Analysis on the Causal Relationship and Improvement Strategy of Information Security Management with DEMATEL

Li-Hsing Ho
Ph. D Program of Technology Management
Chung Hua University
HsinChu, Taiwan R.O.C

Ming-Tsai Hsu
Ph. D Program of Technology Management
Chung Hua University
HsinChu, Taiwan R.O.C

Shu-Yun Feng
Ph. D Program of Technology Management
Chung Hua University
HsinChu, Taiwan R.O.C

Tieh-Min Yen
Department of Technology Management
Chung Hua University
HsinChu, Taiwan R.O.C
ytm1129@ms48.hinet.net

***Abstract*—The study applied Decision Making Trial and Evaluation Laboratory (DEMATEL) to analyze the casual relationship and mutual impact level between the control items of the information security management system. Three core control items of the information security management system are found, Security Policy (SC1), Access Control (SC7) and Human Resources Security (SC4) respectively. They can be provided to enterprises as the direction of continuous improvement, risk reduction and the establishment of competitive advantages. The study applied the methodology value of DEMATEL, which not only has established the causal relationship and mutual impact level between the 11 information security control items, but also provided organizations with the least resource input to resolve practical intricate issues.**

Keywords-ISO 27001; ISO 27002; cause-effect analysis; decision making trial and evaluation laboratory (DEMATEL); information security management system; continuous improvement

I. INTRODUCTION

The Decision Making Trial and Evaluation Laboratory (DEMATEL) was developed by the Battelle Memorial Institute through its Geneva Research Center; it is used to resolve the issues of race, hunger, environmental protection, and energy [1][2]. Scholars have applied DEMATEL to resolve issues in different fields; Hsu applied the Factor Analysis Approach and DEMATEL to analyze the evaluation criteria and the causal relationship of blog design [3]; Wu and Tsai applied DEMATEL to analyze the causal relationship between the evaluation criteria of automobile spare parts [4]; Jassbi, Mohamadnejad and Nasrollahzadeh applied Fuzzy DEMATEL to establish the causal relationship and impact level of strategy maps [5]; Zhou, Huang and Zhang applied Fuzzy DEMATEL to identify the key success factor of energy management [6]; Wu applied Fuzzy DEMATEL to distinguish the key success factor of knowledge management [7]; Tseng applied Grey-Fuzzy DEMATEL to develop the causal decision-making model of service quality [8]; Hu, Chiu, Cheng and Yen integrated IPA and DEMATEL to improve the order-winning conditions of computer network equipment manufacturers [9]; Lee, Li, Yen and Huang respectively applied DEMATEL and Fuzzy DEMATEL to the technology acceptance model of the etching technology industry [10][11]; Chang, Chang and Wu applied Fuzzy DEMATEL to analyze the evaluation importance of suppliers [12]; Ho et al. integrated multiple regression analysis and DEMATEL to amend importance-performance analysis, and applied it to assess the quality performance of suppliers [13]. As such, the methodology of DEMATEL has been successfully applied in many fields.

The purpose of Gabus and Fontela developing the DEMATEL approach is to directly compare the interaction between variables and obtain the causal relationship and impact level with matrix operation in an intricate system, find the core issue and improvement direction by setting the threshold to simplify the relationship of variables, apply the cause-effect diagram to express the variable features and types in the system, and find the core issue and improvement direction in the complicated system [1]. The study, therefore, applied DEMATEL to analyze the interactions and impact levels of the control items in an information security management system, and then further developed the continuous improvement strategy of the information security management system.

II. ISMS REVIEW

The International Organization for Standardization issued ISO 27001 Information Security Management System (ISMS) requirements in 2005 as the basis for organization establishment, and information security management implementation, maintenance and verification [14]; it plays a

considerable key role for the contribution for information security management [15]. ISMS has the consistent terminology to establish an authentication framework, the general perception that information system design requires, and the advantage of increasing interoperability and improving product service standards [16]. Information security includes organization, law, technology and application, etc. [17][18], and the traditional information security focused studies mainly focus on information technology [18]. In recent years, there are some scholars who processed studies focusing on the performance and framework of information security implementation [16][19], there are, however, no related studies focusing on the causal relationship and mutual impact level between the practical security control items of ISO 27001 Information Security Management System and ISO 27002 Information Technology- Security Techniques- Code of Practice for Information Security Management [14][20]. As such, the study focused on the 11 security control items in the information security management system to process analysis on the causal relationship and mutual impact level, find the core security control items, and provide the key information for developing a continuous improvement strategy.

