Information & Computer Security

Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL

Li-Hsing Ho Ming-Tsai Hsu Tieh-Min Yen

The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/2056-4961.htm

Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL

Received 25 April 2014
Revised 29 June 2014
Accepted 7 July 2014

Li-Hsing Ho
Department of Technology Management, Chung-Hua University, HsinChu, Taiwan, Republic of China
Ming-Tsai Hsu
PhD. Program of Technology Management, Chung-Hua University, HsinChu, Taiwan, Republic of China, and
Tieh-Min Yen
Department of Technology Management, Chung-Hua University, HsinChu, Taiwan, Republic of China

Abstract
Purpose – The purpose of this paper is to analyze the cause-and-effect relationship and the mutually influential level among information security control items, as well as to provide organizations with a method for analyzing and making systematic decisions for improvement.
Design/methodology/approach – This study utilized the Fuzzy DEMATEL to analyze cause-and-effect relationships and mutual influence of the 11 control items of the International Organization for Standardization (ISO) 27001 Information Security Management System (ISMS), which are discussed by seven experts in Taiwan to identify the core control items for developing the improvement strategies.
Findings – The study has found that the three core control items of the ISMS are security policy (SC1), access control (SC7) and human resource security (SC4). This study provides organizations with a direction to develop improvement strategies and effectively manage the ISMS of the organization.
Originality/value – The value of this study is for an organization to effectively dedicate resources to core control items, such that other control items are driven toward positive change by analyzing the cause-and-effect relation and the mutual influential level among information security control items, through a cause-and-effect matrix and a systematic diagram.

Keywords Information management, Identification, Information security, Organizational decision-making, Fuzzy logic, British standards

Paper type Research paper

1. Introduction
The International Organization for Standardization (ISO) has announced the ISO 27001 Information Security Management System (ISMS) as the standard for an organization to create, implement, maintain and verify information security management. As for contributions to information security management, this standard plays a critical role

Information & Computer Security
Vol. 23 No. 2, 2015
pp. 161-177

2056-4961
DOI 10.1108/ICS-04-2014-0026

(Gillies, 2011; Karabacak and Sogukpinar, 2006). The ISMS has comprehensive dimensions regarding organization, law, technology, application, etc. (Von Solms, 2006; Siponen and Oinas-Kukkonen, 2007). Furthermore, the ISMS has the advantages of verification scheme creation, compliant terms, general recognition of information system design requirements, intercommunity enhancement and improvement of product service levels (Tsohou *et al.*, 2010). Backhouse *et al.* (2006) indicate that promotion of the ISMS may meet the regulations of government laws and ensure the rights and duties of both trading sides. Saint-Germain (2005) also agrees that promoting the ISMS may reduce corporate operation risks and reduce financial audits. Although the ISMS has the aforementioned advantages, there are still high costs and low benefit barriers to the promotion of the ISMS (Gillies, 2011). Therefore, the development of ISMS-related research has been driven in recent years and has focused on the following six fields:

(1) Information technology (Siponen and Oinas-Kukkonen, 2007);
(2) Efficiency and structure of information security execution (Hagen *et al.*, 2008; Tsohou *et al.*, 2010);
(3) Management scheme of an information security incident (Montesino *et al.*, 2012),
(4) Training and alarm scheme for information security (Stewart and Lacey, 2012; Tsohou *et al.*, 2012).
(5) Risk evaluation models and methods (Qi *et al.*, 2012; Ou Yang *et al.*, 2011).
(6) Continuous improvement of information security management (Gillies, 2011).

Because ISO 27002 is widely used for improving the control and flow of information security (Saint-Germain, 2005), Gillies (2011) utilizes 11 security control items as the key points for an organization to improve continuously. Ou Yang *et al.* (2011) also list the 11 security control items as the evaluation factors for risk control. Therefore, these 11 security control items are critical for ISMS promotion. From the aforementioned research of recent years regarding the 11 security control items in ISO 27002 Information Technology–Security Technology–Information Security Management Practice, research about the cause-and-effect relationship and the influential level applied to make decisions for improvement has not yet been performed. Therefore, this research is based on the 11 security control items in this context. The 11 security control items are listed 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; and
(11) compliance.

Information security management is a complex system with cause-and-effect relationships and mutual influences. To lower the high cost and low effectiveness barriers to the promotion of the ISMS, this research, based on the 11 security control items in ISO 27002 Information Technology–Security Technology–Information Security Management Practice, utilizes the Fuzzy decision-making trial and evaluation laboratory (DEMATEL) method to analyze the cause-and-effect relationship and the mutually influential levels, discover core security control items, provide critical information for the development of improvement strategies and achieve the goal of continuous improvement and competitiveness enhancement for organizations.

2. Literature review

DEMATEL was developed by the Battelle Memorial Institute of the Geneva Research Center to solve problems regarding racism, hunger, environmental protection, energy and so forth (Gabus and Fontela, 1973; Fontela and Gabus, 1976). Since then, many scholars have utilized the DEMATEL method to solve problems in many different fields. Hu *et al.* (2009a, 2009b) used Back-Propagation Neural Network (BPNN) and DEMATEL methods to analyze customer satisfaction regarding industrial computers. Tamura *et al.* (2006) used DEMATEL to study the factors of and improvement tactics for the unsafe feeling customers have with foods. Hajime *et al.* (2005) integrated the quality function deployment (QFD), Teoriya Resheniya Izobreatatelskikh Zadatch (TRIZ) and DEMATEL methods to resolve the design conflict in the development process of innovative products. Nanayo and Toshiaki (2002) utilized a modified DEMATEL method to provide integral evaluation for medical systems. Kenichi and Yoshihiro (2002) used DEMATEL to analyze the function and failure of snow-melting equipment. Kim (2006) integrated the principal component analysis (PCA), analytic hierarchy process (AHP) and DEMATEL methods to perform an impact evaluation of beef cattle farming and agricultural information. Hsu (2011) used factor analysis and DEMATEL to analyze the evaluation criteria of blog design and its causal relationships. Wu and Tsai (2011) utilized DEMATEL to evaluate the causal relations among the criteria in the auto spare parts industry. Jassbi *et al.* (2011) applied Fuzzy DEMATEL framework to model the cause-and-effect relationships of a strategy map. Zhou *et al.* (2011) used Fuzzy DEMATEL to identify the critical success factors in energy management. Wu (2012) used Fuzzy DEMATEL to segment critical factors for successful knowledge management implementation. Tseng (2009) applied Grey-Fuzzy DEMATEL to develop a cause-and-effect decision-making model for service quality expectations. Hu *et al.* (2011) integrated the importance-performance analysis (IPA) and DEMATEL models to improve the order-winner criteria of the network communication equipment manufacturing industry. Lee *et al.* (2010, 2011) utilized DEMATEL and Fuzzy DEMATEL separately to construct a technology acceptance model for the etching technology industry. Chang *et al.* (2011) used Fuzzy DEMATEL to analyze the importance of supplier selection. Ho *et al.* (2012) integrated multiple regression analysis and DEMATEL to modify the importance and performance analysis method for evaluating the quality performance of suppliers, etc. The DEMATEL methodology has clearly been utilized in many fields.

