Chapter 9
The International Experience in Security Risk Analysis Methods

Anca Gabriela Petrescu
Valahia University, Romania

Mirela Anca Postole
Titu Maiorescu University, Romania

Marilena Ciobanasu
Titu Maiorescu University, Romania

ABSTRACT

The goal of information security is to be able not just to put in place measures to detect and mitigate attacks but also to predict attacks, deter attackers from attacking, and thus defend the systems from attack in the first place. Data protection should be based on the lessons learned over time, both within the organization and in other organizations. Over the time, a large number of methodologies for identifying information security risks were proposed and adopted and simplified approach to different methodologies has led to their classification in quantitative and qualitative, especially in terms of metrics used to quantify risk. This chapter proposes an international overview regarding the quantitative and qualitative analysis methods for information risk analysis. In practice almost always use a combination of these methods, depending on the characteristics of the organization investigated the degree of uncertainty associated with the method of analysis and risk management.

INTRODUCTION

Risk management process within the organization allows managers to handle uncertainty and associated risks and opportunities in an efficient manner, leading to increased ability to create added value (He, Chen, Chan & Bu, 2012; Kurosawa, Ohta & Kakuta, 2017).

Implementation of information security measures, however, is not always a smooth process and not slippery (Tropina & Callanan, 2015). In addition to the issues raised by the high cost of implementing security measures, the authorities control law implementation (enforcement) face a number of problems socially (Peltier, 2010).

DOI: 10.4018/978-1-5225-8455-1.ch009

There are cases where data protection measures may affect the privacy of individuals. In these circumstances arises open conflict between human rights defenders and enforcement authorities, which in some cases lead to legislative and procedural ambiguities, as happens for example if the widespread use of cryptographic mechanisms (Chen, Ge & Xie, 2015).

Information society in which we live requires us to identify new safeguards, on the one hand, the information, which otherwise we are indispensable and, on the other hand, the right to privacy (Agrawal & Tapaswi, 2017).

The essential factor needed to ensure the effectiveness of the risk management process within the organization, however, is the firm commitment of the management (Hiller & Russel, 2013). The commitment must be continuous and must involve the top management. Without this element, the initiative to conduct risk management cannot be successful. Keeping risk management policy up-to-date demonstrates that risk management is a dynamic activity, which benefits from the full support of the management board (Krombholz, Hobel, Huber & Weippl, 2015).

This is why, security mechanisms have to be properly designed and commensurate with the specific threats for the specific types of information (Landoll, 2010). Organizations have to expand and deepen their current information security risk frameworks to address these key threats (Wang & Hu, 2014). This process implies a more profound understanding of the risks associated with each threat, and a better capacity of tailoring the security framework to align with the organization's identified risks, regulatory requirements and perhaps most important – the increasing dependencies on information technology.

BACKGROUND

The risk analysis must be approached methodically to ensure that all activities of the organization were evaluated and all risks associated with these activities have been defined (Stepchenko & Voronova, 2015). The results of the risk analysis can be used to outline a risk profile of the organization that provides a rating of the significance of each risk and to prioritize risk management efforts. This process allows the mapping of risks by fields that affect the description of existing control mechanisms and indicates situations where the investment in controlled measures should be raised, lowered or redistributed (Enagi & Ochoche, 2013).

Risk analysis activity contributes to the efficiency and effectiveness of the organization's operations by identifying those risks that require management attention (Karim, 2007). It facilitates prioritization of risk control actions, depending on the impact on the organization and the potential benefit that they bring control measures organization. In this context, when we talk about treatment risks, the range of responses to risk includes tolerance, treatment, transfer and disposal (Coltman, Tallon, Sharma & Queiroz, 2015). However, organizations may decide that it is necessary to improve the control environment.

Some other external entities of the organization, such as customers, suppliers, business partners, external auditors, regulators and financial analysts often provide useful information for an efficient risk management process, but they are not responsible for the effectiveness of this process and also they are not part of the organizational risk management (Table 1).

Like any factor in a complex system, the benefits of information security are weighed against their total cost (including the additional costs incurred if the system is compromised). If the data or resources cost less, or are of less value, than their protection, adding security mechanisms and procedures is not