Information Systems and Economics (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/infse.2023.040403
ISSN 2523-6407 Vol. 4 Num. 4

Analysis of Financial Information Security in the Age of Big Data

Li Ke*

Shandong Rongyue Financial Holdings Co., Ltd, Jinan, Shandong, China
**Corresponding author: like@royojr.com*

Keywords: Big data; Financial information; Safe

Abstract: This paper mainly discusses the security of financial information in the era of big data. With the acceleration of digitalization and networking in the financial industry, financial information security is facing more and more challenges. Firstly, this paper analyzes the main threats and risks faced by financial information security, including hacking, data leakage and improper behavior of internal employees. Then, this paper discusses the application of big data technology in financial information security, including data encryption, data backup, access control and so on. Finally, this paper puts forward some suggestions to strengthen financial information security, including strengthening personnel training, perfecting security management system and establishing information security guarantee system. Through this research, we can provide more comprehensive and effective information security measures for the financial industry.

1. Introduction

With the rapid development of Internet technology, the era of big data has arrived. In this era, massive data are constantly generated, collected and processed, which contains information from all walks of life, among which financial information is particularly important. Financial information refers to all kinds of data related to the financial industry, such as transaction records, customer information, financial statements, etc. The security of this information is very important for the stability and development of the financial industry. Therefore, in the era of big data, financial information security has become a concern.

2. The main threats and risks faced by financial information security

In the era of big data, financial information security is facing more and more threats and risks.

2.1 Hacking

Hacking is one of the main threats to financial information security. Hackers can obtain sensitive information of financial institutions through various means, such as customer account information and transaction records. In the era of big data, the means of hacking are also more diverse and complicated.

Network attack is a main means of hacker attack, and its purpose is to obtain sensitive information or destroy the system by attacking the network system of financial institutions. The forms of network attacks include viruses, Trojans, worms, DoS/DDoS, etc. Social engineering attack refers to an attack way that hackers get sensitive information by communicating with employees or customers of financial institutions. This kind of attack often uses deception, deception and other means to make the victim voluntarily or forced to disclose sensitive information. Internal attack refers to an attack in which employees or partners in financial institutions obtain sensitive information by abusing their authority and stealing passwords. This kind of attack is often more difficult to prevent than external attacks, because the attacker has obtained legal access rights.

In order to prevent hacker attacks, financial institutions need to take various measures, including improving the security management system, strengthening security training, and strengthening access control. In addition, financial institutions need to constantly update technical means and adopt advanced security technologies, such as intrusion detection, data encryption, identity authentication, etc., to improve the security and defense capabilities of the system.

2.2 Data leakage

Data leakage is one of the main threats to the security of financial information, which refers to the behavior of unauthorized individuals or organizations to obtain sensitive data of financial institutions and disclose or sell them. Data leakage may lead to the disclosure of business secrets, customer privacy and financial data of financial institutions, thus bringing serious losses to financial institutions and customers.

There are many reasons for data leakage, including negligence of internal employees, hacker attacks, loopholes of third-party suppliers, etc. Among them, the negligence of internal employees is one of the most common reasons, and they may lead to data leakage due to improper operation or personal motivation. Hacking attacks are also an important reason for data leakage. Hacking attacks can obtain sensitive data of financial institutions in various ways, such as phishing and malware. In addition, vulnerabilities of third-party suppliers may also lead to data leakage of financial institutions, because financial institutions usually cooperate with multiple suppliers, and these suppliers may access sensitive data of financial institutions.[1]

In order to prevent data leakage, financial institutions need to take a series of measures. First of all, financial institutions should establish a sound data protection strategy, including strengthening the training of internal staff and improving the data management system. Secondly, financial institutions need to strengthen the monitoring and prevention of network security, including implementing network security protection measures and strengthening the monitoring and response of security incidents. In addition, financial institutions can also use data encryption, access control and other technical means to protect the security of sensitive data. Finally, financial institutions need to establish a perfect emergency plan, so as to deal with and deal with data leakage in time.

2.3 Misconduct of internal staff

Improper behavior of internal employees is one of the important threats to financial information security. Internal employees refer to employees in financial institutions, including managers, technicians and ordinary employees. They come into contact with sensitive information of financial institutions in their work. If they use or disclose this information improperly, it will cause serious losses to financial institutions.[2]

Internal employees use their authority or technical means to disclose sensitive information of financial institutions, such as customers' personal information, transaction data and financial data. This information may be used for illegal activities, such as fraud and theft, which seriously harms the

interests of financial institutions and customers. Internal employees use their own authority or technical means to conduct malicious operations, such as tampering with data, deleting data, etc., resulting in the business of financial institutions being affected or lost. Because of negligence or ignorance of safety regulations, internal employees misuse or disclose sensitive information of financial institutions, such as revealing passwords to others and sending sensitive documents to the wrong mailbox.

