Design of Risk Analysis and Assessment Model Based on the Business Process

Moon Goo, Lee
Department of Internet Information, Kimpo College, Korea
San 14-1 Ponae-ri, Wolgot-myun, Kimpo Kyounggi-do, 415-761, Korea
Tel: +81-31-999-4660, Fax: +81-31-999-4775
yeon0330@kimpo.ac.kr

Abstract: With dependency of companies and government agencies on the networks growing as ever, current patch-up security solution is not an ideal and effective remedy against the increasing threats. Worse, current security system costs excessive amount of resources to recover from an emergency should such a crisis occur. Thus effective risk management system is necessary for today's business, and at the core of such system is the risk analysis-assessment model. However, most of existing risk-analysis methodologies at work domestically has one critical problem; they've been developed abroad, and have been applied without necessary modifications to reflect the domestic conditions. First, assessment methods have not been clarified. Also non-existent is the mapping process of assets and risks. Secondly, asset-evaluating process doesn't reflect the organizational characteristics of the domestic businesses, which in turn undermines the reliability of such assessment results. To overcome the drawbacks described above, this paper suggests a new risk analysis-assessment model based on the business process approach.

1. Introduction

The suggested model provides the evaluation method per each process in top-down format and it takes the confidentiality, integrity and availability of the asset into the consideration. It also provides a mapping method for linking asset, threat, and vulnerability and tree-shaped risk evaluation method for explicit measurement of risk in each level. Also mapped out in Top-Down format are:

① The information asset evaluation method that reflects the business process approach

Pure asset value that reflects confidentiality, integrity, and availability of the asset, linking method between assets, threats and vulnerability

② Tree-shaped threat assessment method for explicit measurement of risk.

Also, concrete criteria and processes for the risk analysis have been presented to perform a reliable analysis/assessment, and actual cases of the suggested model at work have also been presented.

2. Suggested Risk Analysis Assessment Model

The suggested model provides the evaluation method per each process in top-down format and it takes the confidentiality, integrity and availability of the asset into the consideration. It also provides a mapping method for linking asset, threat, and vulnerability and tree-shaped risk evaluation method for explicit measurement of risk in each level. The followings are also mapped out in top-down format :

1) The information asset evaluation method that reflects the business process approach.
2) Pure asset value that reflects confidentiality, integrity, and availability of the asset, linking method between assets, threats and vulnerability.
3) Tree-shaped threat assessment method for explicit measurement of risk.

Also, concrete criteria and processes for the risk analysis have been presented to perform a reliable analysis, assessment and actual cases of the suggested model at work have also been presented.

Proposed model was designed to overcome the shortcomings revealed from existing methodologies. Overall, the suggested method is a qualitative risk analysis approach, and the asset assessment and threat and vulnerability assessment is presented within 5-point scale. Asset assessment method employs a process that evaluates the value of the assets accurately by linking the relationship between importance of the business processes and assets. Threat and vulnerability assessments take the frequency and impact into the consideration as well.

The followings are the distinctive features of the suggested model :

1) Task importance is weighed through value chain analysis, task process analysis, then is reflected on the asset evaluation process.
2) Risk evaluation reflects the frequency at which the crisis occurs.
3) Vulnerability evaluation reflects the impact of the crisis risk is calculated by multiplying the asset value with evaluation results #1, #2 and #3.

3. Structure of Suggested Model

The suggested model utilizes the task classification method during the asset identification, to establish the relationship between task processes and assets. Also reflected in the analysis are the characteristics within the organization.

3.1 Process Analysis and Asset Assessment

In this step, two things are done:

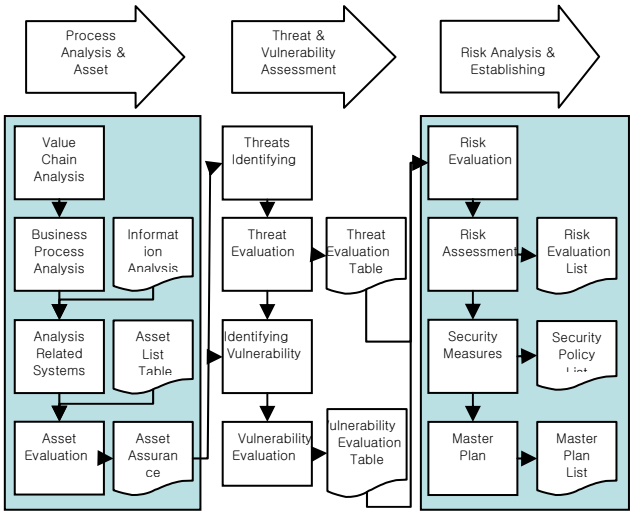
1) Assets of the organization are evaluated through task process anal analysis.
2) Information assets are analyses evaluated by the fixed standard.

