Franklin University

FUSE (Franklin University Scholarly Exchange)

Faculty and Staff Scholarship

2004

A Novel Approach to Information Security Risk Analysis

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Ibrahim Sogukpinar
Gebze Institute of Technology

Recommended Citation

Karabacak, B., & Sogukpinar, I. (2004). A Novel Approach to Information Security Risk Analysis. *The 3rd Asia Pacific International Symposium on Information Technology* Retrieved from https://fuse.franklin.edu/facstaff-pub/39

A Novel Approach to Information Security Risk Analysis

Bilge Karabacak *,   İbrahim Soğukpınar **

*** National Research Institute of Electronic & Cryptology,**

TÜBİTAK, P.O Box 74, 41470 Gebze, Kocaeli TURKEY.

**** Gebze Institute of Technology,**

41400 Gebze, Kocaeli TURKEY.

bilge@uekae.tubitak.gov.tr   ispinar@bilmuh.gyte.edu.tr

ABSTRACT

A number of risk analysis methods became obsolete because of the profound changes in information technologies. Revolutionary changes in information technologies have converted many risk analysis methods into inconsistent, long lasting and expensive instruments. Therefore, risk analysis methods should be adaptively modified or redesigned according to the changes in information technologies, so that they meet the information security requirements of the organizations. By taking these requirements into consideration, a survey based approach is proposed for analyzing the risks of information technologies. This new method is named as Risk Analysis Method for Information Security (RAMIS). A case study is conducted to show the steps of RAMIS in detail and to obtain the risk results. To verify the results of the case study, simulation is performed based on the real statistical data. The results of simulation showed that RAMIS yields consistent results in a reasonable time period by allowing the participation of the manager and staff of the organization.

Keywords: Information Security, Risk Analysis, Risk Management, Simulation, Survey

1. Introduction

A number of information security risk analysis methods have been affected by the enormous changes in information technologies. These methods turned into inconsistent, long lasting and difficult to use instruments [1]. The risk analysis methods that were designed for yesterday's simple information systems are complex in nature. Complicated mathematical and statistical instruments are the main components of these risk analysis tools. Thus, applying these complex risk analysis tools into today's complicated information technologies has become infeasible.

Because the success and continuity of organizations vastly depends on the availability of information technologies, the responsibility of protection of information technologies increased. In 1980s, the responsible staff for protection of information technologies was the head of computer systems department of organization. Today, the company managers are taking this responsibility [2]. Thus, managers of organizations have to understand the risk analysis process that directly affects the protection of information technologies. Moreover, managers may desire to participate in risk analysis process. Yesterday's complex risk analysis methods are not in a structure that may allow the participation of managers.

With these requirements, a new risk analysis method, Risk Analysis Method for Information Security, is proposed. RAMIS is designed for analyzing the risks at complex information systems by allowing the participation of managers and staff.

The steps of a case study are shown briefly to help reader to understand the RAMIS. To verify the results of the same case study, a risk model is setup up with Arena simulation software. The collected real-life statistical data, which is related with the case study, is introduced to the risk model. The result of simulation showed that RAMIS gives correct and realistic risk results.

2. Risk Analysis Methods for Information Security

Basically there are two types of risk analysis methods according to tools used inside them. Quantitative risk analysis methods use mathematical and statistical tools to represent risk. Qualitative risk analysis methods does not use any mathematics, instead risk is stated with the help of adjectives. Risk analysis methods that use intensive quantitative measures will not be suitable for information security risk analysis. On the contrary of the past decades, today's information systems have a complicated structure and their use is widespread. Therefore, intensive mathematical measures to model risk for complex environments will make process difficult. Calculations performed during the risk analysis process will be very complicated. Quantitative methods may not be able to model today's complex risk scenarios. Risk analysis methods which use qualitative measures are more suitable for today's complex risk environment of information systems. But, one important drawback for qualitative risk analysis methods is their nature that yields inconsistent results. Because qualitative methods does not use tools like mathematics and statistics to model the risk, the result of method is vastly depended on the ideas of people who conduct the risk analysis. There is a risk of giving subjective result while using qualitative risk analysis methods.

As two examples, TUAR is a quantitative tool which uses fault trees and fuzzy logic to express the risk [3]. RaMEX is a qualitative tool which does not use mathematical or statistical instruments [4].

