Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method

Ming-Chang Lee

National Kaohsiung University of Applied Science, Taiwan

ABSTRACT

Information security risk analysis becomes an increasingly essential component of organization's operations. Traditional Information security risk analysis is quantitative and qualitative analysis methods. Quantitative and qualitative analysis methods have some advantages for information risk analysis. However, hierarchy process has been widely used in security assessment. A future research direction may be development and application of soft computing such as rough sets, grey sets, fuzzy systems, generic algorithm, support vector machine, and Bayesian network and hybrid model. Hybrid model are developed by integrating two or more existing model. A Practical advice for evaluation information security risk is discussed. This approach is combination with AHP and Fuzzy comprehensive method.

KEYWORDS

Information security risk analysis; quantitative risk assessment methods; qualitative risk assessment method; Analytical Hierarchy Process; soft computing.

1. INTRODUCTION

1.1 Quantitative and Qualitative analysis

Risk analysis is the basis of information protection, risk management, and risk in the process of information protection. Risk analysis includes process such as identification of activity, threat analysis, vulnerability analysis and guarantees. Risk analysis process explains the procedure to define the modalities for implementation such as BS7799. Information security's identification and assessment of the vulnerabilities of system is designed by Goel and Chen [20]. This method usually called matrix-based approach. The risk analysis method developed from the qualitative to the combination of quantitative and qualitative analysis ([18], [39]).

Risk analysis needs some complex steps of information security risk assessment process. It required doing comprehensive and integrated analysis for risk identification, estimation and evaluation. In organization, quantitative and qualitative analysis methods are two fundamental methods to use for analysis of risk on which assets are exposed. But there have some disadvantages for information risk assessment methods (see Table 1).

DOI : 10.5121/ijcsit.2014.6103

1.2 Soft computing and Hybrid model

We must integrate these two methods to play their respective advantages and flexibility in order to achieve the bust results. Typical methods of comprehensive assessment include hierarchical analysis, probabilistic risk assessment and fuzzy comprehensive evaluation method ([10], [19], [49]). Since the Analysis of Hierarchy Process (AHP) can change from the qualitative index into quantitative index [3], therefore, AHP has been widely used in security risk assessment. The other method such as Hybrid model, Hybrid model is developed by integrating two or more existing model.

The rest of this paper is organized as follows. In section 2 we reviewed the literature of information security analysis. We discussed the information security assessment process, quantitative security risk analysis method (including Expect Annual Loss or Estimated Annual Cost) and the process of IT risk assessment in section 3. In section 4, we explained the future research for information risk analysis issues; a future research direction may be development and application of soft computing and hybrid model for information security analysis. In section 5, A Practical advice for evaluation information security risk based on AHP and fuzzy comprehensive evaluation is discussed. We detail examine the steps of AHP and fuzzy comprehensive evaluation method. Section 6 is conclusion.

Table 1: Advantages and disadvantages of Quantitative and Qualitative methods

	Quantitative methods
Advantages	- It allow for definition of consequences of incidents occurrence in quantitative way. - The realizations of costs and benefits analysis during selection of protections. - It obtain more accurate image of risk.
Disadvantages	- Quantitative measures must depending on the scope and accuracy of defines measurement scale. - Analysis‘s results may be not precise and event confusing. - It must be enriched in qualitative description - Analysis conducted with application of those methods is generality more expensive, demanding greater experience and advanced tools
	Qualitative methods
Advantages	- It allows for determination of areas of greater risk in short time and without bigger expenditures. - Analysis is relatively easy and cheap.
Disadvantages	- It does not allow for determination of probabilities and results using numerical measures. - Costs benefits analysis is more difficult during selection of protections - Achieved results have general character, approximates, etc

2. LITERATURE REVIEW

Baskerville [5] has been investigating information security risk analysis science the mid-1980s. He has identified risk analysis checklists for tools used for designing security measures for information systems. Suh and Han [44] present an approach for information security risk analysis that incorporates operational environment continuity. Several methodologies are used in the analysis, such as matrix-based approach [20], paired comparison [41], and asset-function assignment tables (CMS) [12]. Some researchers have been made to develop complex tools for information security risk analysis such as The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [1], CORAS [43], CRAMM [4], Information Security Risk Analysis Method (ISRAM) [24], CCTA Risk Analysis and Management (CRAMM) ([4], [53]), and CORAS ([17], [20], [23], [48]). Facilitated Risk Assessment Process (FRAP) ([6], [33]), the Consultative Objective and Bi- functional Risk Analysis (COBRA) [13], Is Risk Analysis Based on Business Model developed at the Korea Advanced Institute of Science and Technology in 2002 ([29], [41], [44]), the Risk Watch method as a criterion may be annual loss and estimates are selected from the investment return and Matrix-Based method [20].

From the early 2000s, some other security risk modeling techniques were also employed in the risk prediction research area and have shown good performance [22]. This model is called soft-computing, including the Grey relational making approach [19], Fuzzy number arithmetic operational (Liu et al. 2004), Information entropy [26], Fuzzy weighted average approach [10] and Fuzzy measure and Evidence theory [15], Fuzzy AHP method ([45], [46]).