3.1.1 Process Analysis and Asset Assessment

The following is the procedure for selecting actual target asset of risk analysis:

① Task is analyses based on the vision and goal of the organization.
② Core information asset is evaluated based on the result of #1
③ Value chain is evaluated based on the result of #2.
④ Result from #3 is used as the criteria in selecting the actual target of analysis.

Figure 1. Risk Analysis



The direction of the risk analysis is also set in this stage. The evaluator may choose the degree of classification as necessary according to the goal and term of the project.

Table 1. Information asset evaluation grade chart

Class	Upper	Middle	Lower
Asset	Business system	Unit work	Server H/W
			Network system
			Security system
			Database/Application
			PC / Terminal
			Document
			Human resources

3.1.2 Process Analysis

Once the core task process is selected from the overall business process and analyzed, the selected core task process and related information are analyzed by the standard of confidentiality, integrity and availability. To figure out the unit workload, target asset is selected, based on the goal and length of the project. Related systems are analyzed as necessary during this stage once the target asset is selected.

3.1.3 Analysis of related systems

It requires extra analyses of related systems, in addition to longer assessment period, to perform risk analysis by lower class. Assets list include the selected asset, owner of the asset, user groups and authorization of group.

Table 2. Asset evaluation grade

Description / Grade	Confidentiality	Integrity	Availability
Class 5	Leakage/damage of the information can cause critical influence on the task or personnel.	Distortion/damage to the information is critical to the task.	Validated access toward information, system and network should be available at all times.
Class 4	Leakage/damage of the information can cause considerable influence on the task or personnel.	Distortion/damage to the information causes some problem on the task given.	Recovery must be complete within 4 hours should a crisis occur
Class 3	Leakage/damage of the information can cause minimal influence on the task or personnel.	Distortion/damage to the information has some influence and implication on the task given.	Recovery must be complete within 8 hours should a crisis occur
Class 2	Information open to officials within the organization.	Distortion/damage to the information has minimal influence on the task given.	Recovery within 12 hours required.
Class 1	Public information	Distortion/damage to the information has virtually no influence on the task given.	Availability is not important; minimal influence on the task.

3.1.4 Asset Evaluation

Asset value is assessed by the following criteria:
① Importance of the information
② User of the information
③ Potential damage infliction if the data is distorted and lost.
Recovery cost of the data if the data is destroyed.
The value of the Selected Asset is assessed by the following criteria:
- Importance of the information.
- User of the information.
- Potential damage infliction if the data is distorted and lost.
- Recovery cost of the data if the data is destroyed.

Also, same assets can have different asset values (i.e. servers), based on the task each asset is assigned to.
Three steps of asset evaluation process have been assigned to reflect such conditions. The suggested model is taking the qualitative method, and each evaluation per process is graded in 5-point scale. Thus, in asset evaluation process, final result is reached by first analyzing the information asset by confidentiality, integrity and availability, multiplying the analysis result by task importance, then dividing the end result by 5. In short, it is the contribution to the task of the organization that shows the value of information assets.

Table. 3. Asset evaluation process

Steps	Task
Step 1	Evaluating pure asset value→ Assessment based on the evaluation chart
Step 2	Evaluating task importance → Importance of the task process to which the asset is assigned is reflected.
Step 3	Evaluating asset value→ Task importance is directly proportional to the pure asset value grade. 5-point scale is applied to reflect by qualitative.
Evaluation	**(Pure Asset Value X Task Importance) / 5 = Contribution to the task of the organization per each Asset**

3.2 Threat and Vulnerability Assessment

Threats and vulnerabilities that could occur within the organization is calculated, and reflected on the assessment of the risk during this step.

3.2.1 Identifying the threats

Threat against the information asset is assessed by the following procedure:
1) The source of threat is classified by personnel computer, information system.
2) Threats are mapped out in top-down format
Reflect the working condition of the organization on the assessed threat, then use that result to set up the protective measures.

3.2.2 Threat evaluation

Threats are analyzed per each asset, based on the 5 criteria of threats. An example of damage potential, reproducibility, exploitability, affected users, discoverability. Same threat may have different threat assessment value, based on the value of information asset it is influencing. Also, the frequency of the threat is reflected on the threat evaluation. The following is the procedures for threat evaluation:
1) Average damage potential, reproducibility, exploitability, affected user and discoverability values is calculated.
2) Frequency of the threat and vulnerability is multiplied by the result #1.
3) The result from #2 is divided by the total number of threats.

