RISK MANAGEMENT FROM THE INFORMATION SECURITY PERSPECTIVE

Riza Ionuț,
University of Craiova, Management, Romania, rizaionut@gmail.com

We suggest you to cite this article as:
Riza. I, 2017. Risk management from the information Security perspective. *Junior Scientific Researcher*, Vol III, No. 2, pp. 1-8.

Abstract

Risk management has emerged ever since the appearance of human communities and it has developed at a slow rate. Over time, a significant improvement was made, from accepting hazards to the identification, evaluation and control of unwanted events, threat prevention and exploitation of opportunities through scientific risk management actions.

The fundamental role of research in cyber security is to concentrate the efforts on those contexts and conditions which determine the way in which key players reach a common understanding of the way to conceive and eventually answer to certain challenges in cyber security.

In order to build a clear perception of these effects, this work presents the main elements which define cyber space, to come to the aid of turning the management process into an efficient one, especially when talking about cyber space as a space for conflicts, both economic and political.

Keywords: *cyber space, risk management, cyber security, information technology, risk evaluation.*
JEL Classification*:* M150

Introduction

Information security is nowadays a main topic because of ongoing disclosures about security incidents, seen as events through which one can attempt to or unlawfully penetrate an information system, an attack on the confidentiality and / or integrity of information on an automated computer system. This includes the unauthorized viewing or browsing, the interruption or cancellation of a service, the modification or destruction of data, the processing, storing or retrieving of information, the modification of system information about hardware, firmware, or software features with or without the knowledge or intent of the user. Most security incidents are caused by inadequate organization and management, and to lesser extent because of a security system failure. In this context of unpredictability and insecurity, organizations are redefining their approach to security, trying to find a balance between risk, innovation and cost. At the same time, the field of cyber security is subject to dramatic changes, requiring organizations to adopt new practices and new sets of skills, taking into account the fact that cyber security has rapidly evolved from a technical discipline to a strategic concept.

Cyber security risk is currently directly associated with business risk – the lack of interest for security concerns may threaten the future of an organization – but many organizations continue to manage and understand it only in the context of the IT department. As companies become more and more dependent on the proper functioning

of information systems, the security issue of these systems becomes a major priority. Risks are of unequal importance, so it is very important for them to be filtered and prioritized.

The state of knowledge

The term "system" is one of the fundamental, primary concepts with multiple uses in many research fields. Because it is a primary and general concept, it doesn't have a standard and rigorous definition.

According to Sfetcu (2016, p. 97), the term system can be understood, in general, as a multitude of components that interact with one another in an organized manner in order to reached a set objective.

Cyber space, defined by Morningstar (2003, p23) as an environment meant for the dissemination of information in electronic format and it was invented because of the technological development which created new techniques for automation, processing and information transfer from computers to communication networks.

The notion of "Cyber space" was elaborated in 1982 by William Gibson in a short story "Burning Chrome", the concept being popularized two years later in his debut novel "Neuromancer". Defining cyber space is a difficult task, with many definitions ranging from the very complex to the most basic.

Ioana Vasiu (1998, p. 124) argues that the internet is the mega information network which reunites a few thousand networks of different ranks from tens of countries in the world. It is a virtual network made from of a continuously growing number of both public and private local networks, large area networks, regional and national interconnected networks. The history of this network starts in June 1968 when the Advanced Research Projects Agency, within the USA Defence Department employed the Cambridge (Massachusetts) company named Bolţ Beranek and Newman in order to build a network that would unite the research centers throughout the country. Until the fall of the same year, the company was able to interconnect computers from The Stanford Research Institute, The University of California, Santa Barbara and The University of Utah. Afterwards, as the computing protocols and technologies have developed, other institutions joined the network. In 1973, developers have started a project named Internetting Problem, with the objective of interconnecting various isolated networks. In 1983 there were 400 computers connected already. Over time, this huge network would extend to research institutes, teaching institutions, administration, the business environment and eventually, to private users. This way, the internet has become a super information network with a strong public character. Most users navigate the Internet in order to satisfy certain scientific, cultural, educational, professional or business needs but also certain necessities connected to the organization and unfolding of family life or spending free time.

A model of alliance between the army and major technology companies – such as Google and Facebook – is described by Shane Harris (2015, p.123), cyberspace being considered the fifth area of war, alongside land, air, sea and space. Shane Harris offers a detailed overlook at this partnership and explains what the new cyber security regime means for all who spend their daily lives on the Internet.

Misty Blowers (2015) discusses the future of cyber technologies and operations that will influence progress in the social media, cyber security, cyber physical systems, ethics, law, media, economy, infrastructure, military operations and other elements of

social interaction in the following decades. It provides a review of future disruptive technologies and cyber security innovations, it serves as a resource for planning, and presents a strategic vision of the future direction of cyber operations, while informing the military strategist about the future of the cyber warfare.

