Research on Information Security Management and Protection Measures of Financial Enterprises in the Era of Big Data---Take the USA of Industrial and Commercial Bank of China

Chuhan Sun

Business Administration, United International College (UIC), Zhuhai, Guangdong, 519087, China

r130024209@mail.uic.edu.cn

Abstract. The Internet is changing the way people live all the time. With the development of the country's information technology, the transmission and sharing of data information is more and more convenient, which has completely changed the way people live, work, and study. In the era of big data, data has become an important element of enterprise development, and those who have mastered the data have the key conditions for development. But at the same time, information security has become a common concern. Especially for banks in the digital era, the information security of banks will face many security risks. Suppose the information security management system of the bank is not perfect. In that case, the leakage and loss of important information and data will cause very serious consequences and even bring greater risks to the bank's operation and management. Therefore, the protection of information security is particularly important. In view of this, this topic will take the USA of Industrial and Commercial Bank of China (ICBC, USA) as a case study to study its information security management and protection.

Keywords: Era of Big Data, Bank Information Security, Management and Protection Measures.

1. Introduction

1.1. Research Background

With the continuous development of science and technology and the rapid development of information technology, people have entered a new era - the era of big data. Big data, as a new type of data resource, not only changes the way people acquire and process data but also has a profound impact on the development and decision-making in various fields. In the context of today's big data era, the application of big data-related technologies will have an impact on all aspects of people's lives, including travel, office, education, medical care, finance, and other fields. So, for the financial industry, data has become increasingly important.

On October 29-30, 2021, the State Bank of Pakistan (NBP) suffered a serious cyber attack. The bank's back-end systems were affected, including servers used to connect to the bank's branches, back-end infrastructure that controls the bank's ATM network, and mobile applications. According to the bank, although the attack deactivated some of the bank's systems, there was no loss of funds. Immediately after the attack, the bank took steps to isolate the affected systems and carried out emergency recovery efforts over the weekend. In September 2021, Pacific City Bank (PCB), one of the largest Korean community banking service providers in the United States, suffered a ransomware attack. The PCB discovered the security breach on August 30, 2021, and the bank's internal investigation into what happened was concluded on September 7, 2021. As a result of the attack, the bank's loan application forms, tax filings, W-2 information for client companies, payroll records for client companies, full names, addresses, social security numbers, and payroll and tax details were compromised. There are many similar incidents, and it can be seen that the bank's information security protection is very important. If the information security management system of the bank is not perfect, then once hackers attack it, it will cause very serious consequences.

Since the release of the Personal Information Protection Law and the Data Security Law, information security has risen to the height of national security. At the same time, the scope, frequency, and intensity of the investigation and treatment of violations of data security laws and

regulations have been increasing. In the third quarter of 2023, the People's Bank of China and the General Administration of Financial Supervision issued 425 data fines to banks, insurance companies, securities companies, and other financial institutions, with a fine amount of 7.69 billion yuan, involving 266 legal persons. The number of tickets in this quarter increased by 40.3% from the previous quarter and 32.4% from the same period last year, and the number of tickets has steadily increased [1]. It can be seen that the supervision and supervision efforts are also escalating. It can be seen that the financial industry pays more and more attention to information security management. For banks, once information security is threatened, it will cause very serious consequences. Therefore, the research on information security management of banks is very important, and it is hoped that bank managers can pay more attention to information security management and protection.

1.2. Literature Review

Ma Ling highlighted the importance of building a robust information security system for commercial banks, addressing existing issues and proposing solutions [2]. Yao Jian highlighted the role of information security in enterprise development, highlighting threats like leakage, tampering, and data loss that can lead to economic losses [3]. Huo Baodong proposed that commercial banks must pay great attention to information security management, predict the risks existing in the application of new technologies, and put forward relevant suggestions for information security management and protection measures [4]. Wang Zhiyang analyzed Citibank's information security management and proposed solutions, emphasizing the importance of improving the system in the era of big data [5]. Overall, the importance of effective information security management in the banking sector cannot be overstated.

