Computers & Security (2005) **24**, 147–159

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

ISRAM: information security risk analysis method

Bilge Karabacak[a,*], **Ibrahim Sogukpinar**[b]

[a]*National Research Institute of Electronics & Cryptology (UEKAE), P.O Box 74, 41470 Gebze, Kocaeli, Turkey*
[b]*Gebze Institute of Technology, 41400 Gebze, Kocaeli, Turkey*

Received 24 December 2003; revised 27 July 2004; accepted 27 July 2004

KEYWORDS
Information security;
Risk analysis;
Quantitative risk analysis;
Paper-based risk analysis;
Risk model

Abstract Continuously changing nature of technological environment has been enforcing to revise the process of information security risk analysis accordingly. A number of quantitative and qualitative risk analysis methods have been proposed by researchers and vendors. The purpose of these methods is to analyze today's information security risks properly. Some of these methods are supported by a software package. In this study, a survey based quantitative approach is proposed to analyze security risks of information technologies by taking current necessities into consideration. The new method is named as Information Security Risk Analysis Method (ISRAM). Case study has shown that ISRAM yields consistent results in a reasonable time period by allowing the participation of the manager and staff of the organization.

Introduction

The structure and type of information technologies have changed enormously over last decade. The simple stand-alone batch applications evolved into distributed computing environments, including real-time control, multitasking and distributed processing. The process of information security risk analysis has also been affected by these enormous changes. It is claimed to be ''inconsistent, long lasting and difficult to apply'' (Gerber and Solms, 2001). Due to the difficulties of applying complex risk analysis tools into today's information systems, researchers have studied to develop new methods.

Because the success and continuity of organizations vastly depend on the availability of information technologies, the task of protection of information technologies have become more critical than ever. In 1980s, the head of information technologies (IT) department of organization was the responsible staff to protect information systems. Nowadays, some of the company managers

* Corresponding author.
E-mail addresses: bilge@uekae.tubitak.gov.tr (B. Karabacak), ispinar@bilmuh.gyte.edu.tr (I. Sogukpinar).

0167-4048/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.07.004

are taking over this responsibility from the head of IT department (Owens, 1998). Thus, managers of organizations should understand the risk analysis process that directly affects the protection of information technologies. Moreover, managers may desire to participate in risk analysis process. The structure of new risk analysis methods allows the participation of managers (Bilbao, 1992; Kailey and Jarratt, 1995; Jenkins, 1998; C&A Systems Security Limited, 2000; Toval et al., 2002; Jacobson, 2002; Coles and Moulton, 2003).

In this study, a new method named Information Security Risk Analysis Method (ISRAM) is proposed for information security risk analysis by taking today's needs into account. ISRAM is designed for analyzing the risks at complex information systems by allowing the participation of managers and staff. Proposed method consists of seven steps. These steps are exemplified in a case study in order to explain ISRAM clearly. To verify the results of the same case study, a risk model is set up with Arena simulation software. The collected real-life statistical data are introduced into the risk model.

This paper is organized as follows: risk analysis methods for information security are introduced briefly after the Introduction. Then the risk model of ISRAM, explanations and experimental results are presented. The section following that contains some ideas on the verification, comparison and the results of the application. The last section is the conclusion.

Risk analysis methods for information security

Basically there are two types of risk analysis methods. Quantitative risk analysis methods use mathematical and statistical tools to represent risk. In qualitative risk analysis methods, risk is analyzed with the help of adjectives instead of using mathematics. Risk analysis methods that use intensive quantitative measures are not suitable for today's information security risk analysis. In contrast to the past decades, today's information systems have a complicated structure and a widespread use. Therefore, intensive mathematical measures used to model risk for complex environments make the process more difficult. Calculations performed during the risk analysis process are also very complex. Quantitative methods may not be able to model today's complex risk scenarios. Risk analysis methods based on qualitative measures, are more suitable for today's complex risk environment of information systems. However, one important drawback for qualitative risk analysis methods is their nature that yields inconsistent results. Because qualitative methods do 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 results while using qualitative risk analysis methods. Following examples can be given for two types of risk analysis tools which are based on quantitative and qualitative methods. TUAR is a quantitative tool, which uses fault trees and fuzzy logic to express the risk (Bilbao, 1992). RaMEX is a qualitative tool, which does not use mathematical or statistical instruments (Kailey and Jarratt, 1995).

Both qualitative and quantitative risk analysis methods may be supported by software. On the contrary, risk analysis methods that are executed without assistance of software are referred as paper-based methods (Gordon, 1992). There are a number of risk analysis methods that are supported by software (Spinellis et al., 1999). Software-based risk analysis methods may have some disadvantages. First, the cost of such methods is usually high. Second, the main frame of risk analysis process is drawn by software. Thus, some necessary variations of the risk analysis process would not be achieved. Paper-based risk analysis methods consist of meetings, discussions and working sheets. One important drawback for paper-based method is their duration. Because of the nature of the meetings, paper-based methods may take a long time to give the risk results.

