THE MITIGATION MODEL FOR MINIMIZATION OF IT OPERATIONAL RISKS

Lee, Seong.il

Graduate School of Dongguk University, Korea [1]

Lee, Youngjai

Professor, Dongguk University, Korea [2]

Keywords

Mitigation Model, IT Operational Risk, Influence Diagram, Incident Prevention Guidemap

Abstract

Organizations and customers lose if business activities are discontinued by an incident of information systems under the current business environment because they pursue real time enterprise and on demand enterprise. The loss includes the intangible decline in brand image, customer separation, and the tangible loss such as decrease in business profits. Thus, it is necessary to have preparedness in advance and mitigation for minimization of a loss due to the business discontinuity and IT operational risks.

Introduction

Business operations are deeply dependent on Information Technology infrastructure regardless of scale and activities of private sectors as well as public sectors. The advanced technology for performance and improvement of IT tends to be continuously applied to the business operations in organizations.

Although the new technology provides some improved results to the business, problems are exposed in response capabilities of IT operational risks which accumulate through operational experience in long term. Therefore, a strategy concerning IT operational risks has been currently focusing on the emergency response after a crisis occurred. As a result, most organizations have operated disaster recovery systems. However, papers show that a mitigation activity is the best alternative to other methods.

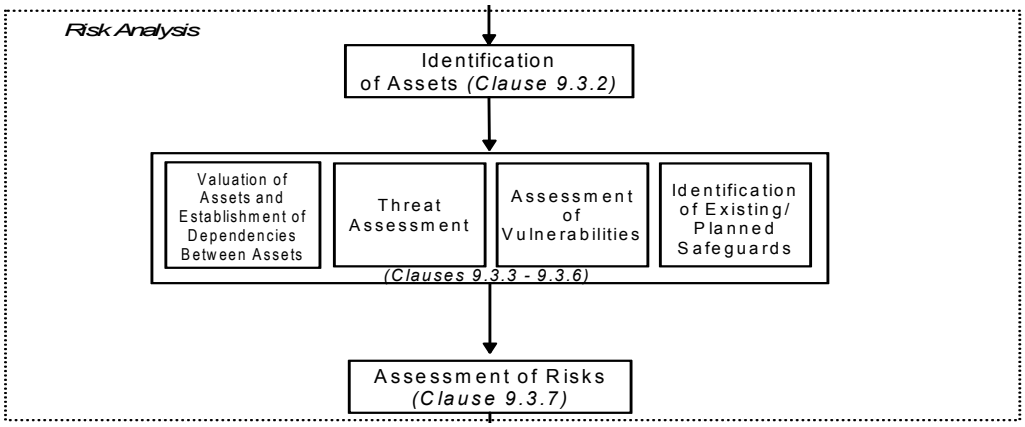
In order to solve the problem, this paper suggests a mitigation model that is able to prevent IT operational risks. The model will be represented by a network model which is composed of the three items as following:

1. Causes, attributes, indicators of an operational risk.
2. A periodic time through an analysis of historical data.
3. An index or a regulation related to the examination of causes of an operational risk.

[1] kidd@dongguk.edu
[2] yjlee@dongguk.edu

Literature Review

The mitigation model is designed on the basis of IT risks assessment. The process of risk analysis and evaluation refers to ISO/IEC TR 13335-3, Guidelines for the Management of IT Security (GMITS): Part 3 - Techniques for the Management of IT Security [1] as showed in [Fig. 1].



[Fig. 1] Process of Risk Analysis and Evaluation in GMITS

- Identification of Assets: the following assets to be protected are selected and listed below
  - information/data (e.g. files containing payment details, product information)
  - hardware (e.g. computer, printer)
  - software, including applications (e.g. text processing programs, programs developed for special purposes)
  - communications equipment (e.g. telephones, copper cable, fibre),
  - firmware (e.g. floppy discs, CD Read Only Memories)
  - documents (e.g. contracts)
  - funds (e.g. in Automatic Teller Machines)
  - manufactured goods
  - services (e.g. information services, computing resources)
  - confidence and trust in services (e.g. payment services)
  - environmental equipment
  - personnel
  - mage of the organization
- Valuation of Assets and Establish of Dependencies Between Assets
- Threat Assessment: factors such as errors, omissions, fraud, theft, employee sabotage, loss of physical and infrastructure support, malicious hacking, malicious code, and industrial espionage are identified. And the following items are measured in terms of the factors.
  - the threat frequency (how often it might occur, according to experience, statistics, etc.), if statistics etc. can be applied,