Emerging technologies like artificial intelligence and the Internet of Things are increasingly being used in the financial industry, but there is a lack of research on their potential challenges and opportunities for banking information security. Therefore, it is necessary to study how to deal with the security risks brought by emerging technologies and how to use these technologies to enhance information security protection capabilities. Bank internal personnel is a part of bank information security, but the current research mostly focuses on technical measures and system design, and relatively few studies on the cultivation of security awareness of bank internal personnel. Although technical measures play an important role in bank information security, human factors are also weak links in information security. Human factors are also weak links in information security, so it is essential to study how to improve employee attention and awareness of information security and reduce the risk of human factors through training and education.

A large number of studies have found that there are many problems in information security management. Therefore, this paper will take the USA of Industrial and Commercial Bank of China as an example to analyze the current situation of information security management, put forward the shortcomings of information security management, and make suggestions. This paper summarizes the most effective protection measures for the financial industry to deal with information security risks.

2. Case Description

2.1. Introduction of ICBC and USA

ICBC USA, a subsidiary of the Industrial and Commercial Bank of China, is a leading commercial bank in the United States, offering a comprehensive range of financial services including corporate, personal, and international banking. Its commitment to providing one-stop financial solutions to both corporate and individual customers in the United States and China.

2.2. Information Management Problem

ICBC Financial Services Co., LTD., a U.S. subsidiary of Industrial and Commercial Bank of China, experienced a LockBit ransomware attack on November 8, causing system disruptions. Although

ICBC headquarters and overseas branches were not affected, the attack affected ICBC Financial's ability to clear pending U.S. Treasury market. Security expert Kevin Beaumont speculates that attackers may have exploited the Citrix Bleed vulnerability (CVE-2023-4966), which was not patched in time. From this case, it can be seen that a good information security management system is very important for the financial industry because it involves whether the security system has enough ability to defend against attacks and make corresponding strategies when attacked. This highlights the importance of a robust information security management system for the financial industry.

3. Analysis on the Problem

Marcus Murray, founder of Swedish cybersecurity firm Truesec, said: "The ransomware attack on ICBC is a major shock for the world's largest financial companies. From the moment it comes to light, the ICBC hack will force the world's largest banks to race to improve their defenses." Below, this article will analyze three aspects of why Industrial and Commercial Bank of America branch this crisis event.

3.1. Information Technology Vulnerabilities

The financial industry is increasingly prioritizing the enhancement of information technology to ensure the security of its data in the era of big data. The defense against network attacks mainly relies on advanced information technology as support to resist the network attacks of criminals. In terms of information security, some banks only pay attention to basic protection measures such as firewalls and anti-virus software, ignoring other important technical measures such as access control and encryption. At the same time, the lack of awareness to upgrade and patch security vulnerabilities in a timely manner makes systems and application software vulnerable to attacks. The Industrial and Commercial Bank of China was targeted due to its failure to patch technical loopholes in time, allowing hackers to exploit this vulnerability, causing some systems to fail and clearing through the U disk. In addition, when the system is found to be unable to operate, ICBC should use more advanced technology to restore the system immediately, rather than having no way but to use a USB flash drive to transmit data. Information security is a complex field that requires professional personnel to be responsible for information security management and response to security incidents. However, banks cannot effectively deal with and manage security risks if they lack sufficient professionals [6].

3.2. Lack of Employee Awareness

Wang pointed out the problems existing in bank information security management, including the lack of security awareness of employees in bank information security management [7]. At present, the management of information security in many banks only requires staff to have technical skills, and there is no risk awareness and security awareness training for information security managers. Employees in enterprises have insufficient awareness of the importance and risk of information security, lack necessary security awareness and behavior habits, and are prone to neglect or negligence of security regulations. In this way, once information security problems occur, employees' emergency response and processing capabilities for security incidents may be insufficient, which will lead to the expansion or chain reaction of security incidents and then cause huge losses for enterprises [8]. Industrial and Commercial Bank of China, due to the lack of security awareness of employees, and when they found technical loopholes but did not solve the problem in time, it suffered from a LockBit ransomware attack. It would have caused part of the system to fail. If the technical problems had been found and the managers had asked the employees to fix them in time, the crisis would not have occurred. In the era of big data, enterprises should not only require information security management employees to have certain skills but also have security awareness. In this way, when an emergency occurs, the bank can make the fastest response to solve the problem and better protect the information assets inside the bank [9].

