Management and Cost Estimation of Security Projects

Yosra Miaoui
University of Carthage, Tunisia

Boutheina A. Fessi
University of Carthage, Tunisia

Noureddine Boudriga
University of Carthage, Tunisia

INTRODUCTION

The compliance with the estimated budget and schedule agreed at the beginning of a given project is becoming more and more difficult to reach in both large and small organizations. In this context, project management is an effective methodical approach of planning, organizing, leading, and controlling resources to achieve organization's goals. It involves identifying requirements, determining clear objectives, and balancing the triple constraint scope, time and cost (Institute, 2013).

Managing a software project should be done differently from an engineering project due to several reasons, including the software intangibility (software have observable effects but their design documents are not directly observable), complexity (software include interactions and concurrent invocations of functions or objects), conformity (even if software are required to conform to existing specifications, defects in program logic are difficult to detect), and flexibility (even if a software modification can be done easily, it can lead to undesirable side effects in the remaining part).

While a security project appears to be in most cases a form of software project, its management should consider additional issues, among which we can cite: a) the dynamicity of the environment hosting or interacting with the security solution, and the diversity of security threats damage and their continuously growing number. In fact, a security solution interacts with malicious and legitimate users, who could change their behavior over time; b) the financial risk associated to the impossibility of providing a complete protection unless an infinite security investment is undertaken; and c) the likelihood that a security solution becomes itself vulnerable over time, especially if the users of the solution are neither trained, nor aware of security threats.

All of the aforementioned issues could rise serious financial losses to organizations, and impact the efficiency of the security project, if not handled suitably. To meet these challenges, organization's project managers should be able to estimate the cost associated to a security project during its design, by finding an economic justification to the related cost. This estimation includes also the computation of the optimal security level and residual risk accepted by the organization, and the demonstration of the benefits expected by the security investment. The cost estimation and financial analysis of a security project should consider, in addition to the industrial source coding of the security packages, the managerial 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.

This article aims at presenting the general framework of software project management and stressing on the particularities of security projects management. The article also discusses the most relevant approaches, techniques and models that are used to estimate costs in diverse domains. A special interest is given to security projects' cost estimation models. In this article, the technical and managerial tasks affecting the cost estimation and the management of project phases are addressed while highlighting the place of the managerial effects on the whole process.

DOI: 10.4018/978-1-4666-5888-2.ch505

The article also discusses future directions that could be investigated to make available useful models for cost security projects estimation.

BACKGROUND

The evaluation of the cost associated to a security project cannot be done using traditional software cost estimation models due to differences between software and security projects. Several works have addressed issues and provided various models for cost estimation of security and risk management projects, helping managers reasoning on the cost associated to security decisions, solutions and projects, before they make or conduct. Several of these models considered a security policy, which is serving as a document specifying the security requirements, as the key element for estimating the effort required to achieve a security project and computing its cost. The estimated effort can be seen from two perspectives. The former is related to the technical issues surrounding the acquisition and development of security prevention, detection, and reaction components, and the update and upgrade of systems, configurations, and libraries. The latter is related to the managerial issues surrounding the development and planning of training programs to employees and security administrator, the development of internal procedures and guidelines, and the development of security strategic intelligence within the enterprise

Efficiently conducting a security project and accurately estimating it before investment are requisite for several types of organizations. Walmart[1], for example, which is a worldwide retail corporation, has developed privacy policies for its offices and deployed multiple levels of security mechanisms including the encryption of user data exchanged over Internet, the use of Verisign SSL certificates to secure the online order information, and the achievement of a Hacker Safe certification. Amazon[2], is offering a set of large computing web services that together create a cloud computing platform. To ensure its customers that they are developing web architectures on a highly secure infrastructure, several important mechanisms are deployed including physical and environmental security, network monitoring and protection, management of configuration changes to the infrastructure, and virtual cloud security.

SOFTWARE PROJECTS MANAGEMENT FRAMEWORKS

In this section, we describe key concepts related to software project management, and highlight on the differences between the management of classical software development projects and the management of security projects.

Definition, Processes, and Guidelines

Projects management is a key tool for strategic planning to organizations. It provides a discipline focusing on the application of techniques and tools for the purpose of planning, organizing, monitoring, and controlling projects. One of the most complex projects is the software projects that result in intangible assets with respect to other engineering projects. In this context, software project management emerged as the art and science of planning and leading software projects (Stellman, 2005). Generally, from the time where the project starts until it ends, five main steps should be followed as described in Figure 1.

- **Initiation:** Important project parameters should be determined before the project effectively starts. They include the objective from the client points of view, the cost to accomplish the project, and the resources that will be allocated during realization.
- **Planning and Design:** Planning include effort estimation, resources allocation, selection of techniques and tools to perform efficient management. Design, on the other hand, aims at engineering the tasks set up during planning and defining an allocation plan of resources.
- **Execution:** It works for the achievement of the objectives defined in the initialization phase as planned during the second phase.
- **Monitoring and Controlling:** In this phase, performance reporting and risk monitoring and control are conducted to continuously evaluate whether people are progressing as expected and in conformance with what has been scheduled.