Decision Assistance in Risk Assessment – Monte Carlo Simulations

Emil BURTESCU
Department of Accounting and Management Informatics,
University of Pitesti, Pitesti, Romania
emil.burtescu@upit.ro

High security must be a primary and permanent concern of the leadership of an organization and it must be ensured at any time. For this, a risk analysis is compulsory and imperative to be done during the risk management cycle. Security risk analysis and security risk management components mostly use estimative data during the whole extensive process. The further evolution of the events might not be reflected in the obtained results. If we were to think about the fact that hazard must be modeled, this concern is absolutely normal. Though, we must find a way to model the events that a company is exposed to, events that damage the informational security. In the following lines of this paper we will use the Monte-Carlo method in order to model a set of security parameters that are used in security risk analysis. The frequency of unwanted events, damages and their impact will represent our main focus and will be applied to both the quantitative and qualitative security risk analysis approach. The obtained results will act as a guide for experts to better allocation of resources for decreasing or eliminating the risk and will also represent a warning for the leadership about certain absolutely necessary investments.
Keywords: *Security, Risk Analysis, Monte-Carlo Method, Likelihood, Impact, Loss*

1 Introduction

If they do not have a solid base the investments in controls that are designed to reduce or eliminate the security risks are difficult to be reasoned. The amounts of money that must be allocated are separated of direct investments in quite many cases, so allocating funds for security represents even a harder decision to take. Information security risk analysis aims to clarify the things somehow and to offer support in order for the decision to be made. Probability, impact, impact class, exposure factor, costs, estimated (annual) losses etc., are just some parameters that will help modeling the security risk. These parameters have a certain degree of uncertainty that will make the achievement of a consensus regarding information security rather difficult. The most often encountered case in such situations refers to the quantification of the probability of occurrence of an event with impact on information security. The main element the risk security team has to determine is the occurrence probability. The answers of the team members will be different in this case. Some will have values with a longer certainty in time, others with a lower certainty and some others' values will be outside the possibility of occurrence. These answers depend on two factors: the team members and their experience.

It is already easy to notice that the values of the given answers will produce uncertainty due to both the random processes that must be quantified and the personal perception and estimation of the team members. So, what values are still possible? Taking into consideration these answers the resource owner must be capable of taking the correct decision based on data that will shape reality as good as possible by offering a decrease in the degree of uncertainty. The Monte-Carlo simulation can offer the answer. This simulation offers the possibility for an analyst to quantify the uncertainty level in an expert's estimations by defining it as a probability distribution rather than just a single expected value [1].

In the following lines we will offer examples of use of Monte-Carlo simulation for both the qualitative and quantitative approach of information security risk analysis.

2 Risk and Risk Analysis

Depending on the domain and context we can offer a various range of definitions for the concept of risk. Some definitions are more complex while other are more simple. According to ISO guide 73 *risk is the combination between the probability of an event and its consequences*. A much more simple definition defines risk as being an event that is expected to happen. In the field of information security, risk is defined as being a threat that can exploit the potential weaknesses of the system. Whatever the field, risk needs two elements in order to occur: *impact* and *probability*.

Impact refers to the action upon the assets of the organization, in the sense that some assets must be protected against certain threats. An asset with a certain value which has a degree of exposure will generate impact. This impact is actually a loss for the organization. Impact rate is defined as:

Impact rate = Impact Class Value *Exposure Factor

Probability refers to the degree at which a threat may occur.

Threat, with its components- vulnerability and mitigation will be successful if vulnerability is high, and will be a failure if mitigation is high. The two elements, vulnerability and mitigation are inversely proportional.

Finally the risk level is defined as:

Risk Level = Impact rate*Probability Rate

A security risk identification process is embedded in the risk analysis process, that determines their magnitude and identifies the high risk areas that require security. Risk analysis represents a part of the set of measures called risk management. When talking about objectives, risk management manages risk in the sense of decreasing it to an acceptable level that will suit the organizational needs, and risk analysis identifies and classifies risks within the organization.

Risk management must be permanent within the organization, while risk analysis is a process that works only when a risk evaluation is needed and asked.

