A Managerial Issues-aware Cost Estimation of Enterprise Security Projects

Boutheina A. Fessi, Yosra Miaoui, Noureddine Boudriga
Communications Networks and Security Research Lab. (CN&S)
University of Carthage
Tunisia
boutheina.fessi@isg.rnu.tn, yosra.miaoui@gmail.com, nab@supcom.tn

ABSTRACT: *While several models are provided in the literature to estimate different features of projects management: duration, effort, cost, and investment, they are not tailored to the cost estimation of security projects. We provide in this paper a new model for the managerial aware estimation of the effort required to conduct a security project. This model takes into consideration the effort related to monitoring, awareness, decision making, organizational, and decision support. Three effort estimation models are proposed depending on the information system size, the complexity of existing security policy, and the enterprise size. In the proposed model, the cost associated to the achievement of a security project is deduced from the estimated effort.*

Keywords: Project Management, Security Solution, Cost Evaluation, Effort Evaluation

Received: 28 February 2013, Revised 28 March 2013, Accepted 31 March 2013

1. Introduction

Project management, often associated with engineering projects, is a process of planning, organizing, motivating, and controlling resources to meet required objectives. Managing projects efficiently is a requisite for organizations. It involves the interaction of different factors, including scope, time, cost, and human resources. In this context, managers should be able to accurately estimate the cost associated to a security project, given its specification, in order to make sure that the enterprise has the sufficient funds to accomplish the project, compare the anticipated benefits against the estimated cost, and decide how to manage the project budget [4].

While several works in the literature considered a security project a software project, one can notice at least the two following main differences. First, differently to a software project, where a specification is an essential part of the development process, a security project is build upon a set of requirements that are derived from the existing enterprise security policy (i.e., a conceptual model of security within the enterprise information systems, that can be described as a set of rules by which users and assets should abide). Second, differently to a software project, a security solution is expected to supervise resources, interact with malicious and legitimate users whose behavior is dynamic and change over time, protect from attacks, and execute countermeasures in a timely fashion. In this content, one can recognize that while a security solution is valuable to protect from attacks, it could become vulnerable over time, especially if the users of the solutions are neither trained, nor aware of security threats.

Considering the dynamic aspects of attacks, users behavior, and supervised resources, and in order to cope with new threats and attacks, it becomes necessary to continuously monitor security solutions and update them. In addition, a set of security procedures and technical guidelines need to be developed to prevent against any misuse of the solution that could affect the security of the information system.

Based on the aforementioned characteristics, the cost estimation and financial analysis of a security project should take into consideration, in addition to the industrial source coding of security programs, a managerial effort required for security monitoring of the new assets to be added or updated on the information system, security awareness and education of technical staff, update of the managerial decisional system, and development of policy and procedures related to the use of information processing facilities.

Estimation of projects investment cost has interested several works in the literature. In [3], the authors provided a model helping to decide on the allocation of security investments by considering the risk associated to security attacks. Other approaches were proposed to evaluate the cost related to software projects [6], [7]. The Constructive Cost Model (COCOMO), is one of the famous models proposed in [2] to estimate the effort required to develop a software depending on the number of source instructions extracted from specification, and a subjective assessments of other attributes related to hardware, personnel, and project (e.g., personnel capability and experience). Due to the highlighted differences between a software specification and a security policy, such a model cannot be used for the purpose of cost estimation of security projects.

SECOMO was proposed in [5] to address this issue. It provided a model for cost estimation of risk management projects, helping managers reasoning about the cost associated to a security networking decisions before they make. However, SECOMO is designed to be used by security solution development enterprises to estimate the effort required to develop the security project. It does not consider the managerial efforts, including, but are not limited to, awareness and organizational security. In addition, SECOMO considers that the effort required to develop a security project is a function of the size of the information system of the enterprise that will deploy the solution. In practice, the effort should also depend on the number of security measures and techniques to be developed in this project.

We propose in this work a new cost estimation model security projects considering the managerial effort required to deploy the acquired security solution. The provided model is founded on SECOMO and COCOMO. It considers managerial efforts related to monitoring, awareness, decision making, organizational, and decision support. Three effort estimation models are proposed according to information system complexity, the strength of the existing security policy, and the sensitivity of the services and data managed by the enterprise.