Bruce Schneier (2003) believes that all of us can and should be security consumers, and the compromises we make on behalf of security with regard to cash expenses, taxes, inconveniences and diminished freedoms should be part of our lives.

Baicu (2006) is of the opinion that in economy, information is one of the most valuable assets of a corporation, probably inferior only to human resources.

Every component of today's society, to which one can add the business environment, is influenced by the fact that we interact in a complex and information-based society in which almost every element is interconnected. Viewed strictly from the business point of view, information is one of the most valuable goods. That is why information security is very important for organizations that wish to do business in the electronic environment.

Method

The method used is based on the systematic approach to identifying and deciding which countermeasures are necessary to be taken in order to protect information as well as resources and auxiliary sources based on the evaluation of threats and vulnerabilities.

The aim of this research is to help government and civilian institution leaders when deciding about security measures against threats to the IT environment towards lowering the probability of compromising sensitive information.

Security threat analysis tackles such issues as principles and responsibilities, the evaluation of security threats, risk management and the method employed in order to neutralize the threats.

Security risk management implies the planning, organizing, leading and controlling of resources in order to make sure that risks are kept within acceptable margins.

Whitten (1999) considers that risk management is an iterative, ongoing process between the current and desired security state, through the evaluation and management of risks.

The success of risk assessment greatly depends on the role of top management within the process. There must be an agreement of management regarding the purpose and domain of risk assessment, with support at all levels of the organization, the reviewing of certain management principles and objectives and the approval of risk assessment results.

The risk assessment should be funded on cumulative data and information and the evaluation activity should include the following actions:

a) identifying the domain and objectives of risk assessment;

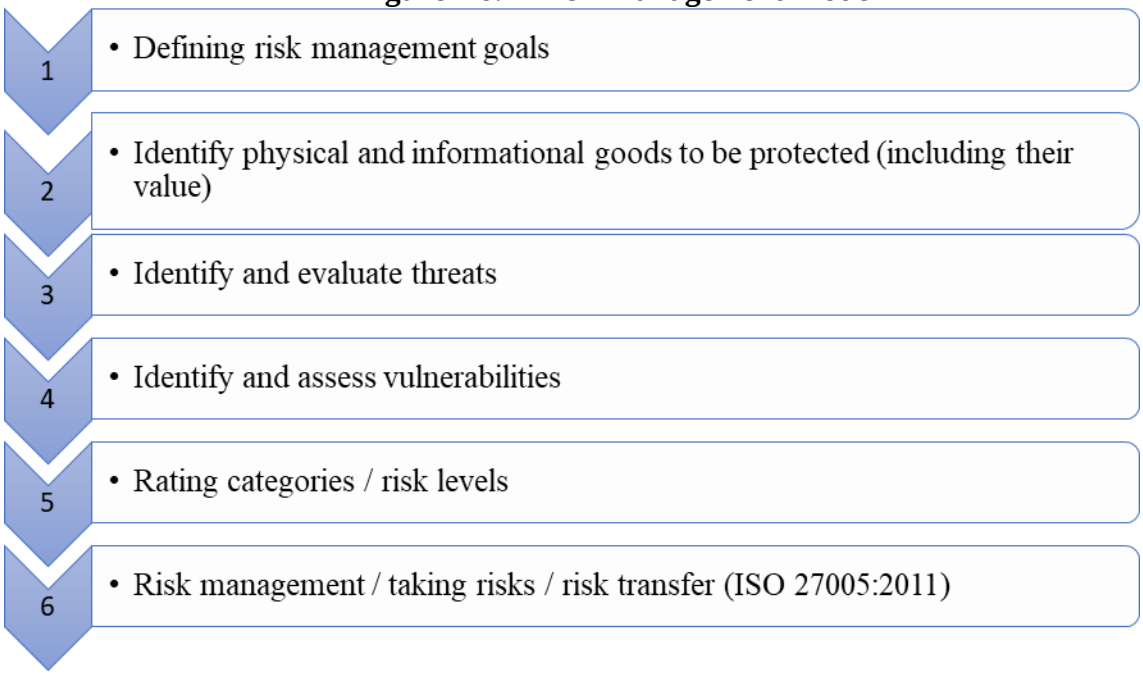
b) identifying the physical goods and information that aid the fulfillment of the organization's mission, as well as their importance (value);

(c) identifying the threat and vulnerability in relation to the risk environment and the level of these threats and vulnerabilities;

(d) identifying the risk level (*ISO 27005: 2011*).

A practical, simplified risk management model is proposed, based on studying the existing standards, a model which is easy to apply and consists of six steps (Fig. No. 1).

