Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(6):851-855

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

A novel decision making approach for the organization information security

Hong-Xuan Hua

Department of Information Science and Engineering, Zaozhuang University, Zaozhuang, P.R. China

ABSTRACT

The implementation and organization of information safety measures is relevant to costs, so a decision model of information security risk based on expenses constraints is established. An illustrative example is presented to give out an optimal allocation plan for safety measures, which makes the risk and running cost minimum and the operating efficiency highest.

Key words: Organization, Information Safety, Risk Decision-Making

INTRODUCTION

With rapid development of information technology, the information systems have become very important assets in organizations. So hostile attacks to information systems are diversified and complicated. The large quantity, complex structure of information systems and the heterogeneity of their application make it very difficult to manage the complex organization information security risk [1]. And the core issue that their safety protection level reaches an ideal condition is the optimal allocation of security resources [2, 3]. A reasonable allocation of security resources plays an important role in complex organization information security risk management. Considering the correlations between expenses and effects of safety measures, this paper builds a decision model for information security risk.

Gordon et al. [4] studied the optimization problem of information security resources in organizations, and proposed an allocation model but did not consider the hierarchal protection for complex information systems. Alberts et al. [5] put forward an idea of hierarchal protection in security and risk management for information systems. They compared and analyzed a single safeguard and a comprehensive safeguard, but still rested on qualitative analysis. Richardson [6] investigated the hierarchal protection of large-scale information systems and deeply analyzed main problems occurring in practical application. In China, Liu Fang [7] presented the steps for safety decision-making. She proposed to select proper safety measures with consideration of purchase cost, maintenance charge and availability of security technology, and removed the influence of errors to final result by sensitivity analysis. However, it was still a qualitative analysis.

MODELLING APPROACH

The decision-making for organization information security risk is that a group of specific safety measures from alternative set is employed to reduce the risk. The organization combines the chosen safety measures, namely that making a safety program to control information security risk is also regarded as an investment behavior. The invested costs are the sum of expenses required to implement various safety measures in the safety program, while their benefits are reduction of security risk. The aim of information security investment by organizations is to make expenses and risk minimum and cost-effectiveness optimal. Meanwhile, it must ensure that the remaining information security risk is acceptable and the investment cost is affordable. Thus, the problem of making a safety program by organizations is actually a multi-objective optimization problem satisfying constraints. And the ultimate goal of safety decision-making is to find a satisfactory solution by multiple decision methods.

The symbols used in this paper are defined as follows.
M : the total sum of information assets owned by an organization;
m : the m^{th} information asset;
V_m : the value of the m^{th} information asset;
V : the value of all information assets owned by an organization, $V=\sum_{m=1}^{M}V_m$;
v_m : the vulnerability for the m^{th} asset;
S : the total number of times for all assets in an organization to be attacked within a period;
S_m : the total number of times for the m^{th} asset to be attacked;
w_m : proportion of attacks to the m^{th} asset within a period in all attacks, $\sum_{m=1}^{M}w_m=1$;
K : the kind of all safety measures;
k : the k^{th} kind of safety measure;
p_m : the defense penetration probability for the m^{th} information asset after being attacked;
$p_m(k)$: when the m^{th} information asset takes the k^{th} safety measure, its probability density of defense penetration after being attacked;
h_k : the factor affecting the protection efficiency of the k^{th} safety measure;
r_m : the new risk introduced by the m^{th} information asset after taking safety measures, indicated by the change of vulnerability of systems;
$r_m(k)$: the new risk introduced by the m^{th} information asset after taking the k^{th} safety measure, indicated by the percentage of vulnerability of systems;
e_m : the loss ratio after the m^{th} information asset is attacked, indicated by the percentage of its asset value;
a_m : the loss ratio when the m^{th} information asset does not take any safety measure;
b_{mk} : The impact factor of loss ratio and expenses after the m^{th} information asset takes the k^{th} safety measure;
R : the total risk of organization information security;
$\overline{R}$: the acceptable risk limitation for organizations;
R_m : the risk for the m^{th} information asset;
C : the total cost required for implementing safety measures;
$\overline{C}$: the expense quota for implementing safety measures;
C_{mk} : the cost required for the m^{th} information asset to implement the k^{th} safety measure, $\sum_{m=1}^{M}\sum_{k=1}^{K}C_{mk}=C$.