Both qualitative and quantitative risk analysis methods may be supported by software. On the contrary of this, risk analysis methods which are executed without assistance of software are called paper based methods [5]. There are a number of risk analysis methods that are supported by software [6]. The risk analysis methods that are supported by software have some certain disadvantages. Firstly, the cost of method will be usually high. Secondly, the main frame of risk analysis process is drawn by software. Thus, some necessary variations during risk analysis process may not be achieved. Paper based risk analysis methods consist of meetings, discussions and working sheets. Paper based methods are more flexible than the methods supported by software. One important drawback for paper based method is their duration. Because of nature of meetings, paper based methods may take a long time to give the risk results.

The Buddy System [7] and Cobra [8] are the examples of risk analysis methods supported by software. The Buddy System is quantitative, Cobra is qualitative in contrary. European Security Forum is an example of paper based method [9].

Both quantitative and qualitative risk analysis methods may be supported by standards like Common Criteria Framework, ISO 17779 and the other ISO standards related with information technologies [10]. These standards put forward robust and well-defined risk analysis methods. However, these methods require the participation of expert risk analysts because of complexity and formality of methods. As an example, CRAMM [11] is a quantitative, software-based risk analysis method that is compatible with standards.

3. Our Approach for Information Security Risk Analysis

By taking the today's information technology environment into consideration, risk analysis method should allow effective participation of manager and staff to the process [2]. In today's technological environment, the risk analysis method for information systems should not contain complicated mathematical and statistical instruments. This will cause a long and complex process [1]. Also, the risk analysis process should not contain pure qualitative measures. This may cause subjective results [5]. The information security risk analysis of today should not extent the risk environment. This causes costly, long lasting and complicated risk analysis process. Also, the risk analysis may give inconsistent results. Risk analysis methods that do not have these properties may not meet the requirements of organizations. RAMIS is designed to have these properties.

The peculiarity of RAMIS is to perform information security risk analysis by using public opinion. Public opinion is obtained by conducting survey. RAMIS is basically a survey preparation and conduction process to assess the security risks in an organization. Survey is composed of questions and answer choices related to the information security problem. Manager, directors, technical personal and usual staff are the candidates for answering the survey questions. The aim of the survey is to understand the effect of information security problem on the system or the organization. In other words, conducting a survey is somewhat making an as-is analysis. RAMIS makes a structured as-is analysis to assess the risk caused by information security problem. The preparation and conduction of the survey and obtaining a risk result from the survey is defined according to the well-defined steps.

The underlying risk model of RAMIS is based on formula (1), which is a fundamental and simple risk formula. [12, 13, 14].

Risk = Probability of occurrence of security breach
X Consequences of occurrence of security breach

Formula (1): Basic Risk Model

Formula (2) is the risk model of RAMIS, which is based on the fundamental risk formula (1).

$$\text{Risk}=\left(\frac{\sum_{m}\left[\tau_1\left(\sum_{i} wi \times pi\right)\right]}{m}\right)\times\left(\frac{\sum_{n}\left[\tau_2\left(\sum_{j} wj \times pj\right)\right]}{n}\right)$$

Formula (2): Risk Model of RAMIS

Formula (2) is composed of two main parts that corresponds to two fundamental risk parameters in formula (1). Two separate and independent survey processes are conducted in RAMIS for the two risk parameters that are probability of occurrence of security breach and consequences of occurrence of security breach.

The parameters that are contained in RAMIS risk model are:

i: The number of questions for the survey to estimate the probability of occurrence of security breach parameter, determined at step-2 and step-3

j: The number of questions for the survey to estimate the consequences of occurrence of security breach parameter, determined at step-2 and step-3

m: The number of participants for the survey to estimate the probability of occurrence of security breach, becomes definite at step-5

n: The number of participants for the survey to estimate the consequences of occurrence of security breach, becomes definite at step-5

w: Weight of the question, determined at step-2

p: Value of the answer choice, determined at step-3

T1: Risk table to analyze the result of probability of occurrence of security breach, constructed at step-4

T2: Risk table to analyze the result of consequences of occurrence of security breach, constructed at step-4

Risk: Single numeric value to represent the risk, obtained at step-6

RAMIS consists of seven main steps. At first step, awareness of information security problem occurs. After the first step, RAMIS process is divided into two parallel sub-processes. One of these sub-processes is for the probability of occurrence of security breach parameter and the other is for the consequences of occurrence of security breach parameter. Hereafter, only the sub-process for the probability of occurrence of security breach will explained. The work done is the same for the other risk parameter.