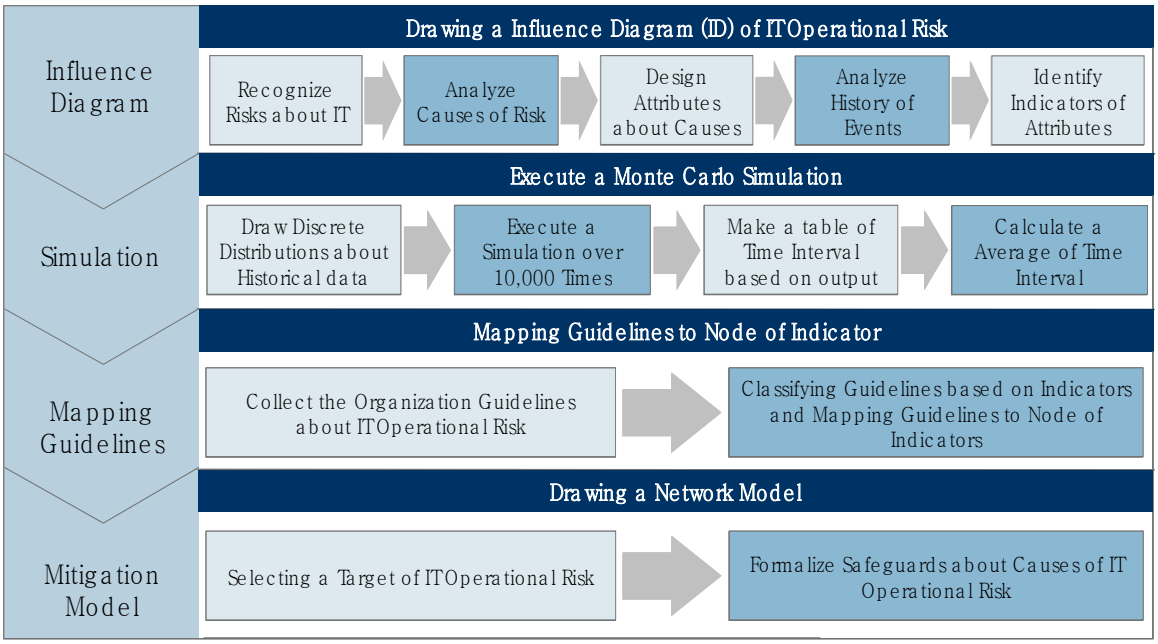
  - the motivation, the perceived and necessary capabilities, resources available to possible attackers, and the perception of attractiveness and vulnerability of the IT system assets for the possible attacker to deliberate threat sources
  - geographical factors such as proximity to chemical or petroleum factories, in areas where extreme weather conditions are possible, and factors that influence human errors and equipment malfunction that create accidental threat sources

- Assessment of Vulnerabilities: the weak points that exist in the physical environment, the organization, the procedures, the personnel, the management, the administration, the hardware, the software, and the communications equipment are identified and evaluated. The following are examples:
  - unprotected connections (for example: to the Internet)
  - untrained users
  - wrong selection and use of passwords
  - no proper access control (logical and/or physical)
  - no back-up copies of information or software
  - location in an area susceptible to flooding
- Identification of Existing/Planned Safeguard
- Assessment of Risks: the result of this step should be a list of measured risks for the impact of disclosure, modification, non-availability, and destruction for each of the assets of the considered IT system.

