A Practical Security Risk Analysis Process and Tool for Information System

YoonJung Chung*, InJung Kim*, and DoHoon Lee*

Abstract: While conventional business administration-based information technology management methods are applied to the risk analysis of information systems, no security risk analysis techniques have been used in relation to information protection. In particular, given the rapid diffusion of information systems and the demand for information protection, it is vital to develop security risk analysis techniques. Therefore, this paper will suggest an ideal risk analysis process for information systems. To prove the usefulness of this security risk analysis process, this paper will show the results of managed, physical and technical security risk analysis that are derived from investigating and analyzing the conventional information protection items of an information system.

Keywords: Risk Management, Asset, Threats, Vulnerability, Countermeasure

1. Introduction

Information systems are experiencing speedy change owing to the recent evolution of the ubiquitous computing network. For this reason, information system products are showing diversification and rapid change. This constitutes an irresistible social trend under which information systems have forged a closer and closer relation with our life, diffusing rapidly the idea that "information is an asset" in our society. Meanwhile, the supply of information protection systems has dropped behind the development of information system technology. This has brought about increasing damage and augmented the demand for information protection consulting to prevent such damage. However, the various conventional information technology security management methods have not undergone comprehensive classification, with insufficient research conducted on the evaluation standards system. As such, specific risk analysis processes are applied without considering the particularities of each country.

Risk analysis is an important stage that constitutes a base for managing information protection and risk in the information protection consulting process. Risk analysis is an evaluation stage for risk management. Since risk management requires accurate evaluation as a prerequisite, risk analysis is an indispensable aspect in managing information protection. To provide consulting efficiency and the efficient use and management of analysis data, automated tools must be used in the risk analysis process. Considering a variety of demands for security risk analysis, this paper will propose a security risk process that takes into consideration its tooling so that it can be applied to an information system, instead of suggesting theoretical or business administration-based risk analysis processes. The remainder of this paper is organized as follows. In the next section, the related work and theoretical background concerning a risk analysis algorithm is presented. We describe the conventional results and offer a risk analysis in Section 3. In Section 4 we present the risk analysis processes of our proposed model and, finally, we offer our conclucions in Section 5.

Manuscript received September 30, 2005; accepted November 15, 2005.
Corresponding Author: In-Jung Kim
* Electronics and Telecommunications Research Institute, Daejeon, Korea ({yjjung, cipher, dohoon}@etri.re.kr)

2. Related Work

A risk analysis process comprises such processes as asset identification, threat analysis, vulnerability analysis and the establishment of safeguards. Risk analysis processes such as BS7799, GMIT and CSE define the procedure and explain the method for implementing it. Accordingly, this section examines the classification of risk as defined in each process.

- **GMITS (ISO/IEC 13335)**: GMITS[1], established as an IO standard, presents a framework for the procedure of risk analysis which is a starting point for information security management.
- **BS7799**: BS7799 [2] is a risk analysis methodology developed by the BSI (British Standards Institute) in Great Britain. It has developed into the standard ISO17799.
- **Risk analysis methodology by CSE**: This methodology from CSE (Communications Security Establishment)[3] in Canada comprises the processes for analyzing threats and risks, identifying hazards, measuring the level of related risks, and defining risk-generating factors, as well as the measures to be taken against the risks.
- **BDSS Bayesian Decision Support System [4])**: Risks are classified normally into physical (entry control,

environmental control, etc.), technological (hardware, OS, applications, network, DB, etc.), and management (security control, computing personnel/user management, security policy documentation, accident response, etc.).

- **FIPS 65 (NIST Document [5])**: Those threats and vulnerabilities related with the assets identified through asset analysis, as the subject of risk analysis, are analyzed. Following areas should be investigated to analyze threats and vulnerabilities.
- **GAO (Information Security Risk Assessment [6])** : GAO combines five vulnerability areas (individual, equipment and application, communication, software and OS) and four damage types to create a classifycation list.