At the second step of RAMIS, all the factors that may affect the probability of occurrence of security breach are listed. This is a vital part of RAMIS to obtain the realistic and objective results from RAMIS. For this process to become successful, at least three people should participate in the listing of the factors. All these people should have general security perspective and be from the company itself. These people should have enough knowledge about the information security problem, its effects and its probable causes. Also, these people should have enough knowledge on the information system that is affected by the problem. After listing all possible factors for the basic risk parameter, numeric values are given to the factors to weigh each factor. Weight factor is used because the listed factors do not affect the probability equally. One factor may have more effect on the probability of the occurrence than the other.

At the third step of RAMIS, the factors are converted into the survey questions and answer choices are determined for each question. All the questions must have the same number of choices for a consistent analysis of the results. At least four answer choices are suggested for a successful analysis. Like the factors, the answers choices to questions have to be selected carefully. Because, the answers selected by survey participants will be the main assessment components for the risk. Thus, certain differentiations have to be supplied between the answers of a question. The choices should be selected so that, each choice should represent a different risk level. The team who lists the factors should work on the selection of the choices. The choices to the questions should be arranged so that the answer choice which affects the probability of occurrence of security breach mostly should be the first choice. The answer choice which affects least should be the last choice. This is an important point because risk amount is calculated quantitatively according to the survey results at step-6. For quantitative analysis, answer choices will be converted into numbers. For a successful analysis, the answer choices should be listed orderly.

At the fourth step, risk tables are prepared. These tables scale the fundamental risk parameters both quantitatively and qualitatively based on the survey results. These tables are the main reference points for the evaluation of the survey results. They prevent the confusion during the assessment of results. These tables scale the possible survey results for two fundamental risk parameters. Risk tables are dynamic tables. Their contents change according to the different surveys conducted. A risk table forms a connection between the result of the survey and the quantitative and qualitative values of risk parameter in consideration.

After preparation of risk tables is over, survey is conducted.

This is the fifth step of RAMIS. This step is the most peculiar part of RAMIS in which ordinary information system users participate actively in risk analysis process. The answers to the survey questions are already valuable information for the sake of whole risk analysis process. But, the main purpose of RAMIS is to convert these answers to numeric values and calculate a single risk value.

At the sixth step of RAMIS, Formula (2) is applied to get the quantitative results from the answered surveys. During this quantitative process, risk tables are used to obtain objective quantitative results.

The last step of RAMIS is the assessment phase. At the assessment phase, not only the numerical survey result, which is obtained at the previous step, are assessed but also the single answer choices of survey participants are examined.

All of these phases allow the active participation of managers and staff to the risk analysis process. During all of these phases, there are no complicated mathematical tools used. The number of survey questions, the types of questions and the structures of risk tables are changeable according to the information security problem. The flexibility of method allows RAMIS to apply to diverse information security problems effectively.

Step-2, 3 and 4 are the most vital parts of RAMIS for an objective risk analysis. Company staff must work carefully during these steps to vanish any subjectivity and incompleteness.

4. Case Study

In our case study, RAMIS is used to analyze the risk arise from computer viruses. Our environment of risk analysis composed of three computers. These computers belong to a small-sized company, let say company-a, and are used by staff to connect to Internet via dial-up technology. These three computers are shared among seventy five company workers, who are potential candidates of survey of RAMIS. Thus, company workers who use one of three computers took action in the survey to obtain the public opinion on computer viruses.

At step-2, separate analyses are made for two main risk parameters, which are the probability of infection and the consequences of infection. In these analyses, the factors which affect these two risk parameters are determined and weighed. Weight factors are appointed as “1”, “2” and “3”, which correspond to least effective, average and most effective, respectively.

Two of the factors that affect the probability of a virus infection are;

The number of downloads per day (Weight Value: 3)

The type of a download (Weight Value: 2)

By using same procedure, the factors that affect the consequences of infection are listed by risk analysis team. A sample list and assigned weights for these factors is;

The type of data at the computer (Weight Value: 3)

The backup condition of data at the computer (Weight Value: 2)

At step-3, all the factors for two risk parameters are converted into survey questions. A sample question, which is converted from the second factor of probability of infection parameter, is below;

2. What type of files do you download?

a. Executables for my personal needs
b. Executables for company
c. Word documents
d. Not applicable

As you realize, the answer choices are placed so that the most influential answer is the first choice and the least influential one is the last choice. The last action taken at step-3 is to give numerical values to each answer choices in decreasing order starting with point 4 for the choice “a” and 1 for choice “d”.