The 11 security control items are shown as follows:

1. Security Policy
2. Organizing Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information System Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity management
11. Compliance

Information security management is a complicated system with a causal relationship and mutual impact. To explore the mutual impact relationship of this type of issue and identify the core items, the study applied DEMATEL to analyze the control items of information security management to find the core items that drive the information security management system, allocate the resource to the core items, develop information security management strategy, and achieve the purpose of organization continuous improvement and competitiveness improvement.

III. METHODOLOGY

The Decision Making Trial and Evaluation Laboratory (DEMATEL) directly compares the mutual impact relationship between variables, obtains the system's final causal relationship and impact level through matrix operation, and finds the core items of a complicated system and the improvement direction. The operation steps of DEMATEL are briefly described as follows.

A. Define variables and establish a measurement scale

Literature exploration and expert opinion are applied to list the variables that impact the system, and the causal relationship and impact level scale and symbols between variables are established. The scale is divided into levels 0, 1, 2, and 3, and they respectively represent "No impact", "Low impact", "High impact" and "Great impact" [13], and symbols "+" and "-" are applied to refer to positive impact and negative impact, respectively.

B. Establish Direct-Relation Matrix

When the amount of variables is n, the variables are compared according to the impact relation and level based on expert opinions. If there are many expert opinions, then the consensus decision or mean will be applied to obtain the n×n direct relation matrix X. In the direct relation matrix X, x_{ij} represents the level that variable i impacts variable j. DEMATEL assumes the variables have no self-impacts, and therefore, the diagonal of the direct relation matrix X, x_{ij} (i = j) is set as 0.

$$X = \begin{bmatrix} 0 & x_{12} & \Lambda & x_{1n} \\ x_{21} & 0 & \Lambda & x_{2n} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M} \\ x_{n1} & x_{n2} & \Lambda & 0 \end{bmatrix}$$

If the system has positive and negative impacts, then a symbol matrix is required to be established.

C. Calculate Normalized Direct-Relation Matrix

There are two methods for the calculation of a normalized direct relation matrix, such as applying the greatest column vector sum as the normalized basis [9][10][11][13]; or using the greatest column or row vector as the normalized basis [21].

Set

$$\lambda = \frac{1}{\underset{1 \le i \le n}{Max} \left(\sum_{j=1}^{n} \left| x_{ij} \right| \right)}$$

$$\lambda = Min \left[\frac{1}{\underset{1 \le i \le n}{Max} \left(\sum_{j=1}^{n} \left| x_{ij} \right| \right)}, \frac{1}{\underset{1 \le j \le n}{Max} \left(\sum_{i=1}^{n} \left| x_{ij} \right| \right)} \right] \quad (1)$$

Then through the calculation of formula (1) and (2), and multiplying the direct relation matrix X with λ, the normalized direct relation matrix N is obtained.

$$N = \lambda X \quad (2)$$

There shall be at least one row in which i's sum must meet the requirement of Formula (3) in the DEMATEL assumption.

$$\sum_{j=1}^{n}|x_{ij}| < \frac{1}{\lambda} \quad (3)$$

D. Calculate the Direct and Indirect Relation Matrix

Multiply normalized direct relation matrix N, and add all the calculated mutual impacted results in the system to obtain direct and indirect relation matrix T, as shown in formula (4) [13]. In addition, exclude direct relation matrix N, and only sum up the calculated results with 2 or more mutual impacts to obtain the indirect relation matrix H, as shown in formula (5) [13].

$$T = \lim_{k\to\infty}\left(N + N^2 + \Lambda + N^k\right) = N(I-N)^{-1} \quad (4)$$

$$H = \lim_{k\to\infty}\left(N^2 + N^3 + \Lambda + N^k\right) = N^2(I-N)^{-1} \quad (5)$$

Set tij as the impact coefficient of the direct and indirect relation matrix T, in which i,j = 1,2,…,n. the row and column sum of direct and indirect relation matrix T can be calculated from formula (6) and (7), and set Di as the sum of the ith row, which refers to variable i being the reason that impacts the sum of other variables; Rj is the sum of the jth column, which refers to variable i as the result and is the sum that is being impacted by other variables. Di and Rj obtained from direct and indirect relation matrix T having included the direct and indirect impact.

