The Fuzzy Integrated Evaluation of Enterprise Information System Security Based on EC

Shaolong Zhang, Ning Zhou and Jiaxing Wu
Center for Studies of Information Resources,
Wuhan University, 430072
zhangshaolong78@yahoo.com.cn

Abstract. As enterprises increase their electronic communication in business activities through network, the security of enterprise information system based on EC becomes crucial for enterprises. This paper proposes a fuzzy integrated security evaluation method based on man-computer combined data collection and fuzzy expert evaluation in Delphi method. The method could reduce the subjectivity of expert evaluation and alleviate the difficulty of data collection and makes possible a better combination of qualitative and quantitative evaluations. Firstly, the evaluation factor and hierarchy structure of security evaluation is constructed. Secondly, according to data collected and the evaluation comment of each expert, the subjection degree matrix is constructed. Finally, a new concept of "degree of assurance" is presented for the quantificational evaluation of enterprise information system security based on. In this paper the study of the case shows that the method can be easily used and its results conform to the actual situation.

1 Introduction

Electronic Commerce is the sharing of business information, maintaining business relationships, and conducting business transactions by means of telecommunications networks [1]. The explosion of the Internet as a ubiquitous business tool has propelled the hype over fruitful electronic commerce opportunities to new heights. But while modern networking technologies such as the Internet offer new tools for making the communication and sharing of information more efficient and faster than ever before, it can significantly increase exposure to information security risks. The risks of enterprise information system based on EC come from Internet and Intranet. Leakage and invalid access of information affect not only a single user or application,

but may have disastrous consequences on the entire enterprise. The security evaluation of enterprise information system based on EC is a process in which the risk factors of the system are analyzed and explained. The basic goal of the security evaluation is to control the risk in acceptability.

By the reason of the uncertainty of the evaluation factor, the fuzzy logic method is used [2]. In this paper an improved fuzzy method is proposed to solve the security evaluation. The rest of this paper is organized as follows. In section 2, an evaluation model is given for security evaluation. In section 3, a case is put forward to illustrate our method. Finally, conclusions are drawn in Section 4.

2 Construction of security evaluation model

In the evaluation of enterprise information security based on EC, we face problems such as the complication of security factors, limited history statistical data and difficulty of data collection. There is no single method to solve these problems. We need an integrated evaluation method which comprises expert evaluation, statistical information and compute technology. To construct security evaluation model, firstly evaluation factors are recognized, then data is collected through man-computer method, at last based on fuzzy subjection theory and Delphi method qualitative evaluation is transferred to quantitative evaluation.

2.1 The recognition of security evaluation factors

Before the evaluation of security, we need a investigation on security factors. Usually system security is evaluated from three aspects which are strategy, management and technology. Strategy refers strategic status and strategic decision of information system security in the enterprise. Management includes organizations and regulations to the information system security and supervision on relative people and materials. Technology refers all kinds of security technologies. But under the EC environment human is to be interactive with enterprise information system based on network, referred with the systematic methodology of "Wuli-Shili-Renli (WSR)"[3], human is the key factor to the enterprise information security. Good guidance and access control to the web users and skills of network administrator are important to security of EC. Thus when we give the recognition of security evaluation factors, human is recognized as one of the top level factors as well as strategy, management, technology which sub-factors are also recognized based on.

2.2 Man-computer combined data collection

Applied with IT technology, most security data could be automatically collected. These technologies include computer log system, real-time scan tools and automatic audit system and so on. Using computer technology can bring benefits. Firstly it could reduce the subjectivity of expert evaluation and make the evaluation method more scientific and objective. Secondly it alleviates the human workload in data

collection which not only cuts down the cost of human labor but also improves the veracity and the coverage of data collection. Some evaluation factors such as access control management and network management could be directly counted and evaluated based on automatically colleted data.

On the occasions that data could not be automatically collected by computer such as situations about training and security rules, questionnaire survey and On-the-spot investigation also could be applied.

2.3 Expert evaluation in Delphi method

The objective of most Delphi applications is the reliable and creative exploration of ideas or the production of suitable information for decision making. The Delphi Method is based on a structured process for collecting and distilling knowledge from a group of experts by means of a series of questionnaires interspersed with controlled opinion feedback (Adler and Ziglio, 1996). According to Helmer (1977) Delphi represents a useful communication device among a group of experts and thus facilitates the formation of a group judgment [4].

Based on data colleted experts make evaluations relying on their individual competence and are subjective, Delphi method is utilized to adjust the fuzzy evaluation of each expert to achieve the consensus condition of the all experts consistent.