At the fourth step of RAMIS in our case study, two risk tables are constructed for two risk parameters.

To construct the risk table of probability of infection parameter, firstly, minimum and maximum numerical values that can be obtained from the survey are found out.

For the survey of probability of occurrence of security breach parameter, there are eight questions and four answer choices for each question. The weight of each question was also determined during our case study. According to these values, the maximum value is obtained for the condition of all the answer choices are selected as “a”. In this case,

$$\text{Maximum Output} = \sum_i w_i \times p_i = 4 * \sum_i w_i = 68$$

In the same manner, the minimum output obtained from a survey is found as 17, at which all the answer choices are selected as “d”.

Table 1 is the risk table constructed for the probability of infection parameter.

Survey Result	Qualitative scale	Quantitative scale
17 – 26	Very Low Probability	1
27 – 36	Low Probability	2
37 – 48	Medium Probability	3
49 – 59	High Probability	4
60 – 68	Very High Probability	5

Table 1: Risk Table for the Survey of Probability of Infection Parameter

68 points presents the highest probability for infection of a virus. 17 points presents the lowest probability for infection of a virus. In Table 1, the values between 17 and 68 are arranged to represent risk levels. As you can see from the Table 1, the possible results from a survey is scaled and matched to quantitative and qualitative values.

In a similar way, another risk table is constructed for the consequences of infection variable.

A final risk table, Table 2, is prepared by using the risk tables of two main risk parameters. Table 2 is constructed by multiplying the quantitative scale values of previous risk tables according to formula (1). The multiplication operation gives the various risk values between 1 and 25. This final risk table will prevent confusions in the assessment of risk. The uppermost row of final risk table shows the values of probability of infection parameter. The leftmost column shows the values of consequences of infection parameter.

Risk=(1)*(2)	1: Very Low	2: Low	3: Medium	4: High	5: Very High
1: Negligible	1:Very Low	2:Very Low	3:Very Low	4:Low	5:Low
2: Minor	2: Very Low	4: Low	6: Low	8: Medium	10: Medium
3: Important	3: Very Low	6: Low	9: Medium	12: Medium	15: High
4: Serious	4: Low	8: Medium	12: Medium	16: High	20: Very High
5:Very Serious	5: Low	10: Medium	15: High	20: Very High	25: Very High

Table 2: The Final Risk Table

After preparation of risk tables for two risk parameters and the final risk table, the questionnaires are ready for the distribution to the staff. Thus, the preparation phase of survey process is over. At step-5, survey questions can be distributed to the relevant staff in hardcopy or it can be answered electronically. All the survey results are recorded carefully. Note that, in our case study, two separate surveys are answered by the staff for two different parameters. But, this is not necessarily done so. One survey may contain the questions of both risk parameters. In our case study, 73 people are participated in the survey of probability of occurrence of security breach and 75 people are participated in the survey of consequences of occurrence of security breach.

After the participation of all the staff to the surveys, Formula (2) is applied by using numerical values that are obtained from surveys. This is the main action taken at step-6. In our case study, the probability of infection of a virus to a computer is found as 2, which is “low” at qualitative scale. The consequence of infection of a virus is found as 4, which is “serious consequence” at qualitative scale. As a result, value of risk is found as 8 which is a medium level risk according to the Table 2.

The most important output of RAMIS is the single risk value obtained at step-6. This risk value is obtained after performing considerable amount of preliminary work. Preliminary work included listing out the factors, designating answer choices, weighting the factors, giving values to answer choices and preparing risk tables. The quality of this preliminary work will definitely affect the accuracy of single risk value.

To obtain consistent and accurate results from a survey, it is important to carefully list the factors and prepare the questions and answers. According to the nature of problem, the number and type of staff that participate in a survey may change. All the staff may participate in a survey that plans to express the risk arise from viruses. However, only computer department staff may be participate in a survey that tries to express the risk for a web server.

As stated earlier, today the company managers are taking the responsibility of production of information systems. Thus, managers of organizations have to understand the risk analysis process that directly affects the protection of information technologies. A single risk value that presents the risk level, which arises from a specific information security problem, is an easy to comprehend risk outcome for company managers.