Table. 4. DREAD Chart

DREAD	Grade
Damage Potential	100% ~ 80% (5) 60% ~ 80% (4) 40% ~ 60% (3) 20% ~ 40% (2) 0% ~ 20% (1)

3.2.3 Identifying the vulnerability

Vulnerability is assessed by the following procedure:
- Evaluate the vulnerability by disclosure, Integrity and denial of Service.
- Reflect the impact (calculated by threat/vulnerability mapping table) on the result #1
- Divide #2 by the total number of vulnerabilities.

Table. 5. Vulnerability evaluation chart

Vulnerability D.I.D.	Crisis	Grade
Disclosure	Confidentiality has been violated.	100% ~ 80% (5) 60% ~ 80% (4) 40% ~ 60% (3) 20% ~ 40% (2) 0% ~ 20% (1)
Integrity	Integrity has been compromised.	
Denial of Service	Availability has been infringed.	

3.2.4 Evaluating Vulnerability

The influence of the impact on the asset should be reflected on the analysis of the vulnerability.
Threat against the information asset is assessed by the following procedure:
1) The source of threat is classified by personnel/computer/information/system.
2) Threats are mapped out in top-down format.
3) The working condition of the organization is reflected on the assessed threat; the result is the basis on which protecti ve measures are set up.

3.3 Risk Analysis and Establish the Master Plan

3.3.1 Risk Evaluation

Risk is, in short, a damage potential a certain type of threat can cause through a specific vulnerability. Risk is evaluated by evaluating it based on standard risk assessment chart or multiplying the size of asset, the degree of threat and the degree of vulnerability.
Degree of Risk is calculated by the following procedure:
1) Related information assets are identified and separated.
2) Gathered results are assessed based on confidentiality, integrity and availability
3) Result #2 is multiplied by pure asset value and task

importance
4) Threat/vulnerability assessment is reflected on the result #3.
Final asset value is presented by integer, thus decimals are rounded off. Also, graded scales 1~5 are replaced by VL, L, M, H, VH. For instance, if Asset A has a confidentiality value of 3, High risk and Medium vulnerability, the degree of threat on Asset A is 7 according to the following chart.

The following procedure is for setting up a protective measures and master plan:
1) Degree of risk is assessed based on the analyzed assets, threats, vulnerabilities.
2) Acceptable Risk is excluded from result #1.
3)

Table 6. Risk Evaluation Production

Threat		Very Low					Low					Medium					High					Very High				
Vulner-ability		VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH
Value of Assets	1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9
	2	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10
	3	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
	4	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12
	5	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13

VL : Very Low, L : Low
M : Medium, H : High
VH : Very High

3.3.2 Risk Assessment

Risk assessment is carried out by the following procedure:
1) Risk of the asset is graded (in a certain scale.)
2) Assess the acceptable risk from the organization, based on the given budget and characteristics of the given task.

3.3.3 Security Measures

Security measures, which can minimize the risk on assets, are grouped by function then the budget and period is reflected on the master plan.

3.3.4 Establishing the Master Plane

Security measures, which can minimize the risk on assets, are grouped by function administrative, physical and technical analysis then the budget and period as assessed by risk-analysis team is reflected on the master plan.

4. Conclusions

As stated above, the suggested model was designed to minimize the existing drawbacks from risk analysis models currently at work. To achieve that goal, it evaluates the asset value by multiplying the pure asset value with task importance, then dividing it by 5.
1) Evaluating the threat by multiplying threat analysis result with the frequency of the crisis.
2) Reflecting the impact of such crisis on the vulnerability.
3) Evaluating the degree of risk by multiplying the result .B y applying the suggested model to the actual projects, you c an expect shorter the time required performing the assessme nt and also more effective risk analysis and assessment res ult as well.

References

[1] All in one "*CISSP Certification*" Mc Graw Hill, 2000.
[2] Gray Stonebumer, Alice Goguen, and Alexis Feringa "*Risk Management Guide for Information Technology Systems*", NIST, Oct., 2001.
[3] Harold F. Tipton and Micki Krause, "*Information Security Management Volume 3*", 4th Edition, Auerbach Publications, pp. 417-430, 2002.
[4] ISO 7497-2, "*Information Processing Systems - Open Systems Interconnection*" - Basic Reference Model - Part 2 : Security Architecture
[5] Lee MoonGoo, "*A Risk Analysis Methodology for Information Systems Security Management*" IEEK, CI. Nov. 2004.
[6] Microsoft Haifa R&D Center, "*Building Secure Software*", Oded Sacher, 2002.
[7] Sandra Olandersson, "*Threats in Information Security using threat Tree Analysis*", Jeanette Fredsson, 2001
[8] TTA, "*Risk Analysis and Management Standards for Public Information Systems Security- Risk Analysis Methodology Model*", 2000.