A multi-attribute information security risk assessment method based on threat analysis ([11], [51], [52]). Zhao et al. [56] use neural network (NN) foe risk evaluation of information security. The evaluation of information security related risks of an organization using multi-criteria decision making method is presented in [21].

The analytic hierarchy process (AHP) has been used in risk applications such as security policy decision making, evaluating information security investments and security risk assessment. AHP is also used to analyze risk based on Business model [44]. For example, use AHP in evaluating information security investment [8]. Ramanathan and Ganesh [34] used a group preference aggregation method in AHP model an evaluation and an intrinsic process for deriving members' weights.

Hybrid model are developed by integrating two or more existing model. Some research is integration of two approaches, such as [55], they studied information security risk assessment methodology research: Group decision making and analytic hierarchy process. Analytic Hierarchy Process offers a technical support for risk analysis by using the judgments of managers and systematically calculating the relative risk value (weight). Eren-Dogu and. Celikoglu [14] argued that Bayesian prioritization procedure provides a more effective way of risk assessment than proposed by the conventional approaches used in AHP [14].

Suh and Han [44] argued that information security risk analysis methods do not adequately reflect the loss from disruption of operations to determine the value of information system assets. The defect of quantitative methods and quantitative methods are: quantitative methods do not measure the loss disruption of operations [44], qualitative methods consider the loss, but their results are subjective and not suitable for cost-benefit decision support ([27], [44]). Some

researches are integration of Quantitative methods and Qualitative methods, such as [48], they studied information security risk model comparing with OCTAVE, CORAS, ISRAM, CORA and IS model. Since the enterprises experience difficulties in assessing and managing their security risks, in implementing appropriate security controls [37]. Hybrid model in information security, such as apply the Fuzzy and Hierarchy analysis model to network security risk assess research ([49], [50]). The integrated of the analytical hierarchy process, Bayesian prioritization procedure, and group decision making to information security risk research by ([2], [28], [55]). Intelligent techniques for information security techniques contain rough sets, soft computing, NN, Fuzzy logic, and decision tree.

3. QUALITATIVE AND QUANTITATIVE APPROACH

3.1 Information security risk assessment process

Information security risk assessment process is the important prerequisite to achieve scientific and effective risk assessment. Information security risk assessment process is shown in Figure 1. It includes preparation of risk assessment, asset identification, threat identification, vulnerability identification, and risk calculation and other stages. It can be divided into six steps in specification operation [18].

Step 1: To determine assessment object: define the information system data, hardware, software assets etc, give a system function, borders, critical assets and sensitive assets, and determine the scope of the assessment.
Step 2: Assessment performance: Develop the evaluation plan in accordance with the requirements, determine the assessment process, select appropriate assessment methods and tools, and set up the system group.
Step 3: Risk identification: Identify critical assets and general assets within the scope of assessment. And identify threats in operating environment and asset vulnerability of their own existence and the existing security measures.
Step 4: Risk analysis: Combined the property of assets, analyzes the possibility and consequences of threat used by vulnerability, and calculate the results of assessment. Analyze the effectiveness and reasonable of existing security measures.
Step 5: Risk assessment: Evaluate the results; give formation of the risk assessment report combined with the expert's opinion
Step 6: Risk control: according the instructions' require to take effective measures to transfer, avoid or reduce risk, in order to control the system risk effectively.