In order to prevent the misconduct of internal staff, financial institutions need to formulate detailed safety management systems, clarify the rights and responsibilities of internal staff, standardize the behavior of internal staff, and prevent the occurrence of misconduct. Strengthen the safety awareness education and training of internal staff, improve the safety awareness and skill level of internal staff, and prevent internal staff from causing safety accidents due to negligence or ignorance of safety regulations. Establish a monitoring and auditing mechanism to monitor and audit the behavior of internal employees, and find and deal with improper behavior in time. Strengthen the management and supervision of internal employees, and severely deal with internal employees who violate safety regulations, so as to form an atmosphere in which internal employees consciously abide by safety regulations.[3]

3. The application of big data technology in financial information security

In the era of big data, financial information security is facing more and more challenges. Therefore, this section mainly discusses the application of big data technology in financial information security. Specifically, it includes data encryption, data backup, access control and so on. These technologies can effectively protect the sensitive information of financial institutions and prevent security problems such as hacker attacks and data leakage. Through the application of these technologies, financial institutions can better protect the information security of customers and improve their trust and satisfaction.

3.1 Data encryption

Data encryption is one of the important safeguards for financial information security in the era of big data. Data encryption refers to converting plaintext data into ciphertext data through some algorithm, so that unauthorized third parties cannot read and understand the data content. The main principle of data encryption is to encrypt and decrypt data through keys to ensure the security of data transmission and storage.[4]

Data encryption is widely used in the financial industry. Transaction data encryption, which encrypts financial transaction data to ensure the security and privacy of transactions. Encryption of stored data, which encrypts the stored data of financial institutions to ensure the security and integrity of the data. Network data encryption, which encrypts the network data of financial institutions to ensure the security and privacy of data transmission. Mobile device data encryption, which encrypts the mobile device data of financial institutions to ensure the security and privacy of data.

3.2 Data backup

Data backup is an important application of big data technology in financial information security. With the acceleration of digitalization and networking in the financial industry, the amount of data owned by financial institutions is also increasing year by year. In order to ensure the security of financial information, data backup has become an essential part.

Data backup refers to copying data to a standby storage device, so that the data can be quickly recovered in case the original data is damaged or lost. In financial industry, the significance of data

backup is very important. The data owned by financial institutions are often very sensitive. Once the data is destroyed or lost, it will bring serious losses to financial institutions. Therefore, data backup is one of the important means to ensure the security of financial information.

Data backup can be achieved by various technical means, including tape backup, hard disk backup, cloud backup and so on. Tape backup is a traditional backup method, which has the advantage of low cost and the disadvantage of slow backup speed. Hard disk backup is a common backup method. Its advantage is faster backup speed, but its disadvantage is higher cost. Cloud backup is a new backup method, which has the advantages of fast backup speed, low cost and high reliability.

When backing up data, it should be noted that the backed-up data needs encryption protection to ensure data security. Secondly, the backup data needs to be checked regularly to ensure the integrity and availability of the backup data. Finally, the backup data needs to be stored in a safe and reliable place to prevent the backup data from being stolen or damaged.[5]

3.3 Access control

Access control is an important application of big data technology in financial information security. In the financial industry, access control refers to the access control of data and systems within financial institutions to ensure that only authorized personnel can access sensitive data and systems. Authentication is the basis of access control, which determines whether users have access to specific data and systems by verifying their identities. In the financial industry, common identity authentication methods include password authentication, fingerprint recognition, iris recognition and so on.

Authority management refers to the management of user's authority, including user's role, authority scope, authority level, etc. Permission management can ensure that users can only access the data and systems they need, and prevent users from accessing sensitive data and systems beyond their authority. Audit log is an important means to record the user's access behavior, which can record the user's login, access, modification and other operational behaviors and save them in a safe place. Through the audit log, abnormal access behavior can be found in time to ensure the security of data and system. Network isolation refers to isolating different network environments to avoid data exchange and interference between different networks. In the financial industry, network isolation can isolate the internal network from the external network to ensure that the data and systems of the internal network are not attacked and interfered by the external network.[6]

4. Suggestions on strengthening financial information security

This section mainly puts forward three suggestions to strengthen the safeguard measures of financial information security. First of all, strengthen personnel training to improve employees' safety awareness and skill level; Secondly, improve the safety management system and establish a sound safety management system; Finally, the information security system is established, and various technical means are used to protect and prevent financial information. These suggestions have important guiding significance and practical value for the financial industry to ensure information security in the era of big data.

4.1 Strengthen personnel training

Strengthening personnel training is one of the key measures to strengthen financial information security. In the era of big data, financial practitioners need to have more comprehensive and in-depth information security knowledge and skills in order to better cope with various security threats and risks. Through regular information security training and education, improve employees' awareness and attention to information security and strengthen their awareness of information security. Through

technical training, employees' understanding and mastery of information security technology will be improved, and their technical prevention ability will be improved. By carrying out management training, we can improve employees' knowledge and understanding of information security management, cultivate employees' awareness and sense of responsibility for security management, and thus improve the information security level of the whole organization. Establish employee information security assessment mechanism, evaluate and assess employees' information security awareness, skills and behaviors, and form an effective incentive and restraint mechanism. By strengthening personnel training, the information security literacy and skill level of financial practitioners can be improved, thus better ensuring financial information security.[7]

