A Security Risk Analysis Model for Information Systems

Hoh Peter In[1,*], Young-Gab Kim[1], Taek Lee[1], Chang-Joo Moon[2], Yoonjung Jung[3], and Injung Kim[3]

[1] Department of Computer Science and Engineering, Korea University
1, 5-ga, Anam-dong, SungBuk-gu, 136-701, Seoul, Korea
{hoi_in,always,comteak,mcjmhj}@korea.ac.kr
[2] Center for the Information Security Technology, Korea University
1, 5-ga, Anam-dong, SungBuk-gu, 136-701, Seoul, Korea
mcjmhj@korea.ac.kr
[3] National Security Research Institute
62-1 HwaAm-dong, YuSeong-gu, 305-718, Daejeon, Korea
{yjjung,cipher}@etri.re.kr

Abstract. Information security is a crucial technique for an organization to survive in these days. However, there is no integrated model to assess the security risk quantitatively and optimize its resources to protect organization information and assets effectively. In this paper, an integrated, quantitative risk analysis model is proposed including asset, threat and vulnerability evaluations by adapting software risk management techniques. It is expected to analyze security risk effectively and optimize resources to mitigate the risk.

1 Introduction

As information communications (e.g., emails, chatting, messengers) or transactions (e.g., e-commerce, m-commerce) through the Internet are exponentially increasing, cyber security incidents (from a virus through email messages to cyber terrors to critical business information systems) are sharply increasing. A trend in cyber security vulnerabilities and virus attacks is shown in Figure 1.

In addition, according to the data of Common Vulnerabilities and Exposures (CVE) operated by MITRE, the number of incidents related with security vulnerabilities was 2,573 in April, 2, 2003. This is enormously increased in comparison with the 1,510 incidents in May, 7, 2001.

It is urgently needed to analyze the risk of the security vulnerabilities and prevent them effectively. The advantages of the security risk analysis are as follows:

- Enabling to develop secure information management
- Monitoring critical assets of organization and protecting them effectively
- Supporting effective decision-making for information security policies
- Establishing practical security policies for organizations
- Providing valuable analysis data for future estimation

However, it is quite challenging to develop a general, integrated security risk analysis model.

* Corresponding author.

D.-K. Baik (Ed.): AsiaSim 2004, LNAI 3398, pp. 505–513, 2005.

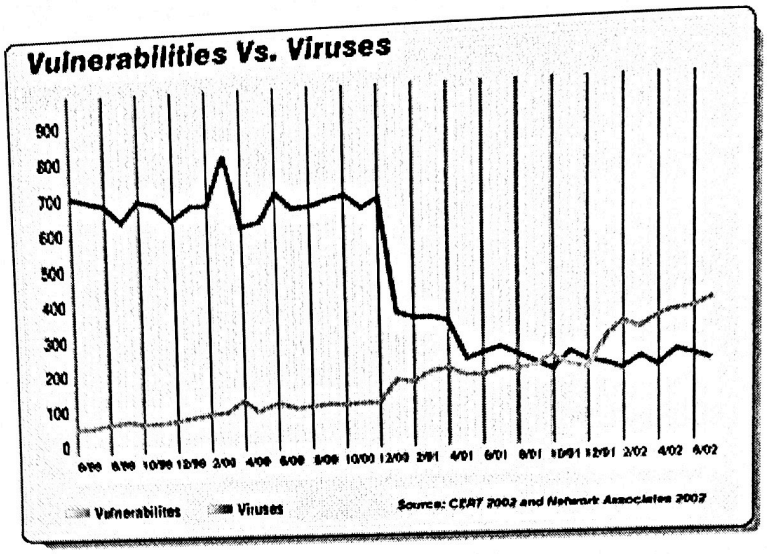

Fig. 1. Increasing Trend in Security Vulnerabilities & Viruses [CERT]

In this paper, a security risk analysis model is proposed by adapting a software risk management model used for the NASA mission-critical systems. Since security is one of software quality attributes, security risk needs to be investigated in the context of software risk. Security risk can also be defined by multiplication of loss (or damage) and the probability that the attacks occur by reinterpreting the concepts of loss and probability in the definition of software risk. However, the definition of loss and measurement of probability need to be adapted in the context of cyber security. In the risk analysis model, the loss (or damage) of assets in an organization due to the cyber security incidents is measured based on assets, threats, and vulnerability as shown in Figure 2. The detailed definition and model will be explained in Section 2. The related work is presented in Section 3, and the conclusion in Section 4.

