Security Risk Management - Approaches and Methodology

Elena Ramona STROIE, Alina Cristina RUSU
Academy of Economic Studies, Bucharest, Romania
ramona.stroie@gmail.com, alinatv17@yahoo.com

In today's economic context, organizations are looking for ways to improve their business, to keep head of the competition and grow revenue. To stay competitive and consolidate their position on the market, the companies must use all the information they have and process their information for better support of their missions. For this reason managers have to take into consideration risks that can affect the organization and they have to minimize their impact on the organization. Risk management helps managers to better control the business practices and improve the business process.
Keywords: *Risk Management, Security, Methodology*

1 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. In order to maintain the authenticity and the accuracy of the information used in the decision process, any organization must use informatics systems to process their information and for a better support of their missions. For this reason, the management risk of the security information plays a very important role in the organizational risk management, because it assure the protection of the organization from the threatening information attacks, that could affect the business activity and therefore its mission.

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*. Therefore, 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. [1]

2 Risk management: definition and objectives

The concept of the risk management is applied in all aspects of business, including planning and project risk management, health and safety, and finance. It is also 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. [2]

The concept of risk management is now fairly universally understood, having been in widespread use for a number of years. It is applied in all aspects of business.

To discuss the definition of the risk management is necessary to explain in advance 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.

Risk management is a process consisting on:

- identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives;
-risk assessment by setting the probability and impact of its production, following threats by exploiting vulnerabilities;
- identify possible countermeasures and deciding which one could be applied, in order to reduce the risk to an acceptable level, based on the value of information resource to the organization. [3]

The goal of performing risk management is to enable the organization to maintain at the highest values the activity results. This process should combine as efficient as possible, all factors which can increase the probability of success and decrease the uncertainty of achieving objectives. Risk management should be an evolving process.

Particular attention should be given to the implementation of the strategies for eliminating or reduce the risk and their appliance, to the analysis of the past evolution of risks and to the present and future prediction of the events. Management process should be implemented at the highest management level.

In IT&C, one of the most important goal of risk management is to accomplish by better securing the informatics systems that store, process, or transmit organizational 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. [1]

3 Risk Management approaches: Proactive and reactive approach

Risk management can be approached in two ways: *reactive* and *proactive*. ***The reactive approach*** may be an effective response to the security risks that have already occurred through creating security incidents. The analysis of the causes of producing security incidents could help the organization to prevent their repetition and be prepared for any possible problems. Companies that respond to security incidents in a calm and rational way, meanwhile they determine the causes that have allowed the incidents to occur, will be able to respond in a shorter time to similar problems arising.

There are six steps that an organization should take into consideration when the reactive approach is applied:

1. Protecting human life and safety

It's the most important and most active of the six. Organizations have to respect laws that protect the employers and that require protection measures to prevent work accidents. Development of computerization of the production process has led many of its activities in an organization so they often can arise where production risks and security of their information systems is likely to endanger human life and health.

2. Controlling damage

It is an activity that consists on stopping or controlling the spread of the damage produced through the risks fulfilled. In case of a cyber-attack, organizations should take actions to protect information, important application and the hardware components, as soon as possible, and minimize the time when the system is not working properly. Sometimes maintaining the system available, during such an attack, may increase the damages.

3. Damage assessment

Damage assessment will be done by restoring activity and after reinstatement of all systems affected by risk. If cyber damage assessment involves conducting detailed investigations on the incident, immediately proceeded to restore or replace hardware, reinstall the software used and recovery affected data.

If the damage assessment takes too long, contingency plans should be considered so that the organization resumes normal activity without bigger damage.

4. Determine the damage cause

During this activity, to discover the starting point of an attack, it is necessary to understand what resources have been targeted by attacks and which vulnerabilities were exploited to gain access or to discontinue the services. It should be investigated the system configuration, and also the patch level, system logs, audit logs and audit trails. These operations help to discover the place where the attack started and what resources were affected.

5. Repairing the damage

This activity is very important because the damage must be repaired in the shortest time in order to restore the information system, to resume organization's activity and to recover the data affected by the attack. That is why every business action plan should include a strategy data recovery. After the damage has been repaired the elimination or the reduction of the vulnerabilities that were exploited during the incident should be considered.