Tree contributions are achieved in this work. First, we provide a model helping managers predicting the cost associated to the acquisition of a new security solution that the security team is requesting. By estimating the anticipated cost, managers could efficiently define and manage their project budget. Second, to the best of our knowledge, we provide the first model that numerically estimate the managerial impact on the cost associated to a security project. Third, in this model, the security policy, which is serving as a specification of the security project, is considered as the key element for estimating the effort required to achieve it and computing its cost.

The paper is organized as follows. Section 2 reviews the SECOMO model and presents its weaknesses in coping with the managerial issues. Section 3 details the identified managerial factors affecting security projects. In Section 4, we describe and discuss the mathematical model for the management-aware cost estimation of security projects. In this section, we also describe the approach used to estimate the parameters of the model and evaluate them. The last section concludes the work and provides future prospects.

2. Reviewing the SECOMO model

SECOMO [5] was provided as an extension to the COCOMO model to provide to security teams a solid basis for determining how much time, cost and personnel are required for carrying out a security project, through estimating the required effort to conduct such a project. The extension was done following the identification of three main differences between security projects and software development. First, a software project output is a product sailed to customers for a use purpose. For security projects, the output is a system including security policy, countermeasures installed on the network, and monitoring tools. The latter are also proper to security projects as they aim at controlling the network security state. Second, the complexity in software cost estimation depends on the software size, whereas in security projects, the complexity is related to the solution size, the heterogeneity of the network resources used by this solution, the interaction between them, and the extent to which they are distributed and visible to outsiders. Third, the factors influencing software development effort and security effort are not the same. For instance, attack frequency and factors which affect mainly the security project, have no effect on software projects.

The SECOMO effort estimation, E, is expressed in $Man \times TimeUnit$ and formalized by the following equation:

$$E = a \times EAF \times S^{b} \tag{1}$$

where a is constant, EAF is an Effort Adjustment Factor based on effort multipliers, S is the solution size, and b represents scale factors. It is noticed that the estimation is based on cost drivers and on complexity of the solution size. The cost drivers are classified into two categories: effort multipliers and scale factors. The effort multipliers are factors that have linear effect on the estimation of effort and are organized into four categories, namely product, personnel, project, and information system. Whereas, the scale factors have an exponential impact on the effort estimation and include four factors, namely precedentedness, team cohesion, project maturity and security strategy.

The solution size is deduced in a semi-automated manner from the security policy. The more the security policy is complicated, the higher will be the value of S. To measure this factor, a good definition of the enterprise resources (hardware, software, personnel, etc.), their security level, and the policy rules, should be performed.

To estimate the effort using equation 1, SECOMO proposed to select a set of scale and effort multiplier factors depending on the complexity and technology used by the enterprise. Three cost estimation models are therefore proposed: basic, intermediate and advanced. In SECOMO, the cost associated to a security project is a function of the estimated effort.

Despite the contribution of SECOMO to the management of security projects, the model is showing some limitations in assessing the cost associated to the managerial issues when conducting a security project. Some limits should be addressed:

- SECOMO is designed to be used by development organizations. It can not be used, as it is, by any organization that aims to assess the total cost of a security project it wants to build. Different parameters, which are intrinsic to the software development company, could not be thus estimated accurately such as team capability and tool experience.

- Some managerial parameters, such as the addition of security monitoring components, strategic intelligence, and design of organizational security documents, are not considered in SECOMO despite their importance and effect in estimating the project cost.

- SECOMO is related to the ISO 17799 [1] security policy standard, where awareness appears as a major factor in estimating the cost. In practice, the cost of a security project should include the managerial effort following the deployment of the solution, including the update of the business processes and working procedures. In addition, it should depend on the type and number of security techniques and measures to be developed in this project. It happens that a large set of managerial and organizational tasks within the enterprise highly depend on the content of the security policy.