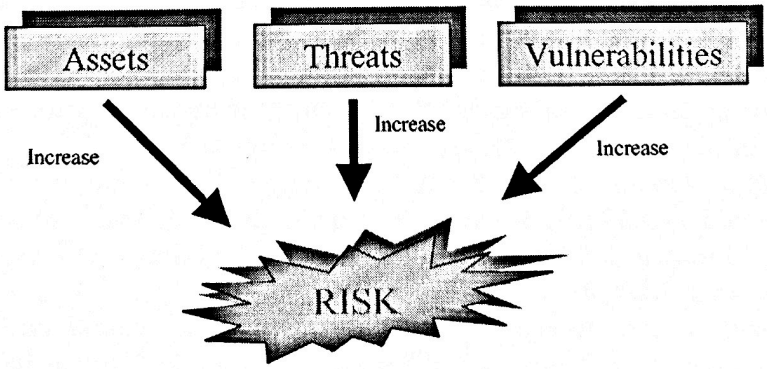

Fig. 2. Security Risk and Related Elements

2 Security Risk Analysis Model

The proposed security analysis model is shown in Figure 3. The four steps are proposed as a security risk analysis process. STEP 1 identifies the assets, threats and vulnerabilities of the target organization (Step 1.2 ~ 1.4) and evaluates them (Step 1.5). The outputs of Step 1 (i.e., assets, vulnerabilities, and threats) are used to analyze security risk in STEP 2. In STEP 3, suitable risk mitigation methods are applied

to decrease the potential threats for the assets. STEP 4 summarizes the initial risks (i.e., before the risk mitigation methods are applied), the types and cost of the risk mitigation methods, the residual security risks (i.e., after the mitigation methods are applied), and their Return-On-Investment (ROI). These helps the decision-makers optimize resources for minimizing security risks. The detailed steps are described in the following subsections.

