AUTOCHTHONOUS APPROACHING IN THE MANAGEMENT OF THE SECURITY RISK

Burtescu R. Emil

Universitatea "Constantin Brâncoveanu" – Piteşti, emil.burtescu@yahoo.com, 0722-736.647

An optimal management for a corporation, no matter what size the corporation is, it must contain the management of the security risk. On the importance that is given to the risk management can depend the well functioning of the corporation. An important role in this process has the owner of the business and the way that this one understands the risk. A good understanding of the risk by the owner will have as effect the allocation of sufficient funds to implement controls meant to bring the risk level in order to be an acceptable one. The autochthonous corporations, in a great part even because of the inexistence of reglementations in this domain, have an empiric approach of the phenomena.

Keywords: approaching, autochthonous, controls, resource owner, risk, risk analysis, risk level, risk management, security, vulnerability.

The restriction to the data access must be a permanent concern of the corporation. Completing or not this will have benefits upon the corporation or, by the contrary, negative effects. The absence of the security measures can be as harming as having too much security measures. A security policy permitted for own users and for the collaborators or clients can have as effect covering security deficits that can be used by the malefactors. Using too many security measures will have as effect complicating the work of its own employees and even the collaborators or clients. What a corporation has to do to maintain an optimal security level of its own data? Can the corporation assure and maintain this security level? Do the owners of the business understand the necessity of the security of data?

For many people the security of data represents the only method for maintaining the business of the corporation, ignoring the other potential threats: the economic environment, the natural environment, the financial environment, public environment, technological environment, etc. In the next lines, we will refer at risks as being only security risks.

For assuring the security measures in a corporation, this can be based on people (preparation, responsibilities, knowledge, and organization), processes (policies, procedures, standards) and technologies (infrastructures, applications)

The risk security management in a corporation represents the process to determine an acceptable level of risk and maintaining or reduced, as is possible, the risk level. The confusion between the risk management and the risk analysis must not be done. Risk analysis has as purpose identifying and classifying the risk in the corporation, and works only in one phase, while the risk management is a permanent process.

The corporations must adopt a risk management formed on four stages (or three in some cases) (figure 1):

1. Risk evaluation.
2. Coordination of the decisional process.
3. Implementing controls.
4. Measuring program effectiveness.

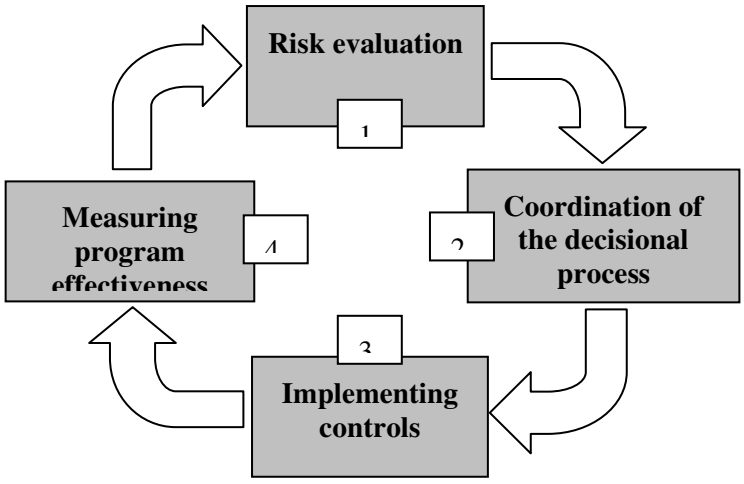

Figure 1. Risk management cycle

Risk evaluation will contain activities meant to identify and classify risks that can affect the corporation's business.

Coordination of the decisional process is meant to identify and evaluate the measures and the control solutions taking account of the report costs-benefits.

Controls implementation means implementation and developing control measures meant to lower or to eliminate risks.

Measuring efficacy, analyzing the efficacy of the adopted control measures and checking if the applied controls assure the established protection level.

It is necessary for the corporation to work permanently and periodic the operations from the risk management cycle to assure at least a controllable risk level.