On the other hand, while assessing the survey results at step-7, not only these calculations are made and not just the final numerical result is considered but also answers to questions are examined in detail.

By examining the answers to the survey questions in our case study, some important results are obtained. Viruses that mostly infect the computers are e-mail viruses. Backing up the data and user security awareness should greatly reduce the probability and consequences of infection. An important fact is that some computer users require urgent security awareness.

The assessment of survey results is an important part of RAMIS. Managers and staff can easily participate in this step and express their opinions.

The survey results are assessed and suggestions are put forward for the risk mitigation process. The outcome of RAMIS is a risk report which clearly puts forward the survey results and assesses these results.

5. The Results of Application, Verification and Comparison

In order to verify the results of RAMIS case study, we have gathered statistical data and run simulation based on statistical data. We have used Arena simulation software to model the risk environment and simulate on the real statistical data.

By making analyses on the pilot network, it is seen that, three main sources of virus are e-mails, downloads and floppy diskettes. So, the gathered statistical data is composed of the number of received e-mails, downloads and floppy usage per day, per computer and per user basis. The statistical data is gathered for one month. During one month, virus incidents are carefully noted. The sources and number of infections are written down.

After the completion of gathering the statistical data, three independent risk models are constructed at Arena software. Three sources of data, which come to computers, are independent of one another. Because of this situation, three independent risk models are constructed.

At the risk models, the data is generated by the entities represented by exponential probability distribution function. Mean value of the probability distribution function is determined according to the gathered statistical data for e-mail traffic, number of downloads and floppy usage. The generated data is passed through the probability of infection and the consequences of infection entities of all three risk models. The probability of infection is constructed according to the statistical data. Consequences of infection entities are constructed after the discussion with experts.

Simulation is run for a period of time which is equal to one year in real life situation. Table 3 depicts a sample simulation result for one computer. It is not possible to write down all the simulation results here.

Risk Report 1	Date:	31 December 2002	
E-mail Virus Model	Time:	2:03:56PM	
Model Parameter	Average	Lowest	Highest
Total e-mails	4929.25	4806.00	5079.00
E-mails comes to computer-1	2449.17	2307.00	2513.00
E-mails without viruses	4920.75	4799.00	5073.00
E-mails with viruses	8.5000	4.0000	15.0000
E-mails with viruses for computer-1	4.4167	1.0000	8.0000
Computer-1 infected viruses	0.5000	0.00	1.0000
Total infected	3.4167	2.0000	8.0000
The number of e-mails that contain viruses but does not infect	5.0833	1.0000	10.0000
The number of infections that cause very serious consequences	1.1667	0.00	3.0000
The number of infections that cause serious consequences	1.0000	0.00	3.0000
The number of infections that cause important consequences	0.5833	0.00	1.0000
The number of infections that cause minor consequences	0.5000	0.00	1.0000
The number of infections that cause negligible consequences	0.1667	0.00	1.0000

Table 3: Sample Simulation Result

The simulation results revealed the similar results with RAMIS. First of all, simulation results show that, the most of the viruses comes from via e-mail attachments. 80 percent of computer viruses arise from e-mails. The same result was obtained while assessing the answers to the survey questions.

The probability of a virus infection is considerable low. As we can see from Table 3 the number of infection is low compared with the number of the e-mails. But, the number of very serious and serious consequences of infection is high. Namely, once a virus infected the network, the consequence of infection is expected to be high. These two results are compatible with the results obtained at the step-6 of RAMIS. At the step-6 of RAMIS, formula (2) was applied and single values for probability of occurrence and consequences of occurrence were found. The value for first parameter was 2 (low) and the value for second was 4 (serious consequences).

"As-if" analyses are made during simulation. According to these analyses, by training the staff, the probability of infection of viruses may be decreased by minimum 20 percent and maximum 50 percent. Backing up data and user security training may decrease the consequences of infection by minimum 30 percent and maximum 80 percent.

While assessing the survey results, answers to the survey question revealed the necessity of user security awareness and back-up. At this point, the simulation results and RAMIS results say the same thing.

As a result, the results of simulation, which is based on gathered statistical data, are compatible with the results of RAMIS case study. RAMIS gives the similar results in a much shorter time period without struggling with statistical data and by allowing participation of staff.

