Risk Assessment Method Based on Business Process-Oriented Asset Evaluation for Information System Security*

Jung-Ho Eom, Seon-Ho Park, Young-Ju Han, and Tai-Myoung Chung

Internet Management Technology Laboratory,
Department of Computer Engineering,
School of Information and Communication Engineering,
Sungkyunkwan University,
300 Cheoncheon-dong, Jangan-gu,
Suwon-si, Gyeonggi-do, 440-746, Republic of Korea
{jheom,shpark,yjhan}@imtl.skku.ac.kr and tmchung@ece.skku.ac.kr

Abstract. We presented risk assessment methodology focused on business-process oriented asset evaluation and qualitative risk analysis method. The business process-oriented asset evaluation is to evaluate asset's value by the degree of asset contribution related to business process. Namely, asset's value is different according to the importance of department to which asset belongs, the contribution of asset's business, and security safeguard, etc. We proposed new asset's value evaluation applied to the weight of above factors. The weight is decided by evaluation matrix by Delphi team. We assess risk by qualitative method applied to the improved international standard method which is added the effectiveness of operating safeguard at information system. It reflects an assumption that they can reduce risk level when existent safeguards are established appropriately. Our model derives to practical risk assessment method than existent risk assessment method, and improves reliability of risk analysis.

1 Introduction

As information communication technology has developed steeply, business dependence on IT system is raising rapidly. As IT system has occupied important role in business, it begins to increase the concern of security on IT system. To protect IT system effectively, it firstly needs to analyze overall IT system risks. That is a risk assessment included the identification and valuation of assets, threat analysis, vulnerability analysis, the existing safeguards analysis and risk evaluation[1,4,5]. We have been studying on develop substantial risk assessment

* This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2006-C1090-0603-0028).

method which could be evaluated risk level according to asset importance in organization. We focus on asset analysis reflected an organization’s information system(IS) characteristics and environment for assessing risk effectively. So, we applied business process-oriented asset analysis which an asset’s importance could be different in organization’s business-process viewpoint, even if assets have same costs. Section 2 describes related work, section 3 presents our model and section 4 demonstrates application of our model. Finally, we conclude in section 5.

2 Related Works

2.1 Risk Assessment

Risk assessment is to assess a combination of the potential adverse business impacts of unwanted incidents and the levels of vulnerabilities and threats. The risk is a measure of the exposure to which an IS and the associated organization may be subjected. The risk assessment’s goal is to identify and assess the risks to which the IS and its assets are exposed, in order to select appropriate and justified safeguards. Thus, the risk assessment is based on the values of the assets, the levels of threats and vulnerabilities and the existing/planned safeguards.

The risk assessment method has two types; qualitative and quantitative methods. The former uses the rating scale which is evaluated with asset, threat and vulnerability rating. The Delphi team decides rating scale with a degree of asset sensitivity, capability and motivation of threat and severity and exposure of vulnerability. The Table 1 is the method of rating scale in ‘CSE Manuals ITSG-04’ [8]. A degree of asset sensitivity is divided into 5 scales; little/no loss or injury (1), minor loss or injury (2), serious loss or business process could be negatively affected (3), very serious loss/injury, business process could fail (4), high loss or grave injury to an organization’s or business process will fail (5).

Table 1. The matrix of risk assessment

	Scale of Threat	1					2					..
	Scale of Vulnerability	1	2	3	4	5	1	2	3	4	5	..
Asset	1											
	2											
	3											

Threat assessment is same as vulnerability assessment method. So, risk assessment is evaluated by combination with asset, vulnerability and threat scale. The latter uses annual loss expectancy(ALE) in [12]. ALE defines damage that may be imposed to IT asset by monetary unit. ALE is used in quantitative analysis representatively since NIST proposed evaluation method by FIPS-65 document in 1979. ALE production method is as following.

$$ALE = Asset\ value(AV) \times Exposure\ factor(EF) \times Threat\ frequency(TF)$$

Asset value and threat frequency is computed in asset and threat analysis. Exposure factor(EF), which displays a degree of asset's exposure against threat, is computed from the ratio of the related safeguard/operating safeguard and non-establishing safeguard on the basis of the relation of asset and threats.