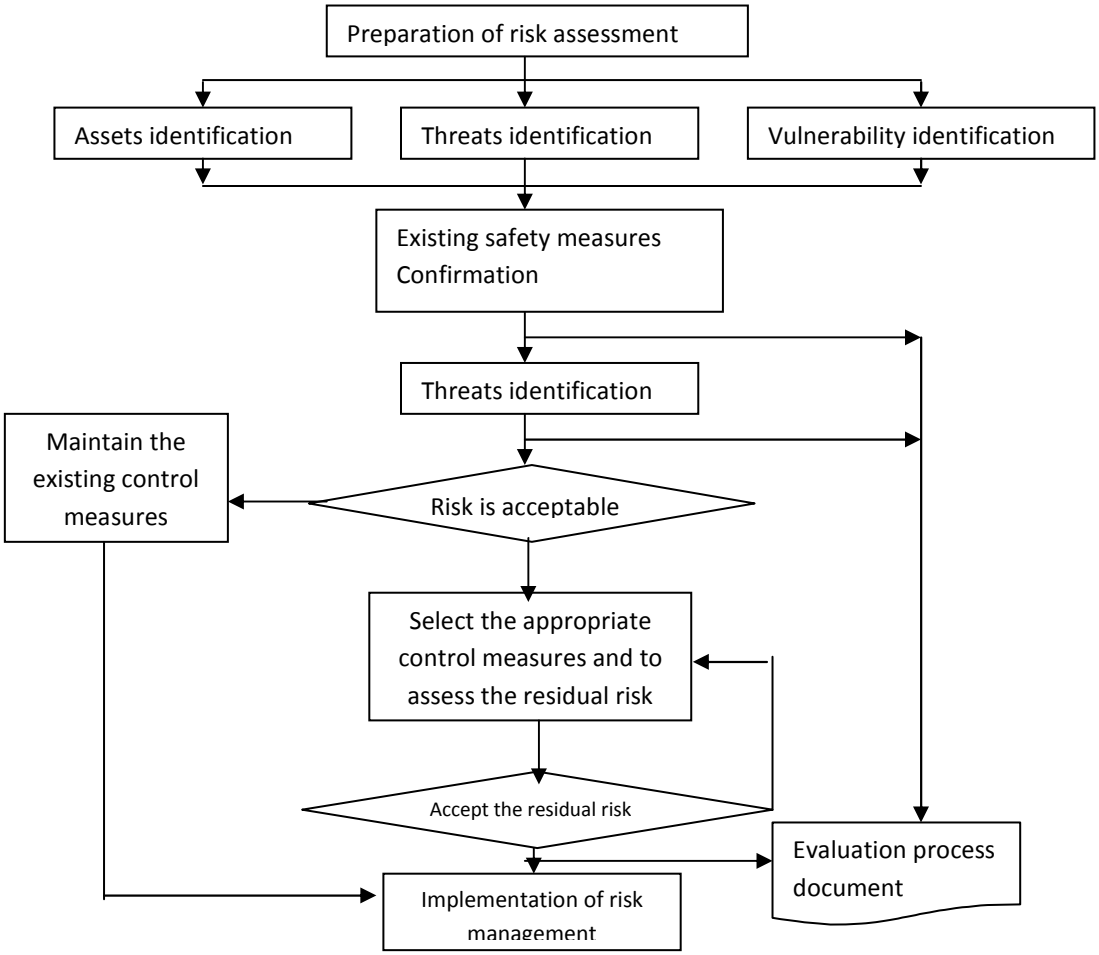

Figure 1: The process of the information security risk assessment [18]

3.2 Quantitative security risk analysis

This approach use two basic elements: the probability of an event occurring and the loss that may be incurred. Quantitative security risk analysis uses one number produced from these elements. Some methods of quantitative security risk analysis are designed by ([35], [38]), such as Risk value, Annual Loss Expected (ALE), Safeguard value, and Return in investment.

(1) Calculation of risk value:

$$R = p \times W \ and \ p = F \times V \qquad (1)$$

Where:

R – Risk value

P – The predicted number of incident occurrence causing loss of assets value in defined period.

W – The value of loss of assets value on single incident occurrence
F – Frequency of threat occurrence
V – It is the measure of probability of usage of specified susceptibility by a given threat.

(2). Annual Loss Expected (ALE)

Annual Loss Expected (ALE), which is the product of probability of occurrence of events which have negative impact on IT and value of caused by them losses. It is presented in the following models.

$$ALE = \Pr obability \times Value\ of\ Loss \quad (2)$$

$$ALE = \sum_{i=1}^{n} I(O_i)F_i \quad (3)$$

Where:
$\{O_1, O_2, ..., On\}$ - Set of negative effects of event
$I(O_i)$ – Value expressed loss resulting from event
F_i – Frequency of i event

(3). Calculation of safeguard value

$$Safeguard\quad value = (ALE\ Before - ALEAfter) - Annual\ \cos t\ of\ countermeasure \quad (4)$$

(4) Return in investment
Business evaluation of identified mechanisms with the use of previously, mentioned ROI

$$ROI = \frac{B}{C} \quad (5)$$

Where:
S – Savings- reduction in ALE, $S = ALE\ (baseline) - ALE(with\ new\ protection)$ B – Benefits, $B = S + \Pr ofit\ from\ new\ ventures$

C – Costs of Protections

4. CURRENT RESEARCH TRENDS

A current research direction may be the development and application of soft computing and hybrid models.

4.1 Soft Computing in Information security risk assessment

AHP support for an organization's information security system to evaluate the weights of risk factors, most of researches seems to prefer the AHP method [21] Bodin and Gordon [8] argued that evaluate the weighting factors needed to combine risk measure. The other researcher used AHP in information security risk evaluation such as ([8], [16], [42]).

Kijo and Luo [57] argued that (1) Soft Computing became a formal Computer Science area of study in early 1990's, (2) Earlier computational approaches could model and precisely analyze

only relatively simple systems, and (3) More complex systems often remained intractable to conventional mathematical and analytical methods. It pointed out that soft computing is suitable for application of information security risk analysis

Components of soft computing include:

- Neural networks (NN)
- Rough sets (RS)
- Grey sets (GS)
- Fuzzy systems (FS)
- Generic algorithms (GA)
- Support vector machine (SVA)
- Bayesian classifier, Bayesian network (BN)

Since to improve the performance of this method, it is necessary a method for reduction the feature subset such as rough sets, genetic algorithm. Rough sets are an effective mathematical analysis tool to deal with vagueness and uncertainty in the area of area of decision analysis [32]. Zhao and Zhang [56] use neural networks (NN) method for risk evaluation of information security. genetic algorithm (GA) belong to the larger class of evolutionary algorithm (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover. Tamjidyamcholo and AI-dabbaggh [47] applied a genetic algorithm (GA) for core point of information security risk reduction in uncertainty.

Guan at al. [21] applied the multi-criteria decision-making method in Evaluation of information security related risks. In Bayesian network method, Feng and Yu [16] used Bayesian network (BN) for identifying the causal relationships of risk factors and predict the occurrence probability of security risk.