Microsoft approach defines rules and responsibilities within the risk management process as following (Figure 1) [2]:

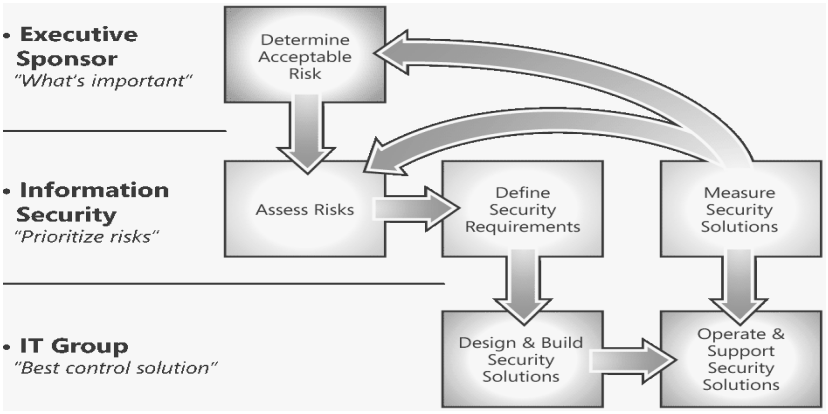

Fig. 1. Rules and responsibilities in security risk management

Source: http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx

The scheme in Figure 1 obviously reveals the fact that the resource owner has the main role. He must define an acceptable risk level for the organization he leads. This is the point where everything starts.

The resource owner will establish the things that are important to be protected within the organization and will impose an acceptable security risk level according to his objectives.

The security Group has the hardest task, the group's main purpose being the classification of risks. Among other tasks we will include risk analysis, defining security demands and measuring security solutions.

The responsibilities of the IT are to choose the adequate control solutions in order to reduce or to eliminate the risk.

In order to establish their effectiveness, the adopted solutions will have to be analyzed.

After this process a feedback with the results will be sent to the resource owner for information on the costs and the solutions that must be adopted. The same results will be sent as feedback also to the risk analysis stage in order to establish the new level of risk.

We can notice that we work with elements of uncertainty right from the owner's involvement. The owner has to define an acceptable level of risk for his organization. The human perception on an event comes into discussion. We will notice the same elements of uncertainty also in the stage of risk analysis where the team will have as objective the quantification of certain events. As stated previously some uncertainties are due to human perception on certain events but

also due to the fact that some events are put under the sign of uncertainty. In the following we will try to model these situations and to offer a solution for them.

3 Qualitative Approach

This particular method refers to small and medium sized companies and is more commonly used that the quantitative method. The terms this method operates with are: high, medium or low – to quantify the probability of the vulnerability level or occurrence; high, medium, low – to quantify the impact; catastrophic, major, moderate, minor, insignificant – to quantify the consequences of the events etc.

These terms are associated numerical values – 1, 2, 3, … 5. Taking into account these values calculations will be made that will lead to the establishment of the risk level. These values offer the faster achievement of a consensus within the risk analysis team. This approach method can lead to values of the risk level that are not correct due to the fact that determining the financial value of assets is not necessary, but especially because the quantification of the occurrence frequency of threats is not necessary. He man who can't perceive correctly or who can't quantify and event correctly is the main culprit.

In order to determine the risk level we will use the previously stated formulae [2]:

Risk Level = Impact Rate * Probability Rate

Impact Rate = Impact Class Value * Exposure Factor

Probability Rate = Vulnerability Level + Control Efficiency

Finally we have:

Risk level = (Impact Class Value * Exposure Factor)*(Vulnerability Level + Control Efficiency)

The risk analysis team members must quantify all of these terms. Discrepancies between the appraisals of the members are likely to appear. Estimating the values for these terms is a challenge and can sometimes be done in a wrong way. The probability of erroneous estimation for these factors is illustrated in the next table (Table 1).