The Buddy System (Jenkins, 1998) and Cobra (C&A Systems Security Limited, 2000) are examples of risk analysis methods that are supported by software. The Buddy System is quantitative, and Cobra is qualitative. SPRINT is an example of paper-based risk analysis method (ISF, 1997).

Both quantitative and qualitative risk analysis methods may be supported by standards and guides like Common Criteria Framework (ISO, 1999), ISO 13335 (ISO, 1996—2001), ISO 17799 (ISO, 2000), NIST 800-30 Special Publication (NIST, 2001) and the other standards and guides related to information technologies (Toval et al., 2002). As an example, CRAMM (CCTA, 2001) is a quantitative, software-based risk analysis method that is compatible with standards. CORA is another risk analysis tool, which is quantitative, software based and compatible with NIST 800-30 guide (Jacobson, 2002). A risk manager can use CORA to perform risk analysis process described in NIST 800-30 guide. These standards put forward robust and well-defined risk analysis methods. However, these methods may require the participation of

expert risk analysts because of complexity and formality of methods.

BPIRM, business process information risk management, is an approach for risk management, which is suggested to close the major gaps found at some risk management practices conducted by organizations (Coles and Moulton, 2003). Understanding the real risks by the business process owner and defining their control requirements are recommended by the method of BPRIM. Also this method is useful for establishing who is responsible for implementing and managing the controls related to these risks throughout all aspects of the business process.

The driving force for changes to information security risk analysis is not just the technology. Information security risk analysis has been affected by the new legal requirements. Therefore, risk management is required novel governance approaches. To overcome this issue, a governance approach is proposed to provide a better framework to manage risks (Moulton and Coles, 2003).

ISRAM: information security risk analysis method

By taking today's information technology environment into consideration, risk analysis method should allow effective participation of manager and staff into the process. In today's technological environment, if the risk analysis method contains complicated mathematical and statistical tools, it may require the expert participation and it may last for a long time. Also, the risk analysis process should not contain pure qualitative measures. This may cause subjective results. Risk analysis methods that do not possess these properties may not meet the requirements of organizations. ISRAM is a quantitative, paper-based risk analysis method that is designed to have these properties.

Risk model of ISRAM

The underlying risk model of ISRAM is based on the following formula, which is the fundamental risk formula (NIST, 2001; McEvoy and Whitcombe, 2002; USGAO, 1999).

$$\text{Risk} = \text{Probability of occurrence of security breach} \times \text{Consequence of occurrence of security breach} \quad (1)$$

The risk model of ISRAM, which is deduced from formula (1), is given by formula (2). Formula (2) consists of two main parts, which are the projections of two fundamental parameters in formula (1).

$$\text{Risk} = \left(\frac{\sum_m \left[T_1\left(\sum_i w_i p_i\right)\right]}{m}\right)\left(\frac{\sum_n \left[T_2\left(\sum_j w_j p_j\right)\right]}{n}\right) \quad (2)$$

where

i: the number of questions for the survey of probability of occurrence, determined at Step-2;
j: the number of questions for the survey of consequences of occurrence, determined at Step-2;
m: the number of participants who participated in the survey of probability of occurrence, becomes definite at Step-5;
n: the number of participants who participated in the survey of consequences of occurrence, becomes definite at Step-5;
w_i, w_j: weight of the question "i" ("j"), determined at Step-2;
p_i, p_j: numerical value of the selected answer choice for question "i" ("j"), determined at Step-3;
T_1: risk table for the survey of probability of occurrence, constructed at Step-4;
T_2: risk table for the survey of consequences of occurrence, constructed at Step−4;
Risk: single numeric value for representing the risk. Obtained at Step−6.

ISRAM is basically a survey preparation and conduction process to assess the security risk in an organization. Two separate and independent survey processes are being conducted for two risk parameters in formula (2). The preparation and conduction of survey, so as the analysis of its results are defined according to the well-defined steps to yield the risk. Formula (2) represents these steps mathematically.

Annual Loss Expectancy (ALE) value may be required for some company managers after risk analysis. ISRAM does not make Single Loss Expectancy (SLE) or ALE calculations during the calculation of "risk". The unit of "risk" is not in dollars. Rather, it is a single numerical value between 1 and 25, which will be defined later in Table 9.

However, while presenting the survey result to senior management, the risk value may be converted to an ALE value by the risk analyst. ISRAM supports an easy conversion from the risk value to the ALE value. A sample conversion for the result of case study is given in the section 'Verification, comparison and the results of the application'.

The method in detail

The aim of ISRAM is to assess the risk caused by the information security problems. To achieve this goal, ISRAM is performed by using public opinion on the problem. Public opinion is obtained by conducting a survey. A survey is composed of questions and answer choices related to the information security problem. Manager, directors, technical personal and common users of computer may be candidates for answering the survey questions. The aim of the survey is to understand the effect of information security problem on the system or organization. In other words, conducting a survey is somewhat making an as-is analysis. ISRAM makes a structured as-is analysis to assess the risk caused by information security problem.