4.2 Improve the safety management system

In the era of big data, the importance of financial information security is increasingly prominent. In order to ensure the security of financial information, a perfect security management system is essential. The establishment of security management system is the basis to ensure the security of financial information. Establish a sound safety management system, clarify the responsibilities and authority of each department, and formulate detailed safety management regulations and processes. In addition, a sound safety management framework should be established to ensure the effective implementation of the safety management system. Strengthen safety awareness education and improve employees' safety awareness and safety literacy. Through regular safety training, skill assessment and safety awareness publicity activities, enhance employees' safety awareness and preventive ability, and promote employees to consciously abide by the safety management system. Establish a security inspection mechanism to conduct security inspection and evaluation of information systems on a regular basis. Through security inspection, we can find and solve security risks and improve the security and stability of information systems. Strengthen security monitoring and early warning, establish a security monitoring center, and monitor the security status of information systems in real time. At the same time, establish an early warning mechanism for security incidents, find and deal with security incidents in time, and prevent the spread and influence of security incidents.

4.3 The establishment of information security system

In order to better ensure the security of financial information, it is necessary to establish a perfect information security guarantee system. Financial institutions should formulate information security management systems, clarify the responsibilities and authorities of various departments, establish a security management framework, formulate security management norms and processes, and ensure the standardization and standardization of security management. Adopt advanced security technical measures to ensure information security. Specific measures include data encryption, network security protection, access control, security audit, etc. Establish a security incident response mechanism to find and deal with security incidents in time and reduce losses. Strengthen the safety education and training for employees, improve their safety awareness and skill level, and prevent employees' improper behavior from causing information leakage and safety incidents. Establish a sound personnel management system to standardize the behavior and authority of employees. Conduct regular safety assessment and monitoring, find security loopholes and risks, and take timely measures to repair and deal with them. Establish a security incident reporting mechanism to inform relevant departments and users of security incidents in a timely manner to protect the rights and interests of users.

5. Looking forward to the future development trend of financial information security

With the advent of the era of big data, the situation of financial information security will be more

severe. In the future, financial information security will face many challenges. With the integration of cloud computing and big data technology, financial institutions will rely more on cloud computing and big data technology to process and store a large amount of data. This also means that financial information security needs to pay more attention to cloud security and big data security. The continuous development of artificial intelligence technology will bring more data security problems. For example, machine learning algorithms may be attacked by hackers, resulting in data leakage. Therefore, financial institutions need to strengthen the safety management and monitoring of artificial intelligence technology. Blockchain technology can effectively improve the security and privacy of data. In the future, financial institutions will apply blockchain technology more widely to protect customers' privacy and data security. With the increasing problem of financial information security, the government and regulatory agencies will also strengthen the supervision of financial institutions and introduce more perfect laws and regulations to protect financial information security.[8]

6. Conclusion

This paper mainly discusses the problem of financial information security in the era of big data, analyzes the threats and risks of financial information security, and studies the application of big data technology in financial information security, and puts forward some suggestions to strengthen financial information security. In the era of big data, financial information security is facing more and more challenges, especially in data leakage, hacker attacks and improper behavior of internal employees. Financial institutions need to take more effective measures to ensure information security. At the same time, big data technology plays an important role in financial information security, such as data encryption, data backup and access control, which can effectively protect the information security of financial institutions. In order to strengthen the security of financial information, this paper puts forward the following suggestions: first, strengthen personnel training to improve employees' safety awareness and skills; The second is to improve the safety management system and establish a sound safety management system; The third is to establish an information security system and adopt various technical means to ensure information security. The research results of this paper provide financial institutions with more comprehensive and effective information security measures, which can help financial institutions better cope with the information security challenges in the era of big data. In the future, with the continuous progress of technology and the continuous development of the financial industry, financial information security will still face new challenges and opportunities, and it is necessary to continuously strengthen research and exploration.

References

[1] Liu Shiqi. "Internet plus Finance" mode of information security risk prevention [J]. China Management Informatization, 2022, 25(18): 103-105.

[2] Zeng Chen. Innovative Internet financial information security risk prevention system and mechanism-taking Liuzhou Bank as a case [J]. China Market, 2022(1): 48-49

[3] Li Zhaoqing. Risks and Countermeasures of Financial Information Security under Mobile Internet [J]. Mobile Information, 2021(8): 117-118.

[4] Rebecca. Financial information security and risk from the perspective of Internet [J]. Trade Exhibition Economy, 2021(24): 65-67.

[5] Xie Ying. Discussion on Internet financial risk supervision in the era of big data [J]. Times Finance, 2018(29): 59-60.

[6] Chen Xi. Legal protection of financial consumers' right to information security in China [J]. Science and Education Guide, 2020(31): 71-72.

[7] Chen Xi. Discussion on the legal protection of personal information security rights of Internet finance consumers [J]. Science and Education Cultural Exchange, 2019(11): 191-192.

[8] Ding Yu. Prevention and control of financial information security risks from the perspective of software legalization [J]. Financial Technology Times, 2020(9): 87-90.