The complexity and multi-hierarchy of organizations determines that organization information security risk decision is a multi-objective optimization problem. And there are two optimization objectives, respectively to make the total risk *R* and total cost *C* minimum. Decision variables are expenses spent in safety measures by different information assets. And since the effects of safety measures depend on expenses, the risks of information assets also change.

There are two constraints, respectively that the organization information security risk should not exceed the risk $\overline{R}$ that the organization is willing to afford and the expenses spent in implementing safety measures on all information assets should not more than the given total cost $\overline{C}$. The decision function can be represented as:

$$\begin{cases}\min R=\sum_{m=1}^{M}R_m\\ \min C=\sum_{m=1}^{M}\sum_{k=1}^{K}C_{mk}\end{cases}\qquad s.t.\begin{cases}R\le\overline{R}\\ C\le\overline{C}\end{cases} \tag{1}$$

DECISION MAKING MODEL

The computing methods for relevant parameters in the decision model are summarized as follows.

1. Single Information Asset Risk R_m

The following factors should be considered when analyzing the information asset security risk:

(1) Asset value V_m . Here, assets belong to organizations, which are valuable information assets for attackers. If the assets are worthless, even they suffer from security threat; there is not any loss, so no risk. In information security risk assessment, there are two ways to represent the asset value, namely the absolute value and the relative value. The former refers to the actual value of assets, denoted by currency. And the latter is a range of asset value given by subjects of assessment according to the value of each asset in information systems and their importance. The absolute value of assets is adopted in this paper to make for representing risks intuitively and security risk decision-making analysis. The assessment of asset values usually employs expert evaluation.

(2) Frequency of attacks S . It means that in a given period, the frequency of information systems being attacked. The more frequently the systems are attacked, the more threatening they suffer, and more easily the loss caused.

(3) Defense penetration probability p_m . It means the probability of loss of information assets caused by attacks breaking through the protection of safety measures. The stronger the protective measures are, the lower the probability is.

(4) Loss coefficient e_m of effective attacks. Attacks that break through the protection of safety measures are called as the effective attack. And the loss coefficient is used to describe the influence or loss to some asset value by effective attacks, denoted by percentage of loss of asset value. And some safety measures can effectively reduce the loss coefficient of information assets.

(5) New risk r_m introduced after safety measures are taken. The implementation of safety measures can reduce security risks and may bring in new risks simultaneously. So when implementing some measures, it should make a comprehensive weigh.

It is obtained from above analysis that, in a given period, the quantitative formula for the safety risk of the *m*th (*m*=1,…,*M*) information asset is:

$$R_m = S_m \times V_m \times r_m \times p_m \times e_m + T_m \qquad (2)$$

In which:

1) S_m is the sum of attacks to the *m*th (*m*=1,…,*M*) information asset, and

$$S_m = S \times w_m$$

2) V_m is the value of the *m*th (*m*=1,…,*M*) information asset.