ISRAM consists of seven main steps as shown in Fig. 1. Of these seven steps, first four steps belong to the survey preparation phase, fifth step is the conduction of the survey and the last two steps are the phase in which results are obtained and assessed. In the survey preparation phase of ISRAM, the questions, the number of the questions, the weight values of the questions, the number of answer choices and the numerical values of answer choices are determined. Finally, the risk tables are prepared.

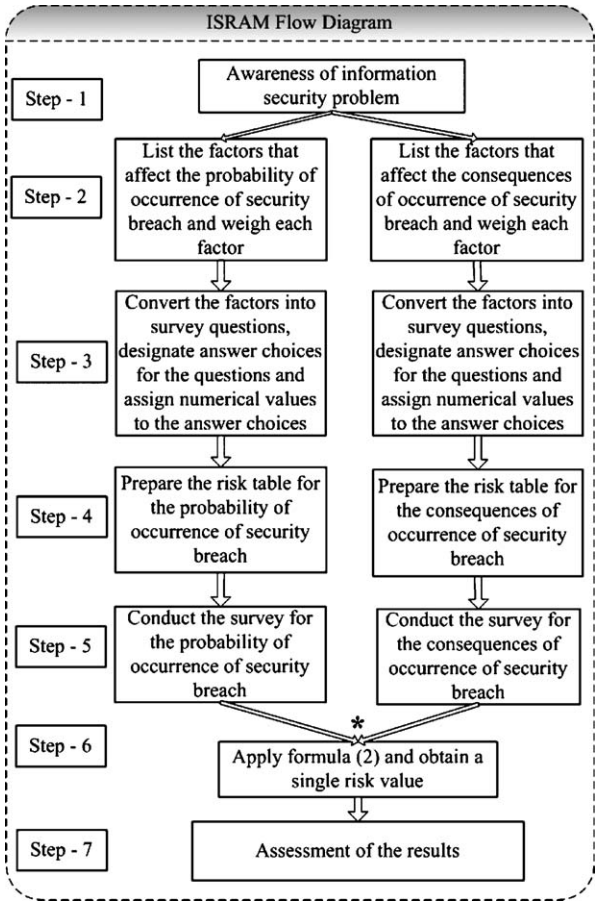

Figure 1 Basic flow diagram of ISRAM.

The existence of information security problem is detected in the first step. After the first step, ISRAM process is divided into two parallel sub-processes. One of these sub-processes is performed for the probability of occurrence of security breach parameter and the other is performed for the consequences of occurrence of security breach parameter. Hereafter, only the sub-process for the probability of occurrence of security breach will be explained according to Fig. 1.

In the second step, all the factors that may affect the probability of occurrence of security breach are listed. After listing all possible factors for the risk parameter, weight values are designated to the factors. One factor may have more effect on the probability of the occurrence than the other. That's why weight values for factors are designated. Weight values of the factors are in fact weight values for the questions. (Factors are converted into survey questions in the third step.) Step-2 is a vital part of ISRAM to obtain the realistic and objective results. To achieve this step, people who have general security perspective and preferably company workers should participate in. These staff should have enough knowledge and awareness on the information security problem, its effects and its probable causes. Also, staff should have enough knowledge on the information system that is affected by the problem.

In the third step, the factors are converted into the survey questions and the answer choices are determined for each question. Each question may have different number of choices. The number of choices should be selected by the risk analyst according to the questions and the case being analyzed. After the answer choices are determined, numerical values are designated to the answer choices. Because certain differentiations have to be supplied among the answer choices of a question. The answer choices and their numerical values have to be selected carefully, because, the answers selected by survey participants will be the main assessment components for the risk. In Step-6, risk amount will be calculated quantitatively according to the answer choices selected by participants. The team who lists the factors should work carefully on the selection of the choices and assignment of numerical values.

In the fourth step, two risk tables are prepared. Risk tables are vital for the quantitative analysis of the survey results. A risk table converts bulk survey

result to meaningful, quantitative and scaled values. To do this, a risk table scales all possible survey results that can be obtained from a single survey. Risk tables are the main reference points for the evaluation of the survey results. They prevent confusions while quantitatively assessing the survey results. The content of a risk table changes according to the surveys conducted. A risk table forms a connection between the result of survey and the quantitative value of the risk parameter under consideration.

Survey is conducted after the preparation of risk tables is over. This is the fifth step of ISRAM. This step is the most peculiar part of ISRAM in which ordinary information system users participate actively into the risk analysis process. At Step-5, the survey questions can be distributed to the relevant staff as hard copy or it can be answered electronically. The questions for two risk parameters can be delivered in one survey or it is possible to deliver separate surveys for two risk parameters. In this case, the number of participants may be different for two surveys. It is important to note that the answers to the survey questions are valuable information for risk analysis process. But the main purpose of ISRAM is to convert these answers into numeric values.