6. Review responses and updating policies

Another activity related to the reactive approach, refers to the process of evaluating the way in which the back-up plans and the strategies of restoring the activity have functioned during the security incident. If there had been some failures in the process, there should be made the replacements or the changes needed.

The ***proactive approach*** of the risk management has several advantages compared with the reactive approached described above. Rather than wait for the occurrence of incidents and then to repair the damage, is better and cheaper to minimize the likelihood or the impact of occurring the risk, from the beginning. Organization's leader should develop plans for protecting the organization's most important assets by implementing controls that reduce the risk of exploitation of organization's vulnerabilities by malicious software, due to malicious or accidental misuse. A proactive approach can help organization to effective reduce the significant effect of the numbers of security incidents that can occur in the future, but will not completely eliminate these problems. Therefore organizations have to develop in parallel the incident response method and proactive approach to security policies.

Proactive approach consists in several main categories of activities:

- Making special training activities for staff whose work is or risk;
- Develop and implement a formalized work procedures to meet safety requirements and quality standards for each of its activities;
- Establish an internal control system on compliance the work procedures developed and on specific legislation in force (of personnel carrying out inspection activities, establish procedures for the conduct of control, the establishment of measures for eliminating the possibility of application dysfunction found in the inspection, etc.)
- Periodic evaluation for the viability of proactive measures is applied in order to reduce or eliminate risks.

4 Risk management process

Risk management is a permanent cycle process that involves activities for establishing, monitoring and ensuring continual improvement of the organization's activity. This process contains four main activities, which have to be permanent applied and developed:

- *Design the management system* involves identifying business requirements, assessing the likelihood and the impact of the risks, including the implementation of a security policy and selecting the adequate countermeasures for the existing risks*;*

- *Implement the management system* involves applying control measures and work procedures, resource allocation, setting the responsibilities and conduct training and awareness programs;

- *Monitoring, reviewing and reassessing the management system* involve an evaluation of effectiveness of controls and working procedures, of business changes, of previous incident reports and of existent risks*;*

- *The improvement and update of the management system* involves correcting the

identified dysfunctions, or eliminating the unsustainable decisions or applying new control measures.

Risk management encompasses three processes: risk assessment, risk mitigation and the reassessment of the residual risk. [1]

Risk assessment process includes establishing criteria under which the evaluation takes place (procedure on existing threats and vulnerabilities, and risks associated with, proceedings concerning the impact and likelihood of identified risks, risk assessment procedures, procedures for identifying measures to mitigate or eliminate risks, procedure for selecting the best measures to mitigate or eliminate the risks) and identifying and assessing risks..

The risk mitigation refers to determining optimal measures to eliminate or mitigate the risks, to planning, implementing the optimized selected measures, according to the plan, and controlling the rightfulness of the implementation process.

Reassessment of the residual risk consist in evaluating the remaining risk after the risk mitigation step and determine whether it is an acceptable level or whether additional measures should be implemented to further reduce or eliminate the residual risk, before before the organization can perform work properly.

5 Risk Assessment for IT systems

Risk assessment is the first process in the risk management methodology. The objectives of the risk assessment process are to determine the extent of potential threats, to analyze vulnerabilities, to evaluate the associated risks and to determine the contra measures that should be implemented. The risk assessment methodology encompasses eight primary steps, as follows:

1. *Define specific working procedures of risk management activity*

To make a proper assessment of the risks to the operation of an IT system needs to be established a system of working procedures that describe in detail each of the operations carried out for this purpose. The development of working procedures needs to consider compliance with existing regulations in the field and ensuring the effectiveness of those activities. In this sense can be considered national or international standards developed and published by professional organizations and associations.[4]

Thus, it requires work to watch these procedures:

- The way of identify and evaluate on existing threats and vulnerabilities, and risks associated with;
- Setting the values of impact and probability of impact and likelihood identified risks;
- The way of risk assessment;
- The way of identifying measures to mitigate or eliminate risks;
- The way of selecting the best measures to mitigate or eliminate the risks.

2. System characterization

This step provides information about the resources, data and boundaries of the IT system. It is very important that to define the specific field of interest, links and dependencies between the resources that are being analyzed. For this step, the responsible person has to collect information about hardware, software, data and information, system interfaces, system mission, persons who support and use the IT system, system security architecture, system security policies, technical, operational and management controls.