4.2 Hybrid models in Information security risk assessment

In order to develop a robust prediction system, a number of models taken from neural networks, decision tree, generic algorithms, Support vector machine, Bayesian classifier, and fuzzy rule based classifier will have to be seamlessly integrated, implemented, tested and validated. Yuan et al. [54] use fuzzy and grey comprehensive (Fuzzy- Grey) evaluation system to evaluate the recovery ability. Some researches use hierarchy process grope decision making (AHP-GDM), such as [55], and [15]. Shi and Deng [40] proposed a novel method integrated grey relational analysis and Grey-AHP evaluation to classification for information systems security. Some approaches of information security risk analysis and assessment are shown as Table 2.

Table 2. Some approaches of information security risk analysis and assessment

Category	Area	Some Approach
Neural Networks	Machine learning	1. Multilayer perception 2. Back propagation 3. Radial function neural network 3. Probabilistic neural network 4. Self-organized competition

Learning vector	Machine learning	Support Vector Machine (SVM)
Soft-computing	Reduction attributes	1. Rough sets of reduction knowledge 2. Grey relational of reduction knowledge 3. Genetic algorithm of reduction knowledge 4. Fuzzy-Rough Sets Approach
Hybrid models	Combination of two or more techniques	1. Rough - Bayesian network 2. Rough Sets – Neural Network 3. Fuzzy-Rough Sets 4. Fuzzy- AHP 5. Fuzzy - ANP 6. Grey –Hierarchy model 7. GA-based neural network approach

5. PRACTICAL ADVICE FOR EVALUATION INFORMATION SECURITY RISK

In this section, we discussed that the evaluation of information security risk assessment used AHP and Fuzzy comprehensive method. The model of the evaluation of information security risk assessment is shown as Figure 2.

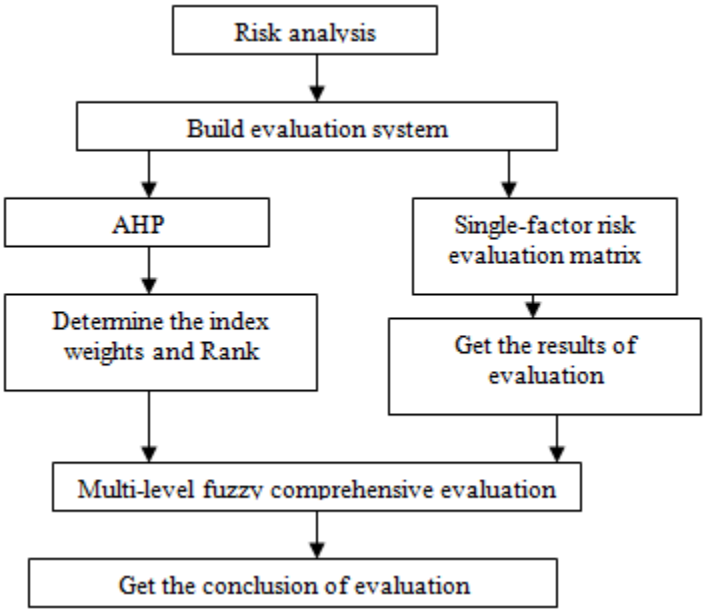

Figure 2: The model of information security risk evaluation

5.1 Analytical Hierarchy Process

Step 1: Structure a Hierarchy

This step AHP breaks down a complex multi-criteria decision-making problem into a hierarchy interrelated decision criteria, decision alternatives [9]. Table 3 is denoted as evaluation index system of information security.

Table 3: Evaluation index system of Information security risk

Decision alternatives	Index of the first criteria	Index of second criteria
Information security risk assessment	Assets (c_1)	Confidentially (c_{11})
		Integrity (c_{12})
		Availability (c_{13})
	Threats (c_2)	Environment factors (c_{21})
		Human factors (c_{22})
	Vulnerability (c_3)	Technical Vulnerability (c_{31})
		Management Vulnerability (c_{32})
	Safety measures (c_4)	Prevent security measures (c_{41})
		Protective security measures (c_{42})

Step 2: Pair-wise comparison

Prioritization procedure starts in order to determine the relative importance of the criteria with each level. The Judgment matrix, as shown:

$$A = \begin{bmatrix} 1 & \frac{w_1}{w_2} & \ldots \frac{w_1}{w_n} \\ \frac{w_2}{w_1} & 1 & \ldots \frac{w_2}{w_n} \\ . & & \\ \frac{w_n}{w_1} & \frac{w_n}{w_2} & \ldots 1 \end{bmatrix} = \begin{bmatrix} a_{11}\, a_{12} \ldots a_{1n} \\ a_{21}\, a_{22} \ldots a_{2n} \\ . \quad . \quad \ldots \quad . \\ \\ a_{n1}\, a_{n2} \ldots . a_{nn} \end{bmatrix} \qquad (21)$$

Where A = comparison pair-wise matrix,

w_1 = weight of element 1,
w_2 = weight of element 2,
w_n = weight of element n.

In order to determine the relative preferences for two elements of the hierarchy in matrix A, multiple pair-wise comparisons are based on a standardized comparison scale of nine levels (Table 4).

