Chapter XIV
Security Risk Management Methodologies

Francine Herrmann
University of Metz, France

Djamel Khadraoui
CRP Henri Tudor, Luxembourg

ABSTRACT

This chapter provides a wide spectrum of existing security risk management methodologies. The chapter starts presenting the concept and the objectives of enterprise risk management. Some exiting security risk management methods are then presented by showing the way to enhance their applications to enterprise needs.

INTRODUCTION

Enterprise **risk management** is the total process of identifying, measuring, and minimizing the uncertain events that can affect the enterprise resources. This implies the process of bringing management as a remedial action, and control into the risk analysis. A main element of risk assessment and analysis is the concept of **vulnerability**. The **vulnerability** is a weakness in any information system, system security procedure, internal controls, or implementation that an attacker could potentially exploit. It can also be a weakness in a system, such as a coding bug or design flaw. An attack occurs when an attacker with a reason to strike takes advantage of a **vulnerability** to **Threat**en an enterprise **Asset**. The second most important element in risk assessment is the concept of a **Threat**, which is any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, or denial of service. We can define risk as the possibility that a particular **Threat** will adversely impact an information system by exploiting a particular **Vulnerability**. The third element in the risk analysis is the **Countermeasure** or lack thereof. A **Countermeasure** is an action, device, procedure, technique, or other measure that reduces risk to an information system. Consequently, the residual risk is the portion of risk remaining after a **Countermeasure** is applied. Residual risk could be of none if a perfect **Countermeasure** exists.

The enterprise information systems security requires controlling the whole techniques and methods used to reduce the risks on the potential related vulnerabilities and **Threat**s. The risks analysis consists in decreasing those on an acceptable level in order to be supported by the enterprise. Successful risk analysis is however nothing more than a business-level decision-support tool, which is a way of gathering the requisite data to make a good judgment call based on knowledge about vulnerabilities, **Threat**s, impacts, and probability.

The risk analysis must thus be coordinated within a well-defined strategy. An organization can reduce the risk to an acceptable level by enhancing its security as well as by sensitizing the personnel and the trade partners as for their responsibilities with regard to the underlined strategies. Security may also contribute to the results of an enterprise insofar as the customers appreciate the reliability of a supplier.

To solve these issues, the answer is not only by mastering the technical solutions that ensure, for instance, system and data confidentiality and integrity, maintaining the safety of networks (firewall, IDS, etc.), controlling the security of the Web applications, updating protections against the attacks and to ensuring the personnel training and sensitizing. These technical skills are essential and must be planned, organized and be structured by using **risk management** methodologies. The concept and objectives of these are presented in the following.

ENTERPRISE SECURITY RISK MANAGEMENT: CONCEPTS AND OBJECTIVES

As a corpus, traditional methodologies are varied and view risk from different perspectives. Examples of basic approaches include the following:

- Financial loss methodologies that seek to provide a loss figure to balance against the cost of implementing various controls.
- Mathematically derived "risk ratings" that equate risk with arbitrary ratings for **Threat**, probability, and impact.
- Qualitative assessment techniques that base risk assessment on anecdotal or knowledge-driven factors.

Each basic approach has distinctly different merits, but they almost all share some valuable concepts that should be considered in any risk analysis. We can capture these commonalities in a set of basic definitions:

- The **Asset**, or object of the protection efforts, can be a system component, data, or even a complete system.
- The risk, the probability that an **Asset** will suffer an event of a given negative impact, is determined from various factors: the ease of executing an attack, the attacker's motivation and resources, a system's existing vulnerabilities, and the cost or impact in a particular business context.
- The **Threat**, or danger source, is invariably the danger a malicious agent poses and that agent's motivations (financial gain, prestige, and so on). **Threat**s manifest themselves as direct attacks on system security.
- The **vulnerability** is a defect or weakness in system security procedure, design,