International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2015)

Research on the University Network Information Security Risk Management Model Based on the Fuzzy Sets

Cai-qiao Huo, Li-zhuang Meng and Kai Chen

Foreign Language Department,Baoding University,Baoding, 071000, China

Keywords: Information security; Risk management; Fuzzy sets; Failure mode and effective analysis

Abstract. Due to the evolution and widespread about the Internet, organizations are easier to attack on the information technology systems. These are caused by data loss and change and those insecurity impact resistant services and business' running. Then, we use a way that is the management of the information security uncertain, such as the failure mode and effects analysis and the fuzzy theory, to reduce the potential failure. This method analyzes the four different sizes of information security: the road to the systems information, the share security, basic equipment and management security. The proposed model, and the simulations model, described by the paper, is applied to a university information security. There are two most important aspects that is belong to the information security risk, the first one is the communication security, the second one is the infrastructure problem.

1 Introduction

The most valuable asset of an organization in an information society must be the information. It includes a constant risk of hazard and the greater and more than ever before. This is due to the evolution of the Internet, and leads organizations to share information without enough protect (Bojanc Bligh Flyers, 2008). To enhance business running, reinforce management decisions and arrange business strategies, the leader and decision-maker from the organizations choose to rely on Internet services and information systems (Kankanhalli Teo, brown, Wei, 2003). So some measures need be made to keep this dependence and the corresponding increase safe behavior from the dangerous, especially in the impact of the safe behavior as information systems become more dangerous attack, this dependence will lead to a corresponding increase in the impact of safe behavior.

Because information security has two parts, one is about the issue of the university issue, another part is the problems that is involves all the behavior of users (Bang, Lee, Bae and Ahnc, 2012), The most important things about these policies are that everyone including all of the business owners and the related partner to run the enterprises with the owner comply these policies when they work. These policies include engaging The ISO standards is including in these policies. These standards are not technical standards. These standards are belonging to the business field. These business standards are a system including the basic infrastructure to protect the organization from the security. According to the front researchers, some things have to do to provide the information security level such as the organizational and the university's culture ,and the change must change the organizational culture, and the managers of the business or the university must be involved in the processes.

First, we will briefly introduce some of the information security risk management methods and direction, to provide a brief background of our method. Then, we will introduce the method, and gives a real case illustrating how method, easy to learn is used to validate the proposed method. Finally, we put forward the discussion and summary statement.

This paper is divided into different sections where Section 2 introduces some information of the security risk management methods and direction. The model and the relation methods discussed in Section 3. Section 4 we discuss a case study illustrating how to use it. Lastly, conclusions are given in Section5.

2 Background

In this section, the approaches to data mining and the common intelligent phishing classification approaches from the other papers will be interpreted. Further, the section starts by showing the phishing life cycle.

2.1 Information security risk management methodologies.

According to Ozkan and Karabacak, the original risk analysis is the basic steps in the system of the risk management. The work to analysis the risk starts from using the information and identifying the sources, then the researchers will try to assess the information risk. Therefore, the information risk organization would be failure just because the decision-maker could not performed very well and choose the wrong counter measures. As far as the risk assessment is concerned, the preliminary ways of assessed is to determine the potential effects, that the potential effects are defined in this paper is the risk assessment of a person when this constitution need happened.

A methodology was proposed by some authors Duren, Buchanan, and Duff. This methodology uses a mixed methods approach not a sample one. In the mix methods, there is a special analysis way to be illustrated, that uses the historical security incident data as the basic mater, chooses the quantitative way to analysis. In this world, now a Delphi study is the classical expert prediction to pool the good ideas of the famous experts in the special field. Then we could apply the analysis to monitoring the information security risk, in some case, the health care services still in the considering.

To implement the practices of the information security management, we need find the basic work described, and then we should remember the important of the information security. The finally, a workable and effective method of risk management is necessary. So, therefore, this paper tries illustrating a multi-dimensional approach method. The method uses the mind of fuzzy logic and failure mode and effects analysis to approach the purpose that is the information security risk management.

