Research of Information System Security Risk

Jianbo Liu, Jun Li, Ji'an Ding, Xia Li

Zibo Normal College, Zibo, Shandong, 255130

Keywords: Information System, Security Risk Problems, Countermeasures

Abstract: Addressing information security issues is inseparable from information security technologies and products. But technology is not the most important in the entire information security system. Scientific information security management is the foundation for establishing an effective information security system. In the case that China's core technology and key equipment are still relatively backward, it is required to give full play to institutional advantages and make up for technical deficiencies through scientific management.

1. Introduction

The security risks of information systems refer to the possibility of security incidents arising from the artificial and natural threats and the fragility of the system and their possible impact. The information security risk assessment refers to the scientific and fair comprehensive assessment of the security attributes of the information system and the confidentiality, integrity and availability of the information system and the information processed, transmitted and stored according to the relevant national information technology standards. It assesses the vulnerability of information systems, the threats to information systems, and the actual negative impacts of vulnerability being exploited by threat sources, and identifies the security risks of information systems based on the likelihood and negative impact of security incidents.

2. Basic content of information security management

Addressing information security issues is inseparable from information security technologies and products. But technology is not the most important in the entire information security system. Advanced information security technologies can only work if they are based on scientific information security management. The security available through technical means is limited, and technical means require appropriate management and procedures to support it. For an information system, the construction of information security management requires at least the participation of all employees in the organization, and may also require the participation of suppliers, consumers, and experts from outside organizations. Information security management is the process of coordinating human, material, financial and other resources through planning, organization, leadership, control, etc., in order to effectively achieve the goal of organizing information security.

In information security management, it is important to study the relationship between various security elements and the related elements of risk management, which is of great significance to information security management. The various security elements involved in information security management are discussed in this model: (1) Containing threatened environments where these threats are constantly changing and are currently only partially exposed; (2) Organizational assets; (3) Asset vulnerabilities (4) Protective measures to protect assets and reduce threats; (5) Protective measures to reduce risks; (6) Acceptable residual risks in the organization. The asset itself has a number of vulnerabilities V that allow Threat T to exploit Vulnerability V to attack assets. In such cases, the organization may choose some safeguards S to reduce the risk R due to threat T and vulnerability V. Often, an organization can reduce risk R to an acceptable level by taking appropriate safeguards S without affecting the organization's normal business operations. At this time, there are still threat T and residual risk RR, but the organization believes that the residual risk R R is acceptable and does not require protective measures S. At the same time, for threats that may

DOI: 10.25236/systca.18.024

not be exposed to Vulnerability V, the organization may choose to use some safeguards S to monitor the organization's environment to ensure that Threat T does not evolve into a risk of exploiting V.

Risk management is an important part of information security management. Achieving effective control and management of risks is the basis of information security management. As shown in Figure 2, the various relationships related to risk are identified as follows: (1) Assets have potential business impacts because of their value, which may lead to increased risks; (2) Vulnerabilities exposed by assets become possible Factors that increase risk; (3) threats to exploit vulnerability and thus increase risk; (4) take protective measures to prevent the occurrence of threats, which can reduce risks; (5) by analyzing risks, the organization proposes protection requirements, and Meet the organization's protection requirements by taking appropriate protective measures.

3. Risk control technical measures

Once the safety requirements have been identified, controls should be selected and implemented to ensure that the risk is reduced to an acceptable level. Controls can be selected from relevant standards or other control sets, or new controls can be designed to meet specific needs when appropriate. The main protective measures that can be used to reduce risk are: (1) Baseline method. This approach is to select a set of safeguards for all systems to achieve the baseline level of protection for the entire system. Recommendations for various standard safeguards are required in baseline documents and utility rules, and protection measures can be taken from other organizations, such as international and national standards organizations, industry sector standards or recommendations. (2) Irregular methods. Conduct informal, results-based risk analysis of all systems. This method is mainly to use personal knowledge and experience. (3) Detailed risk analysis. Conduct detailed risk analysis on all systems. Detailed risk analysis includes the identification and valuation of assets, and an assessment of the extent and vulnerability of these assets. Through these efforts, the selection and adoption of safeguards that are considered correct based on the identified asset risks and support for reducing the risk to an acceptable level as defined by management. (4) Combination method. This approach is a combination of the best approach to baseline methods and detailed risk analysis methods, using a high-level risk analysis approach. First, identify those systems that are high risk or important to business operations. Based on the results, the systems are categorized to determine the appropriate protection, which systems require detailed risk analysis, and which systems are adequate for baseline protection. In general, this method is relatively cost-effective.