With the efforts of many scholars, DEMATEL methodologies in the past 10 years have been mainly directed at solving the following four problems:

(1) The cause-and-effect relationship and the influential level between variables in the system (Hsu, 2011; Jassbi *et al.*, 2011; Tseng, 2009; Wu and Lee, 2007; Wu and Tsai, 2011).

(2) Evaluating the importance of variables (Chang *et al.*, 2011; Hu *et al.*, 2011; Tzeng *et al.*, 2007).

(3) Model analysis of cause-and-effect structures (Lee *et al.*, 2010, 2011).

(4) Identifying critical factors (Wu, 2012; Zhou *et al.*, 2011).

The majority of research has concentrated on combining Fuzzy Theory to solve the problems of fuzzy linguistic terms generated by the cause-and-effect relationship and the influential level of expert opinion surveys. The reason that Gabus and Fontela (1973) developed the DEMATEL method was to acquire the optimal improvement effect with the least resource investment for a complex and difficult system by directly comparing influential relationships between variables, deriving the cause-and-effect relationship and the influential level between variables with matrix calculation, utilizing causality diagrams to express properties and types of variables in the system, simplifying relationships between variables by establishing threshold values and discovering the core problems of a complex system (Lee *et al.*, 2008a, 2008b). Therefore, this research utilizes Fuzzy DEMATEL to analyze the mutually influential levels of information security management items to discover the cause-and-effect relationship and core management factors for the direction of continuous improvement of information security management.

3. Material and methods

Li (1999) proposed that Fuzzy logic is suitable for making a group decision. The research of Hu *et al.* (2010) shows that fuzzy linguistic evaluation scale terms are better than the Likert evaluation scale. Therefore, this research utilizes the Fuzzy DEMATEL method to discuss the cause-and-effect relationship and the mutually influential level. The structure and calculation steps of Fuzzy DEMATEL applied to this research are stated below.

3.1 Developing evaluation criteria

The development of evaluation criteria may be created through brainstorming sessions of the committee or arrangement and application of relevant literature (Lee *et al.*, 2008a, 2008b; Hu *et al.*, 2009a, 2009b). The chosen expert has to have the knowledge or rich experience to solve the problem (Fekri and Aliahmadi, 2008). Nevertheless, these evaluation criteria usually have cause-and-effect relationships or a mutually influential system, and the evaluation of the influential level belongs to fuzzy linguistic terms. Therefore, the Fuzzy DEMATEL method may be utilized to solve problems.

3.2 Designing a Fuzzy linguistic scale

Li (1999) suggested that utilizing a fuzzy linguistic scale for a group decision comes closer to human evaluation and decision characteristics. The fuzzy linguistic measurement scale of the cause-and-effect relationship and the influential level comparison between variables is created after the related variables are determined. The measurement scale is divided into the following five grades, all of which are expressed with a triangular fuzzy number:

(1) they are "no influence";

(2) "very low influence";

(3) "low influence";

(4) "high influence"; and
(5) "very high influence",

The triangular fuzzy number is defined as $\tilde{z} = (l, m, u)$, where l, m and u are all real numbers, and $l \leq m \leq u$, such that the membership function of the triangular fuzzy number is expressed in equation (1):

$$\mu_z = \begin{cases} 0, & x < l \\ (x - l)/(m - l), & l \leq x \leq m \\ (u - x)/(u - m), & m \leq x \leq u \\ 0, & x > u \end{cases} \quad (1)$$

In creating the measurement scale for the cause-and-effect relationship and the influential level comparison between variables, the elements of the fuzzy set are between 0 and 1 (Zadeh, 1965). Therefore, this research refers to the recommendation of Fekri and Aliahmadi (2008) to utilize the membership function of the triangular fuzzy number and, thus, defines the fuzzy numbers as (0, 0, 0.25), (0, 0.25, 0.5), (0.25, 0.5, 0.75), (0.5, 0.75, 1) and (0.75, 1, 1) for their corresponding fuzzy linguistic terms "no influence (N)", "very low influence (VL)", "low influence (L)", "high influence (H)" and "very high influence (VH)", respectively, as shown in Table I.

3.3 Creating a fuzzy direct relationship matrix

p experts are requested to evaluate the fuzzy linguistic terms for the relationship and the influential level between n variables together. From this evaluation, the fuzzy direct relationship matrix $\widetilde{X}$ is acquired, which represents the common decision of the relationship and the influential level between n variables determined by p experts. The direct relationship matrix is represented by a triangular fuzzy number and is expressed as symbol $\widetilde{X}$, and it is given by the following equation:

$$\widetilde{X} = \begin{bmatrix} 0 & \tilde{x}_{12} & \dots & \tilde{x}_{1n} \\ \tilde{x}_{21} & 0 & \dots & \tilde{x}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{x}_{n1} & \tilde{x}_{n2} & \dots & 0 \end{bmatrix} \quad (2)$$

wherein, $\tilde{x_{ij}} = (l_{ij}, m_{ij}, u_{ij})$, and the triangular fuzzy number of the elements $x_{ii}(i = 1, 2, \dots, n)$ in the direct relationship matrix is (0,0,0). Therefore, the fuzzy matrix $\widetilde{X}$ is referred to as the fuzzy direct relationship matrix.