2.2 The Method of Asset Analysis

An asset is a component or part of a total information system to which an organization directly assigns value[7,9]. An asset analysis identifies all assets within a risk analysis boundary, classifies into the same kind of asset, and finally assesses value of each asset. An asset analysis' goal is to identify the most critical components of the organization so that they can be examined for vulnerabilities[5,7]. We observed an existent asset analysis method in the 3 viewpoints; classification, evaluation and level.

- ISO TR-13335 : This researches techniques for the successful management of IT security, and can be used to assess security requirements and risks [1,2,3].
 - Classification: Classify the boundaries of review into asset types such as information/data, hardware, software, equipment, documents, etc.
 - Evaluation: Evaluate by the cost of obtaining and maintaining the asset, and the potential adverse business impacts from loss of 3 security factors.
 - Evaluation Scale: negligible(0)-low(1)-medium(2)-high(3)-very high(4)
- CSE MG-3 : This expands on the standards stated in the Government Security Policy of Canada, provides specific guidance for risk assessment, and safeguards throughout the information technology system lifecycle [8].
 - Classification: Hardware, software, interfaces, personnel, supporting systems and utilities, and access control measures
 - Evaluation: Evaluate based on its replacement cost, its intrinsic value and the consequences, impact or injury resulting from asset compromise.
 - Evaluation Scale: negligible-low-medium-high-very

3 The Proposed Methodology

The proposed methodology is the business-process oriented risk assessment methodology. We assess IS asset with the relationship of business-process than asset's physical value such as purchase cost, annual maintenance expense and so on. We considered that they have a different value according to IS assets contribution to business process, even if they are same kind of asset. We focus on business process-oriented risk assessment methodology according to the contribution degree of asset in the organization's business.

3.1 Business Process-Oriented Asset Evaluation

We classify assets by asset 7 types in the general IS components such as H/W, S/W, network, information, application, user and environment. Then, we reclassify by a business-process oriented method [11].

The proposed asset evaluation considers that asset value could be different according to department utilization, business contribution, user position, etc., even if assets have same type. For example, it has a different value between financial and plan department, even if they are the same kind of PC. For example, it is Department A's server B, application D used with job C, data G, and user E. The examples of standards of specific factors for the business process-oriented evaluation method are as following:

- **Department Utilization(DU)** department's IT utilization according to the organization business
- **Business Contribution(BC)** Asset importance contributing to the organization on business
- **User Position(UP)** Task importance handling by user in the IS
- **Security Safeguard(SS)** Suitability of the safeguard that is established against risk

Table 2 shows an example of an improved asset classification which represents the relationship between the asset type and business-process oriented factors.

Table 2. An example of the proposed asset classification method

			ASSET					
			H/W		S/W		NETWORK	
			Disk	Sever	MS Office	Security Program	Router	LAN
BUSINESS	DU	USER.1						
CONTRI		USER.2			Asset.N			
BUTION		USER.n						

We applied weight to analyze asset according to the scale of business process-oriented classification factors. Weight factors can be applied from 1 to n reflected an IS environment and business process. Also, weight is classified into five levels such as very low, low, medium, high, very high, and applied on a scale of 1 – 5. We selected two business process-oriented classification factors such as department utilization and business contribution, but you can select more factors according to the organization's requirement and Delphi team's opinion.

We made up conversion table for converting quantitative asset cost into the qualitative value as like Table 4 . Delphi team has to create a conversion table based on an average between the organization's maximum and minimum quantitative asset value.