Figure No. 1 Risk Management Model



Source: the author's own data processing, in accord with ISO 27005:2011

Defining risk management objectives / identifying physical and informational assets to be protected and their values / identifying and assessing threats / identifying and assessing vulnerabilities / assessing categories and risk levels / treatment, assumption, risk transfer

Thus, in the stage of defining risk management objectives, one must clearly state the level of accepted risk the manager of the organization wants to achieve in that domain, the timeframe and the resources he wants and he is willing to spend.

In the second stage, one must identify all the sensitive information in a certain security risk domain, whether classified or not, information which can put in jeopardy the organization's interests when compromised and also all the assets – equipment, applications, facilities, procedures – critical to the functioning of the organization. The evaluation of information assets can be done by consulting the owners of such information or other persons that have an authorized opinion on information assets. The evaluation, which can be a qualitative appreciation (for example low, medium or high), can be obtained from the assessment done by the "information owners" or their representatives, using the worst scenario possible which can result in the following actions towards the information: its destruction, unavailability, its release to unauthorized individuals and the modification of the information by unauthorized individuals (Haimes, 1998).

During the threat identification and evaluation, one must identify all threats to information and organization assets which can lead to the loss of confidentiality, integrity or availability; at the same time, one must evaluate the probability of such threats. Threats must be defined according to the domain to which they belong, the

source, motivation, intent, capacity, nature, target, probability, impact, results, etc (Haimes, 1998).

When identifying and evaluating vulnerabilities, one must take into account that, in general, they represent essential weaknesses rooted in environments such as physical assets, organizational assets, personnel, management, procedures, hardware, software or communication equipment, weaknesses which can be exploited. One can now estimate the vulnerabilities that can be exploited by the identified threats and one can evaluate the ease with which they can be exploited, in order to obtain an accurate degree of appreciation of vulnerability significance.

The objective of the fifth stage is to identify and evaluate the risk to which classified or sensitive information and equipment are exposed to, in order to choose those protection measures that are appropriate and efficient.

In the last stage (the sixth in our proposed model), one must propose a solution for each risk; the solutions can be one of the following:

1) To eliminate the risk – the objective is to eliminate all the vulnerabilities, whether real or potential, through thoroughly implementing countermeasures and thus preventing resource losses;
2) To limit the risk of losing the information assets, with the objective of implementing countermeasures to a degree in which the loss can be limited to an acceptable level;
3) To accept the risk of losing / compromising certain informational assets; such a decision can be made when the cost / impact of such loss is not significant or the probability of such loss is small enough or the cost of countermeasures is much too high or not in accord with the costs / impact of estimated losses;
4) To transfer such risks to an organization which is higher up in the hierarchy, when certain identified risks can't be accepted but also they can't be eliminated or dealt with using the available resources (Haimes, 1998).

The process of implementing cyber risk management

Security risk management provides options for dealing with risk, such as reeducation, transfer, elimination, avoidance and acceptance, and it involves planning, organizing, leading and the control of resources in order to make sure that the risk remains within acceptable limits and it has an optimal cost.

Evaluating security risks is not a task to be done just once for an undetermined period of time. It must be done periodically, in accordance with management requests, with the purpose of updating information and data obtained at a certain moment regarding changes in threats and vulnerabilities, changes in the organization's mission, as well as information and assets. Security risk evaluation is the process of quantifying security risks, in this case the identification of threats and vulnerabilities, quantifying their importance and identifying the areas which need protection and countermeasures (Blank and Gallagher, 2012). The evaluation of security risks brings its contribution to the decision regarding which security measures will be necessary and it offers an impartial evaluation of residual (accepted) risk. A benefit that comes from evaluating risks is the development of a so-called heightened security consciousness, visible at all levels of the organization (Blank and Gallagher, 2012).

The initial evaluation of security risks to an organization is the most comprehensive resource. New updates on security risk evaluation can be based on the

initial evaluation data, with possible increases or decreases of its parameters, such as time and resources needed.

The results of the security risk evaluation, the actions taken in order to achieve and maintain the minimum protection standards will be documented in a *Risk evaluation report*, which can include *(ISO 27005:2011)*:

-the domain and objectives of the security risk evaluation;

.-the organization's security objectives in terms of confidentiality, integrity and availability;

-a list of critical assets that must be protected;

-the description of evaluated threats;

-the description of evaluated vulnerabilities;

-the level of estimated risk and its characteristics;

-measures to be taken in order to reduce the risk level;

