International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.81-88
http://dx.doi.org/10.14257/ijsia.2014.8.6.08

A Hierarchical Information System Risk Evaluation Method Based on Asset Dependence Chain

Xin Tong and Xiaofang Ban

China Information Technology Security Evaluation Center, Beijing, China
tongxin2030@163.com

Abstract

The current information security risk evaluation methods are only concerned with the risk of system components, rarely based on business risk perspective. Thus, it is difficult to meet different levels of information security risk comprehension such as the operational staff and the organization's manager. This paper proposes a hierarchical risk evaluation method based on asset dependence chain to quantify the hierarchical risk, the information systems security risks are divided into three levels: the component level, system level and organizational level. By analyzing the assets dependence in three levels, a "business systems-information systems-system components" assets dependence chain is formed. In the end, a hierarchical risk calculation method is presented. The risk analysis result can reflect the level of security risk evaluation needs more comprehensively and objectively.

Keywords: *risk evaluation, risk factor, asset dependence chain, threat*

1. Introduction

Current risk evaluation methods can be divided into knowledge-based methods [1], probabilistic based methods [2], AHP methods [3, 4], model-based methods [5, 6], fuzzy logic-based methods [7], attack graphs based methods [8, 9]. However, these methods are usually limited to the information security evaluation technology, which only evaluate the risk of system components, rarely based on business risk perspective. It is difficult to meet the different levels of information security risks understanding such as organization managers and business decision makers. Therefore, how to increase the technology risk to business risk is worthy of attention.

Due to the multilevel nature of information security risks occurrence, the security risk evaluation should also be hierarchical. The hierarchical risk evaluation method presented in this paper divides risk into three progressive levels: components level, system level, and organizational level, which effectively contribute to concern the risk from the technical perspective to business perspective. Organizational-level security evaluation reflects the security risk of business systems, which provides security information for the decision maker and manager to grasp the organization's business information security. System-level security evaluation reflects the security risk of information systems, which provides security information for the system manager to grasp the system's security. Component-level security evaluation reflects the security risk of components, which provides security information for the system designer and technical maintenance personnel to grasp the security risk situation.

ISSN: 1738-9976 IJSIA

2. Risk Factors Analyses

Information security risk factors include: assets, vulnerabilities, threats and control measures. Risk evaluation determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment. [10].

Risk factors analyses in hierarchical risk evaluation method are also hierarchical. Through component-level risk factors analysis, we can get system-level security risks and organizational-level security risks layer by layer.

2.1. Asset Analysis

Generally, the business importance will be reflected to the values of assets on which it operates. Currently, most assets analyses are based only on the system components. These assets analyses can not directly response the upper layer assets' values, so it is not conducive to the systematic business impact analysis. Therefore, this paper proposes a hierarchical assets analysis method, it more explicit and practical than the method in reference [11]. The hierarchical assets analyses methods include three steps: (1) Assets identification and classification. (2) Assets dependence analysis. (3) Assets evaluation.

Assets identification is mainly on three levels: business systems identification, information systems identification and system components identification. Among them, the business systems are the organizations' the core assets, which can be described in terms of business processes, business activities, business data, etc. Information systems using information technology to achieve a variety of business functions and business processes, supporting business activities and carrying business data. System components refers to the component factors that make up the information systems and maintain their operations, the system components can be described from the hardware, software, environment, information, personnel and institutions.

There is a certain dependence relationship among assets. The associated assets analysis provides an analytical model to clarify the interdependence assets. The dependence expresses the transfer value of the assets: business systems are dependent on information systems that support their operations. Information systems are also dependent on the components that composite and maintain their operation to some extent. Meanwhile, there are dependence relationships among the business systems, among information systems, and among system components. By analyzing the dependence of identified assets, a "business systems-information systems-system components" assets dependence chain is formed. Figure 1 gives an example for three levels asset dependence chain.

