Research on Risk Assessment of Information Security of Universities in China Based on AHP

Miao Wang

Xi'an Peihua University, Xi'an, 710125, China

Keywords: Risk assessment, Information security, AHP

Abstract: The rapid development of the internet has enhanced the teaching management in universities to a great extent, while the risk of information security cannot be ignored in the construction process of smart campus. In this paper, AHP is applied to build a hierarchical structure model to evaluate information security risk, and a safety evaluation index system is determined, which provides a feasible method for risk assessment of information security in universities.

1. Introduction

Nowadays, the terminal of mobile phone and computer is widely used in college campus, and it also integrates the daily life of teachers and students. Under such a background, it is very necessary and urgent to strengthen the security strategy of the risk of information security in Colleges and universities. Especially in recent years, under the influence of the rapid increase of Internet bandwidth and the pace of construction of big data, the development of information security in traditional backward universities has been strongly impacted. It can be seen from this, to do a good job of ensuring the security of information security in universities, to promote the better development of the university education. With the development of computer and network technology, the scale of campus network is becoming larger and larger, and there are many problems in the use of information system. Some colleges and universities lack the system and measures of crisis awareness and risk prevention, and there is no set of information system risk assessment system to prevent risk. It is difficult to deal with the crisis correctly and effectively when the unexpected public events can only be dealt with passively. The information security risk assessment system is not an overnight result. This requires various departments and links to coordinate and coordinate each other, strive to achieve standardization and institutionalization of risk assessment, and gradually form an effective mechanism for monitoring risk. The development of foreign universities has a long history, and many well-known high - level universities are private universities funded by enterprises or run by enterprises. These universities apply the management mode of the enterprise flexibly to the daily management of the school, and the risk assessment and management of information security is a very important part. The islanding phenomenon of information system security has become increasingly prominent. The information security risk assessment from the perspective of risk management, the use of scientific methods and means, the vulnerability of the systematic analysis of the threats facing the information system and the existing evaluation, once the security incident may cause harmful levels, puts forward the protection against the threat countermeasures and corrective measures, to prevent and resolve information security risks and control the risk at an acceptable level, to maximize the protection of information security.

2. Summary of Analytic Hierarchy Process

Analytic hierarchy process (AHP) is a multi-objective and multi criteria decision making method that combines quantitative analysis with qualitative analysis. It can effectively analyze the non-sequential relationship between different levels of target system and comprehensively measure the decision and comparison of decision makers. AHP is a method of hierarchical modeling for the

  DOI: 10.25236/apssh.2019.116

system, and it is also a multi-objective decision analysis method. The application of this method has been successful with many fields: the basic idea of analytic hierarchy process is based on the first analysis to evaluation system about the index, then the index according to some principle is divided into several levels, comparison and analysis of these data, to obtain the weights of different kinds of indexes in the system. In the actual application level can be increased according to the complexity of the system analysis, for example, each program may have sub program, can choose the optimal combination of sub programs, so that the score of the results is more accurate. Involved in the information security risk assessment based on AHP model, in various stages of information security risk assessment using AHP method are analyzed and compared to the corresponding scheme, the analysis system which part of the greatest risk, which minimize the risk, establishing the risk control strategy ready. However, there are some shortcomings in AHP. In the analysis of the need for expert qualitative safety assessment system according to the evaluation scoring method level, scoring results for numerical use cannot accurately reflect the value of all kinds of factors are fuzzy and uncertain, the need to construct a comparative judgment matrix of quantitative risk assessment, the data in the matrix is given by an expert judgment and it has certain one sidedness. Therefore, the conclusions from this calculation are unavoidable. A feasible method is to use the fuzzy mathematics method to calculate the risk based on the analytic hierarchy process, so that the reliability of the calculation results is improved. The basic steps of the risk assessment method based on the analytic hierarchy process are as follows. The decomposition of the system, establish the hierarchical structure model; construct the judgment matrix according to the hierarchical structure model, constructing judgment matrix, if the judgment matrix consistency requirements, processing will continue; otherwise this judgment matrix consistency correction; single level sorting and consistency check. The maximum eigenvalue and eigenvector of the judgement matrix are calculated, and the relative risk weights of related elements in this layer are obtained, namely, single level ranking, hierarchical ranking and consistency checking. According to the results of hierarchical single ranking, we further calculate the combined weights of all elements in each level of the hierarchical structure model compared to the overall goals, and finally get the combined weight of the lowest level elements relative to the overall goals, that is, the total ranking of the layers. Finally, the weight of the indexes of the evaluation system is determined according to the total ranking results.