$$D_i = \sum_{j=1}^{n}|t_{ij}| \quad (i = 1,2,\Lambda\ ,n) \quad (6)$$

$$R_j = \sum_{i=1}^{n}|t_{ij}| \quad (j = 1,2,\Lambda\ ,n) \quad (7)$$

E. Cause-Effect Analysis

Define (Dk + Rk) as the prominence, and k = i = j = 1,2,…,n, as the impact and impacted level of the kth variable, which refers to the core level of variable k in the system; and (Dk - Rk) is defined as a relation, which refers to the impact and impacted difference level of the kth variable, and the causal level of variable k in the system. If the value is positive, then the variable is a reason type, if it is negative, then the variable is a result type. When Dk - Rk is positive and Dk + Rk is great, it refers to variable k being the driving factor of resolving core issues and can be listed as the priority handling object. In addition, through system causal relationship analysis, the improvement priority order of various variables can be determined. However, before the analysis, some thresholds, which have smaller impacts on variables, shall be deleted to simplify the analysis [10][11]. Therefore, the decision-maker can find the driving variable for resolving the core issue in a complicated system and plan suitable decision-making to resolve the issue according to the causal relationship and mutual impact level of variables. The study applied the control items of information security management as the variables, and found the core items that drive the information security management system with DEMATEL to develop an information security management strategy and achieve the purpose of continuous organization improvement and competitiveness improvement.

IV. ANALYSIS RESULT

The design of the study applied the 11 practical security control items of the ISO 27001 Information Security Management System and ISO 27002 Information Technology-Security Techniques- Code of Practice for Information Security Management as variables, and discussed with 3 information security executives and 3 information security field scholars. As the information security control items all have positive impact relationships, only the direct relationship matrix of the 11 security control items are developed. The measurement scale of the direct relationship applied the four point scale, with “0” referring to “No impact”, and “3” referring to “Great impact”.

DEMATEL analysis is processed with information security control items to understand the causal relationship. According to Formula (4), the direct/indirect relation matrix can be obtained, then the value D of each column and the value R of each line according to Formula (6) and (7) are calculated, and the prominence (D+R) and relation (D-R) is obtained, as shown in Table 1.

TABLE I. THE PROMINENCE AND RELATION COEFFICIENT TABLE OF THE INFORMATION SECURITY CONTROL ITEM

Notation	Order-Winner Criteria	D	R	D+R	D-R
SC1	Security Policy	1.771	0.269	2.040	1.502
SC2	Organizing Information Security	0.707	0.442	1.149	0.265
SC3	Asset Management	0.320	0.503	0.823	-0.182
SC4	Human Resources Security	1.446	0.695	2.141	0.751
SC5	Physical and Environmental Security	0.356	0.568	0.925	-0.212
SC6	Communications and Operations Management	0.538	0.954	1.492	-0.416
SC7	Access Control	1.101	1.124	2.225	-0.023
SC8	Information System Acquisition, Development and Maintenance	0.490	0.337	0.827	0.153
SC9	Information Security Incident Management	0.331	1.003	1.334	-0.673
SC10	Business Continuity management	1.018	1.532	2.550	-0.515
SC11	Compliance	0.925	1.575	2.500	-0.649

Divide the sum of prominence and relation by the 11 information security control items to obtain the mean. This value can then be used to divide the cause-effect diagram into four quadrants, as shown in Figure 1. According to the analysis of Figure 1, in the information security control items, those with high prominence and relation are Security Policy (SC1) and Human Resources Security (SC4), which represents that this type of information security control item is the core item of the system; those with high prominence and low relation are Access Control (SC7), Business Continuity management (SC10) and Compliance(SC11), which represents that this type of information security control item will be impacted by other factors; those with high relation and low prominence are Organizing Information Security (SC2), Information System Acquisition, and Development and Maintenance (SC8); and due to the prominence and relation being lower than the mean

1.637 and 0.000, for other information security control items, the causal relationship has a small impact, and they can be regarded as independent.