In the sixth step, formula (2) is applied to get single quantitative risk result from answered surveys. An example of application of formula (2) is given in Table 10, which shows the calculations for our case study.

Step-7 is the assessment phase of ISRAM. In the assessment phase, not only the numerical survey result, which is obtained in Step-6, is assessed but also the answers to the survey questions are analyzed.

All of these phases allow the active participation of managers and staff into the risk analysis process. Among these seven steps, addition, multiplication and division operations are used only in Steps 4 and 6. Other complicated mathematical and statistical calculations are not used in these steps.

Steps 2—4 are the most vital parts of ISRAM for an objective risk analysis. Company staff must work carefully during these steps to vanish any subjectivity and incompleteness.

Practice of ISRAM

In the case study, ISRAM was used to analyze the risk arising from computer viruses. Our environment for risk analysis was composed of 20 computers on a Local Area Network (LAN) as shown in Fig. 2. These computers belong to a research institute and are used by staff to connect to Internet. Every computer has a dedicated user. However, any of the computers in the network can be used by any user. Twenty institute workers took action in the survey to obtain the public opinion on computer viruses.

Step-1: awareness of the problem

As it has been already said in the previous paragraph, the information security problem is caused by computer viruses. Computers which are used in the case study do not have appropriate antivirus software installed. Personal firewall products are installed in a few computers. It is apparent that there is a strong requirement for a structured risk analysis in which the probability of a virus infection and the consequences of an incident is estimated.

Technically oriented people of the institute realize the information security problem and decide to make a risk analysis. The first step of ISRAM is completed.

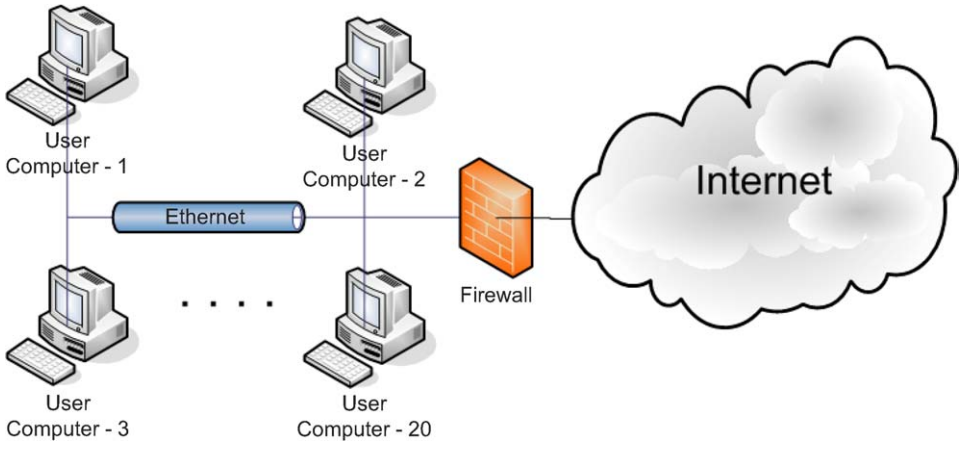

Figure 2 Environment of ISRAM.

Step-2: listing and weighing the factors

At Step-2, separate analyses are made for two risk parameters to determine the factors, which affect these parameters.

After determining and listing all the factors, weight values are assigned to the factors by using Table 1. The value of assets, the strength of already existing countermeasures, and the level of vulnerabilities are all considered during the assignment of weight factors.

After the discussions among risk analysis team, 21 factors are determined that affect the probability of a virus infection. Fifteen factors are determined that affect the consequences of infection. Among these factors, six of them affect both parameters.

Three of the factors are directly associated with vulnerabilities of operating system and patch level (these three factors affect both risk parameters).

Some of the factors that affect the probability of a virus infection and their equivalent weight values are shown in Table 2. (Because of the space constraints, all the factors could not be written.)

Some of the factors that affect the consequences of a virus infection and their equivalent weight values are shown in Table 3.

Six factors that affect both the probability and the consequences of a virus infection and their equivalent weight values are shown in Table 4.

First three factors in Table 4 are directly associated with vulnerabilities of systems. Note that these factors affect both the probability and the consequences of infection. These factors have also considerable weight values.

Step-3: converting factors into questions, designating answer choices and assigning numerical values to answer choices

At Step-3, all the factors are converted into survey questions and answer choices are designated. The number of answer choices can change according to the type and structure of survey question. In our case study, there are a total number of 30 survey questions. Ten of these questions have only two answer choices (six of them are yes/no questions). Sixteen of the questions have four answer choices. Four of the questions have three answer choices. Apart from yes/no questions, all questions have an answer choice, named ''Other:'' If a participant cannot find an appropriate answer among dedicated choices, he/she is expected to write his/her answer there.

After designation of answer choices, Table 5 is used to convert answer choices into numerical values.