3. Conventional Results of Risk Analysis

Risk analysis must be classified in terms of managing the physical and technological dimensions so that security risk analysis can be conducted. Conventional risk analysis [7] evaluates the level of risk to assets and performs detailed risk analysis by analyzing upper-level risks or using basic controls. For this reason, conventional analysis is incapable of analyzing the vulnerabilities in a comprehensive way. Since most risk analysis methodologies and security control items were developed before the development of information systems, data on the process of the introduction and evolution of security systems is insufficient. Therefore, simple security control items do not guarantee an accurate risk analysis. For instance, conventional control items focus only on whether a security organization is run at all, or on how many security staff an organization has. Also, encryption and the correct arrival of information also formed part of the criteria for judgment [8] in terms of the technological control items. These security control items do not allow us to determine the level of risk to the evolving information system. Therefore, it is necessary to find and present new control items [9] and vulnerabilities.

Managing position

1. Lack of security control/missions.
2. Lack of security personnel.
3. Lack of security control items in the security policies/rules/guidelines.
4. Low level of security training for administrators.
5. Users' low security awareness.
6. Developers' insufficient security design.
7. Operators' inexperienced security management.
8. Introduction of unclear security system.
9. Inter-organizational conflict.
10. Disagreements between upper managers and relevant working employees.

Physical position

1. Accidents caused by natural calamities like fire/earthquake/flooding.
2. Insufficient response against artificial attacks including terrorism/war.
3. Insufficient response against attacks causing physical damage to electronic equipment.
4. No way for tapping on the line.
5. Lack of control against unauthorized user's system access.
6. Malfunctions and down times in servers/DBs.
7. Insufficient geographical safety of back-ups.
8. Intentional destruction and leakage of audit recording media.
9. Information leakage and error due to user's carelessness.
10. System overload from inadequate power supply and ventilation.

Technological position

1. Migration from legacy system to new system.
2. Inter-working between different types of equipment.
3. Difference between security algorithm and key control because of the introduction of the security system.
4. Reliability in the OS upgrade/security patch.
5. Exposure of privacy protection through central control.
6. Source code bugs in applications.
7. Setting of complex rules for router/intrusion blocking/ invasion detection system
8. System shutdown by cyber terrorisms/attacks.
9. Limited/impossible system control due to viruses/worms.
10. Errors/exposures of information and DB.

4. Risk Analysis Process

As informatization spreads, dependence [10] on the information system, threats to assets, and vulnerability risks all increase, leaving organizations exposed to information leakage and attacks on the system security. The risk analysis process evaluates the risk of exposure to leakage and attack, and calculates the degree of risk. In other words, the risk analysis process is designed to diagnose the risks of organizations and prevent information leakage and security attacks [11]. The process analyzes and evaluates the assets of organizations, the threats posed to those assets, the vulnerability of the assets, and security countermeasures, thereby contributing to reducing the risk level of organizations. The ultimate objectives of the risk analysis process are to consider the threats to the information system and assess the vulnerability of the information system and its asset value, to analyze and evaluate the asset risk level, to provide countermeasures for removing, accepting or avoiding risk, and, finally, to build a safe environment in which to operate the information system.

4.1 Risk analysis algorithm

The primary algorithm of the risk analysis process proposed by this paper is as shown in table 1, fig. 1, and is characterized by the following:

- **Top-down risk analysis**: This paper analyzes risk by dividing it into upper level risk and lower level risk. In the upper level, upper-level evaluation projects are managed, and the security management of evaluation-targeted organizations is assessed through a survey and interview related with security management based on BS7799. In the lower level, a detailed evaluation is performed. Since upper-level evaluation is carried out primarily through a web survey, it enables independent analysis and evaluation, thereby dispensing with the need for expert analyzers. Evaluation-targeted organizations can perform periodic upper-level evaluation (as in the case of regular auditing) and carry out lower-level evaluation (as in the case of irregular auditing) according to their risk trend. Upper-level evaluation is preliminary. If upper-evaluation provides excellent results, lower-level evaluation can be held back. Therefore, the algorithm can reduce an organization's security management expenditure.