Table 4: Scales for pair-wise comparison [36]

Intensely of importance	Definition
1	Equal importance
3	Moderate importance
5	Strong importance
7	Very strong importance
9	Extreme importance
2,4,6,8	Intermediate values between adjacent scale values

The judgment matrix is as following:

$$A=\begin{bmatrix}1 & 3 & 1.5 & 2\\ 0.333 & 1 & 0.5 & 0.667\\ 0.667 & 2 & 1 & 1.333\\ 0.5 & 1.5 & 0.75 & 1\end{bmatrix} \qquad A_1=\begin{bmatrix}1 & 1.5 & 0.75\\ 0.667 & 1 & 0.5\\ 1.333 & 2 & 1\end{bmatrix}$$

$$A_2=\begin{bmatrix}1 & 0.667\\ 1.5 & 1\end{bmatrix} \quad A_3=\begin{bmatrix}1 & 1.5\\ 0.667 & 1\end{bmatrix} \quad A_4=\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$$

Step 3: Estimate the relative weights

The relative weights are given by the eigenvector W corresponding to the largest eigenvalue $\lambda_{\max}$ as:

$$A\times W=\lambda_{\max}\times W \qquad (22)$$

Where $\lambda_{\max}$ is the largest eigenvalue of matrix A.

(1) Normalized each row vector of A.

$$\overline{a}_{ij}=\frac{a_{ij}}{\sum_{k=1}^{n}a_{kj}} \qquad (i=1,2,.\quad .n) \qquad (23)$$

(2) Summed each column vector of $\overline{A}$

$$\overline{w}_i=\sum_{j}^{n}\overline{a}_{ij} \qquad (i=1,2,.\quad .n) \qquad (24)$$

(3) Normalized each vector of $\overline{W}=(\overline{w}_1,\overline{w}_2\ldots\overline{w}_n)$

$$w_i=\frac{\overline{w}_i}{\sum_{i=1}^{n}\overline{w}_i} \qquad (i=1,2,.\quad .n) \qquad (25)$$

Table 5: The relative weights of second criteria and ranking

First level	First level Relative weights	Second level	Second level Relative weights	Risk value weights	Rank
c_1	0.4	c_{11}	0.333	0.1332	3
		c_{12}	0.222	0.0888	7
		c_{13}	0.445	0.178	1
c_2	0.133	c_{21}	0.4	0.0532	9
		c_{22}	0.6	0.0798	8
c_3	0.267	c_{31}	0.6	0.1602	2

		c_{32}	0.4	0.1068	4
c_4	0.2	c_{41}	0.5	0.1	5
		c_{42}	0.5	0.1	6

The relative weights of first criteria are $W = (0.4, 0.133, 0.267, 0.2)$. The relative weights of second criteria are $W_1 = (0.333, 0.222, 0.445)$, $W_2 = (0.4, 0.6)$, $W_3 = (0.6, 0.4)$ and $W_4 = (0.5, 0.5)$.

Step 4: Check the consistency

The consistency is defined by the relation between the entries of A: $a_{ij} * a_{jk} = a_{ik}$, the . Consistency Index (*CI*) is calculated as:

$$CI = \frac{\lambda_{\max} - n}{n-1} \qquad (26)$$

Where

$$\lambda_{\max} = \sum_{i=1}^{n} \frac{(AW)_i}{nW_i} \qquad (27)$$

The random index (RI) is consistency index of pair-wise comparison matrix which is generated randomly. The table 6 is random indexes of the matrices of order 1–15 can be seen in [36]. The final consistency ratio is calculated by comparing the CI with the random index (RI). Generally, if *CR* is less than 0.1, the judgments are consistent. The formulation of *CR* is:

$$CR = \frac{CI}{RI} \qquad (28)$$

Table 6 : The random index (*RI*)

n	1	2	3	4	5	6	7	8
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41
n	9	10	11	12	13	14	15	
RI	1.45	1.49	1.52	1.54	1.56	1.58	1.59	

Saaty [36] has shown that if the referee is completely consistent then,

- $a_{ij} \cdot a_{jk} = a_{ik}$
- $\lambda_{\max} = n \; and \; CI = 0$

According the above method, the above judge matrix is met consistency test.

5.2 Fuzzy Comprehensive Evaluation Method

Fuzzy comprehensive evaluation method can use in information security risk assessment. The method is a qualitative one and the following is the principle procedures of it:

(1) Establishing element set and grade factor set

According to the nature of the characteristics of the first level index in the evaluation system, the factors set in the evaluating relationship are as follows:

$$U = \{u_1, u_2, \ . \ \ . \ \ ., u_n\}$$

Where, u_j represents the j^{th} evaluation element. Five assessments grades can be determine by:

$V = \{v_1, v_2, v_3, v_{4,} v_5\} = \{high, higher, medium, lower, low\}$

(2) Establishing the single-factor evaluation matrix R from U to V

We assume that 20 experts are selected to compose of expert evaluation term of information security risk. The experts independently decide the level of evaluation factors to the information security risk (see Table 7).

Table 7**:** Expert evaluation Statistics

Second level	High	Higher	medium	Lower	Low
c_{11}	0	3	5	10	2
c_{12}	1	3	3	6	7
c_{13}	2	3	8	3	4
c_{21}	0	1	2	8	9
c_{22}	1	1	2	9	7
c_{31}	0	5	10	4	1
c_{32}	1	3	5	8	3
c_{41}	0	1	4	12	3
c_{42}	0	2	4	10	4

For each u_j, r_{ij} represents the degree of membership on u_j to v_i (i = 1, 2, 3, 4).

