Cost Estimation and Security Investment of Security Projects

Yosra Miaoui
University of Carthage, Tunisia

Boutheina Fessi
University of Carthage, Tunisia

Noureddine Boudriga
University of Carthage, Tunisia

INTRODUCTION

Project management is an important task that should be performed when dealing with security project, since it allows avoiding different project failures. This task is an effective methodical approach of planning, organizing, leading, and controlling resources to achieve organization's goals. It involves, thus, identifying requirements, determining clear objectives, and balancing the triple constraints scope, time, and cost (Institute, 2013).

It is noted that the management of software and security projects are not performed in the same way, due to several reasons, related mainly to the software intangibility, complexity, conformity, and flexibility. It is also shown that the parameters involved in the security cost estimation differ from those of software cost estimation. Therefore, the developed methods should be adapted to consider security specificities.

In this context, organization's project managers should estimate the cost associated to a security project during its design. This estimation should include the computation of the optimal security level and residual risk accepted by the organization. Moreover, it should consider managerial aspects regarding, for example, the effort required for security monitoring of the new assets to be acquired or updated, the security training of the technical staff, the update of the managerial decisional system, and the development of policy and procedures related to the use of information processing facilities, instead of only considering the industrial source coding of the security packages.

Another significant aspect, which should be carefully examined when dealing with security, is related to security investment. The financial budget allocated to security should be well established and managed to avoid under or over expenses. Different security investment models are developed in the literature using various techniques and examining several features. Most of them have focused on determining the optimal security investment allocation based on budgetary aspect, economic, and financial constraints. Recent works are interested to examine more specific security features when assessing the required investment, such as the system vulnerabilities, attacks type, risk factors, data privacy, and insurance.

This chapter aims at examining two aspects related to security project: cost estimation and investment assessment. First, the characteristics of security projects are stressed on and the importance of adopting management is determined. Then, the chapter presents the different cost estimation models dedicated to security project and discusses the technical and managerial factors affecting the cost estimation and the management of project. In addition, a sample review of research works directed toward security investment models is determined. These models are organized according

DOI: 10.4018/978-1-5225-2255-3.ch420

to the type of issues and aspects handled to compute the optimal amount of security investment. Finally, the chapter discusses future directions that could be investigated to make available useful models for cost estimation and investment on security projects.

SECURITY PROJECTS MANAGEMENT FRAMEWORKS

In this section, we examine the objective and features of security project and show the importance of the management task when dealing with these projects.

Definition and Characteristics

Security project is a specific type of project that implements a set of tasks to protect and secure a considered information system from attacks and potential threats. It lies usually outside the core functions of the business and aims to protect critical involved resources.

Security project is different from a software project for at least five features which characterize it:

- First, the security project requires a better knowledge of the security threats and vulnerabilities surrounding the activity of the enterprise, their future severity, and the evolving techniques they will implement. In addition, managing efficiently a security project assumes that the remaining risk related to damaging attacks, unobserved during project design, will be confined in the future. Moreover, the necessity to provide a response to significant attacks supposes that an efficient monitoring of activity and risk assessment are guaranteed.
- Second, the output of security projects is complicated and may include: (1) a security policy customized to the enterprise, its activity, and its environment describing the rules to be enforced, the security Procedures to observed, the detection to perform, and the security invariants to comply with. While a security policy acts as a specification of the security project, it differs from a specification in the way it involves the activity of an incident response team and the procedures it triggers on the occurrence of attacks; (2) a set of preventive, detective, and responsive systems to be deployed in a way that allows flexible configuration and real time connectivity to other information and decision systems in the enterprise; and (3) a set of countermeasures to introduce on preventive and monitoring tools to thwart future attacks along with security procedures and guidelines to be followed by people when immediate reactivity on the managerial procedures is needed.
- Third, estimating security project complexity is influenced by different factors, such as the size of the information system to secure in terms of number and size of interconnected sub-networks; the number of users exploiting the information system resources including customer users connecting remotely and administrators; and the complexity of the security policy defining the measures to implement and rules to enforce.
- Fourth, a great part of the work in a security project is added on the customer network in order to: (i) interview the users, security administrators, and managers, especially during the risk analysis phase to identify the managerial issues that can affect the project; (ii) integrate and configure the developed solution and update the existing networking solutions to guarantee an adequate inter-operation; and (iii) assess the robustness of the resulting security system through auditing and penetration testing.
- Fifth, a security project has to keep under control the variation of the security robust-