International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:5, No:6, 2011

Application of Process Approach to Evaluate the Information Security Risk and its Implementation in an Iranian Private Bank

Isa Nakhai Kamal Abadi, Esmaeel Saberi, Ehsan Mirjafari

***Abstract*—**Every organization is continually subject to new damages and threats which can be resulted from their operations or their goal accomplishment. Methods of providing the security of space and applied tools have been widely changed with increasing application and development of information technology (IT). From this viewpoint, information security management systems were evolved to construct and prevent reiterating the experienced methods. In general, the correct response in information security management systems requires correct decision making, which in turn requires the comprehensive effort of managers and everyone involved in each plan or decision making. Obviously, all aspects of work or decision are not defined in all decision making conditions; therefore, the possible or certain risks should be considered when making decisions. This is the subject of risk management and it can influence the decisions. Investigation of different approaches in the field of risk management demonstrates their progress from quantitative to qualitative methods with a process approach.

***Keywords*—**Risk Management; Information Security; Methodology; Probability

I. Introduction

INFORMATION technology (IT) is of a vital role in many modern informational organizations. Nowadays, the IT infrastructure in organizations is situated within an environment where the number of enemies and invaders who do not like the continuous, safe and helpful existing of computer systems, is increasingly grown. Unfortunately, many organizations cannot react appropriately against new security threats in appropriate time and before the computer systems are abused.

Decreasing the time needed to react against the security threats and increasing the efficiency are common needs of organizations and users. In order to provide the appropriate and organized reaction against security threats, the security risk management has become an essential need in IT institutes. At present, the digital information which is accessible, reliable and protected against possible risks is widely used. This has confronted the individuals and organizations with a new category of threats which influence the existent information.

In many organizations, the need for security risk management is felt after a small security event like virus infection of a computer or attacking the organization's website. The security issues and problems will rise with increasing and intensification of attacks. The organizations are disappointed in rational confronting with the security problems and will resort to passive solutions for their security problems.[1]

Unrestrained increase of successful network-based attacks proves the necessity of implementation of a preventive approach (rather than the passive approach) in security risk management for many organizations.

II. Objective

The main goals of an organization may include preserving the organization entity and preserving its phase in customers', staff's, managers' and investors' minds. These will not be achieved only through unreal classification of documents and information and using the information security labels (secret …), taking separate rooms and sites for information processing equipment, entrance limitations in some places and setting passwords for accessing the systems.[2]

To make safe the movable or immovable, human and immaterial properties of the organization, some planning-related activities are necessary. The planning for preserving the organization resources can be claimed to be relatively performed when the planning covers different aspects of properties preservation, the necessary news and educations have been offered to all staff in all levels, the necessary controls for property preservation have been defined and implemented, the safety-related responsibilities have been defined and assigned, all activities are periodically revised and optimized, and the organization's survival conditions are specified and provided.

The main method to achieve the above goal is establishing an information security management system.[3]

III. Importance of Information Security

Information, their supporting processes, systems and networks are considered as important business capitals. Information privacy, accuracy and accessibility are the bases of immanency in area of competition, helpfulness, accurate performance and economical impact. Organizations and their networks and information systems are increasingly threaten with different types of security risks. These risks include:

Prof. Isa Nakhai Kamal Abadi is an Associate Professor in Tarbiat Modares University, (phone: 98-21-82884387; fax: 98-21-88005040; e-mail: Nakhai@modares.ac.ir).

Esmaeel Saberi, is a PhD Student in Industrial Engineering in Tarbiat Modares University, (phone: 98-912-2372254; e-mail: h.smath80@gmail.com).

Ehsan Mirjafari graduated from Isfahan university in M.sc in Industrial Engineering, now he is an executive manager of Samar rayaneh company, (phone: 98-912-2750739; e-mail: samehsan2000@yahoo.com)

Inhibition by means of computer, spying, internal obstructions, targeted obstructions, water and fire

The damage resources such as computer viruses, computer hacking and denial of service attacks have been increasingly common, influent and complex.[4]

Depending upon the type of the tools, the information systems and services of the organizations have become extremely vulnerable against security threats. Connections between public and private networks and sharing of the available information resources have increased the problems in accessibility control. The tendency to distributed computer environments has decreased the efficiency of concentrated and specialized controls.