Table 1. Risk values and error estimation

Error estimation: Low ← → High

Impact Class Value	Values	Vulnerability Level	Values	Exposure Factor	Values (%)	Controls Efficiency	Values
	2, 5, 10		1, 3, 5		20, 40, 60, 80, 100		0, 1, 2, 3, 4, 5

Taking as example the quantification of controls effectiveness designed to reduce the risk we have to make the sum of answers to the following questions (Table 2).

Table 2. Questions for exterminating the controls effectiveness (Microsoft)[2]

Questions	Answer 0 for Yes, 1 for No
Are responsibilities defined and effectively applied?	
Are warnings communicated and their execution followed?	
Are the processes and procedures well defined and learned?	
Do the existing technology and the existent controls reduce threat?	
Are the current audit practices sufficient for detecting abuses or deficiency control?	
SUM	

Source: http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx

A large variety of answers can be given by the team members to these questions. We can determine the dominant value by summarizing the answers. Consider the dominant value 1(one). What is the probability that this value is closest to the truth? The probability is 50%. Can it be

another value? Obviously yes. Which are these values and what is the probability of occurrence? These are the questions that make the decision hard to be taken.

We will use a Monte-Carlo simulation in order to determine the risk level under uncertainty. The input data is in accordance with the following table (Table 3).

Table 3. The input data for qualitative risk analysis

Impact Class Values		Exposure Factor		Vulnerability Level		Control Efficiency	
Values	Probability	Values	Probability	Values	Probability	Values	Probability
2	0.2	20	0.25	1	0.1	0	0.2
5	0.7	40	0.4	3	0.2	1	0.5
10	0.1	60	0.2	5	0.7	2	0.1
		80	0.1			3	0.1
		100	0.05			4	0.05
						5	0.05
	1		1		1		1

The values highlighted in the table are dominant values because they have received the greatest number of affirmative answers from the team members because they have the highest probability of occurrence. We will be able to simulate the way in which risk evolves over a period of time by associating each value an estimated occurrence value. In our example I have considered a number of 52 steps for simulation, corresponding to the 52 weeks of a year. Generating random numbers statistically independent for the four terms we will have the following values for the risk level (Table 4).

Table 4. Random numbers and obtained values for qualitative risk analysis

Week	Impact Class Values	Exposure Factor	Vulnerability Level	Control Efficiency	**Risk Value**
1	2	20	5	1	2.4
2	10	40	5	0	20
3	10	20	5	3	16
4	5	40	5	1	12
…	…	…	…	…	…
51	5	40	3	1	8
52	2	20	5	1	2.4

Correlating the results with Microsoft data of determining risk level (Table 5) and making a graphic for the obtained results (Figure 2) we will be able to see the evolution for the 52 weeks of simulation.