Some of the questions and their answer choices are shown in Table 6. The weight values of questions and the numerical values of answer choices are also given in parenthesis. In questions column, ''*p*'' in parenthesis means that the factor affects the probability of infection and ''c'' in parenthesis means that the factor affects the consequences of infection. Note that, if the question (factor) affects both parameters (probability and consequences), then first numerical weight value in next parenthesis is for the probability of

Table 2 Some of the factors that affect the probability

Factor	Weight value
The type of attachment of e-mails	3
The number of e-mails per day	1
The number of different websites entered per day	1
The source of floppies	2
The number of files downloaded per day	1

Table 1 Reference table for the weight values of the factors

Weight value	Explanation
3	The factor is directly associated with a severe vulnerability and/or the factor is directly associated with a critical asset and/or there is no countermeasure in place. Because of these reasons, the factor is most effective factor that affects the probability of infection or the consequences of infection. The factor contributes directly to the value of the risk parameter.
2	The factor is somewhat associated with a vulnerability and/or the factor is directly associated with an important asset and/or there is a few countermeasure in place. Because of these reasons, the factor is slightly/normally effective factor that affects the probability of infection or the consequences of infection. The factor contributes somewhat directly to the value of the risk parameter.
1	The factor is a little associated with vulnerability and/or the factor is indirectly associated with an important asset and/or there are enough countermeasures in place. Because of these reasons, the factor is least effective factor that affects the probability of infection or the consequences of infection. The factor contributes indirectly to the value of the risk parameter.

Table 3 Some of the factors that affect the consequences

Factor	Weight value
The backup condition of files	3
The place of files	2
The importance of files in a computer	3
The dependence to files and applications	2

infection and the other one is for the consequences of infection.

For a participant, more than one choice may be applicable. In this case, the most effective choice (the choice which has the largest numerical value) is used during calculations.

$$\sum_i w_i p_i \left\{ \begin{array}{l} i: \text{the number of the questions} \\ w: \text{the weight of the } i\text{th question} \\ p: \text{the value of the selected answer choice of the } i\text{th question} \end{array} \right\} \quad (3)$$

Step-4: preparation of risk tables

Two risk tables are constructed for our case study (one for the probability of infection parameter and one for the consequences of infection parameter). Each of the tables has five levels to represent the level of risk parameter. These dynamic tables scale the possible results of the surveys of the fundamental risk parameters both quantitatively and qualitatively.

For the probability of infection parameter, there were 21 factors, so 21 survey questions are applied. Until now, each of these questions was weighted. Answer choices were designated to each of these questions. Different number of answer choices was designated for survey questions. For each of the answer choices, numerical values between 0 and 4 are determined.

To construct a risk table, firstly, minimum and maximum numerical values that can be obtained from the survey of risk parameter are found. Formula (3) is applied in order to find the minimum and maximum survey results of the probability of infection parameter. For our case study, the value of ''i'' is 21, ''w_i'' is the weight of ''ith'' question, and ''p_i'' is the value of the answer choice for question-i. Maximum value for a survey is found out by assuming that a participant chooses the most influential answer choice for all questions (so that ''p_i'' has its maximum possible value). In this case, ''maximum output'' equals to 128.

Minimum value for a survey is found by assuming that a participant chooses the least influential answer choice for all the questions (so that ''p_i'' has its maximum possible value). The ''minimum output'' is 29 for our case study.

One hundred and twenty-eight points, which is the maximum possible value for a survey result present the highest probability of infection by a virus. Twenty-nine points, which is the minimum possible value for a survey result present the lowest probability of infection by a virus. In Table 7, the values between 29 and 128 are arranged to represent risk levels. Possible survey results presented in Table 7 are scaled and matched to quantitative and qualitative values.

While building the risk table, the possible survey values are grouped evenly and scaled to represent the level of risk parameter. It may not be possible

Table 4 Factors that affect both the probability and the consequences

Factor	Weight value for probability	Weight value for consequences
The operating system of computer	3	3
The update against vulnerabilities	3	3
The type of user account	2	3
The frequency of update	1	2
Access to the shared folders of other computers	1	2
The number of computers which are accessed by sharing	1	2

Table 5 Numerical values of answer choices

Numerical value of answer choice	Explanation
4	Most effective answer choice. Affect enormously the probability of occurrence or consequences of occurrence.
3	Rather effective answer choice. Affect highly the probability of occurrence or consequences of occurrence.
2	Somewhat effective answer choice. Affect considerably the probability of occurrence or consequences of occurrence.
1	Least effective answer choice. Affect slightly the probability of occurrence or consequences of occurrence.
0	No effect on the probability of occurrence or consequences of occurrence.

for all intervals to be divided evenly. In this case, interval of excess should be assigned to the most critical value. Table 7 is the risk table constructed for the probability of infection parameter. In the case study, the interval of ''very high probability'' is 20. The intervals of other four scales are 19.

