Jurnal Teknologi

Full paper

A Huiristic Method for Information Scaling in Manufacturing Organizations

Ghasem Rezaei*, Majid Ansari, Ashkan Memari, Seyed Mojib Zahraee, Awaluddin Mohamed Shaharoun

Faculty of Mechanical Engineering, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia

*Corresponding author:rezaeighasem@yahoo.com

Article history

Received :10 March 2014
Received in revised form :
28 April 2014
Accepted :15 May 2014

Abstract

Protecting information assets is very vital to the core survival of an organization. By increasing in cyber-attacks and viruses worldwide, it has become essential for organizations to adopt innovative and rigorous procedures to keep these vital assets out of the reach of exploiters. Although worldwide complying with an international information security standard such as ISO 27001 has been raised, with over 7000 registered certificates, few Iranian companies are under ISO 27001 certified. Also organization needs to perform a risk assessment in order to determine the organization's asset exposure to risk and determine the best way to manage this. The determination of risk within the methodology is based upon the standard formula, which the risk is calculated from the multiplication of the asset value, threats and vulnerability. The ISO 27001 requires is that 'An appropriate risk assessment shall be undertaken'. One of the main factors for risk assessment is identifying and scoring of Information asset in this process. Due to different values of asset in organizations, the main purpose of this study is to identify and investigate a weighted method to assign different values of assets in order to minimize vulnerability in manufacturing systems. This study also aims at improving asset value scoring by using heuristic methods. A real world case study was selected for implementation of this approach based on ISO27001` in Iran.

Keywords: Assets information; scaling method; heuristic

1.0 INTRODUCTION

Information system security plays a significant role in most organizations and it can impose an extra cost to the organizations. Based on the investigations in 2010 in 738 organization loses 190$ million caused by information security violations[1,2]. In addition, recent literature has shown important costs relevant to information system security violation[3,4,5,1]. The organization tries to adopt innovative and rigorous procedures and methods to keep the information secure and out of the reach of exploiters. In recent years, the security risk analysis for information systems has attracted much attention of researchers in the field[6,7,8].

Security risk analysis is an integrated part of enterprise risk management (ERM) that concentrate on analyzing threats and vulnerabilities to the information resources. However, security risk analysis is very critical and difficult task because of the dynamic and complicate the environment. Risk analysis can be grouped to basic categories: the quantitative approaches, qualitative approaches, and combination.

In the quantitative methods the mathematical and statistical analysis is used to show the risks[8]. Gordon and Loeb[9] developed a mathematical model to obtain the optimum security investment level for information systems. Following that Yue *et al.*[10] Extended their work of formulating and solving the problem based on a risk management paradigm. According to his work additional insight was provided into making an optimum decision by managers. Wu *et al.*[11] suggested a quantitative technique to determine the most important risk for conducting concurrent engineering projects. Moreover, risk-based method was proposed by [12] that make the trees as parametric constraints that authorized to determine probability quantity of security breaches that occurred because of the internal vulnerabilities.

Moreover, there are some qualitative methods to analyze the security risk such as Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) technique that help to define s set of assessment criteria to set up a common basis for finding the impact values because of threats to the important assets [13]. Practical Application of Risk Analysis (PARA) method was proposed by Peltier[14] to assess the systematic evaluation of tangible and intangible risks to provide cost effective measures to decrease risk to an acceptable level.

Additionally, there are other qualitative approaches such as CCTA Risk Analysis and Management Method (CRAMM) are created by the UK Government's Central Computer and Telecommunications Agency (CCTA) and INFOSEC Assessment Methodology (IAM)[15].

Some extensive methods combining both qualitative and quantitative methods have been suggested[15,16]. A similarity value of generalized fuzzy numbers was applied by Chen *et al*.[17] to solve the fuzzy risk analysis difficulties. This method was unable to show the graphical relationships between different security risk parameters applying flow charts or diagrams. Therefore, to deal with this problem Fan and Yu [18] suggested a Bayesian networks (BNs) based procedure. In their method, the BN is organized solely based on domain experts' experience.

One evidential reasoning approach under the Dempster–Shafer theory to analyze the risk of information system security was proposed by Sun *et al*[1] to connect relevant security risk parameters, related countermeasures, and their interrelationships. After that sensitivity analysis was done to assess the effect of important factors on the model's results. It should be noted that the models that are conducted incorrectly or proposed based on questionable assumptions are vulnerable to model risks[19].

The goal of this paper is to propose a new quantitative and qualitative approach for finding the information asset value. This study introduced three hierarchical steps for finding the value of information assets. These steps are: identify information assets, securing of information assets based on each sub-dimensions, identify the final value of information assets based on the sum of all obtained scoring from sub-demotions.