3.3. Imperfect Information Security Management System

Lin pointed out that the main problem of the bank is that the information security management system is not perfect. It mainly includes many aspects, such as incomplete internal control mechanisms and non-standard information security management [10]. Once the information management system is not perfect enough, when there is an illegal attack, employees will not be able to make an emergency response quickly according to the system, and they will be disorganized in front of the illegal attack. In today's changing times, imperfect information management systems will have very big information security risks. The problem of the ICBC this time is also because there is no perfect management system for information security in the management system. If there is a perfect information security management system, the awareness of employees will be enhanced because of the system, and the loopholes in technology will be repaired immediately according to the requirements of the system instead of shelving, which will not cause such serious consequences.

4. Suggestions

4.1. Strengthen Information Technology Support

Guo Xiaoli summarized the current situation of big data information security and put forward corresponding information security protection measures. It includes the guarantee of information security technology [11]. If the Industrial and Commercial Bank had strengthened the technical support and patched the loopholes in the system in time, there might not have been this attack. In the era of big data, only by strengthening information security technology can enterprises avoid information leakage in dangerous situations. For example, in the event of hacker attacks and network fraud, there can be enough technology to support the security of enterprise information and protect the core competitive assets of enterprises [12]. Enterprises can strengthen network security measures, including the use of technical tools such as firewalls to protect enterprise network systems and ensure network security. By establishing a secure backup and recovery mechanism, data can be backed up regularly and a sound data recovery mechanism can be established to cope with possible data loss or damage. Employees should regularly conduct vulnerability scanning and security assessments on the system and timely patch system vulnerabilities to reduce the possibility of hacker attacks. Enterprises can comprehensively strengthen information technology support, effectively protect enterprise information security, and reduce information security risks.

4.2. Enhance Employee Information Security Training and Education

Strengthening the security awareness of employees and conducting regular information security training and education can make employees understand security risks and preventive measures and prevent security loopholes caused by negligence or misconduct of employees. Carry out regular security training for employees to improve their awareness and cognition of information security [13]. ICBC should strengthen the security awareness of employees and ensure that the company has clear information security policies, including regulations on how employees handle sensitive information and how to use company equipment, so that employees clearly know their responsibilities and obligations in information security. Banks should train their staff on what to do in the event of an emergency so that it does not lead to malicious attacks. If employees have a high enough awareness of information security, they will repair system vulnerabilities in time to eliminate security risks and avoid network attacks. Regular information security training courses can educate employees on basic skills like identifying phishing emails, creating secure passwords, and protecting company data, thereby enhancing overall security. Enterprises can regularly organize information security exercises to simulate various information security incidents so that employees can learn how to deal with various security threats and improve their information security emergency response-ability. Establish an internal communication mechanism to allow employees to report security incidents or issues to

the information security team at any time while strengthening the supervision and review of employees to ensure that employees comply with information security policies and regulations.

4.3. Improve the Information Security Management System

By analyzing the current situation of enterprise information security, Zhang Wani proposed measures for enterprise information security management and protection, construction of security system, and improvement of information security system [14]. The information security of enterprises cannot be separated from the perfect management system. Enterprises can formulate and implement information security policies, norms, and processes to clarify their requirements and standards for information security. It can also establish and improve the information security management system, including risk assessment, security control, etc. These systems will make the information security of enterprises perfect and avoid information leakage [15]. It is precisely because of the lack of a sound information security management system in ICBC that the employees did not repair the loopholes in time according to the system, which led to the occurrence of this incident. ICBC should formulate a clear information security policy, clearly specify the information security standards, procedures, and division of responsibilities of the enterprise, and ensure that every employee understands and complies with the relevant regulations. In this way, it is possible to avoid similar incidents. The enterprise may also set up an information security management department responsible for the coordination and supervision of information security affairs, regularly audit and evaluate the information security system, find problems and timely improve and perfect, and ensure that the system is fully implemented. An access control mechanism can be established within an enterprise to restrict employees' access to sensitive information and systems, and strict access control can be implemented to avoid unauthorized access. Only by improving the information security management system and improving the information security level of enterprises can the information assets of enterprises be effectively protected from threats.

5. Conclusion

People are increasingly utilizing vast amounts of data to enhance their quality of life, yet the promotion and application of big data technology require numerous technical personnel to address existing issues. For enterprise information security management, it is necessary to change the system and improve the protection measures according to the changes of The Times so as to protect the information of the enterprise and keep the competitiveness of the enterprise in the development of The Times.