3. Managerial factors affecting security projects

A management-aware estimation of the effort required to conduct a security project, should integrate at least five classes of factors: monitoring, awareness, decision making, organizational, and integration and compliance. Monitoring include the collection and assessment of the different properties and parameters related to the security of the information system, the analysis of the security state, and the generation and management of alerts. Awareness activity copes with collection, analysis, and dissemination of information related to the protection and the safe use of the information system. Decision making include all the activity related to the setting up and update of the risk analysis and decision tools. These tools should be interfaced with the acquired security solutions. Organizational security considers the design and development of security procedures and guidelines, and the update of the organizational network architecture, communication flow, and enterprise procedures. The last class deals with the detection of non-compliance of the security solution with the enterprise security policy. It also takes interest in security hardening of the deployed solution before being exploited. A set of factors are identified for each class.

3.1 Monitoring

To estimate the effort related to monitoring, at least five factors should be considered.

3.1.1 Acquisition / development of security monitoring components (M1)

The effort needed by security administrators to acquire and deploy sensors useful for monitoring the network resources and guaranteeing their safety after the implementation of the acquired security solutions. Since a security solution may become vulnerable over time due to the evolution of threats and attacks, an effort related to the selection and deployment of monitoring solutions should be taken into consideration during the cost estimation of a security project.

3.1.2 Monitoring-related configurations (M2)

The deployment of the acquired security solution introduces new resources to the information system, leading to the need to reconfigure the existing monitoring components, so that administrators can supervise the whole security state of their information system. Intervention from internal administrators and external consultants should be required.

3.1.3 Distribution / cooperative aspect of monitoring components (M3)

Some of the parameters that need to be monitored can not be estimated, unless data are collected from different sensors that are distributed over the different information system of the enterprise. The more the communication technology, protocols, and data used by the information system are heterogeneous and complex, the more will be the effort required to provide for the deployment of the security project.

3.1.4 Vulnerability of the monitored technology / protocol / data (M4)

By introducing new components to the information system, new security threats could be introduced subsequently. The more the software developed by these solutions, or the protocol used by them are vulnerable, the higher will be the effort required to monitor the users behavior and the traffic flow. A special interest should be granted to the detection of cover channels as long as the protocol used by the developed solution is vulnerable to such kind of attacks.

3.1.5 Control station complexity (M5)

The alerts to be collected from the different monitoring components need to be processed by the alert management station. An additional effort is required to configure the station by specifying when and how these statistics will be displayed, and where they will be stored. The control station needs to be interfaced with the enterprise decision making system.

3.2 Awareness

Four factors are considered to estimate the effort related to awareness.

3.2.1 Recruitment (A1)

Efforts provided by the managers of the company to firstly determine the number and description of new positions recruitment that are necessary for the administration, monitoring, and operational usage of the new security solution, and secondly, to describe the appropriate profile of the new candidates for these positions (e.g., qualifications, required experience). To attract highly qualified workers to the company, a recruitment program should be defined (e.g., online announcement, media advertizing)

3.2.2 Training (A2)

Efforts provided by the managers of the company to define the type and number of required trainings to be followed by the managerial and technical staff. At least two types of trainings are required. The former is conducted by external training companies to let administrators and operators develop new skills that are required for the efficient and secure usage of the security solutions. The latter are performed by the security staff to educate and train employees to security awareness, and disseminate the learned information by organizing meetings and internal training sessions, and forwarding bulletins and reports.

3.2.3 Professional certifications (A3)

Efforts provided by managers to organize and plan certification exams in order to validate the professional skills required by their security administrators to efficiently configure, use, and monitor their security solutions. The certification exams allow the trained persons to detect gaps in their understanding of the technical aspects of security.

3.2.4 Strategic intelligence (A4)

Efforts required by the security specialists to collect raw data related to the security of the protected network from various information sources, filter, master, and making sense from the relevant parts of them. The aim is to understand the key threats, assess the potential risk, operate efficiently, and respond to security incidents.

3.3 Decision making

Four factors are considered to estimate the effort related to decision making.

