Information Sciences 232 (2013) 482–500

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A VIKOR technique based on DEMATEL and ANP for information security risk control assessment

Yu-Ping Ou Yang [a,*], How-Ming Shieh [a,b], Gwo-Hshiung Tzeng [c,d]

[a] Department of Business Administration, National Central University, 300 Chung-da Road, Chung-Li City 320, Taiwan
[b] Department of Information Management, National Central University, 300 Chung-da Road, Chung-Li City 320, Taiwan
[c] Department of Information Management, Kainan University, No. 1, Kainan Road, Luchu, Taoyuan 338, Taiwan
[d] Institute of Management of Technology, National Chiao Tung University, 1001 Ta-Hsueh Road, Hsinchu 300, Taiwan

ARTICLE INFO

Article history:
Available online 17 September 2011

Keywords:
VIKOR
Analytic network process (ANP)
DEMATEL
Multiple criteria decision making (MCDM)
Information security
Risk control assessment

ABSTRACT

As companies and organizations have grown to rely on their computer systems and networks, the issue of information security management has become more significant. To maintain their competitiveness, enterprises should safeguard their information and try to eliminate the risk of information being compromised or reduce this risk to an acceptable level. This paper proposes an information security risk-control assessment model that could improve information security for these companies and organizations. We propose an MCDM model combining VIKOR, DEMATEL, and ANP to solve the problem of conflicting criteria that show dependence and feedback. In addition, an empirical application of evaluating the risk controls is used to illustrate the proposed method. The results show that our proposed method can be effective in helping IT managers validate the effectiveness of their risk controls.

1. Introduction

In an era of computers and computer networks, corporations and public organizations have implemented computerization: (i) to reduce labor costs, materials, and financial investment; and (ii) to achieve convenient and effective services. But with the development of computers and computer-networks, the threat of information security incidents that could jeopardize the information held by organizations is becoming increasingly serious; such incidents may even be serious enough to cause the failure of enterprises. To maintain their competitiveness, enterprises should safeguard their information system and try to eliminate the risk of being compromised or to reduce this risk to an acceptable level. There are many studies that deal with methods of information security risk assessment and ways of achieving risk controls. However, few studies calculate the integrated risks or assess the performance of the implemented controls after taking into account the dependence among criteria. Because information-risk factors are usually dependent on each other, it is not advisable to use traditional assessment methods where the assessment factors or criteria are assumed to be independent. Therefore, this study proposes an information security risk-control assessment model (ISRCAM) that combines the *VlseKriterijumska Optimizacija I Kompromisno Resenje technique* (in Serbian, which means Multicriteria Optimization and Compromise Solution), also known as VIKOR, the decision-making trial and evaluation laboratory (DEMATEL), and the analytic network process (ANP) to solve the problem. We hope to use this hybrid MCDM method to accurately model the interdependent risk factors and improve information security. Finally, an empirical example for information security risk control is presented to illustrate our proposed method.

[*] Corresponding author.
E-mail addresses: ouyang.ping@msa.hinet.net (Y.-P. Ou Yang), ghtzeng@mail.knu.edu.tw, ghtzeng@cc.nctu.edu.tw (G.-H. Tzeng).

0020-0255/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2011.09.012

Multiple criteria decision-making (MCDM) methods are often used to deal with problems in management that are characterized by several non-commensurable and conflicting (competing) criteria, and there may be no solution that satisfies all criteria simultaneously. Risk-related assessment often uses MCDM to deal with problems having multiple and conflicting objectives. Liu et al. [19] stated: "Multicriteria-analysis techniques could help decision-makers evaluate risks and countermeasures (controls) when conflicting criteria must be considered and balanced". Thus, MCDM methods can provide IT (information technology) managers with systematic and repeatable methods for evaluating information-security-risk-related problems. Since understanding the performance gaps of the implemented controls to an assumed ideal performance level is important for assessing the effectiveness of the various risk controls, compromise-programming methods can be used to rank the risk-control areas or objectives. Among the MCDM methods, VIKOR and TOPSIS procedures are based on an aggregating function representing "closeness to the ideal". Furthermore, they use the compromise-programming method to rank and improve alternatives. The TOPSIS method was first developed by Hwang and Yoon [10] based on the concept that the chosen alternative should: (a) have the shortest distance from the ideal solution and (b) be the farthest from the negative-ideal solution, using Euclidean distance [10]. However, Opricovic and Tzeng [28] showed that TOPSIS has several shortcomings in its ranking process. Therefore, their study proposed an alternative VIKOR method to replace TOPSIS [27,28]. This research also uses the VIKOR method to rank the risk-control areas and risk values.

