ISSN 2616-5775 Vol. 5, Issue 12: 94-97, DOI: 10.25236/AJCIS.2022.051214

Big Data Information Security Risk Framework and Coping Strategy

Shi Bo[1], Chen Xin[1], Yu Ran[2], Ji Chen[2]

[1]*Beijing Institute of Computer Technology and Application, Beijing, China*
[2]*Jiangsu Aerospace 706 Information Technology Co., Ltd, Nanjing, China*

Abstract: *With the continuous development of the current society and the dawn of the information age, big data has become the focus of people's daily attention. Data collection is becoming more and more important for the development of enterprises, so we should pay attention to the information security issues of enterprises and the country. It is necessary to attach importance to the construction of the data security system, do a good job of security risk framework analysis based on the background of the big data era, pay attention to the internal loopholes of the system, data privacy and data management methods, and improve people's information security awareness by constantly updating equipment, adopting advanced technology for data management and other methods.*

Keywords: *Coping strategy; Information; Risk; Framework; Big data*

1. Introduction

In the big data era, data has become an important resource, which can promote the continuous improvement of social productivity and efficiency. While data serves the social economy, data security has also become the focus of all sectors of society. Big data is a kind of data that has a large scale and cannot be searched and processed with conventional software tools. It has the characteristics of large data volume and complex data types. We should pay attention to the information security issues under the current big data environment, fully analyze the information security risk framework, update the infrastructure, improve personal information security, use technology to further avoid risks, improve the security guarantee of big data information, and ensure the authenticity of data. At the same time, it is necessary to strengthen system security, take good measures to avoid risks, and provide an important guarantee for big data information security.

2. Discussion on Big Data Information Security Risk Framework

2.1. System internal vulnerabilities

The current security problems in the big data environment mainly include the security problems caused by the network, natural disasters and other factors. There are many problems in the system, mainly including imperfect system infrastructure, unprotected data privacy, and imperfect data management methods. Infrastructure mainly refers to the data security problems caused by the aging of infrastructure equipment. The data security problems caused by natural reasons mainly include earthquake, typhoon and other natural factors, which will affect the effective transmission of data, destroy the server, cause data loss in the server, and cause data confusion. Or in the process of data transmission, power failure and other factors will cause line interruption, data loss, and affect the integrity of data. With the continuous development of science and technology, although the hardware equipment has been effectively improved, the data has a certain degree of complexity. In the process of big data application, the storage and processing of data can not meet the requirements: the hardware facilities are not updated in time, and the data storage can not meet the new requirements. The aging of various hardware equipment leads to the slow operation of the system, or even collapse, resulting in the leakage and loss of data, which is not conducive to the effective transmission of data. The data transmission function declines, the system crashes, and the data output security is affected. Data privacy is also an important issue. Data privacy mainly refers to the risk of user privacy disclosure during data analysis and processing. In the process of data collation, different data are integrated from different regions, so that personal information is analyzed by multiple regions, which magnifies the privacy risk. In the process of data

ISSN 2616-5775 Vol. 5, Issue 12: 94-97, DOI: 10.25236/AJCIS.2022.051214

analysis, people need to track multiple pieces of data comprehensively to improve the accuracy of data, make the characteristics of users more obvious, and the data privacy cannot be protected, which seriously threatens the information security of users and increases the risk level. Incomplete data management mode is also a big data security problem at the data management level. Incomplete management is mainly due to data leakage caused by management errors and operation errors, which leads to data exposure. In the process of imperfect data management, due to the complexity of the data management system, it is inevitable that there will be errors in the operation process, which may lead to the system being unable to operate normally, such as tampering with system parameters and deleting system files by mistake. Especially in the face of complex operating systems, it will increase the situation of operational errors, leading to serious data leakage. The operation of technicians does not conform to the specification, which will increase the risk of leakage. Moreover, the quality of the staff is not high, and they may steal data for their own benefit [1].