3.3.1 Update of decision libraries (D1)

By introducing new hardware and software components to the information system, new types of decisions could be generated over these components. Filtering, analysis, and connections reset, are examples of decisions that could be applied on updated information system (after integrating the acquired security solutions). These decisions need to be configured, tested, and implemented by the security administrators before being used.

3.3.2 Decision Support System (DSS) upgrade (D2)

Some types of decisions can not be generated unless the tools and techniques (e.g., neural networks, Bayesian networks) used by DSS are upgraded. An additional effort should be provided if the DSS upgrade requires new add-ons that need to be installed and configured.

3.3.3 (Re) configurations (D3)

Since an enterprise decision making system is based on the use of a set of tools and techniques for data analysis, risk management and attacks prediction, an effort is required to re-configure the existing DSS by adjusting the thresholds and parameters used by these tools and techniques.

3.3.4 Parameters collections (D4)

The new decisions and techniques appended to the DSS require the collection of new parameters. Consequently, a reconfiguration of the different sensors deployed over the network is needed.

3.4 Re-engineering

The effort related to organizational security depends on three factors.

3.4.1 Organizational procedures (O1)

Efforts provided by managers to update and/or create new procedures related to system information resources configuration and operational use. These procedures should comply with the rules defined in the security policy and strategy.

3.4.2 Organizational guidelines (O2)

Efforts provided by managers to update and/or create guidelines.The changes of guidelines aim to improve current technical working, strengthen the actions of technical staff, and prevent against potential misconfiguration and misuse of the protected resources. The effort required to develop these guidelines highly depends on the number and the complexity of the security policy.

3.4.3 Organizational topology upgrades (O3)

Efforts provided by managers to review network-based organizational structure needed for the inte gration of the new security solutions. This could lead to the creation of new communication nodes or links, and the re-structuring the network of the different divisions, allowing employees and managers to communicate efficiently, while abiding by the requirements defined in the security policy.

A modification of the network architecture usually lead to an additional effort required to review the organizational traffic flow by updating routing, filtering, and analysis functions, so that technical and administrative staffs could coordinate without affecting the security of exchanged information.

3.5 Integration and compliance

Three factors are considered to estimate the effort related to the integration of the new security solution, a nd the testingof its compliance to the security policy.

3.5.1 Security Policy compliance testing (I1)

A security project is developed with respect to the enterprise security policy, which plays the role of a specification. Since attacks are dynamic, and their forms could change depending on the system, service, or data they target, the designed security solutions need to be checked against known attack scenarios, and tested whether they respect the requirements specified in the security policy.

3.5.2 Security solution integration (I2)

An effort is provided by the security administrators to integrate the security solution to the information systems. This effort includes the configuration of the host machines where the solution will be implemented, the parametrization required for the interfacing of the solution with the other information system resources, and the configuration of the network connection parameters.

3.5.3 Security hardening of the integrated solution (I3)

Similarly to any software tool, a security solution is itself vulnerable to attacks. Therefore, it should be hardened by eliminating potential vulnerabilities, strengthening configurations, and disabling unnecessary software, libraries, and services available on the operating system where the solution is installed.

4. Management issues-aware cost estimation

We develop a model for effort estimation, depending on the information system size, the complexity of the security policy, and the enterprise size. As in COCOMO and SECOMO, the effort estimation equation depends on the nature and the size of enterprises which are classified into three classes: basic, intermediate, and advanced. In this work, we keep the same number of classes, but we define them differently based on the importance of security management in the enterprise.

In the basic model, the enterprise information system is very limited in terms of communication capabilities and interaction with external environments. It is showing a very little exposure to security threats. Consequently, the enterprise managers consider that the factors discussed in Section 3 do not have an impact on the project cost.

In the intermediate model, the enterprise activity is quite sensitive to security incidents, since its information system is connected to public networks and could face external attacks. In particular, different information systems are used and are in most cases separated from each other. The production network, which process the most sensitive data, is isolated from the external users. Therefore, not all the factors identified in Section 3 are important to consider.

In the advanced model, the enterprise information is showing a high number of connected nodes and links, and provides network services that are accessible from public networks. It should well protect its resources from external threats. In this case, the required security solution is more complex and needs the consideration of all the above described factors. Compared to the intermediate model, this model is suitable for enterprises employing a large number of personnel, conducting a more security sensitive activity, and having more important business processes.