$r_{ij} = \frac{n}{20}$, n represents the number of u_j. R is denoted the fuzzy matrix of element u_j on grade v_i.

$$R = \begin{bmatrix} r_{11} & r_{12} & r_{13} & r_{14} & r_{15} \\ r_{21} & r_{22} & r_{23} & r_{24} & r_{25} \\ & & & & \\ r_{m1} & r_{m2} & r_{m3} & r_{m4} & r_{m5} \end{bmatrix}$$

The single-factor risk evaluation matrixes are:

$U = \{c_1, c_2, c_3, c_4\}$, $U_1 = \{c_{11}, c_{12}, c_{13}\}$, $U_2 = \{c_{21}, c_{22}\}$, $U_3 = \{c_{31}, c_{32}\}$ $U_4 = \{c_{41}, c_{42}\}$

$$R_1 = \begin{bmatrix} 0 & 0.15 & 0.25 & 0.50 & 0.10 \\ 0.05 & 0.15 & 0.15 & 0.30 & 0.35 \\ 0.10 & 0.15 & 0.40 & 0.15 & 0.20 \end{bmatrix}$$

$$R_2 = \begin{bmatrix} 0 & 0.05 & 0.10 & 0.40 & 0.45 \\ 0.05 & 0.05 & 0.10 & 0.45 & 0.35 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} 0 & 0.25 & 0.50 & 0.20 & 0.05 \\ 0.05 & 0.15 & 0.25 & 0.40 & 0.15 \end{bmatrix}$$

$$R_4 = \begin{bmatrix} 0 & 0.05 & 0.20 & 0.60 & 0.15 \\ 0. & 0.10 & 0.20 & 0.50 & 0.20 \end{bmatrix}$$

The results of these evaluations the normalized conditions and the sum of the values of the row vector is 1.

(3)To get the comprehensive results of evaluation

The comprehensive results of information security risk in single-factor evaluation are:

$$B_i = W_i \circ R_i = \{b_{i1}, b_{i2}, bi3, b_{i4}, b_{i5}\} \quad (\text{i} = 1, 2, 3, 4)$$

$$B_1 = \{0.0556, 0.15, 0.29455, 0.29985, 0.2\}$$

$$B_2 = \{0.03, 0.05, 0.1, 0.43, 0.39\}$$

$$B_3 = \{0.03, 0.19, 0.35, 0.32, 0.11\}$$

$$B_4 = \{0.0, 0.075, 0.2, 0.55, 0.175\}$$

(4) Multi-level fuzzy comprehensive evaluation

According to synthetic evaluation result B_i of V , the cluster to U is supposed as R .

$$R = \begin{bmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{bmatrix} \qquad (29)$$

The evaluation of indices U , we make a synthetic evaluation, its synthetic evaluation result records is:

$$B = W \circ R = \{b_1, b_2, b_3, b_4, b_5\} \qquad (30)$$

$$B = W \circ R = \{0.0342, 0.1264, 0.2486, 0.3287, 0.1824\}$$

(5) Get the conclusion of evaluation

According to synthetic evaluation results B, under the principle of maximum subordination, the evaluation level "Lower" corresponding to the maximum subordination in set B should be the evaluation conclusion of information security risk in L-company.

6. CONCLUSION

In this research, we review the paper which had applied AHP model, neural networks, Fuzzy Logic, Group decision making, software-computing and hybrid model in information security risk problem. We find that (1) in the evaluating fields; the application areas include information security risk analysis, information security risk assessment, and information security management. (2) Most of researches seem to prefer the AHP method. (3) Since to improve the performance of this method, it is necessary a method for reduction the feature subset, many hybrids Fuzzy based model and rough model are proposed. (4) Hybrid models are new assessment method. (5) We have a practical advice for evaluation information security risk based on AHP and Fuzzy Comprehensive Evaluation Method.

ACKNOWLEDGEMENTS

I would like to thank the anonymous reviewers for their constructive comments on this paper.