In gathering the information, the persons involved must apply the up mentioned procedures and should use some of the following techniques: questionnaires, the on-site interviews, documents review and automated scanning tools. This activity can be conducted throughout all the eight steps of the risk assessment process.

3. Threat identification

In this step are identified the potential threat-sources. A threat is the potential that a particular vulnerability is exploited by external factors, intentionally or accidentally, in order to produce the associated risks. A threat-source could not represent a cause to a risk, if there is no vulnerability that can be exploited. A threat-source is defined as any

circumstance or event with the potential to cause harm to an IT system. [5]
Threats can be based on human (deliberate or unintentional) or non-human (external or internal to the operating environment) actions. Human threats can occur most often and are the most dangerous ones. In this category are included unintentional acts, such as negligence or errors and deliberate attacks, like unauthorized access to confidential information, destruction of important information, information theft, misuse of data, falsification of information, sabotage the system. The non-human threats don't concern directly the human actions, and could be floods, earthquakes, landslides, avalanches, supply voltage drops, voltage fluctuations etc.

A common taxonomy is CIA (confidentiality, integrity, availability), which defines the characteristics of the organization's data. [5] The components of CIA are as follows :
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.
The following table is a list of examples for threats and their effects over security objective of CIA. This list does not claim to be exhaustive:

Table 1. Threats and their effects over security objective of CIA

THREATS	**The security objectives that are affected**		
	CONFIDENTIALITY	**INTEGRITY**	**AVAILABILITY**
1. *Human*			
1.1. Deliberate human threats			
Interception and espionage	X		
Placing destructive codes	X	X	X
Destruction with intention of date and facilities		X	X
Unauthorized access of data	X	X	
Use of pirated software			X
Falsifying identity	X	X	
1.2. *Unintentional human threats*			
Personnel operating errors		X	X
Programming errors	X	X	X
Technical failure		X	X
2. *Non-human*			
2.1. *External operating environment*			
Fire		X	X
Earthquakes		X	X
Floods		X	X
2.2. Internal operating environment			
Supply voltage drops			X
Voltage fluctuations	X		X

Another taxonomy, called STRIDE, consists in identifying various threat types. STRIDE considers threats from the attacker's perspective. [6]
The components of STRIDE are:
S – Spoofing identity – refers to the situations in which a cyber-attacker can pose as something or somebody else.
T – Tampering – involves malicious modification of data or code.
R – Repudiation – consists in creating a situation in which denying performing an action, could not be confirmed or contradicted by the other parties. Non – repudiation is a system's ability to counter repudiation threats.
I – Information disclosure – involve the exposure of information to individuals who are not supposed to have access to it.

D – Denial-of-service (DoS) – deny or degrade the availability of service to valid users.

E – Elevation of Privilege (EoP) - occurs when a user gains increased capability, often as an anonymous user who takes advantage of a coding bug to gain admin or root capability.

4. Vulnerability identification

The purpose of this stage is to identify the system vulnerabilities (defects/ weaknesses) that can be exploited by potential threats. Vulnerabilities are represented by the system's weaknesses, which, if exploited by some accidents or intentional actions, could result in a violation of system's security. Suggested methods for vulnerabilities identification have to take into account vulnerabilities sources, performances and requirements of the system development. [7] The methodology for vulnerabilities identification depends on the nature of the IT system and the stage of the system development:

- If the IT system is in the design stage, identifying vulnerabilities should be focused on security policies, planned security procedures, system requirements and the analysis of security product distributor.
- If the IT system is under implementation, identifying vulnerabilities should be focused specific information such as the planned features of the system described in the documentation, test results and previous evaluation or the way the personnel appointed to carry out implementation, fulfills his tasks.
- If the IT system is operational, identifying vulnerabilities should include an analysis of specific features of the security system and security, technical and operational measures used to protect the system or the way the personnel appointed to use the system, fulfills his tasks.

One important action in the vulnerability analysis process is the identification of the vulnerability source. Some of these sources are previous risk assessment documentation of the IT system, system's audit reports, security's review reports, vulnerabilities lists, such as the NIST I-CAT vulnerability database, security advisors and system software security analysis. To identify system vulnerabilities different test methods are used:

- Automated vulnerability scanning tolls that are used to automatically scan a group of hosts or a network for known vulnerable services.
- Safety tests and evaluation are special techniques used to identify vulnerabilities in an IT system during a risk assessment process. The purpose of system's security testing is to test the efficiency of the security controls that have been implemented.