We believe that the managerial factors are related to three main measures, namely the information system size (IS), the security policy complexity (SP), and the enterprise size (ES), which all affect the development and deployment of a security solution. The values of the parameters related to the three measures (*IS*, *SP*, *ES*) vary from an enterprise to another. The more the enterprise information system is open to external environments, the higher will be the values of *IS*, and *ES* parameters. In the other side, the more is the risk associated to the enterprise, the higher is the effort required to implement the security policy, and therefore, the higher will be the values of its parameters.

The effort E required to develop a security project within an information system is expressed as the summation of three terms E_1, E_2, and E_3, where each one of them follows the SECOMO form.

$$E = E_1 + E_2 + E_3 \qquad (2)$$

4.1 Basic model

The effort E required to the achieve the security project is given by the following equations:

$$E = \alpha_1 \times IS^{\beta_1} + \alpha_2 \times SP^{\beta_2} + \alpha_3 \times ES^{\beta_3} \qquad (3)$$

$$E_1 = \alpha_1 \times \mathrm{IS}^{\beta_1} \qquad (4)$$

$$E_2 = \alpha_2 \times SP^{\beta_2} \qquad (5)$$

$$E_3 = \alpha_3 \times ES^{\beta_3} \qquad (6)$$

where

- α_1, α_2, α_3, β_1, β_2, and β_3 represent constant factors;
- *IS* (Information System size) provides a measure of the complexity of the existing enterprise information systems that will be secured, and the set of used communication system;
- *SP* (Security Policy) provides a measure of the complexity of the described rules, and the different security mechanisms and countermeasures specified in that policy;
- *ES* (Enterprise Size) provides a measure of the number of business processes, the size of the organization resources, and the geographical distribution of the enterprise.

4.2 Intermediate and Advanced model

The effort estimation equation is described as follows:

$$E = \alpha_1 \times AF_1 \times IS^{\theta_1} + \alpha_2 \times AF_2 \times SP^{\theta_2} + \alpha_3 \times AF_3 \times ES^{\theta_3} \quad (7)$$

$$E_1 = \alpha_1 \times AF_1 \times IS^{\theta_1} \quad (8)$$

$$E_2 = \alpha_2 \times AF_2 \times SP^{\theta_2} \quad (9)$$

$$E_3 = \alpha_3 \times AF_1 \times ES^{\theta_3} \quad (10)$$

where:

- AF_1, AF_2, and AF_3 represent the effort adjustment factors, each one has the form of: $AF_i = \prod_j EM_j$, where EM_j is the effort multipliers factor;

- θ_1, θ_2, and θ_3 are respectively equal to $\theta_1 = \beta_1 + \Sigma w_i$, $\theta_2 = \beta_2 + \Sigma v_j$, and $\theta_3 = \beta_3 + \Sigma u_k$; where w_i, v_j , and u_k represent scale factors.

It is noticed that the effort is expressed by the same equation for the two models, but the main difference consists in the allocation of the scale and effort multipliers cost drivers that should be related appropriately to information system size, security policy and enterprise size.

In the intermediate model, a subset of the different factors identified in Section 3 are considered as effort multipliers and scale factors as denoted by Table 1.

Effort related to	Scale factor Parameters	Effort multiplier Parameters
Information System size	A4, I2	M1, M2, M4, D3, O1, O2
SP complexity	A4, I2	M2, D1, D3, O1, O2, I1
Enterprise size		A2

Table 1. Cost drivers repartition in intermediate model

In the advanced model, the whole set of parameters are considered as cost drivers. Their repartition into effort multipliers and scale factors is described by Table 2.

The introduced parameters in the advanced model are related to the additional effort provided to secure the enterprise information system. For instance, the organizational topology upgrade is necessary for enterprises having a wide network, a large set of business processes, and a complex security policy.