As concerning the level touched by the risk management, this can be situated in one of the next levels:

1. **Inexistent** - the corporation doesn't have security policy well defined and documented.
2. **Ad-hoc** - the corporation realizes the risk. The risk management efforts are made in a hurry and chaotic. The policies and processes are not well documented. The projects of risk management are not coordinated and chaotic, and the results can't be measured and evaluated.
3. **Repeatable**- the corporation has knowledge about the risk management. The process of risk management is repeatable but immature, insufficient documented. There is no formal instruction or a communication concerning the risk management, responsibility being left to the decision of the employer. The corporation does efforts to get better.
4. **Defined** - the corporation adopts a formal decision for the implementation of the risk management. The objectives and the ways to measure the results are clearly defined. The employees are formally instructed at a base level
5. **Controlled** - the risk management is well known in all the compartments and levels of the corporation. There are well defined control and lowering the risk procedures. Efficacy can be measured. The personnel is instructed. The resources are sufficient. The benefits are viewable. The risk management team works to improve permanently the processes and instruments that they use. A large part of the risk evaluation processes, of identifying controls, of analysis of cost-benefits are manual.
6. **Optimized** - the process of risk management is well understood and atomized using specific instruments developed in the corporation or taken from corporations that are specialized in this domain. The sources of risk are identified and are taken measures to limit their effect. The employees are differentially instructed. It is worked on optimizing the processes.

The ideal thing would be that corporation should be at least on the **repeatable** level and to do efforts to gain the **optimized** level. Accessing one of the indicated levels, even if they have to represent a priority for managing the corporation, in many cases, for the autochthonous corporations, this desideratum is hard to gain.

The owner of the business has an important role in this case. He takes part in **two important moments** of the cycle of risk management.

The first moment is the one from the beginning when they must establish what is important for the corporation, that means to define an acceptable risk for the corporation.

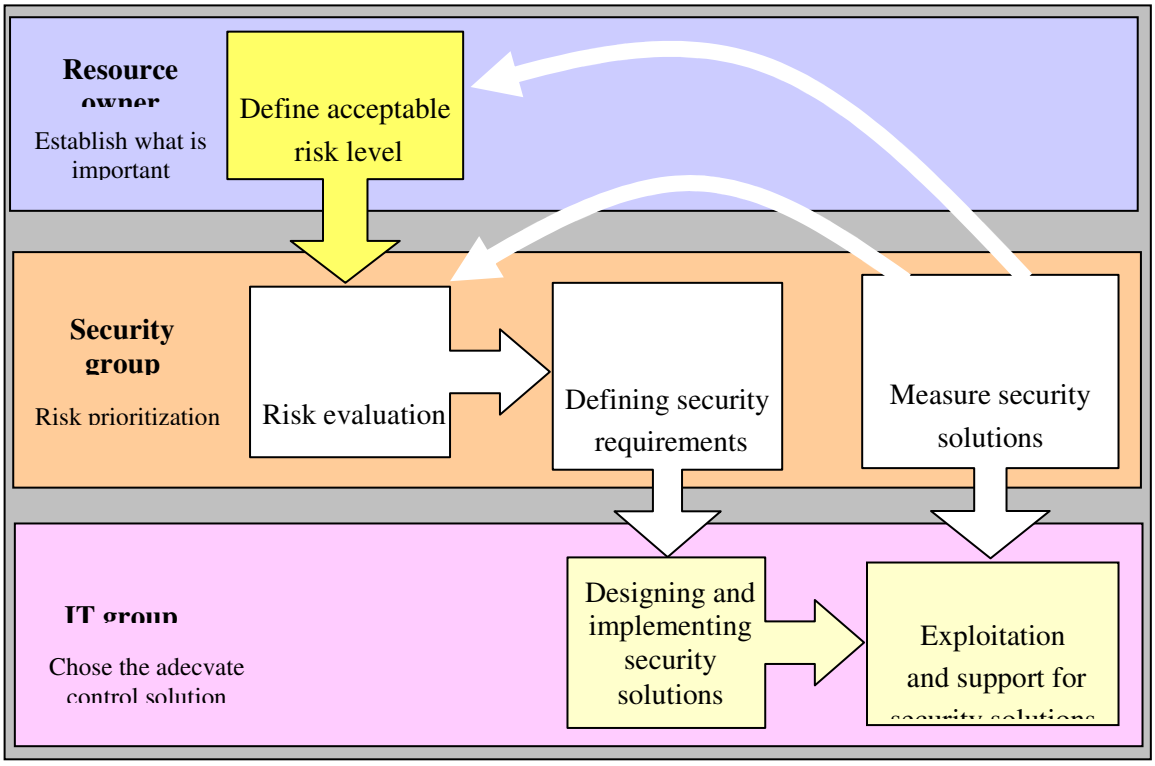

Figure 2. Rules and responsabilities in the security risk management process.