Most information systems are not designed secure. Technical tools are limited in offering the security, and such limitations should be encountered through appropriate procedures and management. Specifying the required types of controls necessitates the accurate design and considering the components.

Information security management requires participation of all staff, suppliers, customers, copartners and up and down parts. Making use of counseling and the expert information out of the organization is also necessary.

Information security controls will be much inexpensive and efficient when they are paid attention in design and needs assessment stages.[5]

IV. Different Management Approaches to the Information Security Problem

Executive and medium managers who directly work with computers are thoroughly aware of security needs of their systems. They know their systems and their weaknesses. However, the upper or superior managers do not use computers or do not have enough awareness of performance of their organization's information systems, due to being busy. Defining long-term strategies to deal with the security problem is dependent on decisions made by upper strategic managers in each organization. It is the duty of executive and medium managers to create in upper managers' minds an appropriate picture of the need to allocate enough power and budget to this vital issue in the organization.[6]

V. How to Provide the Security Needs

Providing the organization with its security needs is the most essential subject in this context, which is achieved as followed:[7]

- The first way to get secure is identifying the risks the organization is faced with. In this way, the threats to properties are determined. The vulnerabilities and their probability of occurrence are assessed and their potential impacts are estimated.
- The second determinant factor is legal, penal, supervisory and formal conditions determined for the organization, its copartners, contract partners and service suppliers.
- The third factor includes a defined set of concepts, goals and information processing conditions specified by the organization in order to support its performance.

V. Information Security Management System (ISMS)

When the first information security management standard was published in 1995, systematic approach to making safe and secure information exchange environments was formed. In this approach, the security of information exchange environments for the organizations cannot be abruptly provided, and this should be performed gradually in a cycle including design, implementation, evaluation and modification stages. For this purpose, each organization is required to perform the following activities based on a specific methodology:[8]

1. Preparing the security plans and projects needed by the organization
2. Preparing the devices and tools needed for continuous safety of the information exchange environment of the organization
3. Implementation of security plans and projects of the organization

VI. Risk Management Methodologies

In this stage, the main objective is to identify the relevant threats, damages and risks. Due to being systematic and comprehensive, this procedure ensures us that no risk is inadvertently skipped over. In this stage, it is very important to identify all risks, regardless of those which may previously been identified or controlled by the organization.

The first step includes preparing a full list of sources of threats, risks and events which may influence the achievement of each of organization's goals. These events may have preventive, decreasing, delaying or facilitating effect on goal achievement.

Generally, a risk can be identified from the following:[9]

a) Its source (for example, in an institute it may include nonconformist staff, untrained staff, competitors, governments …)
b) Specific activities and events (such as unallowable information release …)
c) Consequences and effects (for example, service inaccessibility, loss or profit in the market, increase of the regulations, increase or decrease of universality, crime …)
d) A specific cause of events (for example, error in system design, individual interference, prediction or error in prediction of the competitor's activities)
e) Preventive controls and mechanisms (for example, access diagnosis and control systems, policies, security training, market research and market monitoring)

f) Time and place of events

High-quality information and sufficient knowledge of the organization and its internal and external environment plays an important role in risk identification. Previous information on the organization or other similar (competitive or non-competitive) organizations can also be helpful in accurate prediction of those events which the organization has not yet been faced with.

The following techniques can be used in choosing the risk identification methodology:[10]

- Brainstorming technique
- Structural techniques, such as flowchart, system design browsing, analysis of the systems, studying the risks and their probability, and operational models

Identification of strategic process risks, using other general structures like "what-if" and analysis of the scenarios in use.

The information obtained from this stage is the first input for decision-makers, telling them which risks they are faced with and what is the most efficient methodology considering the related costs.

Risk analysis includes:[11]

- Concentrated test of risk sources
- Their positive and negative impacts
- Probability of occurrence, consequences, and their impact coefficients
- Evaluation of controls or the available processing which minimizes the negative or positive impacts of the risk (these controls can be obtained from a large number of standards)

The risk level is calculated by statistical analyses and integrative calculation of the probability and the impact of risks. All formulations and methods used for such integration should be compatible with the crisis state mentioned in risk management definitions.