4.3 Cost estimation

Having computed the global effort required to achieve a project, as described in equation 2, we follow the same approach used by SECOMO to compute the cost. In this case, the total cost will be an addition of three costs, related to the estimated efforts E_1, E_2, and E_3, respectively. The total cost C is given by equation 11:

Effort related to	**Scale factor Parameters**	**Effort multiplier Parameters**
Information System size	M3, A4, O3, I2	M1, M2, M4, O1, O2, I3
SP complexity	M3, A4, D4, O3, I2	M2, M5, A1, D1, D2, D3, O1, O2, I1, I3
Enterprise size	O3	A2, A3

Table 2. Cost drivers repartition in advanced model

$$C = C_1 + C_2 + C_3 \tag{11}$$

$$\forall i \in [1..3], C_i = \lambda_i \times E_i^{\phi_i} \tag{12}$$

where λ_i represents a constant and ϕ_i depends on the type of the enterprise. In the basic model, ϕ_i is equal to a constant, whereas in the intermediate and advanced models i is equal to a function of the above described cost drivers.

4.4 Parameters estimation and model quantization

The parameters of the models are estimated by using a priori model and the validation is conducted by using a posteriori model. The a priori model is used to collect information from eliciting security experts based on their opinion and judgment.The obtained data are incorporated into a statistical model. One of the techniques, that could be used in the a priori model, consists in distributing questionnaires to experts to collect data and define the cost metric values based on their answers.

The questionnaire needed for the a priori model could include several questions aiming to determine the security level and the size of the related information system, the security policy complexity, and the enterprise size. Moreover, the defined cost drivers (effort multipliers and scale factors) should be understandable by the experts, to efficiently assess, considering the basic, intermediate, and advanced models.

Later, a posteriori model is applied to adjust the model based on the collection of data from enterprises.The real data are collected from enterprises that had conducted security projects using the minimum required skilled personnel.These data, which are obtained from real security experiments, are then combined to the data obtained from the a priori model, using regression tools, in order to obtain the final estimation of the parameter values.

Since the estimated values depend highly on the skills of the technical and managerial enterprise staff and the experience gained by the enterprise in conducting security projects, the a posteriori model is constantly reapplied to integrate the data that can be collected by the conducted the security projects within the lastest period.

5. Conclusion

This work proposed a model for estimating the cost of security projects, considering the impact of the managerial issues. The cost is a function of the information system size, the security policy, and the enterprise size. A set of cost drivers are identified and classified into monitoring, awareness, decision making, re-engineering, and integration and compliance.

The proposed model is very large and could be extended to estimate the operating cost of a security project, and consequently helping managers to efficiently determine the budget to be allocated and reduce the expenses related to the exploitation of a security solution. Furthermore, through the use of this model with different security projects, the enterprise could capitalize on its experience and provides a cost estimation service to other parties. As an additional extension of this work, we would consider the estimation of the residual security risk following the deployment of the acquired security solution.

In a future work, we will estimate the different values of the developed effort and cost estimation models. Since there are different types of a priori and a posteriori techniques that can be used for this purpose, we aim to compare these methods and decide about the most appropriate ones.

References

[1] ISO/IEC 1799:2000 (part 1) (2000). Information technology-code of practice for information security management.

[2] BarryW. Boehm, Chris Abts, Winsor Brown, A., Sunita Chulani, Bradford K. Clark, Ellis Horowitz, Ray Madachy, Donald J. Reifer, Bert Steece. (2000). Software Cost Estimation with Cocomo II. Prentice Hall PTR, August 11..

[3] Derrick Huang, C., Ravi S. Behara. (2012). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics*.

[4] P. M. Institute. (2004). A Guide to the Project Management Body of Knowledge: PMBOK Guide. Project Management Institute.

[5] Jihen Krichen. (2008). Managing Security Projects in Telecommunication Networks. PhD thesis, SUP'COM, November 22.

[6] Marban, O., Menasalvas, E., Fernandez-Baizan, C. (2008). A cost model to estimate the effort of data mining projects (dmcomo). *Information Systems Journal*, 33, 133–150.

[7] Sharma, T. N. Analysis of software cost estimation using cocomo ii. *International Journal of Scientific* & *Engineering Research*, 2 (6) 1–5, June.