Research on Security Risk Assessment and Management of Information System Based on AHP-DEA

Qingqing Cao(✉) and Lanye Wang

Officers College of PAP, Chengdu, China
caoqingqing08@qq.com

Abstract. The openness of the network poses a challenge to the security of the information system. The risk assessment of the security of the information system can find out the weaknesses of the information system and improve the security of the information system in a timely manner. By using delphi method to obtain information system security risk assessment indicators from relevant experts, and build an evaluation index system, the information system security risk of 12 relevant units was assessed by combining AHP and DEA methods, and the assessment result was that the information system security risk of unit 6 was the largest, the unit shall formulate corresponding measures to timely check and fill in gaps to ensure the security and availability of the information system. The research shows that the evaluation of information system security risks can reveal the shortcomings of each unit in information system security, and carry out targeted remedial measures to improve information system security in an all-round way.

Keywords: Information system · safety risk assessment · AHP and DEA methods

1 Research Theoretical Basis

1.1 Relevant Concepts of Information System Security Risk Assessment

Information system is a human-computer system that collects, processes, stores, transmits and retrieves information according to certain application goals and rules [1]. It consists of computer hardware, application software, communication network, data storage, personnel information and rules and regulations. Information system security is to protect the information system from accidental or intentional unauthorized disclosure, modification, damage and loss of the ability to process information. The essence is to protect the security of information. Information system security risk refers to the possibility of information security events and the impact on the organization caused by human or natural threats to take advantage of the vulnerabilities in the information system and its management system [2]. Information system security risk assessment is a stage of information system security risk management. From the perspective of risk management, scientific analysis methods are used to obtain relevant risk factors affecting information system security, analyze their causes, and carry out risk control on their results.

D. Kumar et al. (Eds.): IEIT 2023, AHSSEH 10, pp. 401–410, 2023.
https://doi.org/10.2991/978-94-6463-230-9_47

1.2 Safety Risk Assessment Method

Safety risk assessment can be divided into qualitative assessment, quantitative assessment and combination of qualitative and quantitative assessment according to different assessment methods. This paper summarizes the commonly used methods of safety risk assessment by consulting relevant data. It can be clearly seen from the description of the advantages and disadvantages of these methods that the applicability and limitations of each evaluation method are different, See Table 1 for details.

From Table 1, we can see that many of the safety risk assessment methods described above are prone to subjective problems in the setting of weights. At the same time, there is duplication of information among multiple indicators. Some methods can only analyze a single organization from a microscopic perspective, and cannot compare data in the industry. Therefore, after comparison and analysis, this paper uses the Delphi method and the combination of AHP and DEA to establish the AHP-DEA model. The evaluation process of the method selected in this article is introduced in detail.

(1) Delphi method
The Delphi method usually asks for experts' opinions by letter, and its general process is to sort out, summarize and count the problems to be predicted after obtaining the experts' opinions, and then anonymously feed back to the experts, and then ask for opinions again, and then concentrate and feed back until the consensus is reached.

Table 1. Common methods of safety risk assessment

Method	Merits	Demerits
Analytic hierarchy process (AHP)	It greatly reduces the difficulty of comparing elements with different properties.	It is mainly based on subjective thinking, and the evaluation result is not easy to be recognized by everyone.
Fuzzy comprehensive evaluation method	Easy to operate, mainly solving multi-level and multi-factor problems.	The information between indicators is prone to overlap; The weight setting is subjective.
Factor analysis	The weight setting is scientific and objective.	The demand for data is relatively large, and the statistical work is large.
Data envelopment analysis (DEA)	Comparable with similar products, capable of large-scale application and promotion.	Analysis and evaluation are generally carried out for similar units.
Delphi method	It can give full play to the role of experts, brainstorm and have high accuracy.	The process is complex and takes a long time.
Historical comparison method	It has strong comparability and is easy to find problems.	Historical indicators can only represent the actual level in the past, not the reasonable level.

