Modeling Security Management of Information Systems: Analysis of a Ongoing Practical Case

Jose M. Sarriegi[1], Javier Santos[1], Jose M. Torres[1], David Imizcoz[2], Angel L. Plandolit[3]

[1]Tecnun (University of Navarra), Pº Manuel de Lardizabal 13, 20018, Donostia (Spain), Phone: 34943219877, Fax: 34943311442

[2]s21sec, Edificio Urgull 2º Local 10 (Parque Empresarial Zuatzu), 20018, Donostia (Spain), Phone: 34943317330, Fax: 34943317476

[3]Sener, Avenida Zugazarte, 56, 48930 Las Arenas (Spain). Phone: 34944 817 545, Fax: 34944 817 752

jmsarriegi@tecnun.es, jsantos@tecnun.es, jmtorres@tecnun.es, dimizcoz@s21sec.com, angel.plandolit@sener.es

Abstract

How long could an organization survive without its information systems working efficiently? Frequent changes of the systems to protect, significant delays between efforts and results, the large amount of involved variables and the difficulty to measure some of them make security management a challenge for current companies.

Simulation models provide a virtual environment that can help analysing the dynamic balance between the affected key factors. These key factors include technical controls (Software and hardware elements to protect the system), formal controls (Procedures for guaranteeing an efficient use of technical controls) and security culture (Human factors that affect the compliance of the designed procedures).

This paper presents an ongoing real modelling process, involving a university team and two companies. The paper includes information about the used methodology, the modelling process and the preliminary results of the obtained model. This process has allowed concluding that the obtained benefits are very promising.

1 Introduction

How long could an organization survive without its information systems working efficiently? In the best cases the answer to this question is measured in a few days, in other cases in hours, in worst cases in seconds. Definitively, it is a fact that current companies significantly depend on their information systems.

The relevance of the information systems can also be measured through the exponential growth of the investment in information systems made by any organization, either public or private, profit or no-profit.

The reason of this relevance is that information has become the main resource for current organizations. Organizations no longer compete based on the tangible resources, but rather their competition uses arguments such as the innovation and the knowledge, which need information as an indispensable ingredient (Sveiby, 1997).

On the other hand, current companies are also more and more "connected" both internally, among departments, and also with external agents: customers, suppliers, information sources, Administration, etc. As a consequence, they should open their information systems to facilitate the daily work, but this openness also implies that the vulnerability of these systems increases.

A clear sample of the outlined situation can be verified for the exponential growth of the incidents official informed to the CERT (Center of Internet security expertise, Carnellie Melon) in the last five years (Figure 1).

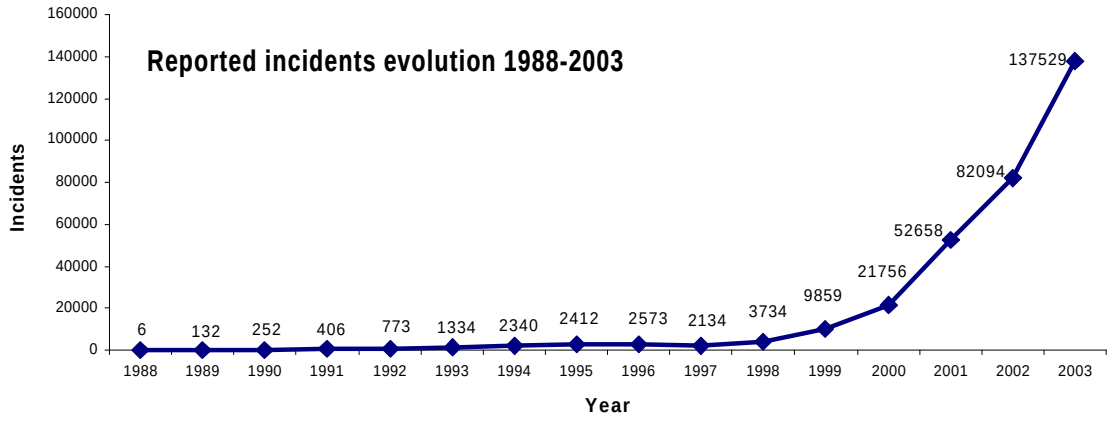

Figure 1: Evolution of the reported incidents (1988-2003)

Therefore, combining both factors, we could say that companies are more and more exposed to have problems in their information systems, due to their connectivity and complexity. Besides, the consequences of those problems might be more and more serious, because their dependence is becoming higher.

If both, the probability of the occurrence of an incident and the importance of its consequences have increased, it can be immediately concluded that the risk the companies are exposed to is significantly higher. This is the cause of the current relevance of guaranteeing the security of the information systems through its correct management.

2 Security Management

The concept of information systems security is wide and it has been interpreted in many different ways. Traditionally the security concept includes the ideas of Confidentiality, Integrity and Availability, corresponding to the initials CIA (Firesmith, 2003).