The information used in calculation of the probability and impact of the risk is usually estimated from these resources:[11]

- Prior experience or saved information (such as event reports)
- Reliable methods, instructions or international standards
- Market analysis
- Primary models and experiences
- Economical, engineering or other models
- The expert opinions

Risk analysis techniques include:[11]

- Interview with the expert and using a questionnaire
- Using the available simulators and models

Checklist and its items

A checklist contains a number of questions in form of a checklist. The questions are designed by the target society in order to find which of the security tasks should be performed in a control form and which should be considered in planning form. Checklist can be a useful tool in managing the control tasks and their related status.[4]

Questionnaire and its items

A questionnaire is also a list of questions, but prepared with a different purpose. Filling in a questionnaire helps prepare a list of active assets, possible threats and executive controls.

Risk analysis can be qualitative, semi-quantitative, quantitative or a combination of all. We give a brief description of each type of analysis.

- Qualitative analysis can be used in the following cases:[4]
  - A primary evaluation for identifying the future risks and analyzing their details
  - Representing the intangible risks (such as validity, culture and picture of the organization …)
  - When acceptable or quantitative information or sources for the quantitative statistical approach are rare
- Semi-quantitative analysis

  Semi-quantitative analysis is intended for assigning values to qualitative evaluations. These numbers are not usually real values and have an index role, which is the pre-requisite of a qualitative approach.
- Quantitative analysis

  In this type of analysis, the values are assigned to both risk impacts and risk probabilities. This information is obtained from different resources. The quality of the analysis depends on the assigned values and the accuracy of the models used.[4]

The risk impact could be obtained by evaluation and processing the results of different events or by estimating from previous information or experimental investigations. Results can be reported in different conditions:[8]

- Financial
- Technical
- Operational
- Human

VII. The Comprehensive Quantitative Risk Evaluation Model

The quantitative model is based on the attacks, the consequences of attacks, the countermeasures, the effects of countermeasures, and two main output or index types. These main outputs are:

- Risk value (VAR)
- Risk rate of capital return (PROI) which is the difference between the net profit of preventive activities and the cost of each control measure to control the security risks.[12]

To obtain the VAR and PROI indices, the types of attacks and their frequency of occurrence in the last year is necessary as the input. Using this information and the percentage of

attacks it covers, the number of attacks in a given year could be predicted.

In this method, a key hypothesis is emphasized; i.e. the close past is a good guide to what happens in the future. In other words, the security threats are expected to only slightly change, relative to the last year.[13]

For the threat i, the frequency of occurrence is denoted with Fi and the coverage with Gi (<1). The coverage represents the amount of information saved and stored in comparison with the number of events actually happened. The ideal state is Gi=1. The following equation gives an estimation of the number of attacks occurred:[13]

Another input parameter of the model is the efficiency of the countermeasure against any threat. For any countermeasure i against the threat j, the efficiency is denoted with Cij.

The probability that all countermeasures fail against the attack i, is:[13]

This equation represents the hypothesis that all countermeasures are independent on each other.

The number of attacks occurring in the absence of any countermeasures against threats is obtained from:[13]

And the number of attacks occurring in the presence of countermeasures is obtained as followed:[13]

There is an important difference between a special threat and its consequences. The countermeasures can neutralize the attacks, but it is the attack consequences which influences the organization. The relationship between the attacks and their consequences is demonstrated by a matrix (αij). For example, the attack i can result in two consequences. The first is missing all information by 100% probability, and the second is inaccessibility of the allowed users by 70% probability. Thus, αij=1 and αi,2=0.7, and for other consequences of threats, αi,j=0.[13]

In this stage, we should consider the losses resulted from attacks. One of such cases is when we consider the annual salary of an expert, denoted with M. The daily cost of an expert is estimated by the equation: P = 1.5M/365, where 1.5 is a factor representing taxes, insurance costs and other overhead costs. The cost P helps estimate the expected amount of losses.

As an input parameter, the days an expert has spent on the following attempts and activities should also be considered:[9]

1. Attempts and activities to identify an attack
2. Attempts and activities to report an attack
3. Attempts and activities to fix the damages due to the attack
4. Attempts and activities to specify the loss of organization's reputation as a result of the attack

For each attack j, we define the nominal loss as followed:[9] where C is the cost parameter which is not present in other elements, and Djk is the amount of loss, in which k represents the four types of losses resulting from the attacks (identification, report, fixing the damages and reconstruction, and backup).