The information security management specification should specify the requirements for establishing, implementing, and maintaining an information security management system. It is pointed out that the implementation organization must follow a risk assessment to determine the most appropriate control object and take appropriate control of its own needs. The steps to establish an information security management system are discussed below. (1) Define strategies for information security management. The information security policy is the highest policy for organizing information security. Different information security policies need to be formulated according to the actual situation of each department in the organization. Information security policies should be straightforward, easy to understand, and documented and distributed to all members of the organization. At the same time, relevant employees should be trained in information security strategies, and personnel with special responsibilities for information security should be specially trained so that the information security policy is truly rooted in the minds of all employees in the organization and implemented in actual work. (2) Define the scope of the information security management system. The scope of the information security management system should be determined in the field of information security management. The organization should construct an information security management system based on its own actual situation, within the entire organization, or in individual departments and areas. At this stage, the organization should be divided into different areas of information security control, so that it is easy to organize appropriate information security management for areas with different needs. (3) Conduct an information security risk assessment. The complexity of an information security risk assessment depends on the complexity of the risk and the sensitivity of the protected asset. The assessment measures used should be consistent with the organization's need to protect the information asset risk. The risk assessment mainly identifies and evaluates information assets within the information security management system, then evaluates the various threats and vulnerabilities faced by the information assets, and identifies existing or planned security controls. At the same time, direct and potential consequences need to be considered together. (4) Information security risk management. Conduct risk management based on the results of the risk assessment. Information security risk management mainly includes the following measures: First, reduce risks. Before considering the risk of passing, you should first consider taking measures to reduce the risk. The second is to avoid risks. Some risks are easily avoided, for example by using different technologies, changing operational procedures, and adopting simple technical measures. The third is to transfer risks. Usually only when the risk cannot be reduced or avoided and accepted by a third party (the transferred party). Generally used for those with low probability, but once the risk occurs, it will have a significant impact on the organization. The fourth is to accept the risk. For those who have taken risk reduction and risk avoidance measures, for practical and economic reasons, as long as the organization operates, there is a risk that must exist and must be accepted. (5) Identify regulatory objectives and select control measures. The determination of the control objectives and the selection of control measures are based on the fact that the costs cannot exceed the losses caused by the risks. Since information security is a dynamic system engineering, the organization should verify and adjust the selected regulatory objectives and control measures in real time to adapt to the changed situation and enable the organization's information assets to be effectively, economically and reasonably protected. (6) Prepare an information security applicability statement. The Information Security Applicability Statement documents the relevant risk control objectives within the organization and the various controls taken for each risk to demonstrate that the organization has thoroughly and systematically reviewed the organization's information security system and will have all the risks that must be regulated. Control is within the acceptable range. Different levels of information systems require different security management capabilities, so information security management capabilities should also be ranked. In the construction of hierarchical information security management system, we must pay attention to the measurement and evaluation of information security management capabilities to ensure that different levels of information systems have the corresponding level of management capabilities. Therefore, it is necessary to strengthen the training of personnel management capabilities, enhance personnel safety awareness, and improve personnel management literacy. At the same time, regular review and improvement of information security management should be strengthened to ensure that the information security management system adapts to changes in information systems in the long term.

Information grading is a business decision on a technology solution. At the information system level, the risk and system tolerance to risk should be weighed. In general, the higher the level of the system, the less tolerant the system is to risk, and the stricter the classification of system information must be. After establishing a grading system, the various types of control measures required should be determined. Control is essentially a security measure applied to an action whose purpose is to limit or manage the action as needed. For example, when an unauthorized act is discovered, the control measures should try to reduce the loss and alert the relevant personnel. In addition, control measures should be monitored and tracked in order to understand the entire process of unauthorized actions afterwards. The purpose of the control measures is to reduce the risk by providing appropriate protection for the defined information packets. Information grading is the division of these information into different logical sets, and the information in these logical sets can be fully protected in a similar way. Information systems should weigh the risks faced by information with the controls that address those risks for maximum efficiency.

4. Conclusion

The rapid development of the interest industry has made information technology an essential part of social development. Information technology has injected fresh vitality into the development of the national economy, and has accelerated the development of the national economy and the improvement of people's living standards. Of course, when people enjoy the great convenience brought by information technology, they also face the threat of various information security issues. The impact of this information security incident is harsh, and it will cause huge property damage and damage to information systems. Therefore, the security of information systems has to attract the attention of the society and the public. Improving the security of information systems and strengthening the risk assessment of information security have become urgent problems to be solved.

References

[1] Ni Jianmin. Information Development and Information Security in China[J]. Journal of Tsinghua University (Philosophy and Social Sciences), 2000(15).

[2] Zhou Youyuan, Zhang Xiaomei. Analysis of the key points of information security management in the implementation of hierarchical protection [J]. Information Security and Communication Confidentiality, 2009 (9).

[3] Zhang Yaojiang. Information Security Risk Management (III)——Risk Assessment (II) [J]. Information Network Security, 2004 (10).

[4] Shi Cheng, Zhang Yuqing, Lei Zhenjia. Self-assessment of enterprise information security risk and its process design [J]. China Financial Computer, 2004 (25).

[5] Li Juan, Liang Jun, Li Yongjie. Research on Information Security Risk Assessment [J]. Computer and Digital Engineering, 2006(34).