Available online at www.sciencedirect.com

SCIENCE DIRECT®

Information & Management 41 (2003) 149–158

INFORMATION & MANAGEMENT

www.elsevier.com/locate/dsw

The IS risk analysis based on a business model

Bomil Suh*, Ingoo Han

Graduate School of Management, Korea Advanced Institute of Science and Technology,
207-43 Cheongryangri-Dong, Dongdaemun-Gu, Seoul 130-012, South Korea

Accepted 26 December 2002

Abstract

The disruption of operations due to IS failure becomes more important as IS has become an increasingly essential component of the organization's operations and can affect its strategic objectives. Nevertheless, traditional IS risk analysis methods do not adequately reflect the loss from disruption of operations in determining the value of IS assets. Quantitative methods do not measure the loss from disruption of operations. Qualitative methods consider the loss, but their results are subjective and not suitable for cost-benefit decision support. There is a lack of systematic methods to measure the value of IS assets from the viewpoint of operational continuity.

This study presents an IS risk analysis method based on a business model. The method uses a systematic quantitative approach dealing with operational continuity: the importance of various business functions and the necessity level of various assets are first determined. The value of each asset is then determined based on these two levels.

The proposed method adds the first stage, organizational investigation, to traditional risk analysis. The process of the method utilizes various methodologies such as paired comparison, asset–function assignment tables, and asset dependency diagrams.
© 2003 Elsevier Science B.V. All rights reserved.

Keywords: Risk analysis; Asset valuation; Business model; Analytic Hierarchy Process (AHP); Asset–function assignment; Paired comparison

1. Introduction

IS was introduced to the business as a means of improving operational efficiency. It was then treated only as a tool for performing an organization's operations. Now, it is, however, an essential component of an organization's survival. Almost no operations of an organization can be performed without IS. Organizations have become so dependent on IS that even a relatively short loss of the availability of a critical system can lead to a total failure of the business. The emergence of e-business accelerates this trend. IS managers, therefore, have to place an emphasis on the IS risk analysis and management.

The disruption of operations can also become more important than the replacement of IS assets. The support of the operation is a major part of risk analysis. So, IS assets should be valued from the viewpoint of operational continuity in addition to their replacement costs.

Traditional IS risk analysis methods cannot adequately reflect the loss due to disruption of operations. Quantitative risk analysis methods measure the value based on its replacement cost. Due to the measurement

* Corresponding author. Present address: Entrue Consulting Partners, 25F, Seoul Finance Center, 84, Taepyungro 1-ga, Chung-gu, Seoul 100-768, South Korea. Tel.: +82-2-3783-0400; fax: +82-2-3783-0333.
E-mail addresses: bmsuh@kgsm.kaist.ac.kr (B. Suh), ighan@kgsm.kaist.ac.kr (I. Han).

0378-7206/$ – see front matter © 2003 Elsevier Science B.V. All rights reserved.
doi:10.1016/S0378-7206(03)00044-2

difficulty, such methods do not measure the loss from the disruption of operations. One of the disadvantages of these methods, the inappropriateness of monetary asset value, is due to the difficulty in measuring the costs. Qualitative risk analysis methods determine loss based on the knowledge and judgment of a risk analyst rather than on precise monetary values. This results in a lack of cost-benefit decision-making and the subjective results.

IS risk analysis requires the identification of mission critical assets, the potential threats that might undermine the mission capability, and the consequences of loss of mission critical assets [10]. To meet these requirements, this study presents an IS risk analysis method based on a business model.

2. IS risk analysis

2.1. Overview

The purpose of risk management is to minimize the expected loss. It is a systematic process. Risk analysis is the basis on which risk management decisions are made. The process has three stages [5,16]:

- asset identification and valuation;
- identification and assessment of threat and vulnerability;
- risk identification and valuation.

The IS assets include hardware, software, data/database, personnel, documentation, and facilities. The hardware, software, and various facilities are tangible while the others are intangible. The boundary of the risk analysis should be established during the asset identification stage to determine the protection priority of each asset. Then, the overall worth of the identified assets can be assessed. The values of hardware and facilities are the replacement costs minus the insurance coverage in traditional risk analysis. Also, in a relatively simple manner, the value of software is calculated as the replacement or development costs minus insurance coverage. However, the worth of the intangible assets cannot be easily determined.

The next stage is to identify all possible threats to the selected assets and their vulnerabilities. Only those threats that are likely to occur need to be identified (e.g. do not assess flood damage at the top of a mountain). Then, the vulnerability can be identified.

The final stage is the assessment of the risk to the current IS. The security profession views risk as having two attributes: injury and probability [1,2]. To measure a risk, each must be determined. *Injury* is caused by a situation that adversely affects assets, resulting in costs or limitations on an organization's ability to achieve its mission, regardless of its mitigation by safeguards. Therefore, the injury level is the loss if the threat is successful. The asset value determined in the asset valuation stage is used for the injury level [26]. *Risk probability* is the chance that a loss or harm will occur over the lifetime of an asset or within a specified period of time, for example, a year. Therefore, the risk probability is the likelihood of threat occurrences determined in the threat and vulnerability assessment stage.

2.2. Risk analysis methods

IS risk analysis methods are classified into: quantitative and qualitative. The quantitative methods develop a level of risk for each hazard. These methods normally calculate the cost of damage when a risk becomes a reality. They usually calculate annual loss expectancy (ALE) for each threat. Quantitative methods include the Courtney method, Livermore risk analysis methodology (LRAM), stochastic dominance method, ALE using program evaluation review technique (PERT), and simulation [19,21].

Qualitative methods assume that a loss cannot be expressed in monetary value or as discrete events. These methods, therefore, attempt to express the risk in terms of descriptive variables (assessment on a Likert scale from 1 to 5, for example) based on the knowledge and judgment of an analyst. They include Delphi techniques, scenario analysis, fuzzy metrics, comparison risk ranking, and the questionnaires.

Any single method cannot completely dominate any other type. Table 1 summarizes the advantages and the disadvantages of each.

2.3. Limitations of traditional risk analysis

In quantitative risk analysis methods, the value of a tangible asset is based on its replacement cost [3]. The methods do not measure the tangible asset value from