2.2. System external vulnerability

The external vulnerabilities of the system mainly refer to the unprotected personal information and the active intrusion of hackers. In the new era, laws, policies and hackers will lead to information loss and leakage. In order to ensure information security, the legal department of our country should pay attention, but in the actual process, the construction of relevant laws is insufficient, and the information resources cannot be comprehensively controlled. And with the continuous growth of data scale, the existing information security technology is not enough to protect the security of information data. Massive data has higher requirements for security protection technology. Security protection technology has not been updated timely, leading to more security vulnerabilities. Monitoring technology cannot monitor data in an all-round way. Some staff members will divulge confidential documents and resources for their own benefit, causing greater harm. Although big data technology can effectively improve the safe operation environment of data, in fact, because people do not pay enough attention to security and the application of encryption technology, they are vulnerable to attacks by hackers, and it is difficult to ensure the authenticity and reliability of data sources, which directly affects the improvement of economic benefits. With the development of the network era, the information of individual users becomes more and more obvious. Because big data has a high value, it will lead to criminals to attack the system and steal data in order to gain benefits, making information security not guaranteed [2].

3. Discussion on the Relevant Measures of Information Security Risk

It is more important to study the value of information data in the big data environment. At the same time, it is also necessary to do a good job in information security protection. We will take various measures to solve this problem. Here is an analysis of the measures.

3.1. Pay attention to the strengthening of information security awareness of staff

At present, with the rapid development of society, people pay more and more attention to the use of the Internet, and various multimedia platforms are gradually emerging. Wechat, Weibo, Tiktok, QQ and other platforms are widely used, resulting in a lack of information security awareness. In order to ensure the rapid and stable operation of social economy, attention should be paid to the security construction of various information tools and network platforms. Users should pay attention to the protection of personal privacy during the use process to avoid information leakage. Avoid exposure of personal location information due to lack of information protection awareness. Relevant institutions should attach importance to the publicity of information protection, strengthen the security awareness of network users, attach importance to the effective management of personal information resources, and strengthen the public's awareness of the protection of personal privacy information. Guide the public not to disclose personal privacy information at will, not to browse insecure Internet sites, and not to register personal information at will. Especially in the context of the latest era, with the continuous development of network technology, individuals should follow the pace of the times, not arbitrarily participate in the registration activities of small gifts, not randomly scan the QR code, to avoid their own information leakage. When your information is leaked, you should pay attention to protecting your personal privacy, call the police in time and ask for legal aid. In the process of security protection, we should further improve our network use security awareness through security education and special lectures, teach people not to browse bad websites, and attach importance to the safe operation and use of information data [3].

ISSN 2616-5775 Vol. 5, Issue 12: 94-97, DOI: 10.25236/AJCIS.2022.051214

3.2. Update information facilities in real time and maintain information system

In the big data environment, there is a risk of information leakage and loss. We should attach importance to establishing an information security framework to update information facilities and maintain information systems with the support of information technology. Facilities are the foundation of big data security. In order to ensure the application effect of big data technology, it is necessary to update the information system in a timely manner, pay attention to the construction of infrastructure, do a good job in maintenance and update management, prevent equipment aging or expiration, and timely check the potential safety hazards in emergency equipment. In the process of building the security risk framework, managers should pay attention to infrastructure work, increase capital investment, constantly arrange staff to inspect and maintain the information system facilities, and constantly update the information system to avoid impact on the use of information data. If problems occur in the use of the information system, emergency measures should be taken and an emergency warning mechanism should be developed. In case of emergencies, early warning and response should be made to ensure the safety of information use [4].