Table 1. Risk Analysis Algorithm

Index	Calculated rules	Resulted range
Level of asset a_i	Delpi	1,2,3,4,5
Cost of asset a_i (ac_i)		Real
Level of Threat a_i (t_{ij})	Delpi	1,2,3,4,5
Level of Vulnerability a_i (v_{ij})	Delpi	1,2,3,4,5
Level of Risk a_i (r_i)	Delpi	1,2,3,4,5
Total asset cost (AC)	$=\sum_{i=1}^{n} ac_i$	Real
Total asset cost level (A)	$=(\sum_{i=1}^{n} a_i)/n$	$1 \cdots 5$ (Real)
Threat of asset a_i (TV_i)	$=(\sum_{j=1}^{m} t_{ij})/m$	$1 \cdots 5$ (Real)
Threat level of asset a_i (TL_i)	$Int(TV_i)$	1,2,3,4,5 (Integer)
Vulnerability of asset a_i (VV_i)	$=(\sum_{j=1}^{m} v_{ij})/m$	$1 \cdots 5$ (Real)
Vulnerability level of asset a_i (VL_i)	$Int(VV_i)$	1,2,3,4,5 (Integer)
Risk value of asset a_i (RV_i)	$=a_i+TL_i+VL_i$	$3 \sim 15$ (Real)
Risk level of asset a_i (RL_i)	$=1,\ 3 \le RV_i < 5$ $=2,\ 5 \le RV_i < 8$ $=3,\ 8 \le RV_i < 11$ $=4,\ 11 \le RV_i < 14$ $=5,\ 14 \le RV_i < 15$	1,2,3,4,5 (Integer)
Total risk level of asset (RL)	$=(\sum_{i=1}^{n} RL_i)/n$	1,2,3,4,5 (Integer)
Safeguard rate of asset a_i (E_i)	$=(7.5 \times RV_i - 17.5)/100$	$0.05 \sim 0.95$ (Real)
Safeguard cost of asset a_i (AD_i)	$=ac_i \times E_i$	Real
Total Safeguard cost of asset (AD)	$=\sum_{i=1}^{n} AD_i$	Real

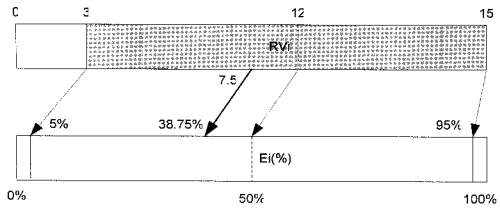

Fig. 1. Proposed Risk Analysis Boundary and Index

- **The Enhancement of the function supports risk evaluation project management**: The algorithm enhances risk evaluation project management functions like management of the risk evaluation team, management of the evaluation participants, understanding of the general situation of organization, and investigation of the information system. Based on this, a risk evaluation project involving many participants can be managed smoothly.
- **Perspective on threats and vulnerability**: The process sees threats and vulnerability as a difference in "perspective". Some assets face many threats, each of which implies the "vulnerability" factor that a given threat (i.e. attack) can be realized. Therefore, vulnerability is the realizability of a threat.
- **ATVR type standard process**: The Asset - Threat - Vulnerability - Risk (ATVR type) process is used most widely. It is the de-facto standard process of risk analysis.
- **Interview support function (questionnaire handling)**: In upper-level evaluation, there is a questionnaire handling process for security management and an interview process for examining core assets. Through these processes, an organization's security matters can be assessed simply.

