Study on Security Policy of Cloud Service based on Risk Characteristic Analysis

Qing-cong Zhao

School of Information Management, Beijing University of Science and Technology Information, Beijing 100192, China

Keyword: Risk characteristic analysis, Cloud service, Security policy

Abstract: Each enterprise has its own unique situation, therefore it is unable to adopt a completely unified security control measures. Thus enterprise should have risk characteristic analysis to determine the appropriate information security attributes as well as the control measures. Different enterprises will adopt different cloud services, and they will put different types and levels of data into cloud services, so different users need different security policies of cloud services.Enterprises need a scientific and rational way to help themselves to determine which security controls are necessary. This paper proposed a method based on risk characteristic analysis to determine the information security control measures needed by the specific enterprise.

Introduction

Cloud service refers to a large number of computing resources connected by the network management and scheduling, forming a computing pool of resources to the user on-demand services. Users access to the required resources and services on the network in an on-demand and extensible way. Now many industries put their attention to the use of cloud services, especially small and medium-sized enterprises -- there is no need for them to purchase hardware and software, computer room construction, IT staff recruitment, they only needs to pay one-time pre-project fee and regular software rental service fee, then they can share the information system through the internet. Cloud services can not only bring huge business benefits to enterprises, but also can bring a lot of information security issues, such as data leakage, loss, malicious attacks and misuse of cloud services and so on [1]. Information security and privacy issues have become the biggest obstacle to the development of cloud services. Because enterprises are in different industries, the scales and operation modes are also different, so the needs of enterprises to protect the core data are quite different, thus the core data storage position and the level of protection is not the same. Therefore, the information security of cloud services can not be in an unified mode. This paper proposed a method based on risk characteristic analysis to analyze the status of information security risk of one enterprise, so as to determine the information security policy that the enterprise needs to use when it is using cloud service.

Organization of the Text

Risk Characteristic Analysis of Information Security

In the process of evaluating and selecting the cloud service supplier,firstly it should have risk characteristic analysis on information security of the organization itself, then it can determine and select different information security attributes and functions on this basis.

Considering Factors

In this paper, the proposed method based on risk characteristic analysis of information security can be considered in the following aspects:

1 The organization of industry: according to national industry classification and code (GB/4754-2011), organization can be divided into different industries, such as financial services, IT services, education, public administration and social security and so on; the type of different industries to protect data is also different, such as the financial industry is mainly to protect the account information of customers', the education industry is mainly to protect the various grades information of students' and so on.

2 The type of data processed and stored in cloud platform: data stored in the cloud, such as information of personal identity, information of account, the related data of intellectual property rights, as well as the key business data and so on. The integrity of data, confidentiality, availability requirements should be mainly considered. The storage methods of different types of data and security mechanisms are quite different.

3 When the integrity of data, confidentiality and availability is destructed, the enterprise may be affected from the following aspects: confidential data is widespread, unauthorized access, data changes unexpectedly, legal users can not normally have access to data or applications.

4 The risk of data: data mainly faced with information security risks, such as data loss, data leakage, malicious internal users, misuse of cloud services and malicious use, the security vulnerabilities of sharing technologies and so on.

5 Information security threats: the main information security threats, such as hardware and software failures, no action or operational errors, network attacks, physical attacks and so on, which needs to consider what events or threats may cause damage to the organization.

6 Risk management of information security: the acceptable degree of organization's information security risk, as well as the concerning degree of organizational top management staff had on the risk of information security.

7 The number of cloud service users: how many users are using the enterprise's cloud services?

The assessment on enterprise risk characteristics is mainly based on the questionnaire survey. In this paper, totally there are fifty nine questions ($N=59$) designed for the above seven factors ($M=9$), which constitutes the questionnaire of risk characteristics. According to the answers to these questions (all level selection is "1, 2, 3, 4, 5"), the M analysis result of each risk factors (risk characteristic value M_x) may be low risk, lower risk, medium risk, higher risk and high risk one of the five things, namely {M_x = high higher, medium, lower, low}. The importance of these seven factors to enterprises is not exactly the same. According to the actual situation of enterprises, in this paper, it granted these seven factors with different weight sets, which can be shown in Table 1:

Table 1 The Considering Factors of Risk Characteristic Analysis

Considering factors	**Attribute value of risk**	**Characteristic value of risk**	**Weight**
Industry that enterprise is located	$F_1=\{ N_1- N_3\}$	M_1	$W_1=1$
Data of cloud platform	$F_2=\{ N_4- N_6\}$	M_2	$W_2=3$
Impact of data breaches on firms	$F_3=\{ N_7- N_{17}\}$	M_3	$W_3=3$
Risk of data	$F_4=\{ N_{17}- N_{27}\}$	M_4	$W_4=2$
Threat of information security	$F_5=\{ N_{27}- N_{43}\}$	M_5	$W_5=2$
Risk management of information security	$F_6=\{ N_{44}- N_{56}\}$	M_6	$W_6=3$
Number of cloud service users	$F_7=\{ N_{57}- N_{59}\}$	M_7	$W_7=2$

Among them, the value of the risk attribute value F of each considering factor is mainly based on the answer of the security problems corresponding to each factor of the enterprise, which should be the average value of the corresponding value of these results (1, 2, 3, 4, 5).

The Calculation of Characteristic Value of Risk

The calculation of the overall information security risk characteristic value of an enterprise can be expressed as:

$$\mathbf{R} = \sum_{i=1}^{n} M_i \times W_i \tag{1}$$

Among them, M_i represents the eigenvalue of one single risk factor; W_i represents the weight of one single risk factor. The overall risk characteristic value of an organization depends on the weighted average of attribute value as well as its weight for one single risk factor.

The risk value defined in this paper can be shown in Table 2:

Table 2 Calculation Value of Risk Characteristic Analysis

Risk level	**Corresponding value**
High	5
Higher	4
Medium	3
Lower	2
Low	1

According to Table 1 and Table 2, assuming that the risk level of all seven security considering factors in the enterprise is low risk (the risk value is 1), we can calculate the overall information security risk characteristic value of enterprise, the minimum value of which should be 16. Similarly, assuming that the risk level of all security considering factors in the enterprise is high risk (the risk value is 5), we can calculate the overall information security risk characteristic value of enterprise, the maximum value of which should be 90.

The characteristic value of information security risk is a comprehensive reflection of the organization's security protection requirements. The greater the characteristic value of risk is, the stronger the information security guarantee the enterprise needs to deploy, and vice versa. In addition, it is important for enterprises to provide adequate financial support and implement appropriate information security measures to convert some pure values into language that managers can understand. Therefore, based on the actual work experience of the author, in this paper, it summarized the corresponding table of risk level of overall risk calculation value, which can be shown in Table 3.

Table 3 The Corresponding Table of Overall Risk Level

The calculation value of overall risk	**Risk level**
72-90	High
56-71	Higher
40-55	Medium
24-39	Lower
16-23	Low

The Control Measures for Information Security

According to the above, the assessment on cloud service risk characteristics of enterprise may lead to five possible conclusions: low risk, lower risk, medium risk, higher risk and high risk. Enterprise should select different control measures according to the different level of risk characteristics. Based on the comprehensive analysis of the requirements of ISO27001 standard, Chinese Information Security Level Protection and NIST 800-53 [2,3], in this paper, it proposed three kinds of security risk control based on the results of characteristic analysis, namely,the basic security measures (B), strengthened security measures (S) and advanced security measures (A). Table 4 proposed the relationship between the risk level and the corresponding level of information security control measures.

Table 4 Risk Level and the Corresponding Level of Information Security Control Measures

Risk level	**Level of information security control measures**
Low, Lower	Basic security measures (B)
Medium	Basic security measures (B) + strengthened security measures (S)
Higher, High	Basic security measures (B) + strengthened security measures (S) + advanced security measures (A)

In this Table, the basic security measures (B), strengthened security measures (S) and advanced security measures (A) should take specific control measures, in this paper, it used the security the control measures presented in NIST 800-53, as shown in Table 5. In NIST 800-53, security control can be divided into three categories--the category of management, the category of operation, the category of technology, eighteen families (including security program management), as well as two hundred and fifty three security control [4].