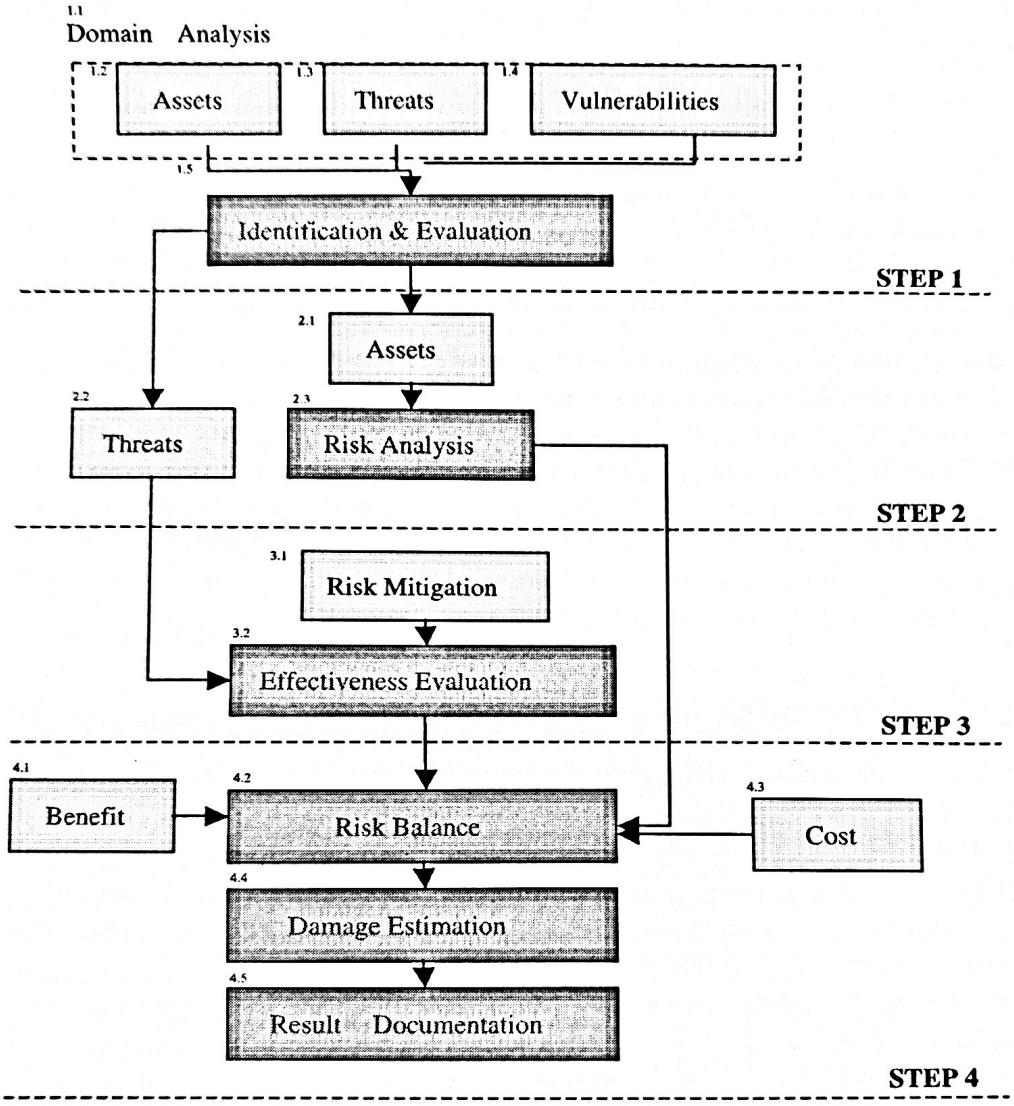

Fig. 3. Security Risk Analysis Model

2.1 Identification and Evaluation of Assets, Threats and Vulnerabilities (STEP 1)

Domain analysis in Step 1.1 is a domain-specific process for customizing the security risk analysis to improve the model accuracy. The types of assets, vulnerabilities, threats, and their probabilities are analyzed per domain. These of military or financial institutes are different from those of academic institutes.

Step 1.2 to Step 1.4 analyzes core assets of an organization (Step 1.2), potential threats (Step 1.3) and vulnerabilities (Step 1.4). The analysis includes what kinds of threats and vulnerabilities exist for a specific asset and the probabilities of threats that will occur. Table 1 shows a general classification of assets, threats, and vulnerabilities based on IT infrastructure.

Table 1. Classification of Assets, Threats and Vulnerabilities

Asset	Threat	Vulnerability
1. Information/Data 2. Documents 3. Hardware 4. Software 5. Human Resource 6. Circumstances	1. Human/Non-human 2. Network/Physical 3.Technical/Environment 4. Inside/Outside 5. Accidental/Deliberate	1. Administering Documents, Personnel, Regulation 2. Physical Circumstances or Facilities 3. Technical Hardware, Software, Communication/Network

Identification & Evaluation (Step 1.5) evaluates the values of the identified assets. Relative and absolute asset evaluation methods can be used. In a relative asset evaluation method, for example, the asset value ranges from 1 to 100. After the assets are sorted according to the order of their importance, we can give 100 to the first important asset in the list, and relative values to others according to the relative importance by comparing the first one. The sorting process may use a criterion or a set of criteria (e.g., monetary value or criticality to the organization missions). The results of the evaluated asset-value in this step are used in STEP 2.

2.2 Risk Analysis (STEP 2)

STEP 2 is the process of evaluating the security risk of the system by summing up all the risks of system components with considering the existing threats in the core assets of the organization and the degree of vulnerabilities per threat. Table 2 illustrates an example of Risk analysis.

Table 2. An Example of Risk Analysis

Probability	Threats Model		Assets Model / Vulnerability Model	AM_1 (PC)	AM_2 (Security Policy)	AM_3 (System S/W)	...
0.5	TM_1 (DoS)	→	VM_1 (unprotected major communication facilities)	0.9	0.6	0.8*	
0.7	TM_2 (Virus)	→	VM_2 (unfit network management)	0.6	0.5	0.9	
0.4	TM_3 (Cracking)	→	VM_3 (unprotected storage devices)	0.3	0.4	0.6	
	...		...				

As shown above, the security risk can be calculated by the relationship among the Asset Model (AM), Vulnerability Model (VM) and Threats Model (TM). TM and VM identify probability of potential threats and effect of vulnerability. We can calculate the security risk against each asset using the following equation:

$$RISK = Loss * Probability$$

The risk is defined as multiplication of loss and probability. In this point, the "Loss" means the decline of the asset value when an asset is exposed to some vulnerabilities. "Probability" means the probability of threat-occurrence from the corresponding vulnerabilities.