In this step, we have to evaluate the business process-oriented asset value(B-PAV). If the qualitative value is QV, the B-PAV formula is as follows;

Table 3. The evaluation standard of BU and DC

	Level	Scale	Standard
D U	Very low	1	do not use virtually IS; business weight is less than 20%
	Low	2	business dependence on IS is low; business weight is 20-40%
	Medium	3	If using an IS, business is gone easy; business weight is 40-60%
	High	4	Most business is achieved due to IS; business weight is 60-80%
	Very high	5	If an IS is not used, business is impossible; business weight is more than 80%
B C	Very low	1	don't use virtually IS; don't influence in operation
	Low	2	Business dependence on an IS is low; the most basic business
	Medium	3	If using an IS, business is gone easy; business achieve certainly
	High	4	Most business is achieved by IS; essential to the organization
	Very high	5	If not using an IS, business is impossible; critical business related to operation

$B - PAV = QV * W$
 W is weight which uses a scale of business process-oriented classification factor.
 $W = (W1 + W2 + W3 + + Wn)/n$

3.2 Risk Evaluation Method

We evaluate risk by such as asset value(AV), threat frequency(Tf), exposure degree(Ed) and effectiveness degree of safeguard(SED). AV is B-PAV. ED is evaluated by vulnerability assessment method in CSE Manuals ITSG-04. Delphi team can acquire Tf's rates through questionnaire or interview with system and security administrators or statistic log file of control systems directly. Risk evaluation formula is as following;

$R = B - PAV * Tf * Ed * SED$
SED influences in protection level according to implementation result(IR), and means different protection degree(PD) on each threat. Also, because there are various kinds of safeguard in a threat, each safeguard value should be reflected. And because effectiveness of safeguard is no actual 100%, The value of SED is;
 $S = 1 - (S_{IR} * S_{PD})$.
So, $R = B - PAV * Tf * Ed * [1 - (S_{IR} * S_{PD})]$.

4 Application of Proposed Method

We take any enterprise as an example. The company has such departments as R&D, financial and plan departments, and uses router(\$350). It has only a firewall for protect IS.

Firstly, we have to convert physical cost into qualitative value by conversion table. Delphi team decides the weights with the evaluation standard of the business process-oriented classification factor. For example, the R&D department UNIX is more important than the Financial Departments. And the Financial

Table 4. An example of conversion table

Qualitative value		
Level	Scale	Standard of the asset physical cost
Very low	1	The asset physical cost is less than \$100
Low	2	The asset physical cost is \$100-300.
Medium	3	The asset physical cost is \$300-600.
High	4	The asset physical cost is \$600-900.
Very high	5	The asset physical cost is \$1,000.

Department’s firewall is more important than the Plan Departments. If we perform like this method, we can decide weight value of each asset. If we evaluate the asset by the Table 4, each B-PAV value is as following Table 5.

Table 5. The result of weights decision and B-PAV calculations

		weights decision						B-PAV calculations					
		R&D		Financial		Plan		R&D		Financial		Plan	
Asset	QV	DU	BC	DU	BC	DU	DC	W	B-PAV	W	B-PAV	W	B-PAV
Router	3	2	2	5	4	4	2	2	6	4.5	13.5	3	9

Tf’s values were derived by Delphi Team which combines experts in the arena of IS security and referred ‘In the past 12 months, which of the following breaches have you experienced?’ in InfoSecurity News May 1997. Tf is considered such 15 items as computer virus, accidental errors and abuse of access privileges and so on. Ed is evaluated by Delphi Team based on vulnerability assessment in CSE Manuals. S_{PD} was derived following Table 6 which represents according to ISO/IEC JTC1/SC27 IT security management guideline. S_{IR} was derived from safeguard list in [3]. It classified 5 levels according to implementation results.

We can calculate SED with Table 6. Router’s SED value is 0.65 according to S_{PD} and S_{IR} is 0.5 and 0.7. Firewall has direct relation to the threat, and is enough to reflect security procedure. And Table 7 is risk assessment value.