System penetration system that can be used in addition to security controls tests to ensure that several IT system components are secure. The goal of this activity is to test the IT system in terms of a threat source and to identify potential defects in the system protection schemes.

As a result of this step, staff dealing with the risk assessment designs a list of security requirements that includes basic safety standards, procedures, processes and transfers of information associated with an IT system in security areas like management, operational and technical area.

Table 2. Vulnerability identification

Vulnerability	Threats	Affected goods
No back-up	Fire Earthquakes Floods Supply voltage drops Voltage fluctuations Use of pirated software Unauthorized access of data Placing destructive codes	Data
Inadequate configuration	Technical malfunction	Data

management	Interception and espionage Unauthorized access of data	
Unauthorized changes of the attributions of programmers with operational staff	Technical malfunction Error programming	Data Software
Inadequate training of staff responsible for data communications	Routing / rerouting wrong messages	Data
Security measures implemented in a wrong way	Denial of Service Unauthorized access of data	Data Software
Non-regularly updating antivirus software	Malicious code	Data Software
Lack of business continuity plans or procedures for data recovery	Fire Earthquakes Floods Supply voltage drops Voltage fluctuations Use of pirated software Unauthorized access of data Placing destructive codes	Data Software Hardware Ancillary facilities

5. Risk's likelihood determination

To determine the likelihood that a potential threat to exploit a vulnerability of the IT system should be considered the following factors:

- Threats-sources' motivation and capability;
- Nature of the existing vulnerabilities;
- Existence and effectiveness of current controls;

The likelihood that a vulnerability be exploited by a particular threat, need to be evaluated in order to determine the associated risk.

An often used scale for evaluating the likelihood of risk is the high, medium or low scale (sometimes it is used the extended versions, as the very low – low – medium – high – very high version). The risk's likelihood high means that the threat-source is highly motivated or very strong or the security controls are inefficient or all these conditions together are cumulative. On another hand, if the risk's likelihood is medium, it is probably, if the threat source is highly motivated or very strong, that the control of the system's security to be good enough to prevent most of the manifestation of the threats. The case of a low likelihood means that the threat's source is weak or poorly motivated or the security controls can prevent or, at least, significantly impede the exercise of the threats.

6. Impact analysis

In this phase of the risk assessment process, it is determined the negative results of a potential exploitation successful of a vulnerability. Before starting the impact analysis, it is necessary to collect information about the role of the system, system and data criticality or system and data sensitivity. This information can be obtained from the existing documentation, such as analysis report of the impact over the mission of the company or the assessment report regarding the critical assets. The negative impact of a security event can be described in term of loss or degradation of the three of the most important characteristics of the information: integrity, availability and confidentiality. [8]

Integrity is lost if unauthorized changes to data or IT system are made by accidental or intentional actions. If loss of data or system integrity is not corrected and the system is used with the corrupted data, wrong results can be obtained and wrong decisions can be made. Violation of system integrity may be the first step of a successful attack made on the availability and confidentiality of an IT system.

If the system availability to end-user is affected, whole organization activity can be affected. Loss of system functionality and efficiency can lead to loss or reduction of the productivity or the employers' performance.

System confidentiality refers to the protection of information against unauthorized disclosure. The impact of unauthorized disclosure of highly classified information can lead to attacks on organization's interests or even on national security.

Tangible impacts can be measured quantitatively in term of loss of turnover, cost of system repair or level of effort necessary for correcting the problems caused by of a successful exploitation of a threat. Some other impacts can't be measured in units and for this reason they are classified and described as high, medium and low.

7. Risk determination

The role of this step it to assess the risk level of an IT system. Risk determination for a pair of a "threat-vulnerability", can be expressed as a function of:

- The probability that a threat source to exploit vulnerability;
- The impact dimension, in case the threat source exploits with success the vulnerability;
- Preparation of existing or planned security controls to be implemented in order to reduce or eliminate risk.