RAMIS is basically a quantitative survey tool for making risk analysis of information systems. Quantitative tools included in RAMIS are simple numbers, risk tables, multiplication and addition operations. There are no complicated mathematical and statistical instruments in RAMIS like other quantitative methods like TUAR. As said previously, qualitative methods may give subjective results. RAMIS is a quantitative tool with well-defined steps and mathematical measures. With careful operation, RAMIS will give objective risk result. The comparison of our case study and simulation results proves this situation.

Software based risk analysis methods have a rigid frame. During risk analyses in which software is used, necessary variations may not be achieved. This is not the case for RAMIS. RAMIS does not have rigid frames. The number of questions and answer choices, risk tables, weight values and the other values may be changed from one analysis to another. RAMIS has well-defined steps. So, the duration of RAMIS is deterministic. There is no risk of long period of analysis like the paper based methods.

6. Conclusion and Future Work

The main advantage of RAMIS over other risk analysis methods is its ease of use. In today's technological arena, risk analysis methods that contain complicated mathematics and statistics may give inconsistent results, take a long time and be costly. These risk analysis methods were particularly designed for 1980s' simple systems. Because the qualitative risk analysis methods may give subjective results, these methods may require expert participation. For today's information systems, a quantitative method which does not contain complicated mathematical and statistical instruments is necessary. Therefore, manager and the staff may effectively participate in risk analysis process. It is suggested that information security risk analysis should be business oriented [13, 15, 16]. RAMIS fulfills both the business and technology requirements by taking today's needs into consideration.

RAMIS may be used for a wide range of problems. From technical problems like the one in our case study, to procedural and political issues like to find out the risk arise from the weaknesses of information security policies. In some cases, the number of survey participants may be very low. But this is not a reason for RAMIS to give inconsistent results. One of such cases is the business oriented surveys like to try to estimate the risk arise from untrained technical staff.

The next step for RAMIS is to develop an automated survey process by using programming tools. This work will ease both the preparation and answering phases of survey.

References

[1] R.V. Jacobson : "CORA. Cost of Risk Analysis. Painless Risk Management for Small Systems", International Security Technology, Inc., 1996.

[2] S. Owens : "Information Security Management: An Introduction", British Standards Institution,1998.

[3] A. Bilbao : "TUAR. A Model of Risk Analysis in the Security Field", CH3119-5/92, IEEE, 1992.

[4] M. P. Kailey, P. Jarratt : "RAMeX: A Prototype Expert System for Computer Security Risk Analysis and Management", Computers & Security, Vol. 14, No. 5, pp. 449-463, 1995.

[5] J. Gordon: "Security Modelling, Risk Analysis Methods and Tools", IEE Colloquium on, 1992.

[6] D. Spinellis, S. Kokolakis, S. Gritzalis : "Security Requirements, Risks and Recommendations for Small Enterprise and Home-Office Environments", Information

Management & Computer Security, 7/3, pp. 121-128, 1999.

[7] B. D. Jenkins : "Security Risk Analysis and Management, , Countermeasures, INC. ", 1998.

[8] COBRA Consultant Products for Windows, An easy to use guide and evaluation aid, 2000.

[9] Business Risk Analysis: Establishing a Risk Analysis Method which is easy to understand and simple to apply. European Security Forum, from Coopers and Lybrand, Europe

[10] A. Toval, J. Nicolas, B. Moros, F. Garcia : "Requirements Reuse for Improving Systems Security: A Practitioner's Approach", Requirements Engineering, 6, pp. 205-219, 2002.

[11] United Kingdom Central Computer and Telecommunication Agency, CCTA Risk Analysis and Management Method, CRAMM User Guide, Issue 1.0, 1996.

[12] Special Publication 800-30: Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, 2001.

[13] N. McEvoy, A. Whitcombe : "Structured Risk Analysis", InfraSec 2002, LNCS 2437, pp. 88-103, 2002.

[14] Information Security Risk Assessment, United States General Accounting Office Accounting and Information Management Division, 1999.

[15] P. Sommer, : Industrial Espionage: "Analysing the Risk", Computers & Security, Vol. 13, No. 7, pp. 558-563, 1994.

[16] R. C. Reid, S. A. Floyd : "Extending the Risk Analysis Model to Include Market-Insurance", Computers & Security, Vol. 20, No. 4, pp. 331-339, 2001.