Fuzzy linguistic terms (linguistic terms)	Fuzzy no. (linguistic values)
Very high influence (VH)	(0.75, 1, 1)
High influence (H)	(0.5, 0.75, 1)
Low influence (L)	(0.25, 0.5, 0.75)
Very low influence (VL)	(0, 0.25, 0.5)
No influence (N)	(0, 0, 0.25)

Table I. Corresponding fuzzy linguistic terms and fuzzy numbers

3.4 Calculating normalized direct relationship fuzzy matrix $\tilde{Z}$

Next, r is defined as the maximum value of row summed triangular fuzzy numbers in the fuzzy direct relationship matrix. r is expressed by equation (3):

$$r = \max_{1 \le i \le n} \left(\sum_{j=1}^{n} u_{ij} \right) \tag{3}$$

The purpose of normalization is to convert the scale of the evaluation criteria into a comparable scale. Therefore, the normalized fuzzy direct relationship matrix $\tilde{Z}$ may be expressed as follows:

$$\tilde{Z} = \begin{bmatrix} \tilde{z}_{11} & \tilde{z}_{12} & \dots & \tilde{z}_{1n} \\ \tilde{z}_{21} & \tilde{z}_{22} & \dots & \tilde{z}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{z}_{n1} & \tilde{z}_{n2} & \dots & \tilde{z}_{nn} \end{bmatrix} \tag{4}$$

where:

$$z_{ij} = \frac{x_{ij}}{r} = \left(\frac{l_{ij}}{r}, \frac{m_{ij}}{r}, \frac{u_{ij}}{r} \right)$$

3.5 Calculating total relation fuzzy matrix $\tilde{T}$

Lin and Wu (2008) defined the total relation fuzzy matrix as: $\tilde{T} = \lim_{w \to \infty} (\tilde{Z} + \tilde{Z}^2 + \dots + \tilde{Z}^w) = \tilde{Z}(I - \tilde{Z})^{-1}$, where $w = 1, 2, 3 [\dots], \infty$.

According to the research of Laarhoven and Pedrycz (1983), if $\tilde{N}_1 = (l_1, m_1, u_1)$ and $\tilde{N}_2 = (l_2, m_2, u_2)$, then their product is approximate to $\tilde{N}_1 \otimes \tilde{N}_2 = (l_1 \times l_2, m_1 \times m_2, u_1 \times u_2)$. Therefore, assuming $z_{ij} = (l_{ij}, m_{ij}, u_{ij})$, the three matrices Z_l, Z_m and Z_u can be extracted with explicit data from the normalized direct relationship fuzzy matrix $\tilde{Z}$. These matrices are expressed in equation (5):

$$Z_l = \begin{bmatrix} 0 & l_{12} & \dots & l_{1n} \\ l_{21} & 0 & \dots & l_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n1} & l_{n2} & \dots & 0 \end{bmatrix}$$

$$Z_m = \begin{bmatrix} 0 & m_{12} & \dots & m_{1n} \\ m_{21} & 0 & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & 0 \end{bmatrix} \tag{5}$$

$$Z_u = \begin{bmatrix} 0 & u_{12} & \dots & u_{1n} \\ u_{21} & 0 & \dots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n1} & u_{n2} & \dots & 0 \end{bmatrix}$$

According to the definition of the total relation matrix with explicit data, $T = \lim_{w \to \infty} (Z + Z^2 + ... + Z^w) = Z(I - Z)^{-1}$, where $w = 1, 2, 3 [\ldots], \infty$. Then, the total relation matrices $[l''_{ij}]$, $[m''_{ij}]$ and $[u''_{ij}]$ of matrices Z_l, Z_m and Z_u are calculated and integrated to produce the fuzzy total relation matrix $\widetilde{T}$, as shown in equation (6):

$$\widetilde{T} = \begin{bmatrix} \tilde{t}_{11} & \tilde{t}_{12} & \dots & \tilde{t}_{1n} \\ \tilde{t}_{21} & \tilde{t}_{22} & \dots & \tilde{t}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{t}_{n1} & \tilde{t}_{n2} & \dots & \tilde{t}_{nn} \end{bmatrix}; \text{where } \tilde{t}_{ij} = (l''_{ij}, m''_{ij}, u''_{ij}) \tag{6}$$

and matrices $[l''_{ij}] = X_l \times (I - X_l)^{-1}$, $[m''_{ij}] = X_m \times (I - X_m)^{-1}$, and $[u''_{ij}] = X_u \times (I - X_u)^{-1}$.

3.6 Calculating the prominence and the relation of defuzzification

First, we calculate the defuzzified total relation matrix, the row sum of influential levels $\widetilde{D}_i$ and the row sum of the influenced levels $\widetilde{R}_j$. Then, we calculate the prominence $(\widetilde{D}_i + \widetilde{R}_j)$ and the relation $(\widetilde{D}_i - \widetilde{R}_j)$, where $i = j = 1, 2, \ldots, n$. This study utilizes the defuzzification method proposed by Opricovic and Tzeng (2003). The advantage of their method is that it uses a larger membership function to give larger explicit values, in addition to utilizing the same average number to separate two symmetrical triangular fuzzy numbers. Assuming $\tilde{t}_{ij} = (l''_{ij}, m''_{ij}, u''_{ij})$ is a regular triangular fuzzy number and t^{def}_{ij} is the corresponding value after defuzzification, we first calculate $L = \min(Z_l)$ and $R = \max(Z_u)$ and then $\Delta = R - L$; the defuzzification is shown by equation (7):

$$\tilde{t}^{def}_{ij} = L + \Delta \times \frac{(m_{ij} - L)(\Delta + u_{ij} - m_{ij})^2(R - l_{ij}) + (u_{ij} - L)^2(\Delta + m_{ij} - l_{ij})^2}{(\Delta + m_{ij} - l_{ij})(\Delta + u_{ij} - m_{ij})^2(R - l_{ij}) + (u_{ij} - L)(\Delta + m_{ij} - l_{ij})^2(\Delta + u_{ij} - m_{ij})} \tag{7}$$