Let us take an example. There is TM_1 (e.g., DoS attack) as a threat against asset AM_3 (e.g., System S/W) shown in Table 2. The threat-occurrence probability is 0.5. When TM_1 occurs, VM_1 is an vulnerability to which asset AM_3 is exposed (in other words, TM_1 may be occurred due to VM_1). Therefore, 0.8 means the decline of the asset-value (AM_3) in this example. In this way, we can calculate the sum of risk related to the system S/W asset (column AM_3). The following result means that.

$$\begin{aligned} Total\ Risk\ of\ AM_3 &= 100 * (0.8 * 0.5 + 0.9 * 0.7 + 0.6 * 0.4) / 3 \\ &= 100 * 1.27 / 3 \\ &= 42.3 \end{aligned}$$

After all, when asset AM_3 is exposed to threat TM_1, the asset-value is decreased from 100 to 57.7 by the decline-rate 42.3 due to the corresponding vulnerability.

Note that one threat can be related to several vulnerabilities. Therefore, an efficient mapping algorithm is needed between threat and vulnerability in this step. The asset-value should also be considered as the value of money against the asset for estimating the amount of total damage in the organization.

2.3 Risk Mitigation and Effectiveness Evaluation (STEP 3)

STEP 3 is a process that shows the list of current security countermeasure in the organization, and selects suitable mitigation methods against the threats, then shows the effectiveness of the mitigation methods. Therefore, the manager who has charge of risk management can decide risk mitigation methods appropriate for the organization. The combination of risk mitigation methods affects on both the probability of threat-occurrence and the vulnerability-rate of assets, finally reduces the whole risk of assets in the organization. Table 3 shows an example that presents the effectiveness of risk mitigation methods.

Table 3. The effectiveness of Risk Mitigation Methods

Mitigation Method / Vulnerability Model	Vaccine	Smart Card	Firewall	...
VM_1 (unprotected major communication facilities)	0.2	0.6	0.1*	
VM_2 (unfit network management)	0.6	0.5	0.5	
VM_3 (unprotected storage devices)	0.3	0.2	0.1	
...				

As shown table 3, we can reduce the vulnerability-rate of VM_1 (e.g., unprotected communication facilities) to 0.1* with the risk mitigation method, firewall. Generally applying a risk mitigation method to some vulnerabilities can reduce the rate of not only one vulnerability but also several related vulnerabilities simultaneously. Furthermore we can get the rate of risk reduction effectively with considering which vulnerabilities can be affected by selecting some risk mitigation methods (step 3.2). As a result, in the above example, the whole amount of risk reduction after applying the risk mitigation method firewall is as follows: (under the assumption the asset value is 100)

$$\begin{aligned} RISK &= 100 * (0.1 * 0.5 + 0.5 * 0.7 + 0.1 * 0.4) / 3 \\ &= 100 * 0.44 / 3 \\ &= 14.7 \end{aligned}$$

The general classification of risk mitigation methods, which can be applied to IT infrastructure, is as followings:

- Access Control: Recognition of a organism, Physical Media(Smart Card), Authentication System based on Password, etc.
- Password Control: Public Key Infrastructure(PKI), etc.
- Internet Security Control: Invasion Detection System(IDS), Firewall, Vaccine, etc.
- Application Security Control: database security, system file security, etc.
- Physical/Environmental Security Control: facilities security, institution security, etc.

The manager of the organization can select and combine the risk mitigation methods under consideration of what asset is important relatively and how mush budget for risk management the organization has (Step 3.1).

2.4 Damage Estimation and Reporting Result (Step 4)

Risk Balance (Step 4.2) concludes the final estimation against the risk calculated Step 2 and 3. In this step, The questions are investigated for the risk management such as *What kind of threats can be reduced? What are residual risks if the risk mitigations are applied? What is the ROI of each risk mitigation?*

The ROI is calculated by the ratio of the benefit and the cost. The benefit is calculated from the following equation: (initial risk) – (residual risk after the risk mitigation method is applied). An ROI example is as follows:

[In STEP 2] Initial risk of AM3 (System S/W) before installing firewall

$$\begin{aligned} Total\ Risk\ of\ AM3 &= 100 * (0.8 * 0.5 + 0.9 * 0.7 + 0.6 * 0.4) / 3 \\ &= 100 * 1.27 / 3 \\ &= 42.3 \end{aligned}$$

[In STEP 3] Residual Risk of AM3 (System S/W) after installing firewall

$$\begin{aligned} RISK &= 100 * (0.1 * 0.5 + 0.5 * 0.7 + 0.1 * 0.4) / 3 \\ &= 100 * 0.44 / 3 \\ &= 14.7 \end{aligned}$$

$$\begin{aligned} \text{Benefit} &= \text{(Initial risk)} - \text{(Residual risk)} \\ &= 42.3 - 14.7 \\ &= 27.6 \end{aligned}$$