The other risk table is for the consequences of infection. The same calculations for maximum and minimum values of survey output were made for the consequences of infection variable during our case study. To find these values, formula (4) is used. This is the same as formula (3), except ''j'' is

Table 6 Some of the questions and their respective answer choices

	Answer choices				
Questions	a	b	c	d	e
What do you do at Internet? (p) (2)	Download (4)	Sending and receiving e-mails (3)	Chat (2)	Reading newspapers and articles (0)	Other:
How many different sites do you visit? (p) (1)	More than 10 (4)	7–9 (3)	5–7 (2)	Less than four (1)	Other:
What type of files do you download? (p) (2)	Executables (4)	Scripts (3)	Documents (1)	No download (0)	Other:
What is the importance of files present at your computer? (c) (3)	Very important and only at my computer (4)	Important, there are copies at other computers (3)	Not important (0)	Other:	–
What is the operating system of your computer? (p) (c) (3) (3)	Belongs to Windows family (4)	Linux/Unix (0)	Other:	–	–
In what account do you use your computer? (p) (c) (2) (3)	Administrator/ root (4)	Normal user (1)	Other:	–	–
Do you update your computer against vulnerabilities? (p) (c) (3) (3)	No (4)	Yes (0)	–	–	–

Table 7 Risk table for the survey of probability of infection parameter

Survey result	Qualitative scale	Quantitative scale
29—48	Very low probability	1
49—68	Low probability	2
69—88	Medium probability	3
89—108	High probability	4
108—128	Very high probability	5

used to represent the questions of the consequences of occurrence parameter.

$$\sum_j w_j p_j \left\{ \begin{array}{l} j: \text{ the number of the question} \\ w: \text{ the weight of the } j\text{th question} \\ p: \text{ the value of the selected answer choice of the } j\text{th question} \end{array} \right\} \quad (4)$$

According to formula (4), ''maximum output'' is found to be 160 and ''minimum output'' is calculated as 47.

Table 8 is constructed for the consequences of infection parameter. For this risk table, interval of excess is 26, which is for ''very serious consequences''. The interval values of other scales are all 21.

A final risk table, Table 9, is prepared by using the fundamental risk formula. The final risk table prevents confusions in the last step of ISRAM, which is the assessment phase. This final risk table is static. The uppermost row of the final risk table shows the quantitative values of probability of infection parameter. The leftmost column shows the quantitative values of consequences of infection parameter. The multiplication of these two values according to formula (1) gives the various risk values between 1 and 25.

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 the method allows ISRAM to apply to diverse information security problems effectively.

Table 8 Risk table for the survey of consequences of infection parameter

Survey result	Qualitative scale	Quantitative scale
47—68	Negligible consequences	1
69—90	Minor consequences	2
90—111	Important consequences	3
112—133	Serious consequences	4
134—160	Very serious consequences	5

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 staff may participate in a survey that plans to express the risk that arises from viruses.

Step-5: conduction of the survey

After preparation of risk tables for two risk parameters and the final risk table, the survey is ready for the distribution to the related staff. Thus, the preparation phase of the survey process is over. At Step-5, the survey questions are distributed to the relevant staff as hard copy. In our case study, one survey, which contains the questions of both risk parameters are submitted to the user. Twenty people participated in the survey.

Step-6: application of formula (2) and obtaining a single risk value

After Step-5 is finished, formula (2) is applied. In our case study, the probability for a computer to be infected by a virus is found to be 3.8, which is close to ''high probability'' at qualitative scale. The consequence of a virus infection is found to be 4.05, which is approximately ''serious consequences'' at qualitative scale. As a result, the value of risk is found to be 15.39, which is high level risk according to the final risk table, Table 9.

Detailed survey results are given in Table 10. In this table, the bulk survey results, simplified survey results (after risk conversion tables) for all participants, values of risk parameters and the final risk value are given. The detail of application of formula (2) is clearly seen in Table 10.

Step-7: assessment of the results

The most important output of ISRAM is the single risk value obtained at Step-6. This risk value is obtained after performing considerable amount of preliminary work including listing the factors, designating answer choices, weighting the factors, giving numerical values to answer choices and preparing risk tables. The quality of this preliminary work definitely affects the accuracy of single risk value.

Table 9 The final risk table prepared from risk tables (Tables 7 and 8)

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

On the other hand, not only these calculations and the final numerical result are considered but also answers given for questions are examined in detail by the risk analysts while assessing the survey results.

By examining the answers to the survey questions in the case study, some important results are obtained. Some of the users have administrative privileges while using their computers, which increases both the probability and consequences. USB storage devices and CD-ROMs (not floppies) widely used in the network. Most of the users do not backup their data. A small group of the users download programs. Half of the participants do not patch their computer. This is a great vulnerability for virus infection. In general, user security awareness should reduce somewhat the probability and consequences of infection.

The structure of ISRAM allows the gross risk and net risk calculations. After user security awareness program is held, the same survey is performed to obtain the net risk value. In our case study, after user security awareness program, risk value is found to be 14.3, which is between medium and high risk but very close to the high risk level.