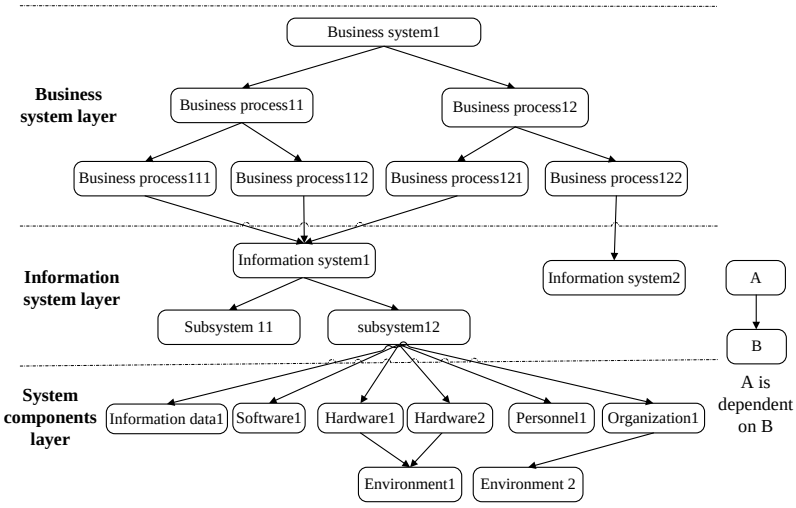

Figure 1. An Example for Assets Dependence Chain

According to the assets dependence chain, the value of different level assets can be quantitative evaluated. First of all, start from the source assets dependence chain, *i.e.*, business system assets, according to the organization's business system value evaluation criteria (shown in Table 1), evaluate and assign the identification of the business process, the value of the business activities and operations data. And then, according to the dependence of organization's business systems on information systems evaluation criteria (shown in Table 2), evaluate and assign the dependence of business processes and business data on information systems that support its operation. Furthermore, according to the assigned values of business system and its dependence on information systems (see Table 2), the values of information systems can be calculated (shown in Table 3). Similarly, along the assets dependence chain, the values of system components can be calculated from that of information systems.

Table 1. Value Evaluation of Business System Level Assets

Asset Value	Evaluation Criteria
Very Low/1	System losses have little effect on the organization's business objectives and interests.
Low/2	System losses have less effect on the organization's business objectives and interests.
Ordinary/3	System losses have general effect on the organization's business objectives and interests.
High/4	System losses have serious effect on the organization's business objectives and interests.
Very High/5	System losses have more serious effect on the organization's business objectives and interests.

Table 2. Dependence Evaluation of Upper Assets on Lower Assets

Dependence of upper assets on lower assets	Evaluation Criteria
Very Low/1	Losses of lower assets have very little effect on upper assets' operation and security.
Low/2	Losses of lower assets have little effect on upper assets' operation and security.

Ordinary/3	Losses of lower assets have some effect on upper assets' operation and security.
High/4	Losses of lower assets have high effect on upper assets' operation and security.
Very High/5	Losses of lower assets have very high effect on upper assets' operation and security.

Table 3. Lower Assets Value Calculation

Asset Value		Dependence of upper assets on lower assets				
		Very Low/1	Low/2	Ordinary/3	High/4	Very High/5
The upper assets' value	Very Low/1	Very Low/1	Very Low/1	Very Low/1	Very Low/1	Very Low/1
	Low/2	Very Low/1	Very Low/1	Very Low/1	Low/2	Low/2
	Ordinary/3	Very Low/1	Low/2	Low/2	Ordinary/3	Ordinary/3
	High/4	Low/2	Ordinary/3	Ordinary/3	High/4	High/4
	Very High/5	Ordinary/3	High/4	High/4	Very High/5	Very High/5

2.2. Vulnerabilities Analyses

Vulnerabilities are likely to be the threat of the use of one or more of the assets of weakness. Vulnerabilities themselves do not cause damage to the assets, only when vulnerabilities are triggered by the external threats. Therefore, in the risk calculation, we shall consider the correspondence between threats and vulnerabilities.

In vulnerabilities analysis, the multilevel nature of their occurrences should also be considered. Vulnerabilities exist not only in the management, but also in the technology. The vulnerabilities severity is related to asset's existing forms, their structures, protection technology, usages, *etc*.