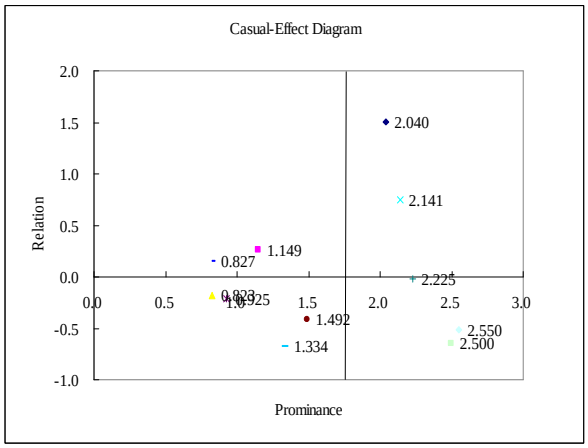

Figure 1: The causal matrix of information security control items

Due to mutual impact relationship of the information security control items being complicated, the study accounted the impact level of the causal relationship being smaller than 0.150 as having no impact, remaining 25%~40% causal relationships which can simplify the complicated causal relationship and be provided to the organization as a decision-making reference when implementing continuous improvement [10][11], shown as Table II.

TABLE II. THE CAUSAL RELATIONSHIP AND IMPACT COEFFICIENT TABLE OF THE INFORMATION SECURITY CONTROL ITEM WITH THE THRESHOLD OF 1.5

Matrix	SC1	SC2	SC3	SC4	SC5	SC6	SC7	SC8	SC9	SC10	SC11
SC1		0.169	0.171	0.185		0.169				0.270	0.270
SC2											
SC3											
SC4						0.205	0.215			0.177	0.253
SC5									0.152		
SC6										0.199	0.179
SC7				0.170		0.159			0.182	0.189	0.225
SC8											
SC9											
SC10										0.240	0.225
SC11							0.185			0.216	

It can be seen from Table 2 that the organization can actively put in resources toward the improvement of 3 security control items and then further drive the improvement of other security control items. (1) When an organization increases the information security instruction and support for the management level focusing on Security Policy (SC1) according to operating requirement and laws and regulations, it can positively impact the improvement of Organizing Information Security (SC2), Asset Management (SC3), Human Resources Security (SC4), Communications and Operations Management (SC6), Business Continuity management (SC10) and Compliance (SC11). (2) When an organization strictly implements Access Control (SC7), it can positively impact the improvement of Human Resources Security (SC4), Communications and Operations Management (SC6), Security Incident Management (SC9), Business Continuity management (SC10) and Compliance (SC11). (3) When an organization helps the employees, outsourcers, and third-party users to understand their responsibility, fit in their identified roles and reduce the risk theft, fraud, and misuse focusing on Human Resources Security (SC4), it can positively impact the improvement of Communications and Operations Management (SC6), Access Control (SC7), Business Continuity management (SC10) and Compliance (SC11).

V. CONCLUTION

Past studies that focus on information security management mainly concentrated on information technology and management framework, and did not establish related studies focusing on the causal relationship and mutual impact of information security control items. Therefore, the study applied DEMATEL to analyze the causal relationship and mutual impact level between the information security control items, establish causal relationship and system matrix, find the core control and improvement item, and put in the least resource to resolve the complicated issue when there is causal relationship in information security management and allow decision-making analysis to be more effectively and accurately provide the information required for business.

The study applied the DEMATEL methodology to process the decision-making improvement analysis and establishment, and find the key improvement items, Security Policy (SC1), Access Control (SC7) and Human Resources Security (SC4), which allows the organization to concentrate resources on improving the abilities of the aforementioned 3 items. This not only improves the quality conformity, but also improves other information security control items at the same time. The limitation of this study was based on 6 experts' experiences and opinions to drive the causal relationships of 11 control items of information security management, lack of empirical research to approve its general application. It will be the important work for research in the near future.

REFERENCES

[1] A. Gabus, and E. Fontela, "Perceptions of the World Problematique: Communication Procedure, Communicating with Those Bearing Collective Responsibility", DEMATEL Report No. 1, Battelle Geneva Research Center, Geneva, Switzerland, 1973.

[2] E. Fontela and A. Gabus, "The DEMATEL Observer", DEMATEL 1976 Report. Switzerland, Geneva, Battelle Geneva Research Center, 1976.