■2.0 METHODOLOGY

In this paper, we propose a new quantitative and qualitative approach for obtaining the information asset value. This study introduced three hierarchical steps for determining the value of information assets. These steps are: identify information assets, scoring of information assets based on each sub-demotions, identify the final value of information assets based on the sum of all obtained scoring from sub-demotions.

In the first step the information assets should be identified. In this identification, all information assets are listed. Next, all assets based on their specification like owner, users of asset and asset location are listed in detail. To classify information assets, we apply British BS7799 standard[20]:

- Information Asset: database, data file, system document, user management, plan document, provision for alternative system
- Documents: contracts, guidelines, company documents, important business documents
- Software Asset: applications S/W, system S/W, development tool and utility
- Physical Asset: computer and communication magnetic disk, power supply, air conditioning, furniture, facilities
- Personnel Asset: individuals, customer, subscriber
- Image and Reputation of a Company
- Service: computer and communication service, warm, light, air conditioning.

The next step is to identify asset value based on sub dimension. The minimum scale of each sub dimension is zero and maximum one is three (Table 2). The definition of each sub dimension is listed in this table. The value of each asset can be defined as the sum of the nine sub dimensions score for each asset. The scoring method for assets is described in Table 3. It should be noted that for each assets the value between 1-3 has been allocated based on expert opinion. For example, consider the Table 3 definition and a PC as one of information assets. To assign scores for this PC, based on its price, it can obtain score's value of 1, 2 or 3 in financial effect sub-demotions. For all sub-demotions value assignments for assets has been discussed in Table 3 as well.

Non relevant criteria for assets take zero value as their score. The value of each asset can be determined using the sum of the nine dimensions.

Finally, value score for each asset calculate by the sum of all obtained score from sub-demotions.

Table 1 Enterprise assets considered by different reference

Assets main groups	
Tangible (Examples)	Intangible
Information: (Policy document)	Goodwill
Information: (Data files)	Service to clients
IT services: (Messaging-active directory)	Public confidence
Software: System (Solaris), Application (Oracle),	Public trust
Utilities (management tools)	Competitive advantage
Hardware: Hosts (Servers) other (Printers)	Imageof the organization
Communication: Network (Routers), (Cable)	Reputation
O Documents: (Management commitment)	Trust in services
Agreements: (Confidentiality-third party)	Employee morale
Information: (Research)	Productivity
Other: (User manuals-training material)	Loyalty
P IT staff: (IT security manager)	Ethics
Employee: (Senior management)	
Users: (Inside/Outside)	
Contractors:(Consultants)	
Owners:(Stakeholders)	
E Services: (Heating-lighting-power-AC)	
Equipment: (Desks-Fax machines-Cables)	
Physical (infrastructure): (Offices-facilities)	

■3.0 CASE STUDY

In this study, a cement plant manufacturer in IRAN was selected as a case study. This company adopted to ISO/IEC 27001(ISMS) [21] to obtain competitive advantage. The objectives were to enhance the risk profile, information systems quality, businesses continuity and brand image. The ISMS scope of this company is all of the assets in a factory and his office in another city. It integrated information security management in its existing integrated management system based on ISO 9001, ISO 14001, Ohsas 18001 (occupational health and safety management) and 10002. These standards share the same general requirements, document structure, and management principles such as the 'Plan-Do-Check-Act'-cycle. Consultants supported implementation, carried out risk assessments and drafted policy documents. Implementation has had a positive impact on the availability of IT systems, service quality, business continuity and customer satisfaction.

In our selected case study, more than 2400 assets have been identified. Six assets were selected as a sample for implementing our method which shows in Table 4. The Table 4 shows scaling of the six information asset of the company that has been selected as the sample.

Table 4 investigates different information assets and classify them based on various aspects. All assets identified by exclusive code. After coding step, attributes including type, specification, user in charge and location assign to assets. Regarding to stratigcal, operational and structural dimensions, each asset takes a score ranging from 1 up to 27 based on Table 3. It should be noted, all scores assignment was done by experts point of view. Finally total score for each asset is calculated by summing of all obtained score. Table 5 shows the significance of different assets based on their obtained score.