The assessment of survey results is an important part of ISRAM. Managers and staff can easily

Table 10 Survey results

Participant-m (m is equal to n in our case study)	Probability of infection (bulk result) $\sum_i w_i p_i$ where $i = 21$	T_1	Consequences of infection (bulk result) $\sum_j w_j p_j$ where $j = 15$	T_2
Participant-1	94	4	103	3
Participant-2	100	4	124	4
Participant-3	74	3	95	3
Participant-4	73	3	112	4
Participant-5	110	5	121	4
Participant-6	97	4	113	4
Participant-7	89	4	129	4
Participant-8	88	3	118	4
Participant-9	99	4	105	3
Participant-10	85	3	135	5
Participant-11	93	4	136	5
Participant-12	124	5	156	5
Participant-13	69	3	98	3
Participant-14	95	4	123	4
Participant-15	96	4	145	5
Participant-16	90	4	119	4
Participant-17	118	5	135	5
Participant-18	71	3	129	4
Participant-19	94	4	113	4
Participant-20	71	3	123	4
	$\left(\frac{\sum_m [T_1(\sum_i w_i p_i)]}{m}\right) =$	3.8	$\left(\frac{\sum_n [T_2(\sum_j w_j p_j)]}{n}\right) =$	4.05
	$\text{Risk} = \left(\frac{\sum_m [T_1(\sum_i w_i p_i)]}{m}\right)\left(\frac{\sum_n [T_2(\sum_j w_j p_j)]}{n}\right) =$			15.39

participate into this step like other steps and express their opinions.

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

Verification, comparison and the results of the application

In order to verify the results of ISRAM case study, we have gathered statistical data and run simulation based on statistical data obtained. Arena simulation software has been used 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 removable media (USB storage devices, floppy diskettes and CD-ROMs). So, the gathered statistical data are composed of the number of received e-mails, downloads and storage media usage per day, per computer and per user basis. The statistical data were gathered for one month. During this month, virus incidents were carefully noted. The sources and number of infections were written down.

After the completion of gathering of the statistical data, three independent risk models were constructed at Arena software because of the independency of sources of data, which come to computers.

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

The gathered statistical data were imported into the risk model and based upon the real statistical data, Arena software simulated the situation of the test network as if one year of period had passed. Table 11 shows the final result of this simulation.

The simulation results revealed the similar results as ISRAM application. As it is seen in Table 11, there are a number of virus infections in one year, which can correspond to the high level of probability. Also, as it can be easily seen from the last five rows of table, most of the infected viruses have serious consequences. These two results are compatible with the results obtained at the Step-6 of ISRAM. At Step-6 of ISRAM, formula (2) was applied and single values for probability of infection and consequences of infection were found. The value for the first parameter was close to high probability level and the value for the second parameter was approximately equal to serious consequences level.

"As-if" analyses are also performed during simulation. If the users perform updates and backup operations, the probability and consequences of virus infections decrease dramatically. But it

Table 11 Simulation results

Risk report 1	Date: 17 May 2004
E-mail virus model	Time: 2:34:51PM
Model parameter	Average
Total e-mails	25342.1000
The number of e-mails that contain viruses	42.6000
The number of e-mails that contain viruses, which infect	32.5000
Total downloads	5245.1200
The number of downloads that contain viruses	12.0732
The number of downloads that contain viruses, which infect	10.0200
Total storage media usage	17445.3400
The number of storage media that contain viruses	8.334
The number of storage media that contain viruses, which infect	6.5300
The number of infections that cause very serious consequences	3.0000
The number of infections that cause serious consequences	19.0500
The number of infections that cause important consequences	5.0450
The number of infections that cause minor consequences	12.9550
The number of infections that cause negligible consequences	9.0000

should not be expected from users to perform these operations.

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

An important advantage of ISRAM is its appropriateness to ALE calculations. In order to present the survey result to the senior management, ALE calculations can be performed. Some managers may desire to see monetary losses rather then single numerical values.

Calculation of ALE can be achieved as in formula (5).

$$\text{Annual Loss Expectancy} = \text{Threat Occurrence Rate per Year} \times \text{Single Loss Expectancy} \quad (5)$$

where, the unit of Annual Loss Expectancy is ''dollars per year''. Similarly the unit of Single Loss Expectancy is ''dollars per worst case occurrence''. ''Threat Occurrence Rate per Year'' can be characterized as ''the probability of virus infection'' and ''Single Loss Expectancy — SLE'' can be characterized as ''the consequences of virus infection''

For ALE calculation, it is necessary to convert the numerical values of two risk parameters to threat occurrence per year and SLE values. In our case study, the probability of virus infection was found to be 3.8 — high probability, the consequence of a virus infection was found to be 4.05 — serious consequences. Risk analysts can convert these results to ''Threat Occurrence Rate per Year'' and ''Single Loss Expectancy'' values by taking companies situation into consideration. For our case study, ''Threat Occurrence Rate per Year'' is designated as 50 occurrences per year and ''Single Loss Expectancy'' is designated as 40$. Therefore, ALE is equal to 2000$. This is more than the cost of an antivirus software package for an institute. Thus, it is easily said that the lack of antivirus software exposes high risk to institute.