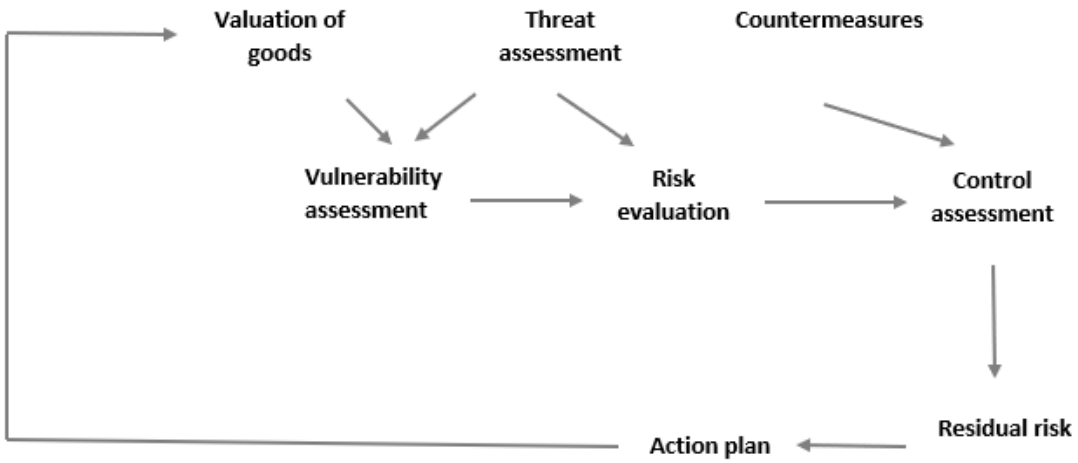
-risk reevaluation procedure;

-measures to be taken in order to manage risks.

The risks identified and characterized after the evaluation can be noted on a *Risk dossier*, in order to be analyzed and treated with the goal of elaborating a *Risk management plan.* This dossier contains the description of the initial risk, evaluated risk, planned action, timeframe and the person in charge.

In the process of implementing security risk management plans, according to this simplified model, one will take into account the relationships between estimated risks based on threat evaluation and on vulnerability evaluation made for the evaluated system which leads to the application of countermeasures which will determine the acceptance of residual (acceptable) risk and the implementing of a plan of measures for reducing or eliminating other risks (Fig. No. 2).

Fig. No. 2 The process of implementing security risk management



Source: the author's own data processing, in accord with ISO 27005:2011

Conclusions

The large number of cyber attacks described in the media on a daily basis point out the importance of the continuous development of human resources, both at the national and the international level in order to rise up to the new cyber threats.

As both humans and organizations continue to transfer data and information through the internet, it is necessary to ensure access to provide a safe cyber space, free of unauthorized breaching into the information systems and computer networks.

Even large organizations, with highly skilled laborers, with significant resources and abilities at their disposal towards information security, suffer major setbacks in terms of cyber security, while organizations with fewer resources are facing even greater challenges.

Thus, heightening the level of system security management must be understood as a continuous process. A system's security is a complex subject, and in order to understand it, one must have demanding knowledge and expertise in various fields such as: psychology, economy, organizational behavior, political science, engineering, sociology, international relations – it is not limited only to informatics and information technology.

Last but not least, the main issue at hand is not the way in which cyber security can be dealt with but rather the way in which it can be managed. Social problems linked to the existence of warfare, terrorism, delinquency, famine, drug abuse and other issues are rarely "solved" or eliminated forever.

In this work, I suggest the use of risk management in information security through models and simulations, by combining in a balanced manner the use of qualitative and quantitative methods to analyze, evaluate, treat and monitor cyber risks.

Bibliography

1. Baicu, F. (2006) Auditul și Securitatea Sistemelor Informatice. Ediția 1. Bucureşti: Victor.
2. Blank, R. M., Gallagher, P. D. (2012) Guide for Conducting Risk Assessments. Ediția 1. Gaithersburg: NIST Special Publication.
3. Blowers, M. (2015) Evolution of Cyber Technologies and Operations to 2035 Advances in Information Security. Ediția 1. Switzerland: Springer International Publishing.
4. Gibson, W. (1982) Burning Chrome. Ediția 1. New York: HarperCollins Publ.
5. Gibson, W. (1984) Neuromancer. Ediția 1. London: Gollancz.
6. Haimes, Y.Y. (1998) Risk Modeling, Assessment, and Management. Ediția 1. New York: Wiley.
7. Harris, S. (2015) @War: The Rise of the Military-Internet Complex. Ediția 1. New York: Eamon Dolan/Houghton Mifflin Harcourt.
8. Morningstar, C. (2003) The New Media Reader. Ediția 1. Londra: The MIT Press.
9. Schneier, B. (2003) Beyond Fear: Thinking Sensibly About Security in an Uncertain World. Ediția 1. Göttingen: Copernicus.

10. Sfetcu, N. (2016) Cunoaștere și Informații. Ediția 1. Seattle: CreateSpace Independent Publishing Platform.
11. Vasiu, I. (1998) Criminalitatea informatică. Ediția 1. Bucureşti: Editura Nemira.
12. Whitten, A. (1999) Information resources management. Ediția 1. Londra: Ideea Group Publishing.
13. ***. Standard internațional ISO/IEC 27005:2011 - Information security risk management.