4.2 Primary functions

The process includes management functions such as log-in (necessary to users), DB management, planning for risk analysis, web surveys, analysis of survey results based on the results saved in DB, and upper-level security level evaluation. Also, the process provides functions such as asset evaluation, threat evaluation, vulnerability evaluation and the provision of security countermeasures through an analysis of lower-level risks as determined by the results of an upper-level survey. Moreover, the process provides such evaluation engines as an upper-level risk evaluation engine,

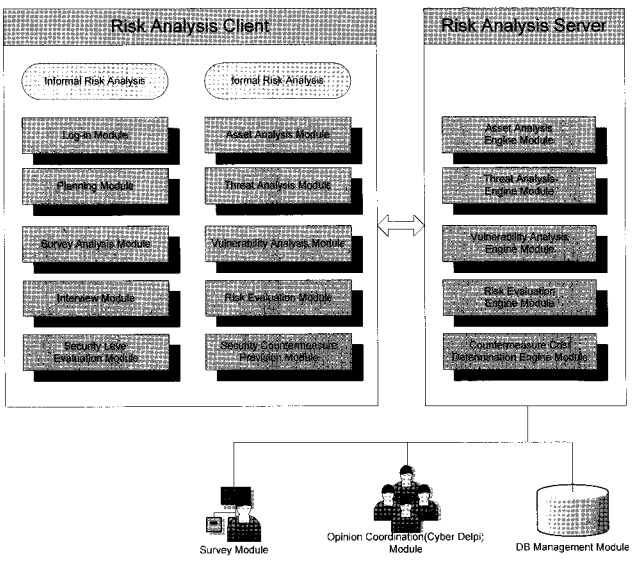

Fig. 2. Proposed Risk Analysis Process

an asset evaluation engine, a threat evaluation engine, a vulnerability evaluation engine, a risk evaluation engine and a security countermeasure cost determination engine. Each of these functions saves data in and loads data from open DBs such as common DB and reference DB, and closed DBs such as provisional DB and evaluation DB. The whole framework of the risk analysis process is as shown in fig. 2. The risk analysis process comprises client, DB, and web server. Each module has the following functions.

Informal Risk Analysis

- Log-in module: This module authenticates users via the entered user ID and password, and provides role-based access control which limits users' functions according to their authenticated roles.
- Planning module: The planning module creates new projects, enables project information entry, selects the evaluators and participants participating in a given project, and provides the entry of information on relevant evaluation-targeted organizations.
- Survey analysis module: This module loads the results of a web survey from DB, analyzes them, and allows a print-out of the survey form.
- Interview module: This module provides the function of interviewing evaluation-targeted organizations and allows the entry, saving and print-out of the interview.
- Security level evaluation module: This module synthesizes the results of a survey and the interviews conducted in the upper-level process, and determines the upper-level risk level according to a predefined upper-level risk analysis measurement.

Formal Risk Analysis

- Asset analysis module: This module evaluates the assets of an evaluation-targeted organization, and provides the function of selecting primary assets subject to evaluation through a data survey and asset examination of the evaluation-targeted organization. Also, the module has the function of entering and evaluating the value and level of the relevant assets. Asset value evaluation and asset level entry are performed by opinion coordination (cyber delphi).
- Threat analysis module: This module examines threats to the primary assets determined in the previous stage. The module evaluates the threats to the evaluation-targeted organization, and provides the function of determining, selecting and evaluating the threats to each primary asset. In entering the threat level, the threat evaluation value of each primary asset is determined through opinion coordination (cyber delphi) and the coordination of the opinions of evaluators and participants.
- Vulnerability analysis module: This module evaluates the vulnerability level of each threat to the primary assets that is determined in the previous stage. The module provides the function of evaluating the vulnerability of the evaluation-targeted organization, and performs the function of investigating, selecting and assessing each primary asset's vulnerability to the selected threats. In entering the vulnerability level, the module inputs each primary asset's vulnerability to each threat through opinion coordination (cyber delphi).
- Risk evaluation module: In this module, risk evaluation values are input automatically according to the predefined risk evaluation measurement based on the level values of asset analysis, threat analysis and vulnerability analysis, all of which are performed in the previous stage. Based on the input result values, the module outputs in a graph format the results of risk evaluation for each asset, each asset group and the evaluation-targeted organization in its entirety.
- Security countermeasures provision module: This module provides security countermeasures for each threat that is evaluated in relation to the assets. The module evaluates the cost of the provided security countermeasures, and allows the entry of results evaluated through opinion coordination (cyber delphi).