Table 4. Vulnerabilities Evaluation

Vulnerability	Evaluation Criteria
Very Low/1	Very difficult to be used
Low/2	Difficult to be used
Ordinary/3	Not easy to be used
High/4	Easy to be used
Very High/5	Very easy to be used

2.3. Threat Analysis

Threat is the external factor which leads to system or organization damage. Threat identification is the process of founding, listing and descripting the threat that assets facing. Any threats to all assets within risk management should be recognized. Threat identification depends on the severity of the consequences when threats implement successfully.

Threat analysis is the process of analyzing and assigning the threat's motivation and behavior ability. Threat subject motive can be analyzed from the threat implementation purpose and the social and personal background of threats subject. The threatening behavior ability can be analyzed from the tool, place, time, scope, intensity and frequency and other factors which the behavior related.

Table 5. Threat Evaluation

Threat Evaluation	Evaluation Criteria
Very low/1	The possibility of a threat occurring is very small, threat occurs very rare or only in exceptional cases. (Occurrence possibility <1%).
Low/2	The possibility of a threat occurring is small, threat generally less likely to occur, or can be confirmed occur few times (Occurrence possibility: 1% -20%).
Ordinary/3	The possibility of a threat occurring is not high, threat may occur under a certain circumstances, or can be confirmed occur some times (Occurrence possibility: 20% -50%).
High/4	The possibility of a threat occurring is high, threat most likely to occur in most cases, or can be confirmed occur many times (Occurrence possibility: 50% -90%).
Very high/5	The possibility of a threat occurring is very high, threat almost inevitable in most cases, or can be confirmed occur frequently (Occurrence possibility > 90%).

2.4. Control Measures Analysis

Control measures are practices, procedures or mechanisms to deal with risks. Control measures as a risk negative phase factor control the positive risk factors (include assets, vulnerabilities, threats subjects, and threats behavior). For example, for component-level assets, by dividing the security domain, deploying assets rationally, and establishing appropriate protection system corresponding to each security domain, so as to provide appropriate security for each asset. To the vulnerabilities, repair system vulnerabilities timely so as to reduce the likelihood of being exploited. To the threat subject, means the use of sanctions computer crime laws (include the theft of state confidential information, the attack of network infrastructure, the spread of the virus, and spam illegal information, the spread of viruses, illegal information, spam, *etc*.,), play a deterrent role of law, so as to effectively curb the threat subjects' motivations. To the threatening behavior, take appropriate security measures to counteract the threat capacity.

3. Risk Calculation Method

The risk calculation in the hierarchical risk evaluation method is from the system components to the business system layer by layer, and the upper asset risk is associated relationship with the underlying asset risk. Thus, calculate the risks of system component's layer assets at first, and then based on the assets' dependence, calculate risks system layer and

business system layer assets layer by layer. In the following, we present the method of how to calculate the system component layer risk, the information systems layer risk and business systems layer risk, respectively.

To the system component-layer assets C, the asset risk is calculated as follows:

$$\begin{aligned} R_C(C,V,T) &= R_C(I_C, g(V_C, T * \Phi(T,C))) \\ &= \left\lceil \frac{1}{N_1 N_2} I_C * \left(\sum_{x=1}^{N_1}\sum_{y=1}^{N_2} V_{C,x} * T_y * \Phi(T_y, C)\right) \right\rceil \end{aligned} \quad (1)$$

Where R_a represents risk, V_a represents vulnerabilities assets a, T represents threat, I_C represents the value of assets C, N_1 is the total number of vulnerabilities, N_2 is the total number of threats.

$$\Phi(T,a) = \begin{cases} 1, & If\ the\ asset\ a\ has\ threat\ T \\ 0, & If\ the\ asset\ a\ has't\ threat\ T \end{cases} \quad (2)$$

To the information system layer assets S, the asset risk is calculated as follows:

$$R_S(I_S, Rank_C, D_C) = I_S * \left\lceil \frac{1}{n}\sum_{i=1}^{n} Rank_{C_i} * D_{C_i} \right\rceil \quad (3)$$

Where R_S represents risk assets of S, $Rank_C$ represents the risk level of the system component layer assets C, D_C represents the dependence of the components layer assets and system layer assets, I_S represents the value of asset S, n is the number of components asset C.