Table 5 The List of Security Measures

Level of security control measures	Number of security measures
Basic security measures (B)	RM-01, 02, 03
	IA-01, 02, 03, 05, 07
	DP-01, 02, 03
	IN-01, 02, 03, 06, 07, 09
	EK-01, 02
	MS-01, 02, 03
	DO-01, 02, 03
	HR-01, 03, 05
	AT-01, 02, 03
	SP01, 02, 03
	SR-01, 02
	IR-01, 02, 04, 05
	CR-01, 02, 03
Strengthened security measures (S)	DP-05, 06
	IN-04, 08
	EK-04
	ST-01, 02
	MS-04
	HR-02
	SR-03
	ST-01, 02, 03
	CS-01
	DE-01
Advanced security measures (A)	IA-06
	RM-04
	EK-03
	TB-01
	IR-03
	SF-05, 06, 07
	DD-01

Enterprises with high risk and higher risk characteristic value have higher information security risk, which are often very attractive to network attackers. These enterprises have very low information security risk tolerance, and therefore they need strong information security risk countermeasures, management and support capabilities to meet the very stringent level of business needs. These companies often take proactive attitude and deploy powerful information security threat detection with analysis capabilities to support the control over the unpredictable risks [5]. These enterprises need to select and deploy B+S+A.

The enterprise with medium risk characteristic value has moderate information security risk, which also has certain attraction to network attacker. These enterprises have general level of information security risk tolerance, the overall level of information security management is not very high, they often need to strengthen risk control and security guarantee, so as to meet the industry compliance as well as the level of business required. As for an enterprise with medium risk characteristic, how to balance the cost of security control and the potential risk is very important. These organizations do not need to choose advanced security measures (A), which should deploy the strengthened security measures (S), namely, B+S.

Enterprises with low risk and lower risk characteristic value have lower level of information security risk. These enterprises are generally not attractive to network attackers. At the same time, these enterprises have less compliance requirements, so that they can accept more security risks, that is to say, they enable themselves to have higher risk tolerance. Although the technology sector may believe that information security risks need funds to control, the company's policy makers may be more concerned about the development of business risk, rather than information security risk. As a result, these organizations often deploy only basic security measures (B) to protect the basic data security.

Cases of Implementation

In this paper, it selected one securities company to analyze the characteristics of information security risk, and recommend the security control strategy based on the analysis result.

Table 6 Considering Factors of Risk Characteristic Analysis

Considering factors	**Characteristic value of risk**
Industry that enterprise is located	$M_1=5$
Data of cloud platform	$M_2=3$
Impact of data breaches on firms	$M_3=5$
Risk of data	$M_4=5$
Threat of information security	$M_5=5$
Risk management of information security	$M_6=3$
Number of cloud service users	$M_7=3$

This enterprise belongs to the financial industry, among all industries the characteristic value can have the highest value, but this enterprise did not put core business data into cloud platform, meanwhile the enterprises had done a lot of work on the risk management of information security, so the characteristic value of these two items is 3. According to the calculating method of Formula 1 as well as the weight value of each factor in Table 1,the final characteristic risk value of information security in this enterprise is calculated to be 64, which belongs to higher risk. Thus the security policy of basic security measures (B) + strengthened security measures (S) + advanced security measures (A) is recommended.

Conclusion

Because each industry is located in different industries, and the scales and operation modes are unique, which lead to the core data that the enterprise needs to protect is quite different.

Moreover, the location as well as the level of protection needed for these core data can not be exactly the same. Therefore, the information security protection of cloud computing is impossible to adopt "one size fits all" model. In this condition, this paper put forward a method based on risk characteristic analysis, so as to analyze the enterprise's specific information security risk, and t on this basis, it can determine the level of information security control measures that the enterprise needed. The risk characteristic method can have comprehensive analysis on the various factors that may affect the information security risk value, including the industry that the enterprise is located, the data type of cloud storage, the effect of data destruction on organization risk, the risk of data, information security threats, information security risk management, as well as the state of cloud service users and so on, which can provide scientific basis and effective implementation method for the enterprises that adopt cloud service platform with information security control measures.

Acknowledgement

This research was financially supported by the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions (CIT&TCD201504059).

References

[1] Jame McCloskey, Maggie Hao. Saas Security Governance Program. Info-Tech Research Group Publication, October 2, 2015:11-12.

[2] Hamzeh Mohammd Alabool, Ahmad Kamil Mhmood, Common Turust Criteria for Iaas Cloud Evaluation and Selection, Computer and Information Sciences(ICCOINS), 2014 International Conference on 3-5 June 2014 1-6.

[3] GB/T 22080-2016/ISO/IEC27001:2013.

[4] NIST 800-53: Security and Privacy Control for Federal Information Systems and Organizations[R]. National Institute of Standards and Technology, USA, 2010.

[5] Security for Cloud Computing Ten Steps to Ensure Success Version 2.0. Cloud Standards Customer Council, 2015.