The Mitigation Model

The mitigation model is developed using 4 steps as shown in [Fig. 2]. In step 1, the causes of IT operational risks are first identified. Also, the indicators which are significant among the causes are found through analyzing the historical events of organizations. Step 2 produces a time interval which indicates the time to monitor the purpose of risk prevention using a simulation technique. Step 3 explains how the organizational guidelines and regulations map the causes and indicators. Finally, step 4 formalizes the causes, the time interval, and the guidelines through a network model. The model is called the mitigation model of IT operational risks.

This model development can be derived from the process of risk analysis and evaluation of GMTIS. However, a special feature of the model focuses on hazards related to business operations rather than ones related to assets in risk analysis. The model is necessary for business continuity.



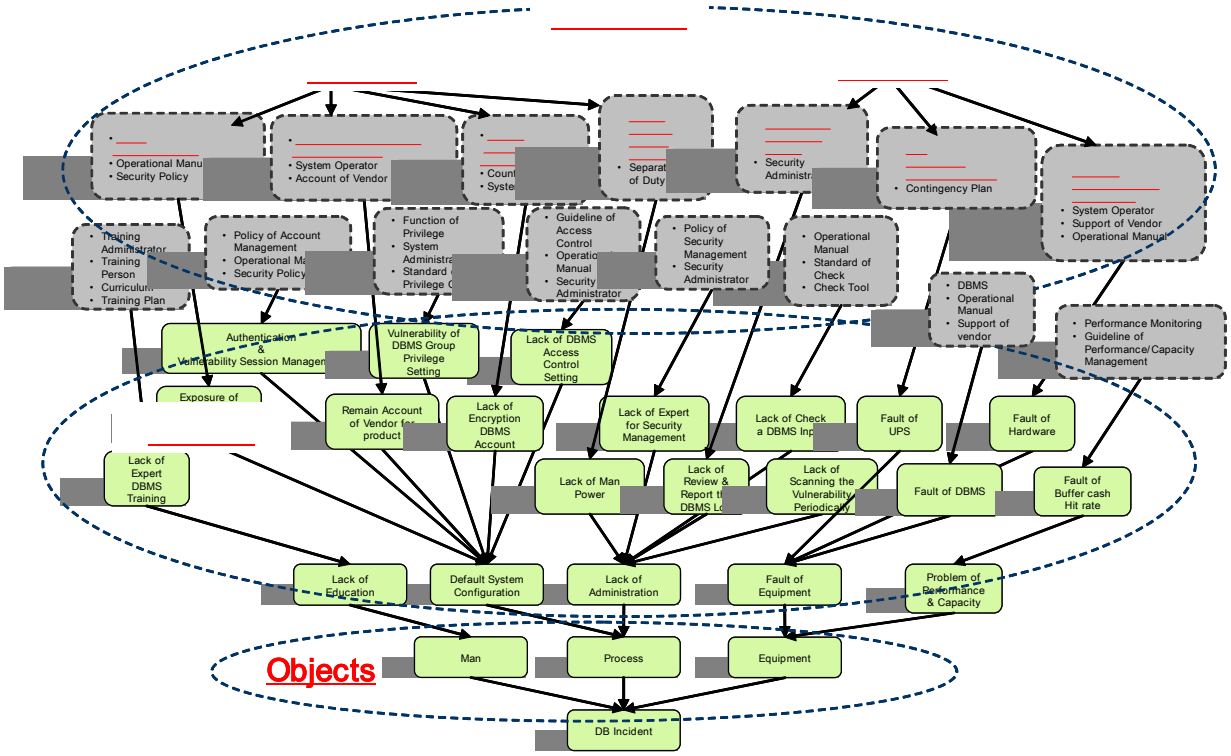
[Fig. 2] The Process of Mitigation Model Development

1. Hierarchical Structure of Incident Analysis

IT operational risks are caused by interruption of business operations. Objects, causes, and attributes of a risk are sequentially identified. Relations among those elements are represented by an influence diagram [2]. [Fig. 3] shows a diagram which displays the objects, the causes, and the attributes with regard to a database incident.

First, objects related to an incident are identified and represented by a tree structure. Second, the objects are classified into many causes and sub-causes in order. Third, the final sub-causes include a few attributes. Finally, one or two indicators which are significant among the attributes are selected by analyzing the organizational historical data of a risk.