If we compare international standard with the proposed method, we evaluate risk reflected organization’s business process, and have more accurate risk assessment considered effectiveness of existent safeguard. As applying correct risk assessment’s results, we can establish security policy and appropriate safeguard against risk. In here, we compare router’s risk value in 3 viewpoints; international standard, method applied to only business process-oriented asset value and proposed method.

As you see Fig.1, if we assess router’s risk at each department, its risk is same. But router’s risk is different if applied to business process-oriented asset evaluation result or the proposed risk assessment method. As financial department takes charge of an organization’s budget which handles business expanse and employee’s salary, if information is leaked out or destructed from threat, an

Table 6. The values of Tf ,Ed , S_{PD} and S_{IR}

	Sever	UNIX	Router		Sever	UNIX	Router
Tf	7.3	5.1	3.7	Ed	4	3.5	2.5
	Value	Description					
S_{PD}	0.0	No relation safeguard and the threat					
	0.165	Safeguard has indirect relation to the threat					
	0.5	Safeguard has direct relation to the threat					
	0.865	Safeguard established for the threat					
S_{IR}	0.1	No safeguard					
	0.3	Identified risk, but no concrete safeguard and occasional protect					
	0.5	set up protection procedure and start to implement safeguard					
	0.7	Reflecting procedure and apply safeguard					
	0.9	Perform the latest safeguard					

Table 7. Risk value

		R&D	Financial	Plan
Router	B-PAV	6	13.5	9
	Tf	3.7	3.7	3.7
	Ed	2.5	2.5	2.5
	SED	0.65	0.65	0.65
	R	36.08	81.17	54.11

Fig. 1. The result of risk assessment for router

organization will be seriously impacted. So, in financial department viewpoint, router’ value with business importance may be high, and risk level may be higher accordingly, and security safeguard may be established strongly.

5 Conclusion

We proposed risk assessment methodology based on business process-oriented asset evaluation and risk evaluation method. We have studied on our research in

2 aspects; business process-oriented asset analysis and concrete risk evaluation formula. The former focuses on asset value according to the importance of business process. Asset value depends on a business contribution of asset. The latter focuses on risk calculation. Our model applies international standard method to effectiveness of existent safeguard. It represents that risk value can be reduced by safeguard's fitness in information system. In future, we will apply our model to risk reduction method. We think that our model's result derives to select the suitable safeguard against risk.

References

1. ISO/IEC TR 13335(Part 1): Concepts and Models for IT Security, ISO/IEC JTC1/SC 27, 1996.
2. ISO/IEC TR 13335(Part 2): Managing and Planning IT Security, ISO/IEC JTC1/SC 27, 1997.
3. ISO/IEC TR 13335(Part 3): Techniques for the Management of IT Security, ISO/IEC JTC1/SC 27, 1997.
4. NIST Special Publication 800-30: Computer Security-Risk Management Guide, NIST, 2001.
5. B. D. Jenkins, 'Security risk analysis and management', Countermeasures Inc, 1998.
6. BS 7799: Guide to Risk Assessment and Risk management, BSI, 1998.
7. C. J. Alberts et al, 'OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation', Software Engineering Institute Carnegie Mellon, 1999.
8. CSE MG-3: A Guide to Risk Assessment and Safeguard Selection For Information Technology Systems, Communications Security Establishment, Jan. 1996.
9. Risk Analysis and Management Standards for Public Information Systems Security-Concepts and Models, TTA-Korea, 1998.
10. Risk Analysis and Management Standards for Public Information Systems Security-Risk Analysis, TTA-Korea, 2000.
11. Jung-Ho Eom, et. al, 'Two-Dimensional Qualitative Asset analysis Method based on Business Process-Oriented Asset Evaluation', Journal of KIPS, pp.79-85, Dec. 2005.
12. Kang Kim, et. al, 'A Risk Analysis Model For information System Security', journal of KIPS, pp.60-67, Sep. 2002.