To measure risk is necessary to identify or develop a method of evaluating it. One such method is the risk level matrix. This matrix is a 3x3 to 5x5 matrix which contains values for threat likelihood on columns and for threat impact on rows. We choose, for our exemplification, the values High, Medium and Low, for both the dimensions. For the 5x5 matrix are added 2 values: Very High and Very Low. Depending on the type of risk, the values could be replaced with numbers. The following matrix is an example of a 5x5 risk matrix:

Table 3. 5x5 risk matrix

Severity of negative impact:	**Threat Likelihood:**				
	Very High	**High**	**Medium**	**Low**	**Very Low**
Very High	Very High	Very High	High	Medium	Low
High	Very High	High	High	Medium	Low
Medium	Mare	High	Medium	Low	Low
Low	Medium	Medium	Low	Low	Very Low
Very Low	Low	Low	Low	Very Low	Very Low

The result of the evaluation the risk, using the proper method chosen, must be interpreted in order to determine the type of the risk (negligible, tolerable or intolerable):

- *The negligible risk* does not need any measure to be applied. It is monitored periodically.
- *The tolerable risk* does not need also any countermeasure to be implemented, but it is permanently monitored and whenever it is identified any growing of its value; it will become the object of some supplementary actions, in order to reduce its level. This means that the level risk is not very high to affect the objectives of the company's activities, so that the leading management could assume its realization without implement all the countermeasures.
- If the risk has an *intolerable level*, then it needs an immediate response. This means that the management team must identify and implement the right measure to reduce or eliminate the risk (risk mitigation). In some cases, in which the risk management team does not have the needed level of means, for implementing certain

measures, the process of decision would be transferred to higher forum of management.

For our hypothetical example, we could define the level very low for the negligible risk, the level low for tolerable risk and the values medium, high and very high for the intolerable risk.

8. Results documentation

After the threat sources and vulnerabilities are identified, risk assessed and provided, the results should be written in an official report. Risk Assessment Report is a report addressed to managers and owners that helps them to take decision concerning security policies and procedures. A risk assessment report presents in a systematic and analytical way the existing risks and how these can be exploited in order to help managers to understand and allocate resources to reduce or correct any losses

6 Risk mitigation

After the risk assessment, any organization has to implement methods to reduce the level of risk. Since it is almost impossible to eliminate all risks, top managers must implement the most effective measures to reduce risk to an acceptable level and to minimize the negative impact of risk on the organization's mission and goals.

There are several methods to reduce risks, which are applied depending on the type of risk:

- **Risk Avoidance.** Where it is possible, managers should choose not to implement some processes and procedures that can generate a higher level of risk or complicates the organization's activity.
- **Risk Limitation.** Risk can be reduced by implementing security measures and procedures. When implementing these measures it should be taken into account the cost and benefits of the implementation. If costs of the risk reduction outweigh the benefits, accepting risk should be preferred to implementing the expensive security measures.
- **Risk Transference.** Risk can be shared with different partners or transferred to insurance companies. This action must be made taking into consideration the risk behavior of the organization and the partner that support and control better the risk.
- **Risk Assumption.** Organizations can choose to acknowledge the existence of risk and monitor it. They also can ignore it, but this action can be very dangerous. The decision to assume a risk must be well documented and analyzed by the management team of the organization.
- **Risk Elimination.** The goal of this action is to eliminate the risk, but most of the options tend to eliminate organization out of the market. An organization that doesn't prefer risk will not survive on the market.

To reduce the risk, organizations should use some tools like:

- Identify all the methods available for reducing the risk and choose the optimal ones.
- Planning the appropriate activities for applying the method previously chosen. If risks are related to activities deadline using activity planning software can reduce risks within reasonable limits.
- Implementing the activities planned in order to mitigate the risks. Some of the measures generally applied are:

  Training the staff dealing with activities at risk - many IT risks are connected to untrained personnel and this affects productivity and work quality. Through training in security field, there can be reduced the likelihood of incidents and their effect.

  Redesigning security measures - organizations should identify those threats and vulnerabilities that generate risks with a strong impact on company's activity and improve the security systems permanently.

When control actions must be taken, the following rule applies: *Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities.* [1]

The methodology of implementing security measures contains several steps:

- Establishing personnel responsible for security

Security personnel is responsible for creating, implementing and evaluating security policies and also for oversight security processes. The only security problem that doesn't concern security personnel is security management. One of the security personnel tasks is defining a security table, an official document indicating the responsibilities of the person involved in this activity and the way security is approached. Another tasks is gathering information about existing policies, information that are valuable in understanding what functions properly in the organization, how information about risk are communicated to the top managers, how is decided the priority of the projects and how the security processes are structured.