Equation (7) is used to calculate the prominence $(\widetilde{D}_i + \widetilde{R}_j)$ and the fuzzy relation $(\widetilde{D}_i - \widetilde{R}_j)^{def}$ after defuzzification and to create the cause-and-effect matrix or the systematic diagram according to those results for analysis. As $(\widetilde{D}_i - \widetilde{R}_j)^{def}$ is positive and the values in $(\widetilde{D}_i + \widetilde{R}_j)$ are very large, the variable i $(i = j)$ is the driving factor to solve core problems and may be listed as the object for the first process. Additionally, the influence relationship of core variables may be determined through the systematic diagram to determine the decision of preferential order with respect to improvement. However, prior to analysis, the variables with less influence should have a threshold value established to delete insignificant factors to simplify the analysis (Ho *et al.*, 2012; Lee *et al.*, 2010, 2011). The advantage of a systematic diagram is that the decision-maker can discover the core variables that influence the complex system according to the cause-and-effect relationship and the mutually influential levels of variables so that the organization can achieve its goal of continuous improvement and competitiveness enhancement (Hu *et al.*, 2009a, 2009b; Lee *et al.*, 2008a, 2008b).

4. Results and discussion

Lee *et al.* (2011) demonstrated that the consensus approach can efficiently and effectively develop the mutual influences and relationships between variables by Fuzzy DEMATEL. The design of this study is based on the 11 security control items in the ISO 27001 ISMS Annex and the ISO 27002 Information Technology–Security Technology–Information Security Management Practice as variables, which are discussed by seven experts, including three high-level supervisors of information security tasks in Taiwan, three scholars in the information security field and one lead assessor of the ISO 27001 ISMS. Because the information security control items do not have a negative influential relationship, the positive fuzzy direct relationship matrix of the 11 security control items can be developed.

This study analyzes the control items of information security to understand their cause-and-effect relationship by utilizing Fuzzy DEMATEL. The fuzzy direct relationship matrix $\widetilde{X}$ derived from equation (2) according to the results discussed by the seven experts is as shown in Table II. The r value derived from equation (3) is 7.25. Then, the total relation matrices $[l_{ij}^{''}]$, $[m_{ij}^{''}]$ and $[u_{ij}^{''}]$ derived from equations (4)-(6) are as shown in Tables III-V. The fuzzy total relation matrix $\widetilde{T}$ is the integration result. $L = 0.0000$, $R = 0.3519$ and $\Delta = 0.3519$ are seen in Table III-V, respectively. Then, the prominence $(\widetilde{D}_i + \widetilde{R}_j)$ and the relation $(\widetilde{D}_i - \widetilde{R}_j)$ of defuzzification are derived from equation (7), as shown in Table VI.

The prominence and the relation have sums divided by the 11 information security control items and averaged to result in 0.6754 and 0.0000, respectively. These values can be used to divide the causal-effect diagram into the four quadrants, as shown in Figure 1. According to the analysis in Figure 1, the information security control items with the highest prominence and relation include security policy (SC1), human resources security (SC4) and access control (SC7), which are core items in the system, while those with high prominence but low relation include business continuity management (SC10) and compliance (SC11), which may also be influenced by other factors; those with high relation but low prominence include organizing information security (SC2) and information system acquisition, development and maintenance (SC8), which may also be influenced by other factors; other information security control items may be regarded as independent due to the small influence of the cause-and-effect relationship because both prominence and relation are lower than the averages of 1.637 and 0.000, respectively.

Because the influential relationships between information security control items are complex, this research considers the influential levels of the cause-and-effect relationship that are smaller than 0.0610 as having no influence to simplify the residual 20 per cent cause-and-effect relationships in the system, as well as to provide a decision norm for organizations when the continuous improvement is implemented (Ho *et al.*, 2012; Lee *et al.*, 2010, 2011). The influential cause-and-effect coefficients and the systematic diagram after the research establishes the 0.0610 threshold value are shown in Table VII and Figure 2.

According to Table VII and Figure 2, the research shows that an organization should actively invest resources in three core control items, while concurrently driving the

Table II.
Fuzzy direct
relationship matrix

$\tilde{X}$	SC1	SC2	SC3	SC4	SC5	SC6	SC7	SC8	SC9	SC10	SC11
SC1	(0, 0, 0)	(0.5, 0.75, 1)	(0.5, 0.75, 1)	(0.75, 1, 1)	(0.25, 0.5, 0.75)	(0.25, 0.5, 0.75)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.5, 0.75, 1)	(0.5, 0.75, 1)
SC2	(0, 0, 0.25)	(0, 0, 0)	(0.25, 0.5, 0.75)	(0, 0, 0.25)	(0.25, 0.5, 0.75)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.25, 0.5, 0.75)	(0, 0, 0.25)	(0, 0, 0.25)
SC3	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0)	(0, 0, 0.25)	(0.5, 0.75, 1)	(0, 0, 0.25)	(0, 0, 0.25)	(0.25, 0.5, 0.75)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)
SC4	(0.25, 0.5, 0.75)	(0.25, 0.5, 0.75)	(0, 0, 0.25)	(0, 0, 0)	(0, 0, 0.25)	(0.5, 0.75, 1)	(0.5, 0.75, 1)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.5, 0.75, 1)
SC5	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.5, 0.75, 1)	(0, 0, 0.25)	(0.25, 0.5, 0.75)
SC6	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.5, 0.75, 1)	(0.5, 0.75, 1)
SC7	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.5, 0.75, 1)	(0, 0, 0.25)	(0.25, 0.5, 0.75)	(0, 0, 0)	(0, 0, 0.25)	(0.5, 0.75, 1)	(0.25, 0.5, 0.75)	(0.5, 0.75, 1)
SC8	(0, 0, 0.25)	(0, 0, 0.25)	(0.25, 0.5, 0.75)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.25, 0.5, 0.75)	(0, 0, 0)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)
SC9	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.25, 0.5, 0.75)	(0.25, 0.5, 0.75)	(0, 0, 0.25)	(0, 0, 0)	(0, 0, 0.25)	(0, 0, 0.25)
SC10	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0)	(0.5, 0.75, 1)
SC11	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0, 0, 0.25)	(0.5, 0.75, 1)	(0, 0, 0.25)	(0.25, 0.5, 0.75)	(0.5, 0.75, 1)	(0, 0, 0)