Table 4 Scoring table

$1 \leq \text{Score} \leq 9$	Low Value
$9 \leq \text{Score} \leq 18$	Valuable
$19 \leq \text{Score} \leq 27$	High Value

■4.0 CONCLUSION

In this study, we tried to shed an innovative method for scaling Information assets in the manufacturing organizations after the identifying of the organization's assets throughout the planning phases of the ISO 27001 certification process. This method was used for an Iranian company during the implementation of ISO 27001. When it came to motivations, enhancing the organization's security level and obtaining competitive advantages. The research shows how to calculate the asset value by combining the nine sub dimension. In summary, it is clear that asset assessment is the cornerstone of Risk Assessment.

To achieve asset value in the Manufacturing organizations, essential steps are needed. These steps are: 1- identify its assets, 2- identifying the value of the each asset base on three dimension (Structural dimension, operational dimension and Strategic dimension) and nine sub dimension (Financial impact, The sensitivity of the company's vision, Functional dependence, Authenticity and integrity, Availability, Authenticity and integrity, Legal effect, Competitive effect, Connection with the company's strategic goals), and 3- The value of each asset can be defined using the sum of the nine dimension. This paper proposes a new asset scaling method. A case study is investigated for the validation of the usefulness of this method. It contributes an effective method for scaling the information system assets such as server, application, and data in terms of confidentiality, integrity, and availability.

In the present context of competitive environment, it is recommended that the Innovative method for Scaling of Information Assets in the Manufacturing organizations in this study should serve as a guiding for the manufacturing and IT manager when implementing ISO 27001 in their companies. The innovative risk assessment method that used in this case study will be reported in a future article.

Table 2 Definition of dimension and sub-dimension or valuation of assets

Dimension	Sub-dimension	Definition
Structural Dimension	Financial Effect	To what extent losing, damaging or disclosing of assets can bring loss for company. Note: only financial effects are considerable. (E.g. if a computer server faces in trouble, how much does it cost for replacement not the cost of recovery of lost data
	The Sensitivity Of The Managers' Vision	To the extent the assets are emphasized by top managers
	Functional Dependency	To what extent losing, damaging or disclosing of assets can bring a problem for internal processes, operations, and core business processes
Operational Dimension	Confidentiality	To what extent assets are confidential from managers' perceptions
	Availability	To what extent availability of the asset is important for users
	Integrity	To what extent losing, damaging or disclosing of assets can reduce the integrity of information in the scope
Strategic Dimension	Legal Effect	To what extent losing, damaging or disclosing of assets cause legal problems.
	Competitive Effect	To what extent the assets of the company are treated as the competitive element
	Connection with Strategic Goals Of Company	To what extent losing, damaging or disclosing of assets can endanger company to achieve the strategic goals

Table 3 Asset scaling method

Scaling Method			Sub-dimension
(3) High	**(2) Medium**	**Low** (1)	
Over than two hundred million Rials	Between twenty to two hundred million Rials	Less than twenty million Rials	Financial Effect
Constantly, Occasionally, reminding manager's attention towards assets is required	Occasionally, reminding manager's attention towards assets is needful	There is not any relevant suggestions for the assets	The Sensitivity Of The Managers' Vision
Without these assets, the main operation of Company seriously cause to damage, stop and delay, that the company will not tolerate	Without these assets, a number of operations have to be stopped and delayed. Tolerance is intermediate	Without these assets, the main operation of the Company cannot be stopped or the resulting delay and resulting stop are tolerable	Functional Dependency
Related assets from the Chief's point of view is entirely confidential	Related assets from the company's vision is not confidential, but there are some considerations		Confidentiality
Unavailability of relevant assets cause serious stop and delay in works which are not tolerable	Unavailability of relevant assets cause to stop and delay in the works and tolerance is intermediate	Unavailability of relevant assets does not have a lot of stops and delay in the works and the stop delay is tolerable.	Availability
Improper functioning of the relevant assets has serious effect on the accuracy and integrity of information	Improper functioning of the relevant assets to the extent the accuracy and integrity of information affect or could affect	Improper functioning of the relevant assets has little effect on the accuracy and integrity of information	Integrity
The loss or damage to assets certainly results in legal suits against the company	The loss of or damage to assets may result in legal suits against the company	Assets have low legal effect	Legal Effect
Competitors do not have the assets that are important to them or having this asset cause a competitive advantage for the company (This asset cause to distinct company unlike the others)	Competitors do not have the relevant assets and currently achieving the assets are not important but in the future might be treated as the important factor (in future the assets might be distinct)	The relevant assets are not an effective competitive factors or the other competitors have the relevant assets	Competitive Effect
The relevant assets do not have a key role in achieving the strategic goals the company or without this achieving strategic goals might be difficult	The relevant assets do not have not a key role in achieving the strategic goals but Indirectly affect the achievement of strategic goals of the company	The relevant assets do not have a key role in achieving the strategic goals of the company	Connection With Strategic Goals Of Company