- Establishing main activities to ensure security

To ensure an effective security within the company, it is necessary to go through some stages that are crucial. The main steps of a security program are presented in order to help any organization to implement a correct security program. There are four important steps that have to be defined from the beginning: risk assessment and documents and data classification; establishing access rights; defining security policies and planning, designing and implementing security controls.

- Defining requirements for improving security quality

Another task of the responsible personnel is to define the requirements for improving security quality. The team proposes solutions for the identified problems, which are important in the process of planning, designing and implementing security measures. This step is often overlooked, but it is vital. Any organization is different and for this reason measures implemented in another company can't be suitable for other. If insufficient time is allocated to the process of defining requirements, unimportant data can be protected from non-existing threats.

- Informing personnel about security measures imposed

Many security programs fail because of a lack of efficient communication. Most of the technical employees believe that technical solutions are sufficient to any problems. It is necessary that any security program to have two essential components: awareness and communication programs. These programs should receive sufficient resources and attention in order to achieve the goals. During the awareness program employees are informed about the impact of the security policies on their behavior. The communication program involves a continue communication between responsible personnel and top managers concerning the efforts and success in maintaining the level security at an acceptable level.

- Auditing and monitoring security

The auditing of security-relevant events and the monitoring system activity are key elements in an analyzing risk process. For recovery from security breaches and for keeping under control the access to information, this step is essential.

In the process of minimizing the level of risk, organizations should consider some security controls that can be classified as follows: technical, management and operational or a combination of these. The purpose of these controls is to prevent and limit the risks in order to achieve the goals.

Technical controls

Technical controls can range from very simple to very complex and usually must be combined in order to determine the system's good functionality. These measures are divided in three categories according to their purpose.

First category includes the basic technical measures that are used to support the implementation of other security measures:

- Identification: identify users, processes and information resources.
- Cryptographic keys: key generation, distribution, storage and maintenance.
- Security administration: are measures that must be configured to meet security system requirements.

- System protection: ensure the quality of IT system implementation in terms of design and manner in which the implementation was accomplished.

Another category includes the measures for prevention that prevent the occurrence of events that have a negative impact on the organization's activity:

- Authentication: these measures verify user identity. Mechanisms used are passwords, PINs, personal identification numbers.
- Authorization: verify if employees are authorized to make changes to the system.
- Protected communications: ensure integrity, confidentiality, availability of sensitive data during their transmission.
- Transaction privacy: protect against loss of privacy of important information.

The third category, detection and recovery measures, detects an adverse event and/or recovers lost information in case of an adverse event:

- Intrusion detection: ensure the detection of possible events with negative impact in order to avoid them or reduce their impact.
- Restore secure state: these measures are capable of bringing the system to last known security state after a security breach occurs.
- Virus detection and eradication: detect, identify and remove viruses to ensure system and data integrity.

Management security controls

These controls are implemented to reduce the level of risk and protect the organization's mission. They are focused on policies, guidelines and standards for information protection. Management security controls includes three categories: preventive, detection and recovery controls.

First controls, preventive management security controls include the following controls:

- Development and maintenance of system security plans in order to support of the organization's mission.
- Implementation of personnel security controls, including separation of duties, least privilege, user computer access registration and termination.
- Technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission.

Second category, detection management security controls, includes:

- Implementation of personnel security controls, including personnel investigation, rotation of duties
- Periodic review of security controls to ensure that they are effective
- Periodic system audits
- The existence of a continuous management process
- The third category, recovery management security controls, includes:
- Provide continuity of support and develop, test, and maintain the operations plans
- Establish the system capacity to respond to the incident and return the IT system to operational status

Operational security controls

Operational security controls are used to correct operational deficiencies that could arise when a threat is exercised. These include preventive and detection operational controls

Preventive operational controls are as follows:

- Controlling data access
- Limiting external data distribution
- Control software viruses
- Ability to create backup copies
- Protect laptops, personal computers, workstations
- Provide emergency power source
- Control the humidity and temperature of the computing

Detection operational controls include the following:

- Providing physical security (motion detectors, sensors and alarms)
- Ensuring environmental security (smoke and fire detectors, fire sensors and alarms)

7 Cost- benefit analysis

The *cost – benefit analysis* represents the estimation and comparison of the relative value and cost associated with each proposed control. This analysis is an efficiency criterion used for choosing the control to be implemented.