Therefore, the scope of security at least includes aspects related to the control of information accesses (Confidentiality), aspects related to the truthfulness of the available information (Integrity) and aspects related to the operability of the system when it is required (Availability).

There are other attributes that could also be included in the security definition, such as responsibility, integrity, trust and ethicality because of the need to approach information security from a more human perspective (Dhillon et al., 2000).

Historically, security was centered in technical aspects and remarkable advances took place in such fields as cryptography, intrusion detection, anti-virus software, firewalls and other security equipments.

The aim of these techniques was offering a technical solution to the security problem. Thus, the goal was to design defense mechanisms that would guarantee the security of the information systems. Later on, it was recognized the impossibility of guaranteeing the full security of a system by means of protection mechanisms. As a result, redundant defensive architectures were demanded, thinking about arguments such as depth defense (Reason, 1997) or multidimensional defense (Torres et al., 2004). Currently, it is still possible to find some approaches that intend to advance in the improvement of the security equipment in order to try to absolutely eliminate the possible influence of people in the security (Nielsen, 2004). Anyway, the more widely extended approach proposes that technology by itself is not enough to guarantee the security of information systems.

There is another relevant element in the current analysis of the security management: incidents generated from the inside of the organization (Melara et al., 2003), (Andersen et al., 2004). Security also began focusing in the perimeter protection, but this has changed since the verification that the insider incidents, caused by people who better know the vulnerabilities, are those that could have stronger consequences. The need of protecting from the inside has significantly increased security complexity.

Once the limitations of the technical solutions have been presented, it can be argued that security is a chain as strong as its weakest link. There are several approaches that explain which security links could be; but to simplify this perspective security can be assimilated to a chain composed by three links (Dhillon et al., 2001): the technical, the formal and the cultural one.

2.1 Security technical link

The technical link of security includes any tool (hardware or software) used for protecting the system from non-desired or anomalous uses. Perhaps, it is the best-known link and undoubtedly the more "visible" one. Currently, there is a great variety of security elements (Venter and Eloff, 2003), such as firewalls, antivirus, physical and logical access controls, intrusion detection and prevention systems, and many others.

All these technological tools are required to reach appropriate security, but they do not guarantee the needed security level (or the affordable insecurity level).

2.2 Security formal link

Security formal link is the group of policies and procedures developed to make a suitable use of the technical elements of security. It would be useless to have the appropriate technical elements if they are not used correctly. It would be like having a car and not knowing how to drive it.

The assignment of responsibilities and training are some examples of the formal link. Security responsibilities must be assigned explicitly to avoid situations such as *"I thought that you were in charge of this"*. On the other hand, the users of the information systems should know which the security systems are, what are they for, and what could it happen if they were not used correctly. A good example could be the reasonably explanation of the need to carry out backup copies periodically.

The security formal management is characterized by the difficulty of having objective metrics and also by the low frequency of incidents, which makes learning more difficult. In fact, several studies verify that the activities related to security are rarely monitored in a structured way (Sarriegi et al, 2005a). For example, there are only few companies which control effective use of backup copies routines.

2.3 Security cultural link

Experience shows that having the appropriate resources and well-defined procedures to manage them, is not enough to make these resources work satisfactorily. There is another factor as important as the previous ones: security culture, which can also be known as human factor, informal control or people attitude. Users of the information systems can always find ways to jump over the security mechanisms, especially if they could get a personal benefit from this action, although it were only a short term benefit, such as making easier their job. This attitude is also explained by risk misperception (Gonzalez et al., 2003)

In fact, many of the security incidents have been caused by human errors. As a consequence, the necessity of developing a security culture has been recognized by almost all the security experts, for example, from the OECD, (OECD, 2002). The development of a security culture would be the most profitable goal for a company, although it supposes a permanent effort whose performance is not visible. In fact, the best result the company could achieve would be that nothing happened.

3 Definition of the problem

Despite its criticism, information systems security is still considered as something implicit in most of the cases, similarly than when buying a car the appropriate security mechanisms are considered included into it. This phenomenon has already been explained in non functional requirements literature (Chung, 1995).

Security tests made to information systems are usually carried out under lead time pressures and they are usually simplified or even eliminated. Rarely these tests include how the system would be recovered after a serious failure or how far the system is vulnerable to undesired uses. As the person in charge of the information system of a company would say *"we only remember security when it fails."*

Another factor that influences security management is managers' profile. They usually have strong technical background, while they haven't developed managerial skills.

Problems related to security embrace a wide range: internal or external attacks, inadequate uses (even the involuntary ones), or incorrect operations of the system. Many of these types of incidents need a particular countermeasure. This is another factor that makes security management a complex task.

Although some measures that look for increasing the security could reduce the normal operation of the processes, recent studies have tried to reconcile both, security and operability (Yee, 2004), (Conrad et al. 2003). Therefore, it can be said that the best security, as the best soccer referee, is the one that goes unnoticed.