3. Evaluation Strategies of Information Security Risk of Universities Based on AHP in China

3.1 Asset Evaluation

Risk assessment is a process in which the scope of the risk should be determined at the beginning. The risk assessment of colleges and universities is mainly due to the requirements of its own strategic objectives, and the scope of risk assessment should be determined according to its strategic objectives. The scope may be the whole information and information system of the University, it may also be a separate information system, and it may also be the key business process and secrecy information of the University. The definition of the scope from the strategic requirements, must rely on the information and information system, the main information related to personnel and departments to consider the aspects, which basically involves the business processes, information assets, geographic scope, risk assessment scope can be described from these 3 aspects. Colleges and universities should make clear the target of risk assessment and provide guidance for the process of risk assessment. The information, system, software and hardware and network that support the normal operation of universities are important assets of the organization. Colleges and universities must face the growing security threats from all sides. The system, application software and network of an organization may be a serious threat. At the same time, because of the increasing degree of information technology in universities and the increasing dependence on information system and service technology, more vulnerability may appear. The risk assessment objectives of the organization are mainly from the needs of the continuous development of the organization business, the requirements of the relevant parties, and the requirements of the laws and regulations. When carrying out risk assessment, colleges

and universities should set up an appropriate organizational structure according to the scope and objectives defined above, to support the whole process, such as the establishment of risk assessment teams composed of management, related business backbone and IT technicians. A complete organization can ensure clearly defined responsibilities in risk assessment process. It can recognize organizational safety status from two aspects of management and technology, and ensure communication and decision-making in risk assessment process.

3.2 Threat Recognition

The threat is a major factor in information security risk assessment, through the analysis of threat identification and threat, there are threats to be listed in the system establish an evaluation system of threat assessment AHP, threat factor in the hierarchy, the first layer is the target layer for each asset, threat factor represents on the system risk of each threat size is the need to calculate the various assets with the threat of the size of AHP in the second layer is the key asset in the system, the third layer is the main threat detection system in a variety of testing tools. After establishing the hierarchy diagram of threat assessment, many experts are graded according to the frequency of occurrence and the size of the impact. The assessor based on expert scoring constructs the triangular fuzzy number complementary judgement matrix. Threats can be caused by one or more intentional, unexpected or environmental events, such as natural disasters, unauthorized access, operational errors, eavesdropping and viruses. An asset may face many threats, and a threat can also affect different assets. Threat identification should identify assets that are caused by or affected by who or something, and analyze the possibility of the threat. To assess the risk of the information system, first, we should analyze the risk of the information system. The risk analysis involves the basic elements of asset threat vulnerability and existing security measures. Each element has its own attributes, the attributes of the assets is the value of assets; the threat of property is the main threat, object, frequency and motivation; attribute of vulnerability is a weakness of the severity of assets; the attributes of the existing security measures is a variety of practices, procedures and implementation mechanism. Evaluation in China started relatively late in the information security risk, but the degree of value is very high, many experts and scholars have done a lot of research work on information security risk assessment. After finding the threat faced by information assets, we should distinguish the frequency or probability of threats based on historical experience and relevant statistical data, to determine the possibility of threat, that is, threat assignment. The attractiveness of assets, the ease of asset conversion to remuneration, the technical content of threat, and the difficulty of vulnerability utilization will influence the possibility of threat.

