of archival information. Firstly, government departments should include the application of artificial intelligence technology in the field of archive management in their budget, increase funding for related projects and technological research activities, and encourage research institutions and enterprises to strengthen research on intelligent archive management technology, in order to provide the necessary technical support for archive information security work. Secondly, pilot projects will be established to promote the full process intelligence of archival work, and corresponding management and incentive measures will be introduced, providing special funds to enhance the enthusiasm of archival institutions in the field of intelligent archival management. Finally, archive information management entities such as enterprises, institutions, social organizations, and government agencies should also budget for the full process intelligence of archive work, actively introduce new technologies, management mechanisms, and excellent archive management talents to further ensure the security of archive information.

4.4. Strengthen the Supervision of the Information Security Industry and Enhance the Security of Digital Archives

In response to the background of digital transformation, relevant departments should provide legal and regulatory guidance for the development of archive information security work, and strengthen the supervision of the information security industry to enhance the security of digital archives and alleviate the problem of illegal collection and use of archive information. For example, relevant departments can adopt a digital archive information security accountability system and accountability system to strengthen supervision of the information security industry. Especially for the phenomenon of “disorderly behavior” and “inaction” in digital archive information security work, strict punishment measures should be taken against individuals, departments, and units in accordance with relevant laws and regulations, such as holding them accountable, issuing public criticism, or canceling evaluations. In this way, it can further constrain the archive management personnel of the archive department and state organs, and prevent archive information security accidents caused by their personal negligence and improper operation. On this basis, it is necessary to further strengthen the supervision and management system for tracking the behavior trajectory of for-profit institutions and third parties involved in the transmission and use of archival information, and to impose penalties such as revocation of professional certificates, suspension of relevant certificates, fines, penalties, and warnings on individuals, institutions, and organizations who violate laws and regulations by using archival information.

5. Conclusion

In the context of digital transformation, significant changes have occurred in the media public opinion environment, information dissemination methods, etc., presenting a new trend of information exchange that is fully effective, inclusive, comprehensive, and holographic. This has further highlighted the openness of archival information and faced new security issues. The academic community and archive management personnel have rapidly increased their attention to archive information security issues and have made many beneficial attempts. Starting from the background of digital transformation, this article analyzes the security issues of archive information formed in the process of digitizing archives in China, and proposes corresponding response strategies, aiming to protect the security of digital archive information and promote the development of archive digitization. This article first summarizes the relevant literature on digital transformation and archive information security, laying a theoretical foundation for subsequent research activities; Subsequently, analyzing the current situation of digital archive information security management, it was found that digital archive information mainly faces security risks such as management loopholes leading to illegal information collection, technical risks leading to information leakage, and profit driven misuse of information; Further analyze these issues, understand their causes, and propose targeted response strategies such as strengthening archive security management through increased awareness, enhancing technical support through the introduction of artificial intelligence, promoting full process intelligence in archive work through increased funding, and enhancing digital archive security through strengthened supervision of the information security industry.

References

1. M. Morton, "The corporation of the 1990s: Information technology and organizational transformation," *Journal of Engineering & Technology Management*, vol. 10, no. S1–2, pp. 190–193, 1991.
2. R. C. Coile, "The digital transformation of health care," *Physician Executive*, vol. 26, no. 1, pp. 8–15, 2000.
3. M. Broersma and F. Harbers, "Exploring machine learning to study the long-term transformation of news," *Digital Journalism*, pp. 1–15, 2018.
4. B. Solis and J. Szymanski, "The race against digital Darwinism: Six stages of digital transformation," 2016, no. 4.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of SOAP and/or the editor(s). SOAP and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.