(2) Analytic hierarchy process
In the early 1970s, the American operational research scientist T. L. Saaty, a professor at the University of Pittsburgh, studied the topic of "power distribution according to the contribution of various industrial sectors to the national welfare" for the US Department of Defense, applying network system theory and multi-objective comprehensive evaluation method, a hierarchical weight decision analysis method is propose. AHP is an evaluation method that decomposes the relevant elements of the decision-making problem into objectives, criteria, schemes and other levels, and carries out qualitative and quantitative analysis on this basis. When evaluating the evaluation index without unified evaluation criteria, the corresponding grade of the evaluation is obtained through the experience judgment of the evaluator, and the evaluation grade is collected for mathematical modeling [5].The main analysis process of this method is as follows: First, create a hierarchy model; The second is to create a judgment matrix, In this paper, we mainly select the 9-level scoring criteria and assign values to each index according to the different impact, so as to create a paired comparison matrix; Third, carry out consistency inspection; The fourth is hierarchical single ranking, which mainly refers to the calculation of the weight of the importance of the factors related to the previous level and the current level according to the elements in the matrix [6].In this paper, hierarchical single ranking refers to the weight of entity security, data security, network security, system security and management security in the information system security risk assessment index system.

(3) Data envelopment analysis
Data Envelopment Analysis (DEA) is an efficiency evaluation model developed by Charnes and other scholars in the United States based on Farrell's technical efficiency boundary method [7], which extends the concept of engineering efficiency of single input and single output to the effective evaluation of the same kind of decision-making with multiple inputs and outputs, is a common efficiency evaluation method to evaluate the relative efficiency of a group of DMUs (Decision Making Units) with multiple inputs and outputs [8].The main analysis process of this method is as follows: First, clear evaluation purpose; The second is to determine the decision-making unit (DMU); The third is to create a multi-input and multi-output evaluation index system; Generally, the output index is the utility index, and the input index is the cost index; Fourth, collect and summarize data; Fifth, select the DEA model and calculate it. DEA has two basic models, C^2R and BC^2. The C^2R model solves the DMU with no change in the return on scale. According to the overall effectiveness of technology and scale, the corresponding technical efficiency value of DMU is calculated. In this paper, C^2R model is selected for calculation; Sixth, analyze the evaluation results and put forward decision suggestions [9].

1.3 Establishment of Information System Security Risk Assessment Index System

The Delphi method can overcome the shortcomings of the expert meeting method. It is to ask questions to the selected experts in the form of investigation and consultation, summarize and sort out the experts' opinions, and then anonymously feed back the obtained opinions to each expert, and then ask for opinions again, sort out and feed back until the opinions are consistent. According to GB17859-1999 Classification Criteria for Security Protection of Computer Information Systems, and in combination with the relevant data of information system security risk assessment research, a questionnaire was designed, and five experts were selected. Through three rounds of anonymous surveys, fifteen evaluation indicators in five major aspects were determined.

1.4 Physical Security

Physical security mainly includes hardware equipment, software equipment and physical environment security. Hardware equipment includes computer equipment, such as computer terminals and servers, network equipment, storage equipment, security equipment, security equipment, etc. Hardware equipment is the basis for the overall operation of the system network. If the hardware equipment is damaged by human, it cannot operate. Software equipment mainly includes system software and application software. The system software, such as the operating system, has security vulnerabilities and other problems. The application software, such as code vulnerabilities and access restrictions, causes software use failures. The security of software equipment affects the implementation of business and the stable operation of the system. The factors affecting the physical environment mainly include natural disasters such as earthquake, fire, flood, electromagnetic interference, insect pest, and temperature, humidity, dust, static electricity, power failure, etc. The occurrence of these factors will lead to security risks in the physical environment.

1.5 Data Security

Data security mainly refers to the security of data storage, data use and data transmission. Data storage mostly relies on databases for storage, such as MySQL, Oracle and other databases, which will have many security vulnerabilities. Hackers steal all user data databases by exploiting system vulnerabilities and other means, so the index set here is database security. In the data transmission stage, the attacker illegally intercepts the data in the transmission, leading to the occurrence of information disclosure events. Therefore, it is necessary to adopt the encryption level identification technology, implement the hierarchical management of information, adopt different intensity encryption protection, and use encryption technology to ensure the security of data transmission. The index set here is data encryption. In the data use stage, attackers steal the identity of legitimate users and illegally read key data, which leads to the occurrence of information leakage events or information systems. Therefore, necessary authentication mechanisms should be added, and security authentication indicators should be set here.

1.6 Network Security

Network security mainly includes network access control, network defense mechanism, and network security equipment configuration. The network is the medium for users to access the system and transmit information. Once a security attack is launched against the network, it will directly affect the normal information communication. Network access control refers to the access to network equipment, such as switches, intranet networks and extranets; Network defense mechanism refers to the ability to prevent network intrusion, viruses, trojans and worms, and the ability to prevent the spread of infection after being infected; Network security equipment configuration refers to whether the configuration of network access equipment, firewall, network audit equipment and other network security equipment meets the actual business needs [10].