Risk Analysis Server

- Asset analysis engine module: This module provides an asset evaluation engine, and performs an algorithm for evaluating the primary assets when the asset evaluation module is running.
- Threat analysis engine module: This module provides a threat evaluation engine, and performs a threat evaluation algorithm when the threat evaluation module is running.
- Vulnerability analysis engine module: This module provides a vulnerability evaluation engine, and performs a vulnerability evaluation algorithm when the vulnerability evaluation module is running.
- Risk evaluation engine module: This module provides a risk evaluation engine, and performs an algorithm for risk level evaluation when the risk evaluation module is running.
- Countermeasure cost determination engine module: This module provides an evaluation engine for determining and analyzing the cost of security countermeasures, and performs an algorithm for determining the cost of security countermeasures when the security countermeasures provision module is running.

Consulting and DB

- Opinion coordination (cyber delphi) module: This module coordinates the opinions on the values through the designated stage, in relation to the entry of asset value and asset level in the asset analysis, entry of the threat level in the threat analysis, and determination of the cost of security countermeasures in the stage of security countermeasure provision.
- Survey module: A surveys is performed on the web. Its result values are saved in the DB through the web server.

- DB management module: This module loads from the DB the data processed in each stage or saves it in the DB.

Threats to the primary information system can occur internally as well as externally. Most of the structure is protected by physical security actions. However, it can be exposed to unknown attacks since the managed protection measures and technical protection measures are insufficient. In particular, most information system facilities use the public network, and are therefore exposed to threats from unspecified persons due to the nature of the public network. The proposed risk analysis process analyzes assets, threats, vulnerability and countermeasures in relation to the primary information system, identifies the risk per asset, calculates the risk level, and helps eliminate security risk factors. This risk analysis process is designed to reduce the level of risk to primary assets operated by an organization. Using the risk analysis process does not lead to improved security functions, but it does help risk evaluators to establish security countermeasures and policies. The proposed risk analysis process is useful in considering the assessment of asset value, the threats to and vulnerabilities of the information system, the evaluation of risk levels, and the provision of countermeasures for removing, accepting or avoiding risk. Finally, the process builds a secure environment in which to operate the information system. Following fig. 3, the tool menu implemented using the proposed risk analysis process is shown.

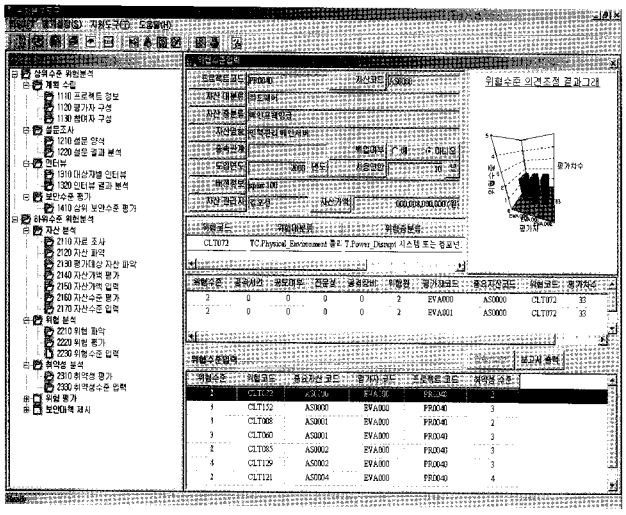

Fig. 3. Proposed Risk Analysis Tools Menu

5. Conclusion

A comparative analysis of the proposed risk analysis process and its conventional counterpart provides the following results.