Conclusion

In this study, a novel method, ISRAM, is proposed for information security risk analysis. The proposed method is based on a quantitative approach that uses survey results to analyze information security risks.

Quantitative tools included in ISRAM are simple numbers related with the survey, risk tables, addition, multiplication and division operations. The main advantage of ISRAM over other risk analysis methods is its ease of use. There are no complicated mathematical and statistical instruments in ISRAM.

Previously, it was mentioned that qualitative methods might give subjective results. ISRAM is a quantitative tool with well-defined steps and mathematical measures. With a careful operation, ISRAM gives objective risk results. The comparison of the case study and simulation results proves this statement.

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 ISRAM. ISRAM 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. ISRAM has well-defined steps, and therefore it is deterministic. There is no risk of long period of analysis like the paper-based methods.

Because ISRAM is a quantitative method which does not contain complicated mathematical and statistical instruments, manager and the staff may effectively participate in the risk analysis process. It is suggested that information security risk analysis should be more business oriented. Thus, less technology and more culture and organization should be used in order to succeed (McEvoy and Whitcombe, 2002; Sommer, 1994; Reid and Floyd, 2001). ISRAM fulfills both the business and technology requirements by taking today's needs into consideration.

ISRAM 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 arises from the weaknesses of information security policies.

References

Bilbao A. TUAR. A model of risk analysis in the security field, CH3119-5/92. IEEE; 1992.

C&A Systems Security Limited. COBRA consultant products for windows. Evaluation & user guide; 2000.

Coles RS, Moulton R. Operationalizing IT risk management. Computers & Security 2003;22(6):487—93.

Gerber M, Solms RV. From risk analysis to security requirements. Computers & Security 2001;20(7):577—84.

Gordon J. Security modelling, risk analysis methods and tools. IEE colloquium; 1992. p. 6/1—6/5.

Information Security Forum (ISF). Simplified practical risk analysis methodology (SPRINT) user guide; 1997. p. 43—57.

ISO. Evaluation criteria for IT security ISO15408, Parts 1 thru 3. Geneva: ISO; 1999.
ISO. Guidelines for the management of IT security ISO 13335, Parts 1 thru 5. Geneva: ISO; 1996—2001.
ISO. Code of practice for information security management ISO 17799. Geneva: ISO; 2000.
Jacobson RV. Using CORA to implement the NIST risk management guide Available from: <http://www.ist-usa.com/Downloads/UsingCORA with NISTSP800-30.zip>; 2002.
Jenkins BD. Security risk analysis and management White Paper, Countermeasures Inc. Available from: <http://www.cs.kau.se/~albin/Documents/RA_by%20Jenkins.pdf>; 1998.
Kailey MP, Jarratt P. RAMeX: a prototype expert system for computer security risk analysis and management. Computers & Security 1995;14(5):449—63.
McEvoy N, Whitcombe A. Structured risk analysis InfraSec 2002. LNCS 2437; 2002. p. 88—103.
Moulton R, Coles RS. Applying information security governance. Computers & Security 2003;22(7):580—4.
National Institute of Standards and Technology (NIST). Risk management guide for information technology systems 2001. Special Publication 800-30.
Owens S. Information security management: an introduction. British Standards Institution; 1998.
Reid RC, Floyd SA. Extending the risk analysis model to include market-insurance. Computers & Security 2001;20(4):331—9.
Spinellis D, Kokolakis S, Gritzalis S. Security requirements, risks and recommendations for small enterprise and home—office environments. Information Management & Computer Security 1999;7(3):121—8.
Sommer P. Industrial espionage: analysing the risk. Computers & Security 1994;13(7):558—63.
Toval A, Nicolas J, Moros B, Garcia F. Requirements reuse for improving systems security: a practitioner's approach. Requirements Engineering 2002;6:205—19.
United Kingdom Central Computer and Telecommunication Agency (CCTA). Risk analysis and management method, CRAMM user guide, Issue 2.0 2001.
United States General Accounting Office (USGAO). Information security risk assessment, <http://www.gao.gov/cgi-bin/getrpt?GAO/AIMD-00-33>; 1999.

Bilge Karabacak received his B.Sc. degree in Electronic Engineering from Bilkent University in 1999, and his M.Sc. degree in Computer Engineering from Gebze Institute of Technology in 2003. Currently he is pursuing Ph.D. degree in Computer Engineering at Gebze Institute of Technology. His interested areas are risk management, network security and application security.

Ibrahim Sogukpınar received his B.Sc. degree in Electronic and Communications Engineering from Technical University of İstanbul in 1982, and his M.Sc. degree in Computer and Control Engineering from Technical University of İstanbul in 1985. He received his Ph.D. degree in Computer and Control Engineering from Technical University of İstanbul in 1995. Currently he is the Assistant Professor at Computer Engineering Department in Gebze Institute of Technology. His interested areas are information security, networking, information systems applications and computer vision.