3.3 Vulnerability Identification

Vulnerability is the asset itself, it can be caused by, using the threat of assets or business target damage, it's also a big factor in information security risk assessment: through questionnaire investigation, interview, a site survey, document review, tool scanning, host audit, network structure analysis, business process analysis, penetration testing etc. methods existing in the system vulnerability list. The establishment of vulnerability assessment level in winter, vulnerability assessment layers, the first layer is the weakness factor system, that is to calculate the exposure degree of vulnerability, is the target layer in the AHP hierarchy, the second layer is the threat layer, it is possible to exploit vulnerabilities threat is the rule layer in AHP third layer; is the actual vulnerability existing in information system. Vulnerability assessment, also known as vulnerability assessment, is an important part of security risk assessment. The weakness is the existence of the asset itself, which can be used by threats and cause damage to the assets or business goals. Due to the lack of adequate safety control, the information assets of universities may be threatened by weakness. These weaknesses may come from organizational structure, personnel, management, procedures, and assets themselves. For example: the lack of protection in the machine room, the voltage fluctuation used by the equipment, the defects of the software, the hacker invasion, the uncontrolled copy of the file, the lack of security consciousness of the personnel, etc. The vulnerability of information assets is analyzed for every asset that needs to be protected, and we can find out the vulnerabilities of every

threat and evaluate the possibility of vulnerable spots being threatened. Similarly, we can take the method of grading assignment to determine the possibility of vulnerable sites being threatened. For example, we can divide the possibility. The confirmation of existing safety measures is needed to confirm the effectiveness of the control measures adopted, and continue to maintain effective control measures to avoid unnecessary work and expenses. For those that are deemed to be inappropriate, we should cancel or adopt more appropriate control alternatives.

3.4 Risk Calculation

According to the definition of risk, risk is the result of three aspects: the threat and vulnerability of assets, and the potential impact of vulnerabilities. Risk is a function of the possibility of a threat, the possibility of being threatened and the potential impact of a threat. According to risk calculation, we get the value of risk, determine the risk level, choose the appropriate treatment and control measures for unacceptable risks, and form risk management plan. The ways of risk treatment include: avoiding risk, reducing risk, transferring risk and accepting risk. Control measures should be selected both management and technology, specifically for all kinds of risk control should be based on the following aspects: the organization of the actual situation to consider safety guidelines, the organization for security and asset classification and control, personnel security, physical and environmental security, communication and operation management, access control, system development and maintenance, business continuity management and compliance. In the choice of risk management methods and control measures, agencies should consider the development strategy, enterprise culture, personnel quality, and pay special attention to the balance of cost and risk, to deal with security risks to meet the laws and regulations and related requirements, management and technical measures to reduce the risk can be. For the risk that is not acceptable, we should select appropriate control measures to evaluate the residual risk and decide whether the risk has been reduced to an acceptable level to provide input for risk management. The assessment of residual risk can be carried out according to the criteria of organizational risk assessment, considering the reduction of the possibility of threat by selected control measures and existing control measures. Some risks may still be at an unacceptable risk after selecting appropriate control measures. We should consider whether to accept such risks or increase control measures by management according to the principle of risk acceptance. The risk is caused by system threat vulnerability on the system will use the attack and the damage to the assets, which will bring to the enterprise system where the impact and loss of assets, therefore, threat and vulnerability of three factors is the direct factor that needs to be evaluated and analyzed in risk assessment.

4. Conclusions

The information society has put forward higher demands on the function and function of colleges and universities. Information security risk assessment is an important evaluation method and decision-making mechanism in the process of establishing information security system. It is an important part of information system risk management. Risk management is a dynamic process of management. It hopes to arouse everyone's attention to information system security in universities. At the same time, I hope this article can provide references for the specific implementation of risk assessment in universities.

References

[1] Kong Suzhen, Liu Yawei. On the Construction of College and University Information Security Risk Assessment System Platform [J]. Value Engnieering, 2015(14): 254-255.

[2] Fu Sha, Song Dan. An Information Security Risk Assessment Method Based on AHP and Fuzzy Comprehensive Evaluation [J]. Research and Exploration In Laboratory, 2012, 31(6): 207-210.

[3] Li Yang, Wei Wei, Liu Yongzhong, et al. Research on Information Threaten Assessment Model

Based on AHP [J]. Computer Science, 2012, 39(1): 61-64.

[4] Wu Wengang, Zhang Zhiwen, Wang Qingsheng. A Information Security Risk Assessment Model Based on AHP and Fuzzy Comprehensive Evaluation [J]. Journal of Chongqing University of Technology (Natural Science), 2017, 31(7): 156-161.