This paper mainly analyzes the reasons for the cyber attack on ICBC from three main aspects and puts forward corresponding suggestions. This paper mainly studies the problem of enterprise information security management and protection under big data, which is very important for the development of enterprises because the huge amount of data allows enterprises to more fully and accurately understand the changes and complexities of the market, so as to make more informed decisions. The mastery of core data is the mastery of important assets. So, information security protection is very important. This article significantly contributes to the protection of enterprises' information security and serves as a reminder to enhance their attention to this area. However, there are some limitations to this article. This paper only uses the method of literature research and does not find more data to support it. In the future, more literature can be found to search for data on this topic, which can better support the readability of the article.

The era of big data brings people both opportunities and challenges. Only through continuous in-depth research and continuous exploration of the boundaries of technology and application can people better cope with and grasp the development opportunities of this era. This paper aims to have some reference for the management and protection of enterprise information security. Only on the premise of ensuring data security and privacy can people better take advantage of big data and promote innovation and progress in various fields of society.

References

[1] KPMG Corporate Advisory Limited, Third Quarter 2023 Financial Regulatory Data Penalty Analysis and Insight Recommendations, 2023.11.23, 2024.2.16, https://kpmg.com/cn/zh/home/insights/2023/11/financial-industry-regulation-2023-q3-data-penalty-analysis-and-insight-suggestions.html.

[2] Ma Ling. Try to talk about the commercial bank the construction of information security management system. Computer programming skills and maintenance, 2020 (8): 113-114+117. Doi: 10.16184/j.cnki.com.prg. 2020.08.040.

[3] Yao Jian. Problems and Countermeasures of Enterprise Information Security. Information and Computer (Theoretical Edition), 2019, 31 (19): 224-226.

[4] Huo Baodong. On Information security Risk Management of commercial banks in the era of Financial technology. China Financial Computer, 2017 (08): 17-19.

[5] Wang Zhiyang. The information security management of commercial Banks - citigroup, for example. Computer knowledge and technology, 2017, 13 (22): 90-91+100. DOI: 10.14004/j.carol carroll nki CKT. 2017.2510.

[6] Tang Yi. The problem of network security management in enterprise information construction research. Modern industrial economy and information technology, 2018, 8 (9): 59-60. DOI: 10.16525/j.carol carroll nki.14-1362/n. 2018.09.24.

[7] Wang Guifu. Problems and Countermeasures of computer information security in grassroots commercial banks -- taking Guyuan City as an example. Financial Technology Times, 2016 (11): 58-60.

[8] Pan Aiwu. Discussion on SME Information Security Problems and Countermeasures. Oriental Corporate Culture, 2012 (17): 66-67.

[9] Liu Yang. Problems and protective measures of enterprise information security management. China Science and Technology, 2018 (20): 27-28. (In Chinese) DOI: 10.3969/j.issn.1671-2064.2018.20.014.

[10] Lin Xuegang. Problems and Measures of information security Management of grassroots central banks. South China Financial Computer, 2010, 18 (08): 54-55.

[11] Guo Xiaoli. Analysis of enterprise information security strategy in the era of big Data [J]. China Management Informatization, 2021, 24 (20): 115-116.

[12] Jiang Du. Research on Enterprise Information Security and Privacy Protection in Big Data Environment. 2021 3rd International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI), Taiyuan, China, 2021, pp. 324-327, Doi: 10.1109/MLBDBI54094.2021.00067.

[13] Zhong Quan DE. Introduction to risk analysis of enterprise data security and protection. Computer knowledge and technology, 2017, 13 (32): 58-60 + 73. DOI: 10.14004/j.carol carroll nki CKT. 2017.3457.

[14] Zhang Wanni. Enterprise information safety management present situation and strategy research. Modern industrial economy and information technology, 2022, 12 (01): 123-124 + 127. DOI: 10.16525/j.carol carroll nki.14-1362/n. 2022.01.043.

[15] Mehrdad Sepehri Sharbaf. 2014. A New Perspective to Information Security: Total Quality Information Security Management. In Proceedings of the 7th International Conference on Security of Information and Networks (SIN '14). Association for Computing Machinery, New York, NY, USA, 56–60. https://doi.org/10.1145/2659651.2659666.