REFERENCES

1. Alberts C, Dorofee A. (2002) "Managing Information Security Risks: The Octave Approach", Addison-Wesley Professional.2002.
2. Altuzarra A. Moreno-Jimnez, J. M, Salvador M. (2007), "A Bayesian prioritization procedure for AHP-group decision making". European Journal of Operation Research, Vol.18, No. 1, pp. 367-82.
3. Award, G.. A., Suitan E, Ahmad, N, Ithnan, N, Beg, A. H. (2011), "Multi-objective model to process security risk assessment based on AHP-PSO", Modern Applied Science, Vol. 5, No. 3, pp. 246-20.
4. Barber B, Davey J. (1992) "The use of the CCTA risk analysis and management methodology" CRAMM. MEDINF092, North Holland, pp. 1589-1593.
5. Baskerville R. (1993), "An analysis survey of information system security design methods: Implications for Information Systems Development". ACM Computing Survey, pp. 375-414.
6. Behnia A, Rahsid R. A, Chaudhry J. A. (2012), "A survey of information security risk analysis methods", Smart Computing Review, Vol. 2, No. 1, pp 79-93.
7. Bialas A. (2006), Security of information and services in modern institution and company (in Polish), WNT, Warsaw 2006.
8. Bodin L. D, Gordon L. A, Loeb M. P. (2005), "Evaluation information security investments using analytic hierarchy process". Communications of the ACM, Vol. 48, No. 2, pp. 78-83.
9. Boroushaki , S. and Malczewski, J., (2008), "Implementing an extension of the analytical hierarchy", process using ordered weighted averaging operators with fuzzy quantifiers in ArcGIS, Computer and Geosciences, 34, pp. 399-410
10. Chang, P. T., Hung K, C. (2005), "Applying the fuzzy weighted average approach to evaluation network security systems". Computers and Mathematics with Application, Vol. 49, pp. 1797-1814.
11. Chen A, Wang X. H, Huang H. (2004), "Research on multi-attribute information security risk assessment method based on threat analysis". Computer Engineering and Design, Vol. 30, No. 1, pp. 38-40.
12. CMS. CMS information security risk assessment methodology. CENT MEDIMED MEDICAID SERV 2009, Vol. 1, No. 1, pp.1-20.
13. Elky S. (2006), "An introduction to information system risk management". SANS institute InfoSec reading Room. 2006.

14. Eren-Dogu Z. F. Celikoglu C. C. (2011), Information security risk assessment: Bayesian prioritization for AHP group decision making". International Journal Innovation Computer Information Control, Vol. 8, No.11, pp. 8019-32.
15. Feng N, Li M. (2011), "An information systems security risk assessment model under uncertain environment". Applied Soft Computer, Vol. 11, No.7, pp. 4332-4340.
16. Feng N. and Yu, X., A (2012), "Data-driven assessment model for information system security risk management", Journal of Computers, Vol. 7, No. 12, pp. 3103-3109.
17. Fredriksen R, Kristiansen M, Gran, B. A, Stolen K, Oppurud T. A, Dimitrakos T. (2002), The CORAS framework for a model-based risk management process. In the Proceeding of the 21th International Conference on Computer Safety, Reliability and Security, 2002.
18. Fu S, Xiao Y. (2012), "Strengthening the research for Information security risk assessment". International Conference on Biological and Biomedical Science Advanced in Biomedical Engineering, Vol. 9; pp. 386-392.
19. Gao Y, Luo J. Z. (2009), Information security risk assessment based on grey relational decision making algorithm" , Journal of Southeast University, Vol. 39, No. 2, pp. 225-229.
20. Goel S, Chen V. Information security risk analysis - a matrix-based approach. University at Albany, SUNY, 2005.
21. Guan B, Lo C, Wang P, Hwang J. Evaluation of information security related risks of an organization-the application of the multi-criteria decision making method. In the Proceeding of IEEE the 37th Annual International Camahan Conference on Security, 2003, p. 168-75.
22. Hoffer J. A, George J. E, Valacich J. S. (1999), "Modern systems analysis& design". Addison-Wesley-Longman. New York, N.Y., USA; 1999.
23. IST. A brief history of CORA, International Security Technology Inc (IST Inc.). 2002. http://www.ist-usa.com Accessed 16-6-2013.
24. Karabacaka B, Songukpinar I., (2005), "ISRAM: Information security risk analysis method", Computer & Security, March, pp. 147-169.
25. Keramati A, Yousefi N. (2011), "A proposes classification of data mining techniques in credit scoring". In the Proceeding of 2011 International Conference of Industrial Engineering and Operations Management, Kuala Lumpur, Malaysia, Jurnal 2011, pp. 22-4.
26. Liu F, Dai K, Wang Z. Y. (2004), "Research on the technology of quantitative security evaluation based on fuzzy number arithmetic operation", Fuzzy Systems and Mathematics, Vol. 18, No. 4, pp. 51- 54.
27. Liu Y, Lin Q, Meng K.(2010), "Research on quantitative security risk assessment method of an enterprise information system based on information entropy", Computer Science, Vol. 37, No. 5, pp. 45-48.
28. Lo C. C, Chen W. J. (2012), "A hybrid information security risk assessment procedure considering interdependences between controls", Expert Systems with Applications, Vol. 39, pp. 247-257.
29. Loch K. D, Carr H. H, Warkentin M. E. (1992), "Threats to information systems: today's reality, yesterday understands". MIS Quarterly, Vol. 16, No. 2, pp.173-186.
30. NIST Sp 800-30, sp800 30ri.pdf, Step. 2012. http://csrc.nist.gov/publication/nistpubs/800_30_r1.pdf. (Accessed 16-6-2013).
31. Nobre, F. F., Trotta, L. T. F., Gomes, L. F. A. M., (1999), "Multi-criteria decision making: an approach to setting priorities in health care", Symposium on statistical bases for public health decision making, Vol. 18, No. 23, pp.3345-3354.
32. Panigrshi S, Kundu A, Sural S, Majumder A K. (2009), "Credit card adds fraud detection: a fusion approach using Dempster-Shafer theory and Bayesian learning". Information Fusion, Vol. 10, No. 4, pp. 354-363.
33. Peltier T. R. (2000), "Facilitated risk analysis process (FRAP)". Auerbach Publication, CRC Press LLC, December 2000.
34. Ramanathan R, Ganesh L. S (1994), "Group preference aggregation methods in AHP: an evaluation and an intrinsic process for deriving members' weights". European Journal of Operation Research, Vol. 79, No. 2, pp. 249-265.