[In STEP 4] ROI (Return On Investment)

$$= 27.6/4 * 100 = 690$$

(assuming that the cost of firewall is 4 units)

Damage Estimation (Step 4.4) calculates the total damage against the core asset in the organization based on the each risk calculated in step 2. The damage against the asset is a sum of the recovery cost, which is used to recover the asset before the threat is occurred. The recovery cost can be calculated as follows:

Total Cost = Acquisition Cost + Operation Cost + Business Opportunity Cost

The Acquisition Cost is an early cost of buying or installing an asset. The Operational Cost is a cost against human resource, who is able to recover the damaged asset. Finally the Business Opportunity Cost is the business loss by losing opportunity to earn monetary gains.

Result Documentation (Step 4.5) is a process that prints the result such as the risk per each asset, the list of mitigation method, the Return on Investment, the damage and so on. Through this step, the organization can decide their risk management policy

2.5 Implementation of the Security Risk Analysis Model

Based on the security risk analysis model, a security risk analysis program is developed as shown in Figure 4.

3 Related Work

As information security management becomes more important recently, advanced information security organizations, such as BSI in Britain [7] or NIST in USA [2, 3, 4, 5, 11], have been developing guidelines or methodologies for the national defense by themselves, and also 'Guidelines of the Management of IT Security' as a standard in ISO/IEC [9].

In the past, many researches have been done for security risk assessment [1, 6, 8, 10]. The representatives of security risk assessment are as follows: *Information Security Assessment Methodology (IAM), Vulnerability Assessment Framework (VAF), and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).*

IAM is a security assessment method to analyze potential vulnerabilities of an organization, and use for an educational program of the US Department of Defense with the experiences of National Security Agency (NSA) for 15 years.

VAF is a methodology for vulnerability assessment which was developed by KPMG Peat Marwick LLP with the commission of Critical Infrastructure Assurance Office in 1998. With the minimal essential infrastructure of the relevant organization, it analyzes the vulnerability data aggregated from selected assets, and then calculates the vulnerability grade as a result of qualitative assessment.

OCTAVE is a security assessment method which was developed by Software Engineering Institute of Carnegie Mellon University in USA. The security assessment consists of three steps: making file of threat scenarios based on assets, recognizing the vulnerabilities about major facilities, and assessing the risk and developing security strategies.

They are partially supporting the risk analysis process with a focus of vulnerability analysis and assessment. However, there is no integrated risk analysis based on software risk theory and the quantitative approach, which are used in this paper.