- Problem of individual difference between evaluators: This is solved by the "Delphi method".
- Simplified risk evaluation function: A top-down security management and risk analysis strategy is adopted for cost-effective and "simplified" risk evaluation. Three survey methods are used.
- Standardized security management control (adaptability): Subject to BS7799 (ISO/IEC-17799) security control items.
- Function of reflecting the security policy of the evaluation-targeted organization: It is possible to change the evaluation standards (ex: asset value level) and weight according to the security policy of the evaluation-targeted organization shortly before evaluation.
- Function of information collection: Organization information is collected effectively using three survey functions and an individual interview function.
- Function of project management: The function of managing the evaluation project is enhanced (ex: evaluator management).
- Function of information input: Information can be input easily through GUI and the graphical method.
- The number of evaluation levels: Three or five stages are used. Universal rating criteria used in conventional methods are adopted.
- Asset investigation: Assets are visualized as icons using a graphic editor. Differentiated methods for classifying and valuating assets are employed.
- Threat investigation: A predefined technical threat list is used (ideal for CC based risk analysis). A differentiated threat level evaluation method is employed.
- Vulnerability processing: Vulnerability is defined as the "realizability" of threats.
- Evaluation method: The standards and methods for evaluation are differentiated for each evaluation-targeted attribute (in evaluating assets and threats). New risk evaluation methods are used (ex: Accurate evaluation can be provided through risk value using real values instead of integer values).
- Method of providing countermeasures: It is possible to use predefined countermeasures for each threat and consider the cost of implementing each countermeasure.

Since there are no guidelines for security evaluation in relation to the risk analysis process, it is virtually impossible to evaluate. NIST provides selection guidelines for the risk analysis process. A self-evaluation based on those guidelines has provided good results. Future studies are likely to analyze residual risk, inter-working with established vulnerability DB, and plans for building countermeasure DB in order to enhance the functions of the risk analysis process.

Reference

[1] ISO/IEC JTC 1/SC27, Information technology -

Security technique Guidelines for the management of IT security (GMITS) -Part 3: Techniques for the management of IT security, ISO/IEC JTC1/SC27 N1845, 1997. 12. 1.
[2] BSI, BS7799 - Code of Practice for Information Security Management, British Standards Institute, 1999.
[3] CSE, Threat and Risk Assessment Working Guide, Government of Canada, Communications Security Establishment, 1999.
[4] Staker, "Use of Baysian belief networks in the analysis of information system network risk," Information, Decision and Control, pp. 145-150, Feb. 1999.
[5] NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems. August 2001.
[6] GAO, Information Security Risk Assessment - Practices of Leading Organizations, Exposure Draft, U.S. General Accounting Office, August 1999.
[7] Solm, R., Guidelines to The Management of Information Technology Security, Vol.6, No.5, 1998,pp.221-223.
[8] Ministry of Finance and Economy Republic of Korea, Security Guide of Information Communication Infrastructure for the MOFE association organization , 2002. 11.
[9] http://www.sans.org/top20
[10] Hamoud, Chen, Bradley, "Risk Assessment of Power systems SCADA", Power Engineering Society General Meeting, pp. 764 vol 2, July 2003.
[11] Zorkadis, Karras, "Security modeling of electronic commerce infrastructure," EUROCOMM2000, pp. 340-344, MAY 2000.

YoonJung Chung
She received the BS and MS degrees in Computer Engineering from Sung-kyunkwan Univ. in 1997 and 1999, respectively. During 1999~2000, she stayed in Hanaro Telecom Inc. to manage the NMS, SMS and Security Solutions. And now she is working at the NSRI(National Security Research Institute). Her current research interest is in the area of information security, vulnerability analysis and risk analysis

InJung Kim
He received his M.E. degree in Electronic Engineering from Chungnam National University, Korea, in 1992. He joined ADD (Agency for Defense Development) in 1992 and remained until 2000. In addition, since 2000, he has working in NSRI (National Security Research Institute). He is currently a Ph.D. candidate of Computer Engineering in Sungkyunkwan University. His current research interest is in the area of information security, network security, risk analysis

DoHoon Lee
He received the BS and MS degrees in Computer Engineering from Hanyang Univ. in 1889 and 1991. During 1991~2000, he worked at ADD(Korea Agency for Defense Development). And now he is working at the NSRI (National Security Research Institute). His current research interest is in the area of information security consulting and cyber threat forecasting etc.