The expected loss ELi can be calculated by using the nominal loss. In this calculation, the severity of the attack is indicated by Sj,*. If consequences of an attack is ten-fold that of an attack of the same type, the severity is denoted with Sj,10, and if it is 100-fold or 1000-fold that of an attack of the same type, the severity is indicated by Sj,100 and Sj,1000, respectively. Therefore, we have:[13]

Through combining the previous outputs, the expected loss in presence and in absence of countermeasures can be calculated. Now, we can obtain the residual losses for consequences of each attack, denoted by ELCJ. The related equation resembles that of the expected loss in presence of countermeasures:[13]

In previous sections, we considered and calculated the residual risks and their effects. However, the profits gained from any control or countermeasure should also be calculated and considered in decision-making process. We indicate the capital costs with r and a specific period in year with t. the expected loss in the absence of countermeasures is calculated as followed:[13]

Stage 1 is devoted to evaluation of superficial aspects of the organization. During this stage, the analysis team defines the conditions for evaluating the effects which will be later used for risk evaluation. Specifying the importance of the organization's properties and evaluation of its current security methods are also performed in this stage.

The team members perform all activities and collect additional information when needed. The team selects 3 to 5 important assets for a comprehensive analysis based on their relative importance in the organization. Then, the security needs and a threat profile are defined for each important asset.[14]

During this stage, the analysis team performs high-level monitoring of computer infrastructures within the organization, focusing on areas in which the security is an essential need. The team, first, analyzes how the individuals apply the computer infrastructures to access the important assets.[14]

During the third stage, the team specifies the risks of the important assets of the organization and decides on how to encounter with them. Based on the analysis of collected information, the team proposes a protective strategy for the organization and a plan for decreasing the risks of important assets.[14]

VIII. Evaluation of Security Risks of a Bank

In order to analyze the effects of possible threats on assets and equipment of a bank, the value-generating processes in the bank were first identified through interview with the bank experts and three degrees of importance, namely 1, 2, 3, were assigned to the processes. This resulted in a classification of services, shown in Fig. 1.

To identify the risks and their level, a list of all information properties should first be prepared. In this step, all the information properties of the bank were identified in the scope of the information security management system of the bank. The assets and their relevant services are listed in Table 1.

All possible threats should be recognized in this step and a list should be prepared indicating all threats against the information properties in the scope of project.

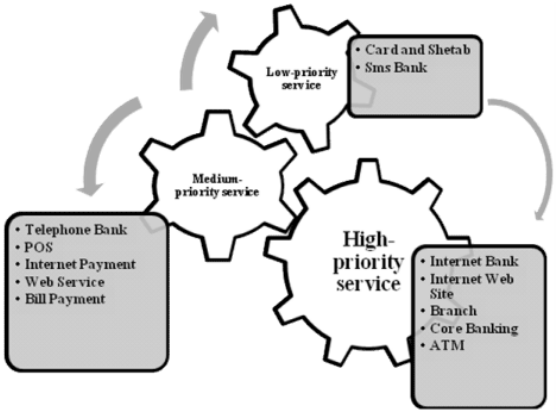

Fig. 1 Classification of value-generating processes in the bank

Possible threats for the equipment and services of the bank were first investigated. We considered four threat types for the equipment, including hardware problems, software problems, disconnection problems and physical threats. Then, a list of the most important possible threats for the bank's equipment was prepared, as shown in Table 2.

For an elucidate analysis and simple results, the obtained qualitative results were converted into quantitative values in this phase, as indicated in Table 3.

Table 3: Conversion of qualitative parameters into quantitative

In this step, the acceptable and inacceptable risks should be determined.

Through analyses performed for all equipment, a detailed list of threats was prepared. From this list, the threats able to stop the bank services were extracted.

Firstly, the PI index was defined as the product of values for probabilities and effects, indicating the priority of the threat before considering the priority of the service. The values for priority of service were then included in the matrix of priority of threat and values were assigned to threats based on the value of their effect on processes in the organization.

In addition, the final index was defined, representing the amount of risk of each threat for each of the equipment considering the importance of the relevant process. This index is obtained by multiplying the PI by the value for priority of service.