Flowchart for the Delphi Method follows as [5]:

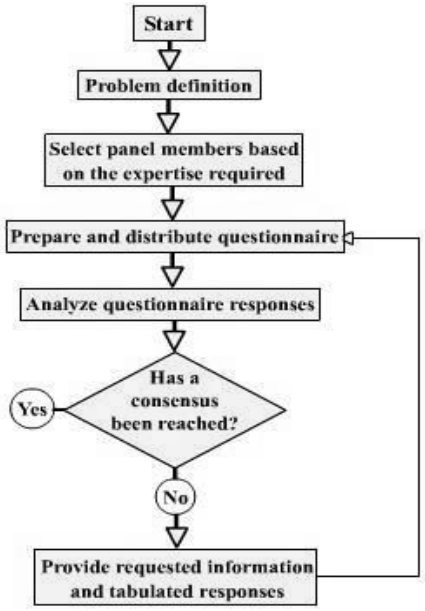

Figure 1. Flowchart of Delphi Method

2.4 Integrated Fuzzy Evaluation

The major steps of evaluation are as the following.

Step1. Construct the hierarchical structure. The top layer is the focus of the goal, and the bottom level, consists of the alternatives under evaluation. The factors and any sub-factors used to make the decision comprise the middle levels [6]. The factors is divided into s subsets which defined as $Y_1,Y_2 \ldots Y_S(Y_i \cup Y_j=\phi(1\leq i,j\leq s\ i\neq j))$. Each subset Y_i is constructed by the factors in the next level denoted as X_{in}, so the characteristic vector of each subset Y_i is presented by the expression.

$$Y_i= (X_{i1},X_{i2},\ldots,X_{in})$$

Step2. Construct the judge set. The expert group which is composed of information system experts, enterprise manager and end users provides all the judgements of the set. Suppose the judge set has m judgements, judge set V is V= {$V_1, V_2,\ldots, V_m$}.

Step3. Build fuzzy evaluation matrix. We can construct the fuzzy reflection f: $Y \rightarrow F(V)$, Y is the whole of the factor set and F(V) is the whole of the fuzzy set in V. The reflection f means the degree of the support from the factor Y_i to each judgement in the judge set [7]. The subjection vector of Y_i to the judge set V is $R_i= (r_{ij,k})$ n*m(i=1,2,…,s; j=1,2,…,n; k=1,2,…,m). $r_{ij,k}$ is the subjection degree of factor x_{ij} to judgement V_k given by expert which meets the requirements that the range of the value is [0,1] and the count of values $\sum r_{ij}$ =1.

Step4. Estimate the normalized priority weights. The priority weight vector of subsets is presented by the expression.

$$A_i= (a_{i1},a_{i2},\ldots,a_{in}),\text{and}\ a_{ij}=1$$

There are several methods such as AHP method and dual correlation function method to give priority weights. According to the particularity of enterprise information system security based on EC, in the case of this paper the weights are given by experts in Delphi method.

Step5. Calculate evaluation vector B_i corresponding to subset Y_i. The calculation formula is

$$B_i=A_i \bullet R_i= (b_{i1},b_{i2},\ldots,b_{im}).$$

Weighted average means is applied to each vector B_i to take valuable information of each evaluation into account. The expression is

$$b_{ik}=\sum_{j=1}^{n} a_{ij}\ r_{ij,k}(k=1,2,\ldots,m).$$

Step6. Calculate the whole fuzzy evaluation. Each subset Y_i is treated as a single element and B_i is treated as evaluation vector of Y_i, The fuzzy evaluation matrix is

$$B=\begin{pmatrix} B_1 \\ B_2 \\ \cdots \\ B_S \end{pmatrix}_3 =$$

Referred with priority weight vector of each subset A which is represented as A= $(a_1,a_2,\ldots,a_s)$ and $\sum_{i=1}^{s} a_i=1$, the final evaluation $T=A\bullet B=(t_1,t_2,\ldots,t_m)$ is calculated.

2.5 Quantificational evaluation result of security

It is difficult to give quantificational result to final evaluation. To achieve a quantificational evaluation result, the degree of assurance is introduced which is denoted as G..

To calculate G, judge set V should be quantified first. For example, judgement "Very High" would be evaluated as 100. Quantified judge set $V'=\{V'_1, V'_2,\ldots,V'_m\}$.

$$G=\sum_{i=1}^{m} t_i V'_i.$$

3 The case

In this case the hierarchy structure is constructed; evaluation factors are divided into four subsets which are Strategy, Management, Technology and Human. Sub-factors and the alternatives under evaluation are shown as Tables 1 (priority weight in the brackets).

The judge set V is $V=\{V_1, V_2, V_3, V_4, V_5\}$ which shows the risk probability level. Its meaning is " V_1 Very High, V_2 High, V_3 Medium , V_4 Low , V_5 Very Low".