Table III.
[l''_{ij}] Total relation matrix

l''_{ij}	SC1	SC2	SC3	SC4	SC5	SC6	SC7	SC8	SC9	SC10	SC11
SC1	0.0005	0.0175	0.0174	0.0262	0.0091	0.0091	0.0008	0.0002	0.0005	0.0177	0.0183
SC2	0.0000	0.0000	0.0086	0.0000	0.0088	0.0001	0.0001	0.0001	0.0088	0.0000	0.0001
SC3	0.0000	0.0000	0.0001	0.0000	0.0172	0.0000	0.0001	0.0086	0.0003	0.0000	0.0002
SC4	0.0086	0.0088	0.0002	0.0005	0.0002	0.0175	0.0176	0.0000	0.0005	0.0009	0.0180
SC5	0.0000	0.0000	0.0000	0.0000	0.0000	0.0002	0.0003	0.0000	0.0173	0.0002	0.0086
SC6	0.0003	0.0000	0.0000	0.0003	0.0000	0.0000	0.0003	0.0000	0.0002	0.0176	0.0176
SC7	0.0003	0.0002	0.0000	0.0174	0.0000	0.0091	0.0008	0.0000	0.0174	0.0091	0.0179
SC8	0.0000	0.0000	0.0086	0.0002	0.0001	0.0001	0.0086	0.0001	0.0002	0.0001	0.0002
SC9	0.0000	0.0000	0.0000	0.0002	0.0000	0.0087	0.0086	0.0000	0.0002	0.0002	0.0003
SC10	0.0174	0.0005	0.0003	0.0177	0.0002	0.0005	0.0006	0.0000	0.0002	0.0006	0.0179
SC11	0.0003	0.0000	0.0000	0.0006	0.0000	0.0002	0.0173	0.0000	0.0089	0.0174	0.0006

Table IV.
[m''_{ij}] Total relation matrix

m''_{ij}	SC1	SC2	SC3	SC4	SC5	SC6	SC7	SC8	SC9	SC10	SC11
SC1	0.0013	0.0265	0.0264	0.0353	0.0184	0.0182	0.0017	0.0005	0.0015	0.0271	0.0283
SC2	0.0000	0.0000	0.0172	0.0000	0.0177	0.0003	0.0003	0.0003	0.0177	0.0000	0.0003
SC3	0.0000	0.0000	0.0003	0.0000	0.0259	0.0000	0.0003	0.0172	0.0007	0.0000	0.0005
SC4	0.0173	0.0177	0.0008	0.0013	0.0006	0.0267	0.0266	0.0000	0.0015	0.0023	0.0278
SC5	0.0000	0.0000	0.0000	0.0000	0.0000	0.0005	0.0009	0.0000	0.0262	0.0005	0.0173
SC6	0.0007	0.0000	0.0000	0.0007	0.0000	0.0001	0.0007	0.0000	0.0005	0.0266	0.0266
SC7	0.0009	0.0005	0.0000	0.0264	0.0000	0.0184	0.0019	0.0000	0.0264	0.0185	0.0276
SC8	0.0000	0.0000	0.0172	0.0005	0.0004	0.0003	0.0173	0.0003	0.0005	0.0003	0.0005
SC9	0.0000	0.0000	0.0000	0.0005	0.0000	0.0176	0.0173	0.0000	0.0005	0.0008	0.0009
SC10	0.0264	0.0011	0.0007	0.0268	0.0005	0.0012	0.0014	0.0000	0.0005	0.0014	0.0274
SC11	0.0007	0.0000	0.0000	0.0014	0.0000	0.0008	0.0262	0.0000	0.0179	0.0264	0.0014

Table V.
[u''_{ij}] Total relation matrix

u''_{ij}	SC1	SC2	SC3	SC4	SC5	SC6	SC7	SC8	SC9	SC10	SC11
SC1	0.1254	0.2508	0.2584	0.2735	0.2376	0.2497	0.2054	0.1373	0.2045	0.3064	0.3519
SC2	0.0964	0.0643	0.1673	0.1111	0.1747	0.1193	0.1256	0.0917	0.1916	0.1255	0.1500
SC3	0.0932	0.0945	0.0702	0.1076	0.1975	0.1115	0.1218	0.1493	0.1260	0.1212	0.1467
SC4	0.1949	0.2009	0.1465	0.1327	0.1470	0.2625	0.2713	0.1157	0.1826	0.2020	0.3221
SC5	0.0946	0.0955	0.1002	0.1099	0.0680	0.1193	0.1308	0.0854	0.2188	0.1296	0.2083
SC6	0.1068	0.1017	0.1063	0.1229	0.1073	0.0867	0.1357	0.0899	0.1312	0.2371	0.2589
SC7	0.1369	0.1340	0.1338	0.2492	0.1352	0.2320	0.1517	0.1126	0.2623	0.2488	0.3146
SC8	0.0929	0.0939	0.1629	0.1128	0.1058	0.1148	0.1815	0.0546	0.1219	0.1246	0.1468
SC9	0.0938	0.0944	0.0987	0.1139	0.0998	0.1798	0.1824	0.0840	0.0889	0.1324	0.1543
SC10	0.1771	0.1198	0.1212	0.1969	0.1209	0.1401	0.1523	0.0971	0.1427	0.1251	0.2762
SC11	0.1152	0.1103	0.1148	0.1413	0.1159	0.1411	0.2391	0.0971	0.2091	0.2462	0.1521

improvement of other information security control items. The following three are the priority of security control items:

(1) The improvement of organizing information security (SC2), asset management (SC3), human resources security (SC4), business continuity management (SC10) and compliance (SC11) may be positively influenced if

Table VI. Prominence and relation coefficients of defuzzification

Notation	Information security control items	D	R	D+R	D−R
SC1	Security policy	0.6034	0.2427	0.8461	0.3607
SC2	Organizing information security	0.2670	0.2470	0.5139	0.0200
SC3	Asset management	0.2432	0.2859	0.5291	−0.0427
SC4	Human resources security	0.4719	0.3488	0.8207	0.1231
SC5	Physical and environmental security	0.2472	0.2929	0.5401	−0.0458
SC6	Communications and operations management	0.2796	0.3579	0.6375	−0.0783
SC7	Access control	0.4565	0.3960	0.8525	0.0604
SC8	Information system acquisition, development and maintenance	0.2317	0.1752	0.4069	0.0565
SC9	Information security incident management	0.2332	0.3919	0.6250	−0.1587
SC10	Business continuity management	0.3447	0.4209	0.7657	−0.0762
SC11	Compliance	0.3362	0.5552	0.8914	−0.2190

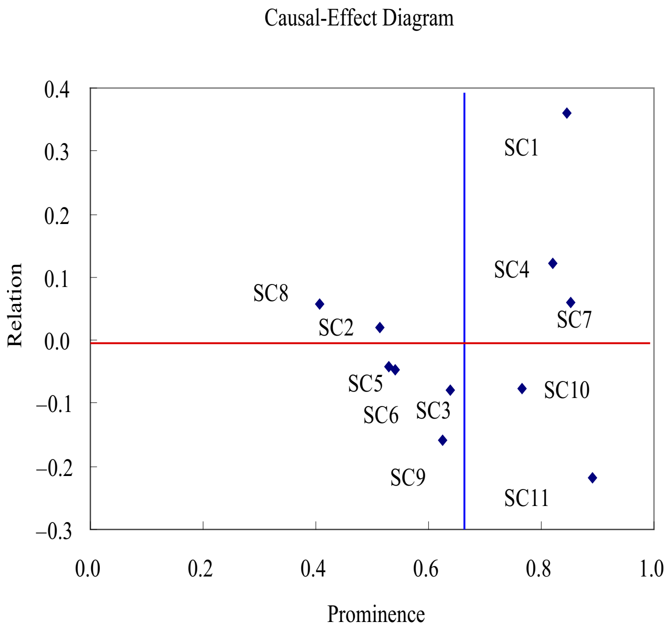

Figure 1. Cause and effect of information security control items

the organization improves the indication and support of the management level for the information security in terms of operation request and law regulations with respect to the security policy (SC1) of information. The research results of Ou Yang *et al.* (2011) show that the security policy (SC1) of information is the core item that influences the above five control items with respect to organizational management when an organization drives information security management. The research of Kraemer *et al.* (2009) shows nine factors of personnel and organization that will result in weak information security, in which the lack of policy commitment and high-level manager support is the driving factor that results in weak information security. As the budget is lacking, the resource investment will be reduced; thus, technology cannot be upgraded, personnel training will be reduced and so forth.

(2) For human resources security (SC4), an organization drives employees, contractors and third-party users to understand their duties and assume responsibilities for their recognized roles to reduce the risks of stealing, deception and misuse, such that the improvement of communications and operations management (SC6), access control (SC7) and compliance (SC11) may be positively influenced. The research results of Asai and Fernando (2011), Ashenden (2008), Colwill (2009) and Treck (2006) all indicate that human resources play a critical role on information security management. If human resources security is not managed, problems can occur regarding

Table VII. Influential cause-and-effect coefficients with a 0.0610 threshold value

Matrix	SC1	SC2	SC3	SC4	SC5	SC6	SC7	SC8	SC9	SC10	SC11
SC1		0.0665	0.0677	0.0781						0.0761	0.0838
SC2											
SC3											
SC4						0.0687	0.0701				0.0791
SC5											
SC6										0.0642	0.0680
SC7				0.0662					0.0684		0.0777
SC8											
SC9											
SC10											0.0715
SC11							0.0643			0.0656	

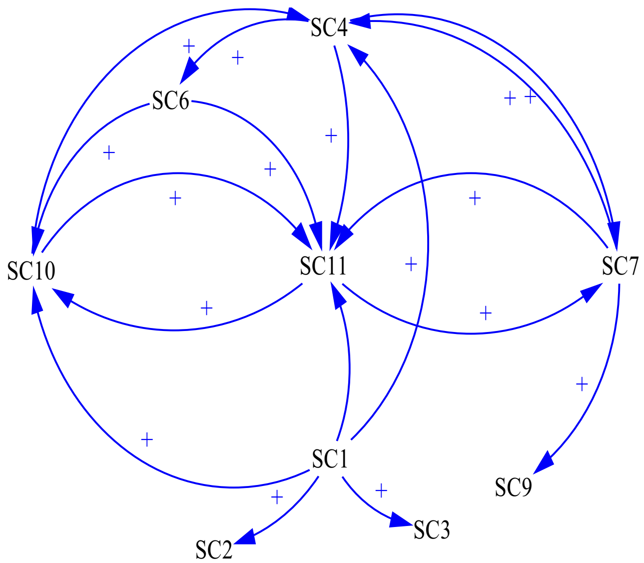

Figure 2. Systematic diagram of information security control items

employees using confidential information of previous companies, unintentionally opening confidential information, sharing corporate information with friends and not having interest in or not paying attention to information security management and undertaken duties, etc. These issues comply with the results of this research.