In order to make a cost – benefit analysis an organization must follow the next steps:

- Determining the impact of implementing new measure or improving the existing one
- Determining the impact of not implementing new measure or improving the existing one
- Estimating the cost of implementation which includes hardware and software purchase, cost of implementing new policies and procedures, training cost and system maintenance cost
- Assessing the costs and benefits of implementation controls.

The organization must determine the accepted level of risk to decide whether a measure will be implemented or not. The following rules should be followed when deciding if a measure is implemented or not:

- If the implementation reduces the level of risk more than is necessary, a less expensive alternative should be chosen
- If the implementation costs more than the benefit that would be obtain after the implementation, another control should be sought
- If the implementation does not reduce the level of risk enough, more effective controls preferable with a similar cost should be sought
- If the implementation reduces the risk at an acceptable level and is cost-effective. The measure should be implemented

8 Control analysis

After the implementation of security policies, in case the occurrence of security incidents, the organization must re-evaluate the entire risk management system, is being made as appropriate approaches for change, in the way to improve the security policies. Security policies can be technical or non-technical. Technical controls are safeguards incorporated into computer hardware, software or firmware such as access control mechanism, authentication mechanism, encryption methods and the non-technical ones are management and operational controls like policies, procedures and personnel and environmental security.

Technical and non-technical control described above can be classified into preventing controls and detective controls. Preventing controls inhibit attempts to violate security policies, meanwhile detecting controls alert violation or attempted violation of security policies. These controls are implemented during the risk minimization phase.

9 Conclusion

Since the economic environment is really fierce and constantly changing, organizations that desire to remain on the market should pay greater attention to risk management process. Managers' responsibility is very high and for this reason information security risk management is of fundamental concern to all organizations. 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; 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 it will develop and more easily obtain the targeted results.

References

[1] G. Stoneburner, A. Goguen, A. Feringa, *Risk Management Guide for Information Technology System*, 2002.

[2] S. Southern, "*Creating risk management strategies for IT security*", *Network Security"*, 2009, pp.13-14.

[3] Information Systems Audit and Control Association, *Certified Information Systems Auditors*, 2006, pp.85-89.

[4] The Department of Trade and Industry, "*Achieving Best Practice in Your Business Information Security: Protecting Your Business Assets*", pp. 8-22, Available at: http://webarchive.nationalarchives.gov.uk/tna/+/http://www.dti.gov.uk/files/file9985.pdf/

[5] R. Bojanc, B Jerman-Blazic, "An economic modeling approach to information security risk management", *International Journal of Information Management*, pp. 413-414, 2008. Available: http://www.sciencedirect.com

[6] M. Howard, S. Lipner, "The security development lifecycle", United States of America: Microsoft Press, 2006, pp. 114-116.

[7] E. Humphreys, "Information security management standards: Compliance, governance and risk management", *Information Security Technical Report I3*, 2008, pp. 247-249. Available: http://www.sciencedirect.com

[8] M. Siponen, R. Willison, "Information security management standards: Problems and solutions", *Information and Management*, vol. 46, pp.269-270, 2009. Available at: http://www.sciencedirect.com

[9] E. Burtescu, *Securitatea datelor firmei*, Editura Independenta Economica, 2005.

Elena Ramona STROIE has graduated The Bucharest Academy of Economics Studies, Faculty of Cybernetics, Statistic and Economic Informatics in 2008. She holds a Master diploma in Informatic Systems for Economic Processes and Resources Management from 2009 and in present she is a PhD Candidate in Cybernetics and Economic Statistic with the Doctor's Degree Thesis: Methods of Risk Analysis and Assessment in an Information System. Her areas of interests are: Information System Security, Risk Analysis Management.

Alina Cristina RUSU has graduated The University of Craiova, Faculty of Automatics, Computers and Electronics, *Computers Engineer*. She holds a Master diploma in *IT & C Security* from Academy of Economics Studies and present she is a PhD Candidate in Economic Informatics with the Doctor's Degree Thesis: *Protection of confidential information in a computer system.* Her areas of interests are: Information Systems Security, Risk Analysis Management and Security Policies in Informatics Systems.