Table 1. Evaluation factors of the case

NO	Top factors	Sub-factors	Alternatives
1	Strategy (0.15)	Strategy status of IT department (0.5)	Information literacy of enterprise leader
			Investment of IT construction

2		Security information system construction plan and budget (0.5)	Long-term plan of information system construction
			Investment of information system construction
3	Management (0.3)	Laws and regulations (0.2)	Protection from laws and regulations
			comprehensive rules and regulations within enterprise
4		Human management (0.3)	qualifications examination of system administrator and operators
			on-the-job training
			division of privileges
5		Environment management(0.2)	firewall and router setting
			temperature and humidity control, power management, wiring management
6		Risk management(0.3)	establishment of information system backup mechanism
			preparation of emergency predetermined plan
10	Technology (0.4)	Operating system (0.2)	Legal operating system software
			system patch update
			password protection and logon privilege management
			anti-virus protection
11		Safety in transmission(0.3)	encryption in IP package
			reliable transmission in VPN
			integration in data transmission
12		Network access control(0.1)	access control of web users

			adoption of security authentication protocol such as SSL and SET
13		Security audit system(0.2)	Tracing and collecting audit data including system log, firewall log
14		Encryption key management (0.2)	creation and management of encryption key based on absolutely safe regulations
15	Human (0.15)	Human resource management(0.5)	Employment of important people
			reservation of technical personnel
16		Human education(0.5)	enterprise interior training mechanism

The experts make judgements of the subjection to the judge set V. Evaluation matrixes R1, R2, R3 and R4 are:

$$R_1=\begin{pmatrix} 0.25 & 0.35 & 0.30 & 0.10 & 0.00 \\ 0.35 & 0.35 & 0.20 & 0.10 & 0.00 \end{pmatrix}$$

$$R_2=\begin{pmatrix} 0.35 & 0.35 & 0.20 & 0.10 & 0.00 \\ 0.35 & 0.35 & 0.20 & 0.10 & 0.00 \\ 0.50 & 0.30 & 0.10 & 0.10 & 0.00 \\ 0.10 & 0.20 & 0.55 & 0.10 & 0.05 \end{pmatrix}$$

$$R_3=\begin{pmatrix} 0.15 & 0.25 & 0.25 & 0.15 & 0.20 \\ 0.45 & 0.30 & 0.25 & 0.00 & 0.00 \\ 0.20 & 0.25 & 0.35 & 0.10 & 0.10 \\ 0.20 & 0.20 & 0.25 & 0.25 & 0.10 \\ 0.50 & 0.40 & 0.10 & 0.00 & 0.00 \end{pmatrix}$$

$$R_4=\begin{pmatrix} 0.45 & 0.30 & 0.15 & 0.10 & 0.00 \\ 0.35 & 0.25 & 0.30 & 0.10 & 0.00 \end{pmatrix}$$

Calculate evaluation vector Bi

$B_1=A_1 \bullet R_1=$ (0.300 0.350 0.250 0.100 0.000),
$B_2=A_2 \bullet R_2=$ (0.305 0.295 0.285 0.100 0.015),
$B_3=A_3 \bullet R_3=$ (0.325 0.285 0.230 0.090 0.070),
$B_4=A_4 \bullet R_4=$ (0.400 0.275 0.225 0.100 0.000),

The final evaluation T is also calculated as

$T=A \bullet B=$(0.32650 0.29625 0.24875 0.09600 0.03250)

Referred with the definition in section 2.5, judge set V is quantified as V′={100，80，60，40，20}.

The degree of assurance G=T•V′=75.765.

Suppose it defines the value G from 0 to 30 to be very dangerous, from 31 to 60 to be unsafe, from 61 to 70 to be normally safe, from 71 to 85 to be well guarded, from 86 to 100 to be perfect, The security in this case is normally safe but it need improves and reinforced.

4 Conclusion

In this paper, an integrated evaluation method of enterprise information system security based on EC is presented. Each risk factor is estimated by the experts and for calculating the quantificational security evaluation of the whole system, the degree of assurance is introduced. The case result in this paper shows that the proposed method is scientific and tally with the actual situation.

Acknowledgements

This research is supported by the Social Science Foundation of Education Department of China under Grant No.05JZD00024.

Reference

1. V. Zwass, “Electronic Commerce: Structure and Issues”, *International Journal of Electronic Commerce*, Vol. 1, Nr. 1, pp.3-23, 1996..

2. J. H. M. That and V. Carr, “A proposal for construction project risk evaluation using fuzzy logic” , *Construction Management and Economics*, no.18, pp.491-500, 2000.

3.Xu Xiulin, Hu Kejin, Research of Enterprise Information Security Based on WSR Method, Network and Computer Security in China, no.2, pp.13-16, 2006.

4. The Delphi Method Definition and Historical Background 2007, http://www. iit.edu ~it/delphi.html, 2007-3-20.

5. The Delphi Method 2007, http://www.ryerson.ca/~mjoppe/ResearchProcess 841TheDelphiMethod.htm, 2007-3-20.

6. M. A. Mustafa and J. Bahar, “Project risk assessment using the analytic hierarchy process”, *IEEE Transactions on Engineering Management*, vol.38, no.1, pp.46-52, 1991.

7. D. M. Zhao , “ Comprehensive Risk Assessment of the Network Security”, *Computer Science*, vol.31, no.7, pp66-69, 2004.