(3) An organization can perform access control (SC7) tasks strictly to positively influence the improvement of human resources security (SC4), business continuity management (SC10) and compliance (SC11). The research of Ma *et al.* (2008) shows that confidence, authority, responsibility and ethics are the management focuses for a highly sensitive information organization, with the most important information security control items coming from access control (SC7). The research of Chang and Lin (2007) shows that an organization has a strong and effective influence on information security management if it is control-oriented. This finding complies with the results of this research as well.

Furthermore, according to the research of Ou Yang *et al.* (2011) regarding the utilization of DEMATEL on information security risk management analysis in Taiwan, although the information security control items are divided into two groups, organizational management and operation technology, and the consensuses of 13 experts are less than 5 per cent, for respective analyses, there are still six items that comply with the results of the research, including security policy (SC1), asset management (SC3), access control (SC7), information system acquisition, development and maintenance (SC8), business continuity management (SC10) and compliance (SC11), while the other six items have minor differences in causality and relation. In summary, the result of this research is highly reliable and may be used as the decision norm for information security promotion and continuous improvement.

The 11 information security control items play an important role when implementing the ISMS. The results of this study assist organizations to understand the complexity of cause-and-effect relation and mutual influence of the 11 information security control items. The management implications of the results are that the organizations can effectively dedicate resources to core control items, such that other control items are driven toward positive change with low cost and high benefit, and that the organizations can easily get competitive advantages by adopting the improvement strategies on enhancing these three core control items.

5. Conclusions

This study applies and utilizes Fuzzy DEMATEL to improve the process for analyzing and making decisions, as well as to determine the core control items, including security policy (SC1), human resources security (SC4) and access control (SC7), on which an organization should concentrate its resources to improve their capabilities, as well as to synchronously drive the improvement of other information security control items.

In the past, research on the ISMS has focused mainly on information technology, risk analysis and managerial schemes without establishing studies regarding solving the high cost and low benefit barrier for ISMS promotion, as well as the cause-and-effect relationship and the mutual influence of information security control items. The value of this study is for an organization to effectively dedicate resources to core control items, such that other control items are driven toward positive change by utilizing Fuzzy DEMATEL to analyze the cause-and-effect relation and mutually influential level between information security control items, as well as determining the core control items through a cause-and-effect matrix and systematic diagram. Therefore, this study provides an organization with accurate and effective decision information to lower the ISMS promotion barrier with respect to high cost and low benefit, such that the goal of the organization regarding continuous improvement and competitiveness enhancement is achieved.

The limitations of this study are that the adopted expert group decision technology belongs to consensus decision, which may be influenced by individual personalities. Moreover, the study is limited to the conclusion acquired from ISMS promotion experiences in Taiwan. For future research, international expert groups and Delphi decision technology may be adopted to acquire more general research results. Another valuable topic that should be mentioned for future research is how does the risk assessment and management influence on the 11 information security control items when conducting ISO 27001?

References

Asai, T. and Fernando, S. (2011), “Human-related problems in information security in Thai cross-cultural environments”, *Contemporary Management Research*, Vol. 7 No. 2, pp. 117-142.

Ashenden, D. (2008), “Information security management: a human challenge?”, *Information Security Technical Report*, Vol. 13, pp. 195-201.

Backhouse, J., Hsu, C.W. and Silva, L. (2006), “Circuits of power in creating de jure standards: shaping an international information systems security standard”, *MIS Quarterly*, Vol. 30, pp. 413-438.

Chang, B., Chang, C.W. and Wu, C.H. (2011), “Fuzzy DEMATEL method for developing supplier selection criteria”, *Expert Systems with Applications*, Vol. 38 No. 3, pp. 1850-1858.

Chang, S.E. and Lin, C.S. (2007), “Exploring organizational culture for information security management”, *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438-458.

Colwill, C. (2009), “Human factors in information security: the insider threat-Who can you trust these days?”, *Information Security Technical Report*, Vol. 14, pp. 186-196.

Fekri, R. and Aliahmadi, A. (2008), “Identifying the cause and effect factors of agile NPD process with fuzzy DEMATEL method: the case of Iranian companies”, *Journal of Intelligent Manufacturing*, Vol. 20 No. 6, pp. 637-648.

Fontela, E. and Gabus, A. (1976), *The DEMATEL observer, DEMATEL 1976 report’*, Battelle Geneva Research Center, Geneva.

Gabus, A. and Fontela, E. (1973), “Perceptions of the world problematique: communication procedure, communicating with those bearing collective responsibility”, DEMATEL Report No. 1, Battelle Geneva Research Center, Geneva.

Gillies, A. (2011), “Improving the quality of information security management systems with ISO 27000”, *The TQM Journal*, Vol. 23 No. 4, pp. 367-376.

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

Hajime, Y., Kenichi, I. and Hajime, M. (2005), "An innovative product development process for resolving fundamental conflicts", *Journal of the Japan Society for Precision Engineering*, Vol. 71 No. 2, pp. 216-222.

Ho, L.H., Feng, S.Y., Lee, Y.C. and Yen, T.M. (2012), "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.

Hsu, C.C. (2011), "Evaluation criteria for blog design and analysis of causal relationships using factor analysis and DEMATEL", *Expert Systems with Application*, Vol. 39 No. 1, pp. 187-193.

Hu, H.Y., Lee, Y.C. and Yen, T.M. (2009a), "Amend importance-performance analysis method with Kano's model and DEMATEL", *Journal of Applied Sciences*, Vol. 9 No. 10, pp. 1833-1846.

Hu, H.Y., Lee, Y.C., Yen, T.M. and Tsai, C.H. (2009b), "Using BPNN and DEMATEL to modify importance-performance analysis model-a study of computer industry", *Expert Systems with Applications*, Vol. 36, pp. 9969-9979.

Hu, H.Y., Lee, Y.C. and Yen, T.M. (2010), "Service quality gaps analysis based on Fuzzy linguistic SERVQUAL with a case study in hospital out-patient services", *The TQM Journal*, Vol. 22 No. 5, pp. 499-515.