[3] C. C. Hsu, "Evaluation criteria for blog design and analysis of causal relationships using factor analysis and DEMATEL", Expert Systems with Applications, Vol. 39, No. 1, pp. 187-193, 2011.

[4] H. H. Wu, and Y. N. Tsai, "A DEMATEL method to evaluate the causal relations among the criteria in auto spare parts industry", Applied Methematics and Computation, Vol. 218, No. 5, pp. 2334-2342, 2011.

[5] J. Jassbi, F. Mohamadnejad and Nasrollahzadeh, H, "A fuzzy DEMATEL framework for modeling cause and effect relationships of

strategy map", Expert Systems with Applications, Vol. 38, No. 5, pp. 5967-5973, 2011.

[6] Q. Zhou, W. Huang and Y. Zhang, "Identifying critical success factors in emergency management using a fuzzy DEMATEL method", Safty Science, Vol. 49, No. 2, pp. 243-252, 2011.

[7] W. W. Wu, "Segmenting critical factors for successful knowledge management implementation using the fuzzy DEMATEL method", Applied Soft Computing, Vol. 12, No. 1, pp. 527-535, 2011.

[8] M. L. Tseng, "A cause-effect decision making model of service quality expectation using grey-fuzzy DEMATEL approach", Expert Systems with Applications, Vol. 36, No. 4, pp. 7738-7748, 2009.

[9] H. Y. Hu, S. I. Chiu, C. C. Cheng and T. M. Yen, "Applying the IPA and DEMATEL models to improve the order-winner criteria: A case study of Taiwan's network communication equipment manufacturing industry", Expert Systems with Applications, Vol. 38, No. 8, pp. 9674-9683, 2011.

[10] Y. C. Lee, M. L. Li, T. M. Yen and T. H. Huang, "Analysis of adopting an integrated decision making trial and evaluation laboratory on technology acceptance model", Expert Systems with Applications, Vol. 37, No. 2, pp. 1745-1754, 2010.

[11] Y. C. Lee, M. L.Li, T. M. Yen and T. H. Huang, "Analysis of fuzzy decision making trial and evaluation laboratory on technology acceptance model", Expert Systems with Applications, Vol. 38 No. 12, pp. 14407-14416, 2011.

[12] B. Chang, C. W. Chang, and C. H. Wu, "Fuzzy DEMATEL method for developing supplier selection criteria", Expert Systems with Applications, Vol. 38, No. 3, pp. 1850-1858, 2011.

[13] Ho, L.H., Feng, S.Y., Lee, Y.C. and Yen, T.M., "Using modified IPA to evaluate supplier's performance: Multiple regression analysis and DEMATEL approach", Expert Systems with Applications, Vol. 39, No. 8, pp. 7102-7109, 2012.

[14] BS ISO, "BS ISO 27001 Information technology – security techniques – information security management systems – requirements", British Standards Institute, London, 2005a.

[15] B. Karabacak, and I. Sogukpinar, "A quantitative method for ISO 17799 gap analysis", Computers & Security, Vol. 25, pp. 413-419, 2006.

[16] A. Tsohou, S. Kokolakis, C. Lambrinoudakis and S. Gritzalis, "A security standard's framework to facilitate best practices' awareness and conformity", Information Management & Computer Security, Vol. 18, No. 5, pp. 350-365, 2010.

[17] B. Von Solms, "Information security – The fourth wave", Computers & Security, Vol. 25, No. 3, pp. 165-168, 2006.

[18] M.T. Siponen and H. Oinas-Kukkonen, "A review of information security issues and respective research contributions", The Database for Advances in Information Systems, Vol. 38, No. 1, pp. 60-81, 2007.

[19] J.M. Hagen, E. Albrechtsen and J. Hovden, "Implementation and effectiveness of organizational information security measures", Information Security Measures, Vol. 16, No. 4, pp. 377-397, 2008.

[20] BS ISO, "BS ISO 27002 Information technology – security techniques – code of practice for information security management", British Standards Institute, London, 2005b.

[21] G. H. Tzeng, C. H. Chiang and C.W. Li, "Evaluating Intertwined Effects in E-Learning Programs: A Novel Hybrid MCDM Model Based on Factor Analysis and DEMATEL", Expert Systems with Applications, Vol. 32, pp. 1028-1044, 2007.