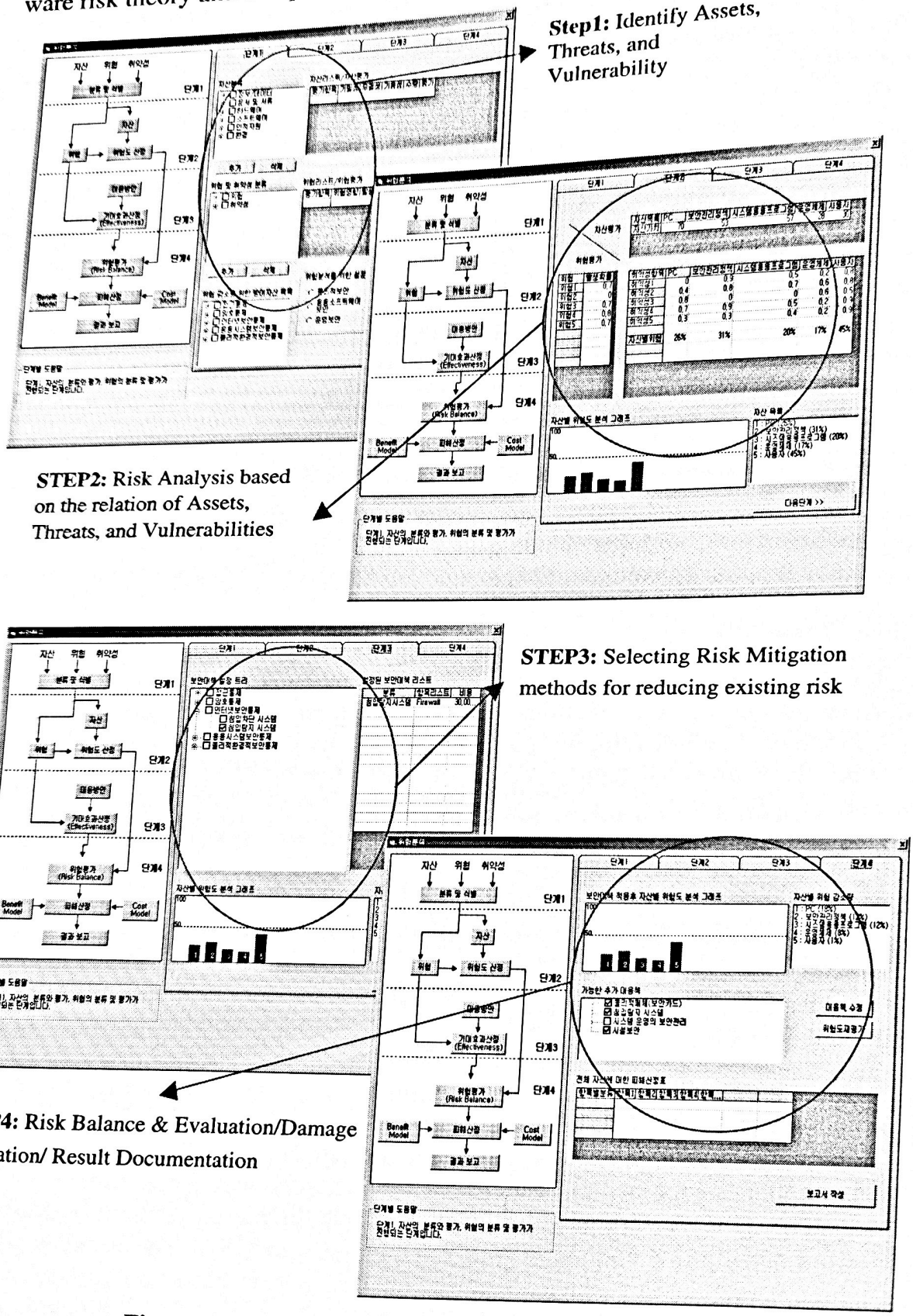

Fig. 4. Execution of Security Risk Analysis Program

4 Conclusion

Information security is a crucial technique for an organization to survive in these days. However, there is no integrated model to assess the security risk quantitatively and optimize its resources to protect organization information and assets effectively. In this paper, an integrated, quantitative risk analysis model based on definition of software risk is proposed including asset evaluation, threat evaluation, and vulnerability evaluation. Domain analysis model, one of components in the proposed model, makes it possible to analyze security incidents and estimate the damage cost per domain.

Our contribution is to apply the concept and techniques of software risk management for security risk analysis. As a result, the security risk can be evaluated quantitatively based on loss of the assets and its probability. In addition, we consider risk mitigation techniques to reduce the relevant risks and understand residual risks

In future, we will focus on the following: development of detailed guidelines of each model with examples, development of an automatic analysis system or tool for risk analysis and risk mitigation with visualization feature, optimization of proposed security policies in the proposed model, and case studies to improve the proposed model.

References

1. GAO, "Information Security Risk Assessment - Practices of Leading Organizations," Case Study 3, GAO/AIMD-00-33, 1999. 11.
2. NIST, "Guide for Selecting Automated Risk Analysis Tools", NIST-SP-500-174, Oct. 1989.
3. FIPS-191, "Specifications for Guideline for The Analysis Local Area Network Security," NIST, Nov. 1994.
4. NIST, "Risk Management Guide for Information Technology Systems," NIST-SP-800-30, 2001.10.
5. FIPS-65, "Guidelines for Automatic Data Processing Risk Analysis, NIST, 1975
6. GAO, Information Security Risk Assessment - Practices of Leading Organizations, Exposure Draft, U.S. General Accounting Office, August 1999.
7. BSI, BS7799 - Code of Practice for Information Security Management, British Standards Institute, 1999.
8. CRAMM, "A Practitioner's View of CRAMM," http://www.gammassl.co.uk/.
9. 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.
10. R.S. Arnold, S. A. Bohner, "Impact Analysis – Towards a Framework for Comparison," Proceedings of Conference on Software Maintenance, IEEE CS Press, Los Alamitos, CA, pp. 292-301 1993.
11. G. Stoneburner, A. Goguen, A. Feringa, "Risk Management Guide for Information Technology Systems," Special Publication 800-30, National Institute of Standards and Technology, October 2001.