Hu, H.Y., Chiu, S.I., Cheng, C.C. and Yen, T.M. (2011), "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.

Jassbi, J., Mohamadnejad, F. and Nasrollahzadeh, H. (2011), "A fuzzy DEMATEL framework for modeling cause and effect relationships of strategy map", *Expert Systems with Applications*, Vol. 38 No. 5, pp. 5967-5973.

Karabacak, B. and Sogukpinar, I. (2006), "A quantitative method for ISO 17799 gap analysis", *Computers & Security*, Vol. 25 No. 6, pp. 413-419.

Kenichi, F. and Yoshihiro, N. (2002), "Study on function and failure analysis of snow melting machines", *Transactions of the Japan Society of Mechanical Engineers*, Vol. 68, pp. 3447-3455.

Kim, Y.H. (2006), "Study on impact mechanism for beef cattle farming and importance of evaluating agricultural information in Korea using DEMATEL, PCA and AHP", *Agricultural Information Research*, Vol. 15 No. 3, pp. 267-280.

Kraemer, S., Carayon, P. and Clem, J. (2009), "Human and organizational factors in computer and information security: pathways to vulnerabilities", *Computer & Security*, Vol. 28 No. 7, pp. 509-520.

Laarhoven, P.J.M. van and Pedrycz, W. (1983), "A fuzzy extension of Saaty's priority theory", *Fuzzy Sets and Systems*, Vol. 11 Nos 1/3, pp. 199-227.

Lee, Y.C., Hu, H.Y., Yen, T.M. and Tsai, C.H. (2008a), "Kano's model and decision making trial and evaluation laboratory applied to order winners and qualifiers improvement: a study of the computer industry", *Information Technology Journal*, Vol. 7 No. 5, pp. 702-714.

Lee, Y.C., Yen, T.M. and Tsai, C.H. (2008b), "Using importance-performance analysis and decision making trial and evaluation laboratory to enhance order-winner criteria:

a study of computer industry", *Information Technology Journal*, Vol. 7 No. 3, pp. 396-408.

Lee, Y.C., Li, M.L., Yen, T.M. and Huang, T.H. (2010), "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.

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

Li, R.J. (1999), "Fuzzy method in group decision making", *Computers and Mathematics with Applications*, Vol. 38 No. 1, pp. 91-101.

Lin, C.J. and Wu, W.W. (2008), "A causal analytical method for group decision-making under fuzzy environment", *Expert Systems with Applications*, Vol. 34 No. 1, pp. 205-213.

Ma, Q., Johnston, A.C. and Pearson, J.M. (2008), "Information security management objectives and practices: a parsimonious framework", *Information Management & Computer Security*, Vol. 16 No. 3, pp. 251-270.

Montesino, R., Fenz, S. and Baluja, W. (2012), "SIEM-based framework for security controls automation", *Information Management & Computer Security*, Vol. 20 No. 4, pp. 248-263.

Nanayo, F. and Toshiaki, T. (2002), "A new method of paired comparison by improved DEMATEL method: application to the integrated evaluation of a medical information which has multiple factors", *Japan Journal of Medical Informatics*, Vol. 22 No. 2, pp. 211-216.

Opricovic, S. and Tzeng, G.H. (2003), "Defuzzification within a multicriteria decision model", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 11 No. 5, pp. 635-652.

Ou Yang, Y.P., Shieh, H.M. and Tzeng, G.H. (2011), "A VIKOR technique based on DEMATEL and ANP for information security risk control assessment", *Information Science*, Vol. 232, pp. 482-500.

Qi, L., Qingling, D., Wei, S. and Jine, Z. (2012), "Modeling of risk treatment measurement model under four clusters standards (ISO 9001, 14001, 27001, OHSAS 18001)", *Procedia Engineering*, Vol. 37, pp. 354-358.

Saint-Germain, R. (2005), "Information security management best practice based on ISO/IEC 17799", *Information Management Journal*, Vol. 39 No. 4, pp. 60-66.

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

Stewart, G. and Lacey, D. (2012), "Death by a thousand facts criticizing the technocratic approach to information security awareness", *Information Management & Computer Security*, Vol. 20 No. 1, pp. 29-38.

Tamura, H., Okanishi, H. and Akazawa, K. (2006), "Decision support for extracting and dissolving consumers' uneasiness over foods using stochastic DEMATEL", *Journal of Telecommunications and Information Technology*, Vol. 4, pp. 91-95.

Treck, D. (2006), "Using systems dynamics for human resources management in information systems security", *Kybernetes*, Vol. 35 Nos 7/8, pp. 1014-1023.

Tseng, M.L. (2009), "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.

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

Tsohou, A., Karyda, M. Kokolakis, S. and Kiountouzis, E. (2012), "Analyzing trajectories of information security awareness", *Information Technology & People*, Vol. 25 No. 3, pp. 327-352.

Tzeng, G.H., Chiang, C.H. and Li, C.W. (2007), "Evaluating intertwined effects in e-learning programs: a novel hybrid MCDM model based on factor analysis and DEMATEL", *Expert Systems with Applications*, Vol. 32 No. 4, pp. 1028-1044.

Von Solms, B. (2006), "Information security-the fourth wave", *Computers & Security*, Vol. 25 No. 3, pp. 165-168.

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

Wu, W.W. (2012), "Segmenting critical factors for successful knowledge management implementation using the fuzzy DEMATEL method", *Applied Soft Computing*, Vol. 12 No. 1, pp. 527-535.

Wu, W.W. and Lee, Y.T. (2007), "Developing global managers' competencies using fuzzy DEMATEL method", *Expert Systems with Applications*, Vol. 32 No. 4, pp. 499-507.

Zadeh, L.A. (1965), "Fuzzy sets", *Information and Control*, Vol. 8, pp. 338-353.

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

Corresponding author
Tieh-Min Yen can be contacted at: ytm1129@ms48.hinet.net