Chinese Business Review, ISSN 1537-1506
December 2011, Vol. 10, No. 12, 1106-1110

Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches

Stroie Elena Ramona
Academy of Economic Studies, Bucharest, Romania

Due to rapidly development of information systems, risk and security issues have increased and became a phenomenon that concerns every organization, without considering the size of it. To achieve desired results, managers have to implement methods of evaluating and mitigating risk as part of a process well elaborated. Security risk management helps managers to better control the business practices and improve the business process. An effective risk management process is based on a successful IT security program. This doesn't mean that the main goal of an organization's risk management process is to protect its IT assets, but to protect the organization and its ability to perform their missions. During this process, managers have to take into consideration risks that can affect the organization and apply the most suitable measures to minimize their impact. The most important task is choosing the best suited method for analyzing the existing risk properly. Several methods have been developed, being classified in quantitative and qualitative approaches of evaluating risk. The purpose of this paper is to present the advantages and disadvantages of each approach taking current needs and opportunities into consideration.

Keywords: risk management, risk analysis, risk assessment, quantitative approach, qualitative approach

Introduction

Today's economic context is characterized by a competitive environment which is permanently changing. To face this fierce competition, managers must take the correct strategic decisions based on real information. The management risk of the security information plays a very important role in the organizational risk management, because it assures the protection of the organization from the threatening informational attacks that could affect the business activity and therefore its goal.

An effective risk management process is based on a successful IT security program. The risk management process should not be treated primarily as a technical function carried out by the IT experts, who operate and manage the IT system, but as an essential management function of the organization and its leaders (Stoneburner, Goguen, & Feringa, 2002).

Risk Management's Definitions and Objectives

The concept of the risk management is a very common term amongst those concerned with IT security. A generic definition of risk management is the assessment and mitigation of potential issues that are a threat to a business, whatever their source or origin (Southern, Creating risk management strategies for IT security, 2009).

Stroie Elena Ramona, Ph.D. candidate, Information Researchers, Department of Economic Cybernetics, Academy of Economic Studies.
Correspondence concerning this article should be addressed to Stroie Elena Ramona, Alexandru cel Bun Street, 22, Bucharest, Romania. E-mail: ramona.stroie@gmail.com.

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in order to reduce risk to acceptable levels, activity which can increase the probability of success and decrease the uncertainty of achieving objectives. Risk management should be an evolving process (Certified Information Systems Auditors, 2006).

The most important goals of risk management are accomplished by better securing the IT systems that store, process, or transmit the organization's information; by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget and by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management (*Achieving best practice in your business information security: Protecting your business assets*).

Risk Analysis—General Perspective

Risk management consists of two main activities: risk assessment/analysis and risk mitigation (*An introduction to computer security: The NIST handbook*). Risk assessment process includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Risk mitigation refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process.

During the process of risk analysis risks in the system have to be discovered, in order to find all possible threat paths from potential attackers to assets of concern (Chivers, Clark, & Cheng, 2009). The process identifies, quantifies or qualitatively describes risks and prioritizes them against the risk evaluation criteria established within the course of the context establishment process and according to objectives relevant to the organization (*An introduction to computer security: The NIST handbook*).

Risk analysis should include processes of security risk identification, risk degree determination and identification areas with a high level of risk that should be secured. Risk analysis should be implemented to identify organization's assets and controls that should be applied to ensure an acceptable security level, to warn the management board about imminent risks and to indicate the necessity of corrective measures. The greatest benefit of the analysis consists of allowing managers to examine all current identified concerns, prioritize the level of vulnerability and select an appropriate level of control or accept the risk (Thomas, 2001).

To discuss the definition of the risk management, it is necessary to explain the meaning of the three main concepts:

- Risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome);
- Threat is the potential cause of an unwanted impact on a system or organization (ISO 13335-1). Threat can also be defined as an undesired event (intentional or unintentional) that may cause damage to the goods of the organization;
- Vulnerability is a weakness in system procedures, architectural system, its implementation, internal control and other causes that can be exploited to bypass security systems and unauthorized access to information. Vulnerability represents any weakness, administrative process, act or statement that makes information about an

asset to be capable of being exploited by a threat.

Quantitative Approach of Risk Analysis

The goal of quantitative approach is to calculate numeric values associated to each component that result after risk evaluation. It is estimated the real value of the assets taking into consideration the cost of replacement, the cost of the productivity loss, the cost of brand reputation damage and other values that represent direct or indirect assets for the organization.

Quantitative approach of risk consists of few steps that have to be followed. During the first step the company's assets are identified and evaluate in order to estimate potential loss in case of an attack. Replacement costs have to be established in case an asset is partially or completely destroyed. Every asset, in case of loss or malfunctioning, has an impact on one of the three main elements necessary to ensure security: confidentiality, integrity and availability. Confidentiality is the property of the data which defines the fact that the information is not compromised through being accessed by unauthorized users. Integrity is the property of the data which defines the fact that information is not altered by unauthorized users, in a way that is detected or undetectable by authorized users. Availability ensures that principals (users and computers) have appropriate access to resources (Bojanc, Jerman-Blazic, An economic modeling approach to information security risk management, 2008).

After these steps, the Annual Estimated Loss can be calculated as a sum of the value of each affected asset weighted with the frequency of occurence of each threat.

The last step in quantitative analysis consists of establishing the measures that should be implemented and their Return on Investment (ROI). During this step there are identified the threats that produce the biggest annual estimated loss (AEL) and the measures that should be implemented in order to reduce the loss. For each measure it identified:

- The threats that can be reduces by implemeting the measure;
- Annual estimated loss for each threat;
- A rate of the measure efficiency;
- Return on investment (ROI).