The VIKOR method was developed by Opricovic [26]. Development of the VIKOR method began when Yu [45] proved the L_p-*metric* for a distance function. The VIKOR method introduced the multicriteria ranking index based on a particular measure of "closeness to the ideal/aspired level" and was introduced as an applicable technique within MCDM [26]. This method focuses on the ranking of a set of choices in the presence of conflicting criteria, which helps decision-makers select the "best" compromise choice [27]. The VIKOR method was developed as an MCDM method to solve discrete decision problems with non-commensurable and conflicting criteria [40,41,27–29,31]. However, few papers discuss conflicting (competing) criteria with dependence and feedback using this compromise solution method. Therefore, we developed the VIKOR method based on the ANP and DEMATEL methods to solve the problem of conflicting criteria with dependence and feedback [30]. In addition, using the methods can help us rank the gaps for the risk-control objectives/areas. However, the VIKOR method ranks and selects alternatives based on all the established criteria. Namely, it uses the same criteria to assess each alternative; thus, using traditional VIKOR to rank their orders is unsuitable when each control clause/aspect of information-security risk has its own criteria (different criteria or objectives). Furthermore, because, in practice, each enterprise or government agency has different information-security risk controls, direct comparison is also not possible. Hence, this research adopts an improved VIKOR method, called VIKORRUG—VIKOR for Ranking Unimproved Gap [31]—for ranking the information-security-risk-control objectives and control areas.

ANP was proposed by Saaty as a new MCDM method to overcome the problems of interdependence and feedback among criteria and alternatives in the real world [34]. ANP is an extension of AHP based on the concepts of Markov Chain, and it is a nonlinear dynamic structure [35]. ANP is the general form of AHP [36] and has been used in MCDM to relax the restriction on hierarchical structure. ANP has been applied successfully in many practical decision-making problems [15,17,21,22,39,46]. Furthermore, a hybrid model combining ANP and DEMATEL to solve the dependence and feedback problems has been successfully used in various fields [8,18,42]. When dealing with ANP, we found that using the traditional method of normalizing the unweighted supermatrix is not reasonable. In the traditional method, each criterion in a column is divided by the number of clusters so that each column adds up to unity. Using this normalization method implies that each cluster has the same weight. However, there are different degrees of influence among the clusters of factors/criteria in the real world. Thus, the assumption of equal weights for each cluster to obtain the weighted supermatrix is unrealistic and needs to be improved [32]. Thus, this study uses the results from DEMATEL to improve the normalization process in ANP. Thus DEMATEL [3,4,6,7,44] is used not only to construct the interrelations between factors/criteria in building an NRM (network relations map) but also to improve the normalization process of ANP.

In conclusion, the contribution of this study is to propose an ISRCAM model for criteria with interdependence and feedback to assess the performance of the risk controls of an information system. The results will help IT managers of businesses or government agencies to understand the control areas or control objectives that should be enhanced to conform to the aspired levels or needs. In addition, by using DEMATEL to generate an NRM, the proposed method can help IT managers analyze the reasons behind why some controls having larger gaps and needs to be improved. Furthermore, we use an empirical example of an enterprise information-security controls assessment to show the steps of a novel MCDM that combine VIKOR, DEMATEL, and ANP [30] to solve the problem of conflicting criteria with dependence and feedback. Our results show that this proposed method helps us deal with conflicting problems of criteria with interdependence and feedback and improves the normalization of the supermatrix to reflect reality.

The rest of this paper is organized as follows. In Section 2, the research framework is proposed. In Section 3, the hybrid MCDM model is described. In Section 4, a numerical example with applications is illustrated to show the proposed methods in real case. Discussions and conclusions are presented in Sections 5 and 6, respectively.

2. Research framework

The risk management process model [1] includes four steps: (1) risk assessment; (2) risk remediation; (3) risk monitoring and review; and (4) risk management enhancement. The first step involves identifying and analyzing the vulnerability of