The second **moment** is the one when they **will be able to allocate funds to implement, maintain and improve security**. Because of this it is important for the owner of the business to understand firstly what security risk implies and the fact that this can be lowered or eliminated by investing money. *I consider that the greatest risk that a corporation can have is the risk not to understand the meaning of the risk.*

In this situation a **first** approach of the owner of the business, referring to risk could be:

- this can't happen at my company, and on risk analysis is made and the investments in security are equal with 0, risk management being inexistent.
- the necessity of security is partially understood but because having no money, it's not invested in security, just like the situation that we mentioned earlier.

The **second** approach goes from the premise that something must be done. In this way, all the job must be done by the IT group, if there is one. If there is no IT group, all the work must be done by the person that has in charge the IT section and who has only elementary knowledge about security. We can't even talk about risk analysis anymore. In this situation we can say that the company has an Ad-Hoc type of risk management (chaotic would better suite this situation).

The **third** approach will lead to a repeatable risk management level, that tends to be defined. We meet this situation when the owner of the business is not made only by one person, but by a group of people, and these people can cooperate, not totally, necessity of security. In this case the investments in security exist, even if these investments do not cover all the security deficits.

The **fourth** approach has constrictive aspects or it has important elements. This will lead to a controlled risk management level and even optimized. The defining elements in this situation are:

- the company belongs to a domain in which security has priority;
- the company is in a collaboration process with another company that has an optimized risk management process;

- the company, even if it is autochthonous. Has an external management.

If the company belongs to a domain in which data sensitivity has priority, then there are strict reglementations that the company has to obey to function in the domain. In this category there are included companies or organizations from the defensive, internal affairs, banking population evidence domains. For the companies and organizations from the United States there are reglementations mentioned in Orange Book of Security.

In case of collaboration with a company that has an optimized risk management level, it is necessary that the company should obey at the security demands proposed by the partner. No company that has a high level of security and a controlled or optimized management will not risk to share data with a partner that has a lower level of security.

There are companies that even from the beginning take measures for lowering the risk. This situation is met in the most cases at the companies that come with a management from western countries.

This last approach is based on a very well understanding of the risk and of the necessity of security, that will generate enough funds for investments meant to reduce the risk level for the company.

The main reason for which autochthonous companies do not invest in security is represented by the costs. There are situations when, even if all the steps for developing controls that are meant to lower the risks were made according demanding in domain and by specialized personnel, the sum that was allocated was lower that it wad demanded. In this case we can talk about a **financial enforced security**. The group named to implement controls had to do different things to be able to have enough money, sometimes some vulnerabilities being left discovered.

The second reason is represented by the fact that even if this thing is demanded there are no companies or specialized personnel for such a thing. Preparing your own personnel is extremely expensive because of the initial prepare and payment but even with the ulterior costs. Companies that are specialized in this domain are few and not known. Lately these companies began to be seen on the market. Demanding specialized companies presents many advantages: the existence of specialized personnel and lowering the costs by externalizing security services.

The next facts must be understood in order to assure an optimal security level:

- Investments in security do not create direct benefits but have the great advantage because they lower the potential loss. In many of the cases, 20% of the costs are reflected in 80% of the benefits, concerning lowering the risk and assuring security.
- Assuring the corporation's data security is like an "insurance policy" in case of a disaster.
- A minimal security level is preferred in case any kind of level does not exist. A minimal level of security does not represent the optimal of security.
- Assuring the security must be a continuous process, implemented by the strict risk management cycle.

Reference:

1. E. Burtescu. *Securitatea datelor firmei*, Independența economică, 2005.
2. L. McCarthy, *IT Security: Risking the Corporation*, Prentice Hall PTR, 2003.
3. P.E. Proctor, F.C. Byrnes, *The Secured Enterprise*, Prentice Hall PTR, 2002.
4. http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx
5. http://csrc.nist.gov/