In selecting control measures it should be taken into account maximizing of return on investment (ROI) and minimizing annual estimated loss. The value of ROI grows by increasing the rate of eficency to the maximum or lowering the costs of implementing measures.

Qualitative Approach of Risk Analysis

Qualitative approach is being used mainly by small organizations. The method does not use statistic values to evaluate the risk in an organization. Instead, relative values are being used as data entries for the value of potential loss. The method uses terms like (see Table 1):

- Often/high, important, rare/low to refer to the probability of risk occurrence and their impact;
- Vital, critical, important, general to refer to the type and classification of the information;
- Numbers 1, 2, 3 (Burtescu, 2005).

This method can be applied following the next steps:

- Establishing the level of losses in case a vulnerability is exploited by a threat and the score awarded for each level of losses;

- Establishing the costs of disasters;
- Establishing disaster occurrence probability;
- Establishing the consequences of the disasters;
- Establishing qualitative risk analysis matrix.

Table 1

Qualitative Risk Analysis Matrix

Consequences					
Probability of occurrence	Insignificant	Minor	Moderate	Major	Catastrophic
	1	2	3	4	5
A (Almost certainly)	I	I	E	E	E
B (Probably)	M	I	I	E	E
C (Moderate)	R	M	I	E	E
D (Unlikely)	R	R	M	I	E
E (Rare)	R	R	M	I	I

Notes. The significance of the elements in the table is as follows: E: Extreme risk. Immediate action is required in order to minimize it. A detailed list of assets and management plans is required for this action to be implemented with success. Strategies should be designed and followed during the process; I: High risk. Immediate action is required in order to minimize it. Management plans have to be well developed in order to minimize the level of risk; M: Moderate risk. This risk should be taken into consideration by the manager; R: Reduced risk. Actions specified in the routine procedures should be taken.

Advantages and Disadvantages of Qualitative and Quantitative Approach

For a better understanding of the advantages and disadvantages of the quantitative and qualitative approach it was chosen a table representation (see Table 2).

Table 2

Advantages and Disadvantages of Qualitative and Quantitative Approach

Approach	Quantitative approach	Qualitative approach
Advantages	—Risks are sorted by their financial impact, assets by their financial value —The results can be expressed in a specific management terminology —The evaluation and the results are based on objective methods —Security level is better determined based on the three elements: availability, integrity and confidentiality —A cost-analysis can be implemented for choosing the best suited measures —Management performance can be closely watched —Data accuracy improves as the organization gains experience	—This approach makes easier to understand and observe the level of risk —Methods of calculation are simple to understand and implement —It is not necessary to quantify frequency occurrence of the threats —It is not necessary to determine the financial value of the assets —Monetary value of information is not determined, which makes the analysis process easier —Quantitative calculation of frequency and impact are not necessary —Estimated cost of the measure that should be implemented are not calculated —The most important areas of risk are evaluated
Disadvantages	—The methods of calculation are complex —Without an automatic tool the process can be really difficult to implement —There are no standards and universally accepted information for implementing this method —The values of risk impacts are based on subjective opinions of people involved —The process handles a long time —The results are presented only in monetary values and are hard to understand by persons without experience —The process is very complex	—The evaluation of risk and its result are subjective —It is possible that the reality is not defined correctly because of the subjective perspective of the author —The performance of risk management are hard to follow because of their subjectivity —A cost benefit analysis is not implemented, only a subjective approach of the author and that makes difficult the implementation of controls —Insufficient differentiation between major risks —Results depend on the quality of risk management team

Conclusion

This process is a long term cycle and its importance should not be missed at any time. All steps must be followed, risk identification not being enough for saving an organization from disappearing from the market.

Risk identification should be done with greater care, and all risks must be identified and treated carefully. The evaluation and assessment of potential threats, vulnerabilities and possible damage is very important. After this assessment is done, necessary controls should be implemented in terms of cost effectiveness and the level of risk reduced by the implementation. To identify the most appropriate controls a cost analysis has to be done. Its results help managers implement the most efficient controls that bring the greatest benefit to the organization.

Risk management helps managers to better control the business practices and improve the business process. If the results of risk analysis are well understood and the right measures are implemented, the organization not only that will not disappear from the market, but will develop and more easily obtain the targeted results.

References

Bojanc, R., & Jerman-Blazic, B. (2008). An economic modeling approach to information security risk management. *International Journal of Information Management,* 413-414. Retrieved from http://www.sciencedirect.com

Burtescu, E. (2005). Securitatea datelor firmei. Editura Independenta Economica, 2005

Chivers, H., Clark, J. A., & Cheng, P. C. (2009). *Risk profiles and distributed risk assessment.* Retrieved from http://www.sciencedirect.com

Information Systems Audit and Control Association. (2006). Certified information systems auditors, 85-89.

National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce. (n.d.). *An introduction to computer security: The NIST handbook*, 59.

Peltier, T. R. (2001). *Information Security Risk Analysis.* Auerbach.

Southern, S. (2009). *Creating risk management strategies for IT security*. Network Security, 13-14. Retrieved from http://www.sciencedirect.com

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology system. National Institute of Standards and Technology.

The Department of Trade and Industry. (n.d.). *Achieving best practice in your business information security: Protecting your business assets,* 8-22. Retrieved from http://webarchive.nationalarchives.gov.uk/