35. Rot A. (2008), "IT risks assessment: quantitative and qualitative approach". WCECS, 2008, October 22-24, San Francisco, USA.
36. Saaty T. L. (1980), "The Analytical Hierarchy Process: Planning, Priority Setting", Resource Allocation. McGraw-Hill, New York, NY, USA.1980.
37. Sadok M, Spagnoletti P. (2011), "A business aware information security risk and analysis method". Information Technology and Innovation treads in Organization, pp. 453-460.
38. Schechter E. (2004), "Computer security strength & risk: a quantitative approach". Harvard University, Cambridge, Massachusetts, USA. 2004.
39. Shedden P, Smith W, Ahmad A. (2010), "nformation security risk assessment: towards a business practice perspective". In the Proceeding of the 8th Australian Information Security Management Conference, pp. 119-130.
40. Shi, H. and Deng, Y. (2012), "A grey model for evaluation of information systems security", Journal of Computer, Vol. 7, No. 1 , pp.284-291.
41. Shukla N, Kumar S. A (2012), "Comparative study on information security risk analysis practices". In the Proceeding on Issues and Challenges in Networking, 2012, November 2012, pp. 28-33.
42. Sommestad, T., Ekstedt, M. and Johnson, P., A (2010), "Probabilistic relational model for security risk analysis", Computer & Security, Vol. 29, No. 6, pp. 659-679.
43. Stolen K, den Braber F, Dirmitrakos T. (2002), "Model-based Risk Assessment –The CORAS Approach". 2002. http://www/nik.no/2002/stolen.pdf
44. Suh B, Han I. (2003), "The IS risk analysis based on business model". Information and Management, Vol. 41, No. 2, pp. 149-158.
45. Syamsuddin, I. and Hwang, J., (2010), "The use AHP in security policy decision making: An open office calc application", Journal of Software, Vol. 5, No. 10, pp. 1162-1169.
46. Syamsuddin, I. (2012), "Evaluation of strategic information security with fuzzy AHP method". American Journal of Intelligence Systems, Vol. 2, No. 1, pp. 9-13.
47. Tamjidyamcholo A, AI-Dabbagh R. D (2012), « Genetic algorithm approach for risk reduction on information security". International Journal of Cyber-Security and Digital Forensics, Vol. 1, No. 1 pp. 59-66.
48. Vorster A, Labuschagne, L. (2005), "A framework for comparing different information security risk analysis methodologies". University of Johannesburg. 2005.
49. Wang C. J., Lin G. Y., (2006), "The model of network security risk assess based on fuzzy algorithm and hierarchy". Journal of Wuhan University, Vol. 52, No. 5, pp. 622-627.
50. Weiss J. D(1991). "A system security engineering Process". In the Proceeding of the 14th National Conference Security Conference, 1991 Washington, DC.
51. Xiao M, Fan S. X, Wu Z. (2009), "A threat-centric model for information security risk assessment", Journal of Wuhan University of Technology, Vol. 31, No. 18, pp. 43-45.
52. Yang Y, Yao S. Z.(2009), "Risk assessment method of information security based on threat analysis". Computer Engineering and Applications, Vol. 45, No. 3, pp. 94-96.
53. Yazar Z. A (2011), Qualitative risk analysis and management tool – CRAMM, SANS Institute InfoSec Reading Room. 2011.
54. Yuan, C. Li, J., Zhang, R. and Liu, J.,(2013), "Grey and fuzzy evaluation of information system distress recovery capability", 2nd International Conference on Advances in Computer Science and Engineering, CSE2013, pp. 298-302.
55. Zhang X, Huang Z, Wei G., Zhang X.(2010), "Information security risk assessment methodology research: Group decision making and analytic hierarchy process". In the Proceeding of IEEE the 2nd World Congress on Software Engineering, pp.157-60.
56. Zhao D, Liu J, Zhang Z. (2009), "Method of risk evaluation of information security based on neural network". IEEE international Conference on Machine Learning and Cybernetics, Vol. 1, No. 6, pp.1127-1132.
57. Kijo, H. and Luo, J. (2012), " Analysis on the competitiveness of Chinese steel and the south Korean", Software Computing in Information Communication Technology, Vol. 2, No. 1, pp. 451-460.

Authors

Ming-Chang Lee is Assistant Professor at National Kaohsiung University of Applied Sciences. His qualifications include a Master degree in applied Mathematics from National Tsing Hua University and a PhD degree in Industrial Management from National Cheng Kung University. His research interests include knowledge management, parallel computing, and data analysis. His publications include articles in the journal of Computer & Mathematics with Applications, International Journal of Operation Research, Computers & Engineering, American Journal of Applied Science and Computers, Industrial Engineering, International Journal innovation and Learning, Int. J. Services and Standards, Lecture Notes in computer Science (LNCS), International Journal of Computer Science and Network Security, Journal of Convergence Information Technology and International Journal of Advancements in computing Technology.