Table 5. Corresponding between risk value and risk level

Risk Value	**Risk Level**
41 – 100	High
20 – 40	Medium
0 – 19	Low

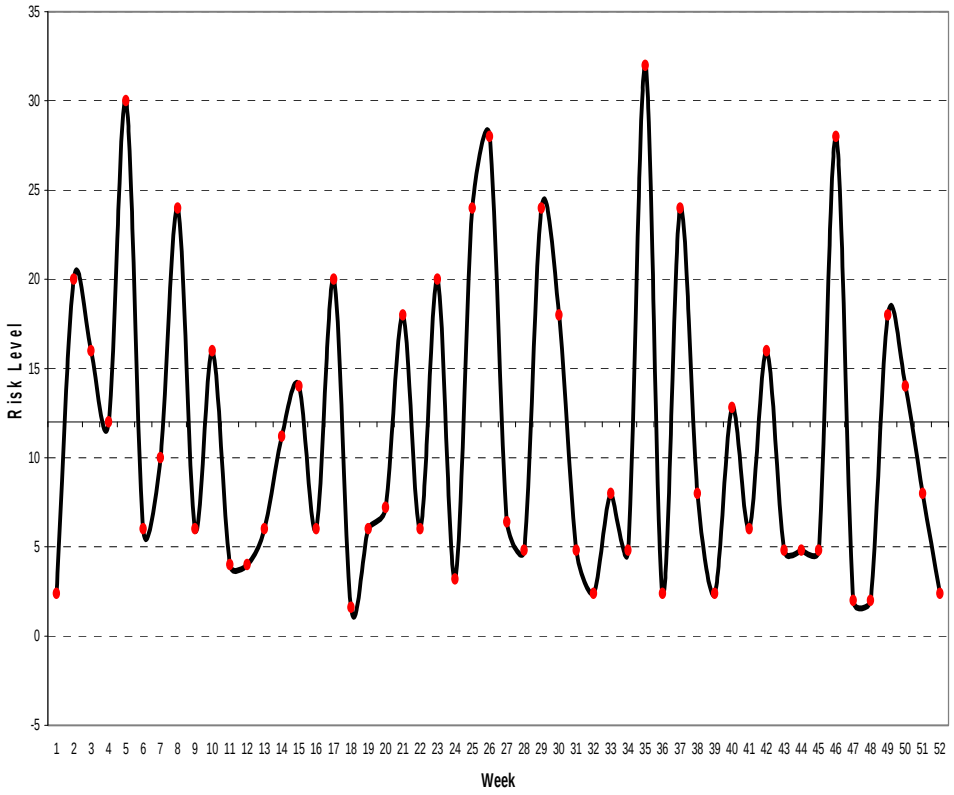

Fig. 2. Estimated risk level evolution

Compared to the reference value of a risk value of 12 (according to Impact Class Values = 5, Exposure Factor = 40, Vulnerability Level = 5 and Control Efficiency = 1) we can draw the following conclusions:

The risk level does not reach High. There are only 8 weeks in which the risk level can be Medium. In most of the weeks (44 weeks) the risk level is Low- similar to the one obtained with the dominant values. It may be considered that extreme measures are not necessary in order to reduce the risk generated by this event.

4 Quantitative Approach

Quantitative analysis works with statistical data in the field. It is more suitable for large companies which have their own specialized personnel for risk analysis. Due to the fact that the company creates a database with the history of the events the accuracy of the method tends to increase over time. Also, in the same time the company gains experience. Due to this fact calculating the impact is very important. Reaching a consensus is even more difficult this time because now we have a wide range of values.

Let's take the example of an organization that has a number of assets which are the subject of threats that will produce a certain level of losses (Table 6).

Table 6. Assets, occurrence rate and losses expectancy

		Losses expectancy per every threat			
		Workstation	Data server	Web server	Local Printer
	Pieces	*20*	*1*	*1*	*10*
Threat	Occurrence Rate				
Voltage shock	5	500	10,000	500	500
Theft	0.5	100	1,000	100	0
Reveal	3	50	1,000	300	0
Strikes	2	200	300	50	400

In order not to complicate the things even more we will consider that the values of estimated losses for each asset and threat have been correctly estimated. The rate of occurrence of a threat is the only element of uncertainty. Taking into consideration this data, the following question arises: What is the total value of Annual Losses Expectancy (ALE)? Taking into account the occurrence rates as the ones in the table, the total value of annual losses – ALE – has a value of 152650 monetary units. Now another question comes up: What will be the value if the threat occurrence rates vary around the values in the table? Obviously we will use a Monte-Carlo simulation. The input data are in accordance with the following table (Table 7).

Table 7. The input data for quantitative risk analysis

Voltage shock		Theft		Reveal		Strikes	
Values	Probability	Values	Probability	Values	Probability	Values	Probability
4	0.2	0.25	0.1	2	0.2	1	0.2
5	0.5	0.5	0.6	3	0.6	2	0.7
6	0.2	0.75	0.2	4	0.2	3	0.1
7	0.1	1	0.1				
	1		1		1		1

The dominant values are highlighted in the table. Even if these values are obtained by evaluations much more rigorous than the qualitative analysis, they can be contradicted over time. This time we want to see how the annual losses expectancy level evolves. We will use a number of 50 evaluations with statistically independent values for each threat (Table 8).