3) p_m is the defense penetration probability for the *m*th (*m*=1,…,*M*) information asset after being attacked; in chapter four, methods for forecasting information security risk probability in consideration of different safety measures are provided based on evidence network theory. The defense penetration probability for the *m*th (*m*=1,…,*M*) information asset after being attacked when the *k*th (*k*=1,…,*K*) safety measure is taken is defined as:

$$p_m(k) = v_m \times \exp(-h_k C_{mk})$$

In which, v_m is the vulnerability of the *m*th (*m*=1,…,*M*) asset; C_{mk} is the cost spent in implementing the *k*th (*k*=1,…,*K*) safety measure by the *m*th (*m*=1,…,*M*) information asset; Coefficient h_k denotes the factor affecting the protection efficiency of the *k*th (*k*=1,…,*K*) safety measure. Then the defense penetration probability for the *m*th (*m*=1,…,*M*) information asset after being attacked when all safety measures are taken is

$$p_m = v_m \times \exp(-h_1 C_{m1} - h_2 C_{m2} - \cdots - h_K C_{mK})$$

4) e_m is the loss of the *m*th (*m*=1,…,*M*) information asset after being attacked successfully, denoted by the percentage

of this asset value. In practical application, some measures can reduce the loss. And the more money invested into safety measure, the less the loss is. It can be represented as

$$e_m = a_m - \sum_{k=1}^{K} b_{mk} \times C_{mk}$$

In which, a_m denotes the loss ratio when information assets do not take any safety measure; coefficient b_{mk} denotes the impact factor of loss ratio and expenses after measures are taken. If the measures cannot reduce the loss ratio, then $b_{mk} = 0$.

5) r_m is the new risk introduced after safety measures are taken, indicated by the ratio of vulnerability of information assets,

$$r_m = \prod_{k=1}^{K} r_m\left(k\right)$$

If new risks are introduced after safety measures are taken, then $r_m\left(k\right) > 1$;

If new risks have not been introduced after safety measures are taken, then $r_m\left(k\right) = 1$.

6) T_m is the risk of information assets when considering the transmissibility of attacks

In an organization environment, all information systems are interconnected. Since after the m^{th} (m=1,…,M) information asset is attacked effectively, its correlative ones will also be attacked, its risks should not only consider the loss suffered from attacks to the asset itself, but also the losses caused by transmissibility of attacks.

If the transmissibility of attacks is considered and the effective attack only transmits once, then the risk brought to other assets by the m^{th} (m=1,…,M) information asset after being attacked effectively in a period is

$$T_m = S_m \times p_m \times \sum_{k=1,k\neq m}^{M} \left(\frac{w_k}{\sum_{i=1,i\neq m}^{M} w_i} \times V_k \times p_k \times r_k \times e_k \right)$$

2. Organization information asset risk R

The risk of the m^{th} information asset can be obtained from formula (2). It is the sum of all information asset risks

$$R = \sum_{m=1}^{M} R_m \tag{3}$$

3. Cost spent in implementing safety measures C

In order to control the information security risk, an organization needs to take various safety measures. Its cost is the sum of expenses spent in implementing different safety measures on each information asset

$$C = \sum_{m=1}^{M} \sum_{k=1}^{K} C_{mk} \tag{4}$$

CONCLUSION

Specific to the characteristics of organization information security risk micro-management, this chapter employed a quantitative method to model the risk decision, so as to meet the demand for organizations' precise management in micro level. Firstly, the features of safety measures and their selection strategies were analyzed; then considering the relationship between costs and information security measures, the decision model based on expense constraint was established and an approach based on the feedback genetic algorithm was presented.

REFERENCES

[1] OY Adisa, *Construction Management and Ec.*, **2010**, 28(5), 509-526
[2] JS Shane, *J. MANAGE. ENG*., **2009**, 25(4), 221-229
[3] Xing LN, Chen YW and Yang KW, *Appl Soft Comput*, **2010**, 10(3): 888-896
[4] ReVelle CS, Eiselt HA, *Eur J Oper Res*, **2008**, 184: 817-848
[5] Xing LN, Yang KW, Chen YW, *Eur J Oper Res*, **2009**, 197(2): 830-833
[6] Ma WJ, Jiao BQ, *Res J Chem Environ*, **2012**, 16(S1): 137-139
[7] Lin C; Hu J; Kong XZ, *Chinese Journa*., **2012**, 35(1), 1-15