PI = Probability * Effect

Final index of the threat = PI * Priority of service index

TABLE I
STANDARD THREATS MATRIX

	PI Index						
Service Priority		1	2	3	4	6	9
	1	Yellow	Yellow	Yellow	Yellow	Blue	Blue
	2	Yellow	Yellow	Blue	Blue	Red	Red
	3	Red	Red	Blue	Red	Red	Red

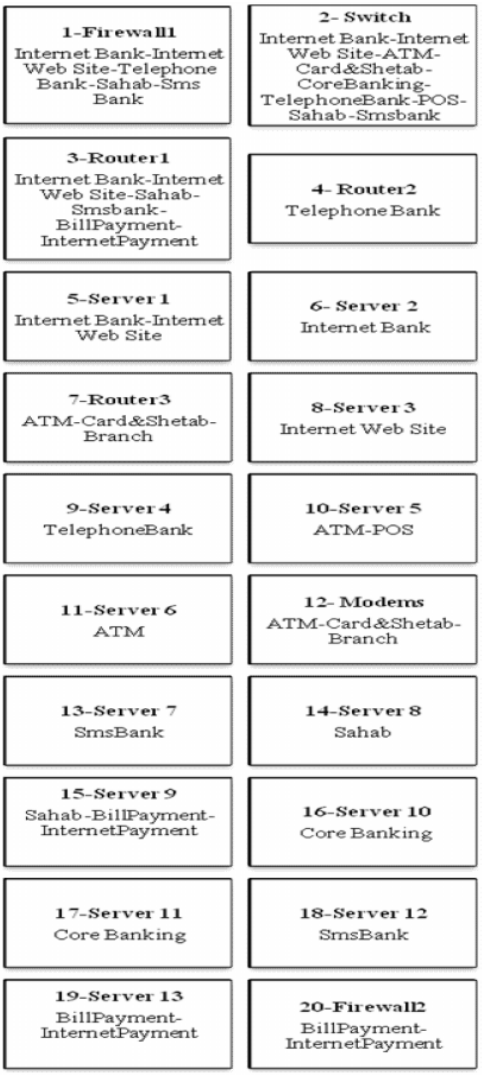

Fig. 2 List of the bank's assets and the utilizing services

TABLE II
LIST OF POSSIBLE THREATS

1	Problems in electrical systems	10	Data manipulation
2	Disconnection	11	Non Repudiation
3	Inaccessibility to third party services	12	Information revelation
4	Hardware problems	13	Denial of service (DoS)
5	Physical access to systems	14	Incorrect usage by the user
6	Natural events	15	Use of non-standard equipment

7	Hardware larceny	16	Inappropriate maintenance of the equipment
8	Out of date antivirus programs	17	Open ports
9	Impersonation		

TABLE III
ONES TO ANALYZE THE THREATS

Process importance			Occurrence probability			Threat effect		
Low	Medium	High	Low	Medium	High	Small	Medium	Large
1	2	3	1	2	3	1	2	3

As seen in Table 4, the zone 1 in the priority matrix was recognized, based on investigations, to contain threats of small effect on the bank's business and was highlighted in yellow. Zone 2 contains threats of medium priority, highlighted in blue. Zone 3 was recognized to contain the threats with large effects on the bank's business and was highlighted in red.

In this step, the risk related to each property was calculated based on mentioned equations and using the probability of making use of the vulnerability and the amount of its effect.

Extracting the hazardous threats

The effects of all threats on the equipment in the bank were investigated in the previous step and the final index of threat was calculated using the priorities of processes in the bank which were specified by clientele. Threats which, if occurred, lead to hazardous effects on the bank's regular services were extracted (considering the occurrence probabilities). Table 5 indicates the threats which, if occurred for related equipment or specific services, result in severe and occasionally destructive effects on electronic services of the bank.

IX. Conclusions

In this paper, the definition of risk and its management methods in different systems including the information systems were presented. Different approaches in risk identification, reduction and evaluation were also discussed in detail. As mentioned earlier, the area of information technology is a dynamic and sensitive area, in that it deals with the most important resource in the organization, i.e. the information. Furthermore, we continually encounter with new technologies with their own features, advantages and disadvantages, which necessarily we cannot avoid. Therefore, in such conditions, the risk management is required to be reiterated in a cycle in order to ensure safety and security in utilization of new technologies for the organization managers. However, it should be considered that different organizations are subject to different levels of risk, depending upon their type of activities and sensitivity of their assets; hence, they should implement the appropriate risk management processes. During many years, a shift from quantitative methodologies to qualitative ones with process approach was occurred in information security risk management methods.