This diagram which displays relations among attributes, causes, and objects provides some information to mitigate a risk. For instance, this diagram shows what the operation manager monitor prioritizes to prevent a risk.



[Fig. 3] An Example to Show a Relation of Objects, Causes, and Attributes about a Database Incident

2. Incident Prevention Guide map

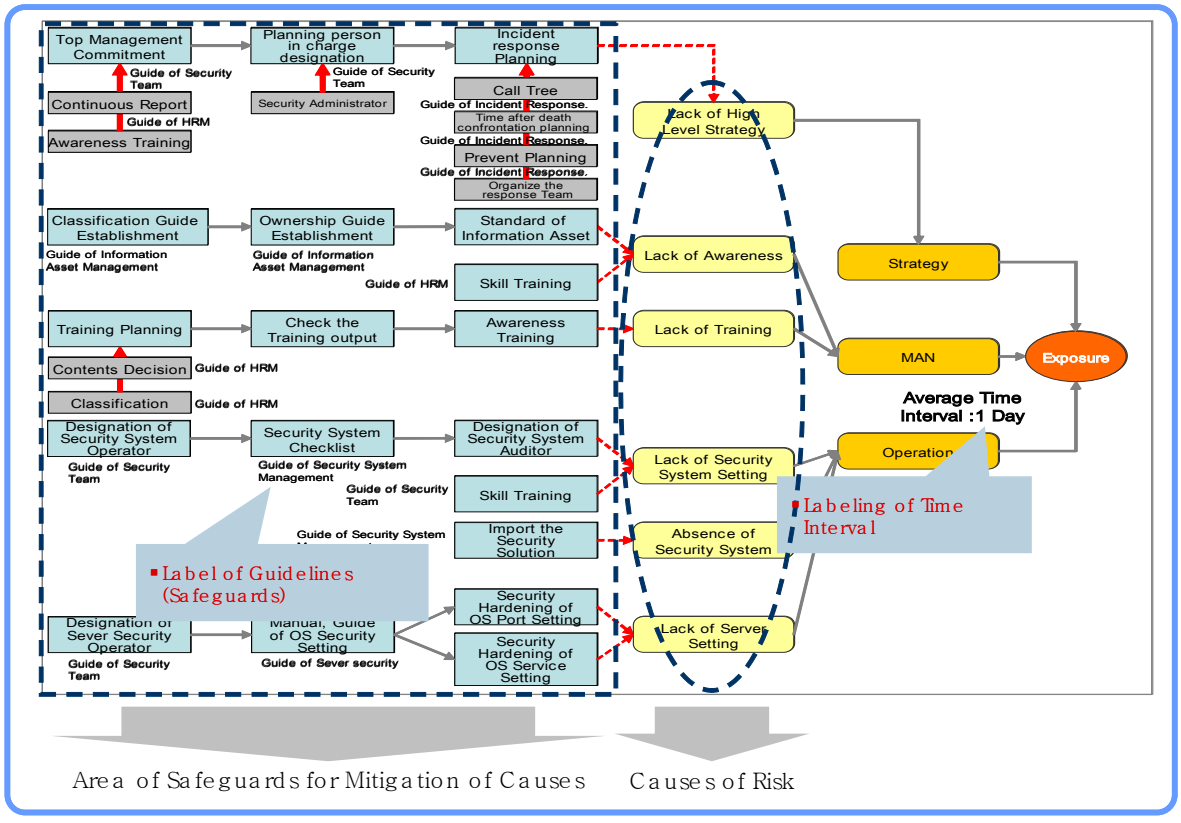
Incident prevention guide map (mitigation model) is represented by a network model [3] shown in [Fig. 4]. This guide map includes a time interval and guideline as well as causes about an incident.

First of all, the time interval is a periodic time to check paths (where the model is composed of each path) in order to prevent an incident. The time interval calculates based on the historical records of a specific risk in the organization. If there is not enough data, the Monte Carlo simulation [4] (with discrete distribution made by some records) can be used to produce the time interval.