Table 5 Results analysis

Asset Code	Asset Type	Asset Specification	Users in (user, charge)	Location	Strategic Dimension			Operational Dimension				Structural Dimension			Total Scale
					Connection With The Company's Strategic Goals	Competitive Effects	Legal Effect	Authenticity and Integrity	Availability	Confidentiality	Effect on Process and Functional	Financial Impact	The Sensitivity of The Company's Vision	
1	Computer	PC	Quality Assurance Expert	Quality Assurance Room	1	0	0	1	1	0	1	1	2	7
2	Computer	PC	Production Statist	Production statist room	1	0	0	1	2	0	1	1	1	7
3	Computer	ISA Server(Wireless)	Computer Expert	Server Room	2	1	0	3	3	2	3	2	3	19
4	Computer	Novell Server	Computer expert	Server Room	1	0	0	2	2	1	1	2	1	10
5	Computer	PC	Sale Employee	Sales	1	0	0	1	1	0	1	1	2	7
6	Cable	Cate 5E	IT manager	Enclosure Company	1	0	0	3	3	0	2	1	2	12

References

[1] Sun, L., R. P. Srivastava, and T. J. Mock. 2006. An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems*. 22(4): 109–142.

[2] Gordon, L.A., *et al*. 2005 *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

[3] An, M., Y. Chen, and C. J. Baker, 2011. A Fuzzy Reasoning and Fuzzy-Analytical Hierarchy Process Based Approach to the Process of Railway Risk Information: A Railway Risk Management System. *Information Sciences*. 181(18): 3946–3966.

[4] Büyüközkan, G. and D. Ruan. 2010. Choquet Integral Based Aggregation Approach to Software Development Risk Assessment. *Information Sciences*. 180(3): 441–451.

[5] Campbell, K., *et al*. 2003. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*. 11(3): 431–448.

[6] Cavusoglu, H., B. Mishra, and S. Raghunathan. 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*. 9(1): 70–104.

[7] Ekelhart, A., *et al*. 2007. Security Ontologies: Improving Quantitative Risk Analysis. In System Sciences, 2007. *HICSS 2007. 40th Annual Hawaii International Conference on*. IEEE.

[8] Karabacak, B. and I. Sogukpinar. 2005. ISRAM: Information Security Risk Analysis Method. *Computers & Security*. 24(2): 147–159.

[9] Gordon, L. A. and M. P. Loeb. 2002. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*. 5(4): 438–457.

[10] Yue, W. T., *et al*. 2007. Network Externalities, Layered Protection and IT Security Risk Management. *Decision Support Systems*. 44(1): 1–16.

[11] Wu, D. D. *et al*. 2010. A Risk Analysis Model in Concurrent Engineering Product Development. *Risk Analysis*. 30(9): 1440–1453.

[12] Grunske, L. and D. Joyce. 2008. Quantitative Risk-based Security Prediction for Component-based Systems with Explicitly Modeled Attack Profiles. *Journal of Systems and Software*. 81(8): 1327–1345.

[13] Alberts, C. J. and A. Dorofee. 2002. *Managing Information Security Risks: the OCTAVE Approach*. Addison-Wesley Longman Publishing Co., Inc.

[14] Landoll, D. J. and D. Landoll. 2005. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. CRC Press.

[15] Alter, S. and S. Sherer. 2004. A General, But Readily Adaptable Model of Information System Risk. *Communications of the AIS*. 14(1): 1–28.

[16] Salmela, H. 2007. Analysing Business Losses Caused by Information Systems Risk: A Business Process Analysis Approach. *Journal of* Information *Technology*. 23(3): 185–202.

[17] Chen, S.-J. and S.-M. Chen. 2003. Fuzzy Risk Analysis Based on Similarity Measures of Generalized Fuzzy Numbers. *Fuzzy Systems, IEEE Transactions on*. 11(1): 45–56.

[18] Fan, C.-F. and Y.-C. Yu. 2004. BBN-based Software Project Risk Management. *Journal of Systems and Software*. 73(2): 193–203.

[19] Wu, D. and D. L. Olson. 2009. Enterprise Risk Management: Coping with Model Risk in a Large Bank. *Journal of the Operational Research Society*. 61(2): 179–190.

[20] Von Solms, R. 1998. Information Security Management (3): The Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security*. 6(5): 224–225.

[21] Fenz, S. *et al*. 2007. Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. In Dependable Computing. PRDC 2007. *13th Pacific Rim International Symposium on*. 2007: IEEE.