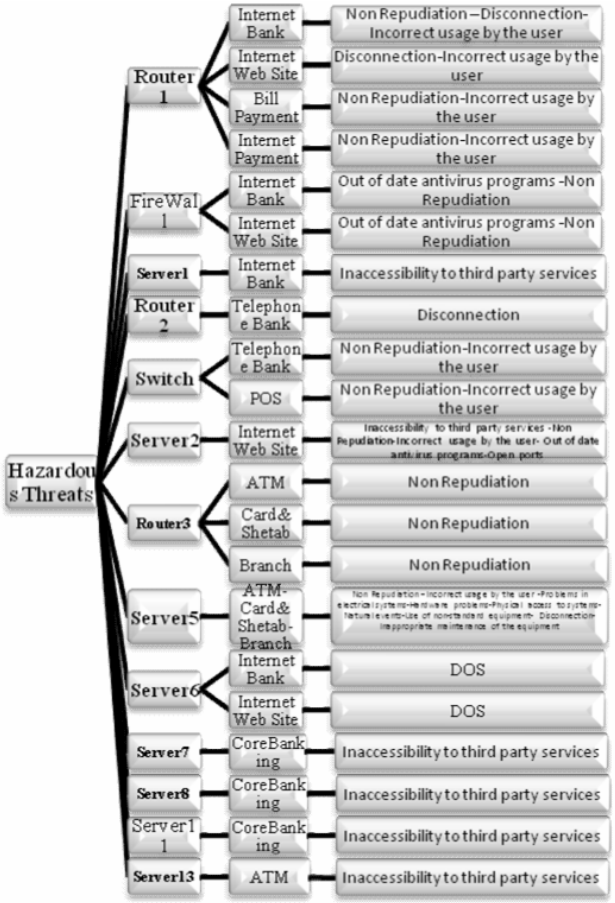

Fig. 3 Hazardous threats

References

[1] A. Arora, D. Hall, A. Pinto, D. Ramsey, and R. Telang. Measuring the risk-based value of IT security solutions. IEEE IT PRO, November/December 2004.

[2] Atsec information security corporation,"ISMS Implementation Guide" ,2007,www.atsec.com

[3] B. Blakley. A measure of information security in dollars. In Proceedings (online) of the First Annual Workshop on Economics and Information Security (WEIS'02), Berkeley, CA, May 2002.

[4] C. Alberts and A. Dorofee. An introduction to the OCTAVE method, January 2001. http:

[5] //www.cert.org/octave/methodintro.html.

[6] Christopher Alberts, Audrey Dorofee, James Stevens & Carol Woody, "OCTAVE-S Implementation Guide-Volume 1: Introduction to OCTAVE-S",January 2005

[7] Christopher Alberts, Audrey Dorofee, James Stevens & Carol Woody, "OCTAVE-S Implementation Guide-Volume 2: Preparation Guidance",January 2005

[8] Christopher Alberts, Audrey Dorofee, James Stevens & Carol Woody, "OCTAVE-S Implementation Guide-Volume 10: Example Scenario",January 2005

[9] D. Greer, K. Hoo, and A. Jacquith. Information security: Why the future belongs to the quants. IEEE Security and Privacy, pages 24–32, July/August 2003.

[10] D. Tan. Quantitative risk analysis step-by-step, 2002. SANS Institute Reading Room paper#849. http://www.sans.org/reading_room/whitepapers/auditing/849.php.
[11] J. Meritt. A method for quantitative risk analysis. In Proceedings of the 22nd National Information Security Systems Conference, Arlington, VA, October 1999.
[12] K. Soo Hoo. How Much Security Is Enough? A Risk Management Approach to Security. PhD thesis, June 2000.
[13] L. Gordon, M. Loeb, and T. Sohail. A framework for using insurance for cyber risk management. Communications of ACM, pages 81–85, March 2003.
[14] Mohammed A. Bashir and Nicolas Christin , "Three Case Studies in Quantitative Information Risk Analysis" , 2007
[15] Secure insight analysis, 2007. http://wwwdastet.msbai.com/.