1.7 System Security

System security mainly includes system backup, security level and system maintenance. System backup refers to the ability to regularly backup, implement remote backup, heterogeneous backup and other backup methods, and establish a disaster recovery backup center to prevent data loss or damage. Security level refers to the ability to purchase and use information security products of corresponding level and implement security technical measures according to the information security protection level. System maintenance is to upgrade and maintain the original system in a timely and convenient manner according to the problems found in use and new work requirements.

1.8 Management Security

Management safety mainly includes management system, management organization and management personnel. Management safety risk mainly comes from human factors and is caused by improper management. Management system refers to the current corresponding security management rules and regulations are not perfect, or the implementation of relevant security management rules and regulations is not in place, resulting in non-standard information system security management and affecting the normal operation order of the information system. The management organization mainly reflects the unclear responsibilities and the insecure supervision mechanism. The responsibility and authority refers to the clear responsibility and authority of each department and personnel of the organization to prevent confusion of responsibilities or lack of supervision. In terms of management personnel, it mainly reflects that there are too few professional management personnel or the quality of existing management personnel is low, and they do not have the sense of security and confidentiality, which is easy to cause work errors or spread the corresponding content through secret stealing, which brings huge losses to the organization.

The final information system security risk assessment index system is shown in Table 2.

Table 2. Information system security risk assessment index system

Information system security risk assessment Index system	Physical security	Hardware device
		software device
		Physical environment security
	Data security	database security
		data encryption
		Safety certification
	Network security	Network access control
		Network defense mechanism
		Network security device configuration
	System security	System backup
		Safety level
		system maintenance
	Manage security	management system
		management organization
		Management talents

2 Information System Security Risk Assessment Based on AHP-DEA

Five experts were asked back to back by using the Delphi method, according to their practical experience and understanding of the relevant importance of these elements, the questionnaire was scored. According to the scale corresponding to the mode representing the results of the importance between the two indicators, a judgment matrix was established, and the weight values of the first-level indicators were obtained as shown in Table 3.

The After calculating the weight of the first level index using AHP method, DEA method is used to deal with the second level index, and the information system security risk of the participating units is compared according to the calculation results. Now 12 units are selected as the evaluation objects, and the 12 units participating in the evaluation are selected as the 12 decision-making units DMU1, DMU2, DMU3, DMU4… DMU12. For each decision-making unit DMUj (j = 1, 2,… 12), the secondary indicators under

Table 3. Weight values of primary indicators

	Physical security A1	Data security A2	Network security A3	system security A4	management security A5
Weight value	0.133	0.2433	0.1467	0.2583	0.2183

each first-level indicator can be used as the output indicators. Set the input indicators as the selected 12 evaluation units. Because all of them are of the same type and meet the same set indicators, the input data of these 12 evaluation units are set as 1. In order to normalize the secondary indicators under each primary indicator, it is necessary to calculate the evaluation value of the secondary indicators. Grade the secondary indicators under each primary indicator by inviting 2 superior experts and 3 experts from the unit. Now take the secondary indicators under network security as an example to illustrate. When sending questions to experts, clarify the meaning of each comment and the evaluation characteristic points to the members of the expert group to avoid the evaluation deviation caused by human factors. The indicators in the questionnaire are divided into five levels, namely 5, 4, 3, 2, 1, which means that the indicators are rated very good, good, relatively good, average and poor. Then take the arithmetic sum of experts' evaluation on a certain indicator as the value of the output indicator. As shown in Table 4.

Table 5 shows the DEA efficiency values of 12 units in network security by using DEAP software.

From the above efficiency index, we can see that in terms of network security, unit 1 has the largest information security risk, followed by unit 10, unit 3, unit 4 and unit 12. These units should check and fill in the gaps in network security, make up for the weaknesses, and enhance the security of their information systems.