Table 8. Random numbers and obtained values for quantitative risk analysis

Tragging	Voltage shock	Theft	Reveal	Strikes	**ALE**
1	4	0.5	3	2	127150
2	5	0.5	3	2	152650
3	5	1	2	2	151900
4	4	0.5	3	2	127150
5	4	0.25	3	2	126375
6	7	0.5	2	2	201350
7	4	0.5	2	2	124850
…	…	…	..	…	…
10	7	0.75	3	2	204425
49	6	0.5	3	2	178150
50	5	0.5	3	2	152650

The representation of the obtained values after the simulations is exemplified in the following figure (Figure 3).

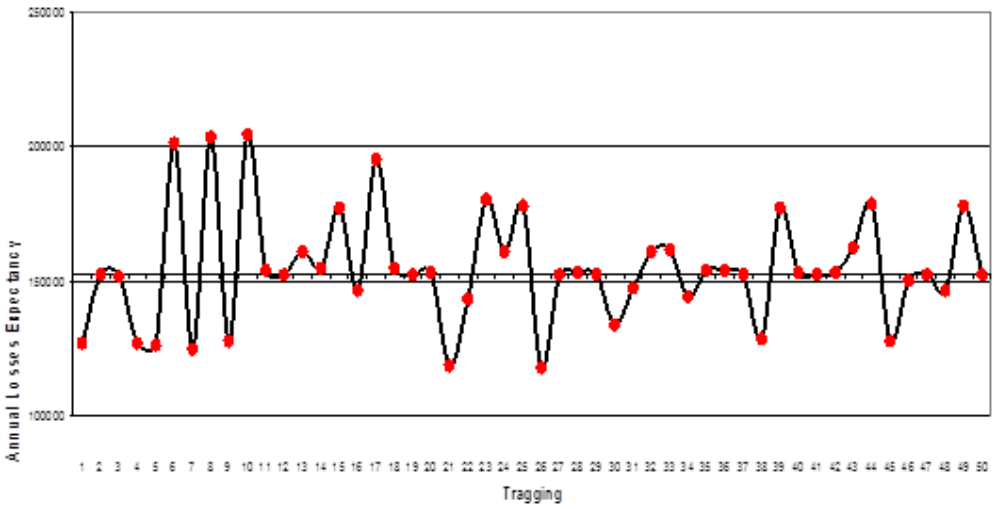

Fig. 3. Annual Losses Expectancy evolves

The computed values for the estimated annual losses have a deviation of ± 25% compared to the reference value. This is not an alarming value especially because we talk about estimation and this can be corrected during the controls' implementation.

5 Conclusions

What will the Monte-Carlo simulation do is to allow the risk analysis team to run different scenarios in order to be able to make estimations of all the possible future situations. Running different scenarios we will have the possibility to manage uncertainty for the future and to think in future terms. It is extremely important to know what will happen tomorrow before thinking what is happening today. Based on the data generated by the scenarios controls meant to reduce risks the level of investments and last but not least the controls meant to reduce risks will be chosen.

The simulation is well suited to the events that are uncertain over time but it can be used for different scenarios in which the perception on an event is different from one individual to the other. In the latter case better results are given by the Delphi method. Using the Monte-Carlo simulation for security risk analysis will be expanded in security risk management. This will involve running scenarios to determine the risk level reduction for different applied controls or to establish the investment level for ensuring security.

References

[1] J. R. Conrad, 2005, *Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations*, http://infosecon.net/workshop/pdf/13.pdf

[2] Microsoft Corporation, 2006, *The Security Risk Management Guide*, *http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx*

[3] E. Burtescu, 2010, *Business Information Systems*, SITECH, Craiova, Romania.

[4] E. Burtescu, 2008, The Network's Data Security Risk Analysis*, Informatica Economica,* Vol. XII, no. 4/2008, pp. 51-53

[5] E. Burtescu, 2006, Network Security Risk Level*, Informatica Economica,* Vol. X, no. 4/2006, pp. 107-110,

[6] E. Burtescu, 2005, *Data Security of the Company*, Independenta Economica, Pitesti, Romania.

Emil BURTESCU has graduated the Polytechnics University of Bucharest, Faculty of Aerospace Engineering. He holds a PhD diploma in Economic Cybernetics and Statistics at Faculty of Cybernetics, Statistics and Economic Informatics, Bucharest Academy of Economic Studies.