2.2 The failure mode and effects analysis methodology.

By using the failure mode and effects analysis, there are three factors of assessing the risk. The risk priorities of failure modes are the risk priority number(W), the three factors are: occurrence (R), severity (E), and detection (T). Then, the RPN is defined in Eq. (1).

$$W = R * E*T \qquad (1)$$

The best way to optimize the security is to minimize the cost and the fee when the security systems were damaged, in another word, is trying to maximize the systems value by setting the first order partial differentiation of Π in Eq. (1) with respect to l to 0; that is,

$$\frac{\partial \Pi}{\partial l} = -\frac{\partial \beta}{\partial l} q - 1 = 0 \qquad (2)$$

since both l and Bata have no relationship with the w. in there, the purpose is try to attach maximum, not minimum, of Π:

$$\frac{\partial^2 \Pi}{\partial l^2} = -\frac{\partial^2 \beta}{\partial l^2} q \le 0 \qquad (3)$$

3 The information security risk management model

Thought about the assessed the risk to the company with respect to university IT security problem, especially multiple dimensions in this paper.multiple dimensions. It is necessary to construct a decision model, which the model has to keep the accordance with the vision of Belton and Stewart.

3.1 The Security Risk

In practice, the traditional sense of service providers the ability of the security risk assessment is through a comprehensive identification and analysis system under the framework of threat and vulnerability and its potential impact on the assets to determine the level of safety and resistance risk ability. But in the university network information environment, multiple service providers to buy cloud service providers may hire to provide other services infrastructure services or software services, according to the system status of dynamic selection. Therefore, according to the characteristics of dynamic and multi participation in university network information, university network information security standards should support the safety assessment on cloud service process flexible and complex, need the calculation and evaluation methods of providing cloud services security capacity of the corresponding.

University network information system operation needs to establish a set of safety standards and assessment system, safety target validation, safety service level evaluation, measure the cloud user security goals and a cloud service provider security service ability, safety verification of university network information platform system; short board for university network information platform and reinforcement, to further improve the safety assessment system scientific and cloud resource pool platform, provides the important reference to the service providers to construct a security service; the other on the basis of the detection and evaluation of scientific testing methods, the safety accident occurs during rapid implementation of accountability, to avoid the buck.

3.2 The Analysis Algorithm

Fish-Search is the first priority evaluation strategies about how to optimize the candidate URL algorithm. It is the initial conditions of the user's query keywords, and the seeds of a given URL. This method by keyword matches to determine the relevance of a page. The page relevance directly determines the page containing the candidate URL crawl priority.

Vector space model assumes that the articles in terms of the role of the document category are independent of each other. So it can put the document as a series of unordered collection of entry. The model with feature as the document representation, coordinate the document in the form of vector expressed as a single point in the multidimensional space, select words as the feature vector of each component.

Hyperlinks B and C child node in proportion to the topic is very big, the possibility of their other children topic will be large. The father node, the node is called authority high topic relevance, should be preferred to crawl. And A small proportion of children topic, it will reduce the possibility of other children topic, it crawl priority should be lowered. HLA for each URL to calculate a hyperlink score S, used to indicate the priority of the URL. The crawler each time from the URL in the queue S value highest URL to crawl. The final result is shown in equation 2.

$$\begin{aligned} Fomula &= \sum_{l=1}^{N} S_{li} \times \beta_k + \sum \varphi(d_j)/t \\ S(Ci) &= SIM(Ci) + Fomula \end{aligned} \qquad (2)$$

In this structure, each Main Spider online is learning in the process of creep, adjacent information learning. The result of the crawling through setting the time interval, send Super-ZT-Spider collection of relevant information. By Super-ZT-Spider integrated all the results of the analysis of the crawler, deep feedback relevant information. The comprehensive assessment of the structure to search the web the relevance of information, the information distribution to the various Main Spider, update the classifier, begin the next round of search, until the search task to complete.