3.3. Reasonably avoid risks with the help of information technology

Big data has been widely used, mainly because company managers can play an effective role in company operations. In order to improve the security of the use of information data in the new era, it is necessary to attach importance to the use of information technology by managers to reasonably avoid risks, conduct good supervision and control over the use of information technology, do a good job of big data security protection, improve security awareness, and realize the significance of security monitoring. If information risks occur, they should be solved at once, and attention should be paid to the application of encryption technology, firewall and other technologies. In the process of firewall construction, we should pay attention to the current application of proxy firewall and monitoring it, and play its role. We should use computers scientifically and rationally. We should try our best to avoid running programs of unknown origin, hide IP addresses, and update virus-killing software in the system. A complete information system is formed during the use of internal information in the market to effectively reduce the invasion of hackers and viruses. In their work, staff should actively explore information risk avoidance technology, constantly optimize the market operation environment, improve the process of information construction, and further ensure the authenticity of information data. In the process of big data, staff should put forward corresponding requirements, conduct in-depth analysis on the data, deeply explore the potential effective value of the data, and make scientific and reasonable decisions and predictions based on the analysis results. During the implementation, the staff shall follow the principle of fairness and justice, establish a sense of responsibility and maintain good professional ethics. Data authenticity is the main basis for decision-making. If the data does not have credibility, it will affect the actual effect of decision-making and prediction. In the process of data collection, it is necessary to comprehensively control and check the authenticity of data, check the source of data, and delete false information. Robust statistics and adversarial machine learning methods should be adopted to minimize malicious data and adverse effects caused by data, and to detect the authenticity of data [5].

3.4. Pay attention to the self-management of the market

As the main organizer of big data information, Internet organizations should pay attention to the application of information technology in order to achieve transformation and upgrading during the operation of economic activities, and have the obligation to maintain the security of big data. In the process of safety monitoring, the information shall be used in a standardized way and professional protective measures shall be established. Internet organizations should process information and data, take into account the personal privacy and security of users, build a complete information protection mechanism, and ensure the use of information technology. In the process of information transmission, it is necessary to establish the corresponding encryption technology, which can reduce the occurrence of information leakage caused by non-operation through key opening. In order to reduce the risk problems in the use of information data, Internet organizations should set corresponding access permissions and comprehensively restrict the members who can access data. Once data leakage occurs, members should be restricted to find the source of information leakage. Strictly abide by the service data information security policy formulated by Internet organizations, constantly standardize the data operation behavior, eliminate the data leakage problem caused by improper operation, and ensure the security of information data throughout the network.

ISSN 2616-5775 Vol. 5, Issue 12: 94-97, DOI: 10.25236/AJCIS.2022.051214

4. Conclusion

To sum up, we should attach importance to the protection of information resources in the context of the big data era, conduct in-depth research and mining on big data technology, establish a good security framework system, build security risk measures for big data information, make a good analysis of the security risks existing in the operation of big data, strengthen big data technology facilities, vigorously adopt science and technology, effectively avoid security problems, continuously improve the authenticity of information data, and focus on cultivating personal information security awareness, further improve the security of data and effectively avoid risks through various measures.

Further improving the security of data through various initiatives is helpful to avoid risks. We need to conduct in-depth research and mining on big data technology to establish a good security framework system. At the same time, we need to build security risk measures for big data information to analyze the security risks in the process of big data operation. It is also necessary to strengthen big data technology facilities and vigorously adopt science and technology to effectively avoid security problems. At last, constantly improving the authenticity of information data is important to cultivate personal information security awareness.

References

[1] Zhang Xiaowei. Research on Big Data Information Security Risk Framework and Countermeasures [J]. Computer Knowledge and Technology, 2021, 17(27):42-43+61.
[2] Cui Chen. Research on information security risk framework and coping strategies under the background of big data [J]. Electronic Test, 2021(08):60-62.
[3] Cai Min. Research on Big Data Information Security Risk Framework and Countermeasures [J]. Electronic Technology & Software Engineering, 2019(05):214.
[4] Xin Gaofeng, Xiao Jing. Research on Information Security Risk and Countermeasures of Big Data [J]. Electronic Product Reliability and Environmental Testing, 2018, 36(06):47-50.
[5] Wu Yufeng. Research on Big Data Information Security Risk Framework and Countermeasures [J]. PC Fan,2018(06):63.