In the same way, the DEA efficiency values of each unit in terms of physical security, data security, system security and management security can be obtained. The weight of the first-level indicators and the score of the second-level indicators under each first-level indicator are obtained through the previous calculation. After the normalization of the

Table 4. Network security input and output index values

	Output index 1	Output index 2	Output index 3	Input index
DMU1	15	17	21	1
DMU2	14	18	13	1
DMU3	12	19	13	1
DMU4	18	14	12	1
DMU5	20	12	18	1
DMU6	14	19	20	1
DMU7	16	13	23	1
DMU8	14	19	21	1
DMU9	16	20	15	1
DMU10	19	12	15	1
DMU11	21	11	20	1
DMU12	10	19	17	1

Table 5. DEA efficiency index and ranking results of each unit in network security

	Efficiency index	Sequencing result
DMU1	0.991	6
DMU2	0.900	12
DMU3	0.950	10
DMU4	0.951	9
DMU5	0.984	7
DMU6	0.993	5
DMU7	1.000	1
DMU8	1.000	1
DMU9	1.000	1
DMU10	0.947	11
DMU11	1.000	1
DMU12	0.970	8

Table 6. Final evaluation score

	Evaluation score	Sequencing result
DMU1	0.08629	1
DMU2	0.08408	2
DMU3	0.08123	11
DMU4	0.08243	10
DMU5	0.08375	4
DMU6	0.08121	12
DMU7	0.08338	6
DMU8	0.08267	8
DMU9	0.08357	5
DMU10	0.08282	7
DMU11	0.08386	3
DMU12	0.08265	9

score of the second-level indicators, the final total ranking of the 12 units is carried out using the formula $\sum_{i=1}^{12} W_i \overline{\theta_{ij}^*}$. The final evaluation scores of 12 units are shown in Table 6.

According to the results, the final evaluation scores of the 12 units are ranked from high to low as Unit 1, Unit 2, Unit 11, Unit 5, Unit 9, Unit 7, Unit 10, Unit 8, Unit 12, Unit 4, Unit 3, and Unit 6. Results The information system security risk of unit 6 was the largest, followed by unit 3 and unit 4. The information system security level of unit 1 is higher, and the unit with higher information system security risk can learn from the relevant practices of the unit with higher information system security level, so as to learn from each other, develop corresponding measures, and timely check and fill in the gaps to ensure the security and availability of the information system.

3 Conclusion

To sum up, building a set of security risk assessment index system for information systems can provide quantitative tools and scientific theoretical methods for information system security risk assessment. Based on the information system security risk assessment index system, this paper makes a comprehensive and scientific risk assessment on the information system security of 12 units of the same type, and finds out the units with important risk hidden dangers. Units with high risks need to formulate corresponding improvement measures according to the evaluation results, reduce the occurrence of risks and the possibility of losses caused by risks, and improve the security level of information systems as a whole. Because the risk assessment of information system is a complex system engineering with many influencing factors, the research in this paper inevitably has certain limitations. It is recommended to use emerging technologies such as big data technology to carry out the risk assessment of information system security in order to promote the orderly development of management work.

References

1. China National Standardization Administration Information Security Technology Information Security Risk Assessment Specification [EB/OL].
2. Li Zhiyong. Information security risk management [M]. Beijing: Chemical Industry Press, 2020-3-4.
3. Liu Yajuan. Research on financial performance evaluation of T Media Company based on AHP-DEA model [D]. Shaanxi: Xi'an Petroleum University. 2021.
4. Ma Feicheng, Lai Maosheng. Information Resource Management (Third Edition). Beijing: Higher Education Press, 2018.
5. Song Chao. Research on hospital information system security risk assessment based on network analytic hierarchy process [D]. Zhejiang: Zhejiang University, 2022.
6. Qin Xiaowei. Research on the whole-cycle risk management of construction projects of construction enterprises based on the analytic hierarchy process. The fourth meeting of the eighth session of the China Construction Accounting Association and the 2022 annual meeting, 2022-12-29.
7. Yang Guoliang, Liu Wenbin, Zheng Haijun. Overview of Data Envelopment Analysis (DEA). Journal of Systems Engineering, 2013, 28 (6): 840–860
8. Pongpanich R, Peng K C. Assessing the operational efficiency of agricultural cooperative in Thailand by using Super-SBM DEA approach. International Journal of Scientific and Research Publications, 2016, 6(5): 247–253. LI Xuan. The application of artificial intelligence knowledge graph technology in the field of psychology research [J]. Chinese high-tech, 2022(3).

9. Ma X J, Wang C X, Yu Y B, Li Y D, Dong B Y, Zhang X Y, Niu X Q, Yang Q, Chen R M, Li Y F, Gu Y H. Ecological efficiency in China and its influencing factors—a super-efficient SBM metafrontier-Malmquist-Tobit model study. Environmental Science and Pollution Research, 2018, 25(21): 20880–20898.
10. Huang Lifeng, Pei Wei, Lu Nan. Risk assessment and management of confidential information security [C]. International academic exchange seminar on smart city and information construction, 2016-12-15.