To the business system layer asset B, the asset risk is calculated as follows:

$$R_B(I_B, Rank_S, D_S) = I_B * \left\lceil \frac{1}{m}\sum_{i=1}^{m} Rank_{S_i} * D_{S_i} \right\rceil \quad (4)$$

Where R_B represents the risk of assets B, $Rank_S$ represents the risk level of the system layer asset S, D_B represents the dependence of the systems layer assets and business layer assets, I_B represents the value of the assets B, m is the number of system assets S.

In summary, by calculating the risk, asset risk in order to determine the upper level of systemic risk and to take appropriate security measures to control risk aversion, in order to determine whether the risk is acceptable, the unacceptable risk to take action. Note is that, for the calculation of risk with a mean value method helps determine the risk level of unity.

Table 6. Risk Classification

Risk Level Rank	Evaluation Criteria
Very low/1	Risk Value 1-25, causing the system little affected.
Low/2	Risk Value 26-50, causing business systems less affected.
Ordinary/3	Risk Value 51-75, causing the business system have some impact.
High/4	Value at risk 76-100, causing the business system affected seriously.
Very High/5	Risk value ≥ 101, causing the business system affected more seriously.

4. Conclusions

Traditional information security risk evaluation methods are only concerned about the risk of system components, while the lack of fine-grained analysis and articulate expression of business risks. Thus, it is difficult to meet the different needs of different levels of safety evaluation, such as business people, managers and other organizational personnel. The hierarchical risk evaluation method proposed in this paper the security risk of information system divide into organizational information systems security risk level, system-level and component-level hierarchy of three progressively upward, effective solution to the needs of different levels of management personnel for information system security evaluation helps risk analysis by the technical risks rise to business risks. Through hierarchical analysis of the assets, threats and vulnerabilities, a hierarchical risk quantitative method is proposed, which solves the mapping between the assets chain and risk transfer chain, thus further expand the meaning of information security risks and epitaxy.

Currently, the hierarchy risk evaluation method has been applied to specific risk evaluation practice. Practice shows that the proposed method in this paper can accurately outline the system's security status, so that the two sides can reach an agreement to evaluation result more easily.

References

[1] J. Guan, M. Lei, X. Zhu and J. Liu, "Knowledge-based Information Security Risk Evaluation Method", Journal of China Universities of Posts and Telecommunications, vol. 20, **(2013),** pp. 60-63.
[2] P. Zhang, S. T. Lee and D. Sobajic, "Moving toward Probabilistic Reliability Evaluation Methods", International Conference on Probabilistic Methods Applied to Power Systems, AMES, USA, **(2004),** pp. 906-913.
[3] Y. Wang, H. Fei and P. Jiang, "On the FAHP Method in Information Security Risk Evaluation", Computer Engineering & Science, vol. 28, no. 9, **(2006),** pp. 2-4.
[4] H. Xu and X. Jiang, "Research on Business Types Recognition Based on the Method of AHP-ELECT RE", Computational Risk Management, Part 3, **(2011),** pp. 275-283.
[5] B. Kaabacak and I. I. Sogukpinar, "Information security risk analysis method", C'omputers & Security, vol. 24, no. 2, **(2001),** pp. 147-159.
[6] J. Aagedal, F. den Braber, T. Dimitrakos, B. A. Gran, D. Rapti and K. St Len, "Model-based Risk Assessment to Improve Enterprise Security", 5th international EDOC conference, **(2002)**, pp. 51-62.
[7] T. Ngai and F. Wat, "Fuzzy Decision Support Systems for Risk Analysis in E-commerce Development", Decision support system, vol. 40, no. 2, **(2005),** pp. 235-255.
[8] L. Wang, A. Singhal and S. Ajodia, "Toward Measuring Network Security Using Attack Graphs", Workshop on Quality of Protection. New York: ACM, **(2007)**, pp. 49-54.
[9] K. Ingols, R. Lippmann and K. Piwowarski, "Practical attack graph generation for network defense", Proc. of the 22nd Annual Conf. on Computer Security Applications, **(2006)**, pp. 121-130.
[10] ISO/IEC 27005: 2008 Information Technology – Security techniques - Information security risk management, Berlin: German Institute for Standardization, **(2008)**.
[11] S. Bomil and H. Ingoo, "The IS Risk Analysis based on a Business Model", Information & Management, vol. 41, **(2003),** pp. 149-158.