3.3 Fuzzy model.

In the paper, the fuzzy sets are constructed thought about the membership functions' form that could reflect the security risk. To evaluate the fuzzy sets type is also essential. The paper's standpoint of the fuzzy set suitability for the managing optimization procedures. In the university, the real numbers are defined as some most usually used membership function. They conclude fore types：tri-angular, trapezoidal, Gaussian, and Exponential-like membership functions. In this paper, we used the trapezoidal fuzzy number, record a Q. It can be illustrated as follows:

$$f_Q(x) = \begin{cases} 0 & if \quad x < q_1 \\ \dfrac{x - q_1}{b_1 - q_1} & if \; q_1 \le x \le b_1 \\ 1 & if \; b_1 \le x \le b_2 \\ \dfrac{x - q_2}{b_2 - q_2} & if \; b_2 \le x \le q_2 \end{cases} \qquad (4)$$

where Q = (q1, b1, b2, q2) could represent the variable (in the real case).

When we assume the b1 = b2 = q , the function number, the triangular fuzzy number, would be: Q = (q1 , qj , qi, q2) = (q1, qm , q2).

It is reviewed in this section that fuzzy set theory's fundamental operations. The crisp number is expanded obviously, then the number has the ability to support the determination of the fuzzy number.

4 Case Study

A university lab has tried to apply the proposed model. There are enough experts who involve the case studies. The performed steps are illustrated as follows:

Step 1: The expert provides the fuzzy number. In many situations, we get enough information and think about all the measurable risk factor, and then the experts are likely to provide a precise number or a range of possible number.

Step 2: Fuzzy number determination Table 1 shows the Fuzzy number for each failure mode.

Tab.1 Fuzzy number for each dimension

Dimension Fuzzy number	
D1 – The way to the information and systems	(278.425; 329; 754.5;1328)
D2 – Communication security	(432.175; 574; 893; 1490)
D3 – Basic structure	(354.175; 423; 883.5; 1612)
D4 – Security management	(292.175; 387; 585; 1867)
D5 – The secure systems development	(243.125; 432; 342;1534)

Step 3: Based on the each failure mode's fuzzy number, we can compute the total fuzzy number. The purpose of the practice is to compare each dimension and rank them about risks.

In this study, a model of IS security risk management was formulated and tested on an academic group research project in a public organization, examining the five dimensions.

5 Conclusions

This paper's purpose is to settle the problem about the network security management of university. This method analyzes the four different sizes of information security: the road to the systems information, the share security, basic equipment and management security. The proposed model, and the simulations model, described by the paper, is applied to a university information security. There are two most important aspects that is belong to the information security risk, the first one is the communication security, the second one is the infrastructure problem. The above analysis shows that the fuzzy sets and the failure mode and effects analysis methodology are kinds of effective method to keep the information security of the university.

References

[1] J. Adler - Milstein, Bates, Paperless healthcare: progress an challenges of an IT-enabled healthcare system, Business Horizon 53 (2010) 119–130.

[2] J. Adler-Milstein, D.W. Bates, A.K. Jha, U.S. regional health information organizations: progress and challenges, Health Affairs 28 (2) (2009) 483 –492.

[3] A HI MA /H IMS S, The Privacy and Security Gaps in Health Information Exchange,White Paper by the AHIMA/HIMSS HIE Privacy and Security Joint Work group, 2011.

[4] R. Bojanc, B.J. Blazic, Towards a standard approach for quantifying an ICT security investment, Computer Standards & Interface 30 (2008) 216 –222.

[5] A. Appari, M.E. Johns on, In formation security and privacy in health care: current state of research, International Journal of Internet and Enterprise Management 6 (4) (2010) 279 –314.

[6] V. Viduto, C. Maple, W. Huang, D. Lopez-Perez, A novel risk assessment and optimi-sation model for a multi-objective network security countermeasure selection prob-l em, 53 (2 01 2) 59 9 –610.

[7] J. Walker, E. Pan, D. Johnston, J. Adler-Milstein, D.W. Bates, B. Middleton, The value of health care information exchange and interoperability, Health Affairs, Supple-mental Web Exclusive, 2005, (W5-10-W5-18).

[8] W. Wallinger, R. Govindan, S. Jamin, V. Paxson, S. Shenker, Scaling phenomena in the internet: critically examining criticality, Proceedings of National Academy of Science 99 (1) (2 00 0) 25 73–2580.

[9] J. Wang, How may IT security affect competitive advantage? The Fourth ABIT Annual Meeting, Monroeville, Pennsylvania, 2004.