Secondly, the organization develops policy, regulations, index, and guidelines to inspect some incidents which will occur in the future. However, the problem is when and how those indexes will be used appropriately. The guide map solves the problem.

Finally, the influence diagram shows a hierarchy structure which illustrates indicators, attributes, causes, and objects about an incident. By analyzing the diagram, safeguards (to mitigate according to the causes) are designed. A cause formalizes a path which gathers the safeguard, the guideline and the periodic time together. Thus, an operation manager checks this path to prevent an incident. If an incident occurs, the path will be investigated. Also, the data will be stored according to the diagram's hierarchy structure.

.



[Fig. 4] An Example of Incident Prevention Guide map

Results – Expecting Effect

The following are expected effects if the model is developed:

1. Minimization of loss through an inspection in advance.

The incident prevention guide map should be contributed to mitigate an incident of IT operation by showing a procedure of examination periodically. That is, the manager figures out which attributes and safeguards should be checked upon on a time based on a cause related to an incident.

2. Record accident data in specific detail.

Most organizations tend to be negligent to record any accident data. There would be no effectiveness in accumulation because accident data in IT operations may be poor. If an operational risk occurs, objects, causes, attributes, and other aspects will be documented according to the structure of the influence diagram and the incident prevention guide map. The records will be used to calculate a periodic time and to produce a living incident prevention guide map.

The paper leads to conclude that organizations can mitigate IT operational risks if a hierarchy structure of risk analysis and an incident prevention guide map will develop according to a category such as IT security, Server, Network, and Application etc.

References

1. ISO/IEC TR 13335-3, Guidelines for the Management of IT Security (GMITS): Part 3 - Techniques for the Management of IT Security
2. Influence Diagram
3. Network Model
4. Monte Carlo Simulation
5. Butler, J., Contingency Planning and Disaster Recovery Strategies, Computer Technology Research Corp., 1994.
6. Carlton, R. A., "Telecommunications Disaster Planning," DATAPRO, 1994.
7. CCTA, An Introduction to Business Continuity Management, The Government Centre for Information Systems, 1995.
8. Colleen Gorden, "How to Cost Justify a Business Continuation Plan to Management, Disaster Recovery Journal, Vol 13, Issue 6, 2000, http://www.drj.com
9. Commission of the European Communities Security Investigations Projects, Risk Analysis Methods Database, Project S2014 - Risk Analysis, Report Number 9744(S2014/WP08), Version 1.0, Jan. 1993.
10. Jackson, Carl B., "Business Continuity Planning: The Need and the Approach," DATA PRO, February 1994, 101-109.
11. Leo A. Wrobel, "Conduct a Hard-hitting Business Impact Analysis", Disaster Recovery Journal, Vol 11, Issue 4, 1998, http://www.drj.com
12. Moore, Pat, "How to Plan for Enterprise-Wide Business and Service Continuity," Strohl Systems, 1997.
13. Patricia A. P. Fisher, "How to Conduct a Business Impact Analysis", Disaster Recovery Journal, Vol 9, Issue 3, 1996, http://www.drj.com

14. Mark Jablonowski, "Prioritizing Disaster Recovery Plan using risk maps",Disaster Recovery Journal, Vol 13, Issue 3, 2000, http://www.drj.com
15. Keith Baker, "New Challenges Face Business Continuity Planners", Disaster Recovery Journal, Vol 13, Issue 5, 2000, http://www.drj.com
16. Scott Ream, "How Mature Is Your Business Continuity Program?", Working Paper, 2002.
17. Smith, M. and J. Sherwood, "Business Continuity Planning," Computers & Security, (Vol. 14, No. 1) Jan. 1995, pp.14-23

Author Bibliography

Mr. Seongil Lee, Doctoral candidate, Dongguk Universiry, Seoul, Korea

Concern area: Security, Business Continuity, Disaster Management

Dr. Youngjai Lee, Professor, Dongguk University, Seoul, Korea

Concern area: Business Continuity, Intelligent Decision Support, Information Management