On the other hand, it is complicated to discover the value added by security and therefore, it is complicated to justify some investments in security, since the results are not visible. However, in the last years, the level of enforced legal requirements that

affect business security has increased notably; for example the SOA (Sarbanes-Oxley Act) law in USA or the LOPD law (Ley Organica de Proteccion de Datos) in Spain, which enforces individual data confidentiality.

Recently some methodologies have been developed that seek to cover this gap and obtain reliable data for returns from security investments (Anderson, 2001) (Gordon et al., 2005), but they have not been widely used.

Security management models are currently being adopted by businesses, but there is still a long path to go, mainly in SMEs (Small and Medium Enterprises). At the European level, the most extended management model is based on the ISO17799 norm. In USA, there are other models such as COBIT, the CERT-CC Security Improvement Modules and the IT Infrastructure Library (ITIL).

Recently another aspect has acquired special relevance when analyzing the management of the information systems security: the role carried out by people (Trcek, 2004). Some proposals come from the social Engineering and they demonstrate that the human errors can lead to the failure of implemented security policies (Mitnick et al., 2002).

Definitely there are several causes that make the security management of information systems a dynamic and complex problem:

- The frequent modifications of the systems to protect due to changes in the business processes, software upgrades, hardware modifications, new security mechanisms, norm's upgrades, etc.
- The significant delays between efforts and results, for example, since an awareness program launches until this campaign offers some benefits.
- The large amount of variables that affect and that are affected by security. Besides, these variables are also multiply interrelated and any modification in one of them can affect the rest of variables immediately or some time afterwards.
- Some variables which determine significantly the security are difficult to measure, such as the commitment of the employees to security. In other cases, due to confidentiality reasons or due to the lack of formalization of their management, there are no available historical data.

3.1 Modeling: A Step forward in the solution

The last objective of research in the information systems security management should be the identification of the measures that allow guaranteeing a dynamic balance of all the key factors that affect security management information systems.

In order to reach this objective this paper suggests the development of a simulation model process. Its objective is not obtaining a precise model that allows establishing the optimum values of the parameters that govern the behavior of the system. The objective consists of acquiring a deep knowledge of the critical factors and their interrelationships for the right operation of the system.

Simulation models provide a virtual environment in which the managers can "learn from the experience" in a controlled scenario. The model captures the interrelations

among the different parts of the system under study and it provides a graphic interface that allows the managers to interact with the model (reports, graphics and spreadsheets).

But the model is not the only result obtained from the modeling process. The construction of an explicit model allows integrating the different partial perspectives that can appear over a problem, offering some learning to all the participants in the project.

Another aspect that should be considered is that it is not possible to experience with the real system and the experimentation with the simulation models has become the most powerful research tool to carry out these experiments.

Hence, the modeling process of a complex system offers two results: the obtained model and the learning achieved during the modeling process. The goal of the modeling process is not building a device to substitute decision-makers. The model process tries to improve the decision capacity of the decision-makers.

4 Modeling security management of information systems: A practical case

The project exposed here corresponds to the real modeling process of the information systems security management carried out by Tecnun, S21sec and Sener.

Tecnun contributes to the project with its modeling experience and with its knowledge in security management. S21sec is a consultant company specialized in security and Sener is an engineering company, client of S21sec in security issues.

The modeling process has been based on the Group Model Building methodology (Richardson et al., 1995), (Andersen et al, 1997), (Andersen et al., 2004).

The modeling process has included 6 meetings. All the members of the modeling team have worked on their own between these meetings. The schedule and content of the meetings is showed in table 1.

Meeting	Objetives of the meetings
Meeting 1	Present the Project methodology Introduce System Dynamics and Group Model Building
Meeting 2	Define stakeholders and clusters of security policies
Meeting 3	Identify behavior of the main variables in different scenarios
Meeting 4	Define security metrics and identify indicators to validate the model Drafts of the causal loop diagrams
Meeting 5	Validation of causal loop diagrams Drafts of the simulation model
Meeting 6	Validation of the simulation model

Table 1: Schedule of the project

The main objective of this modeling process has been to demonstrate the validity of the methodology. Only members from university had previous modeling knowledge.

4.1 Starting point

Sener was implementing a management system for the security of its information systems based on the ISO17799 norm. In this project Sener collaborated with S21sec, a company dedicated to the consultancy in security, with wide experience in the implementation of this type of systems. Tecnun team had large experience in modeling of complex systems.

Initially, people from S21sec and Sener were not familiarized with System Dynamics, so the project has been useful to validate the contribution of this modeling technique to the analysis of a well-known problem.

4.2 Definition of stakeholders and policies

This step identifies the agents who can affect the evolution of the security in a company, classifying them according to two dimensions: level of interest and influence capacity. The summary of the identified stakeholders can be seen in figure 2.

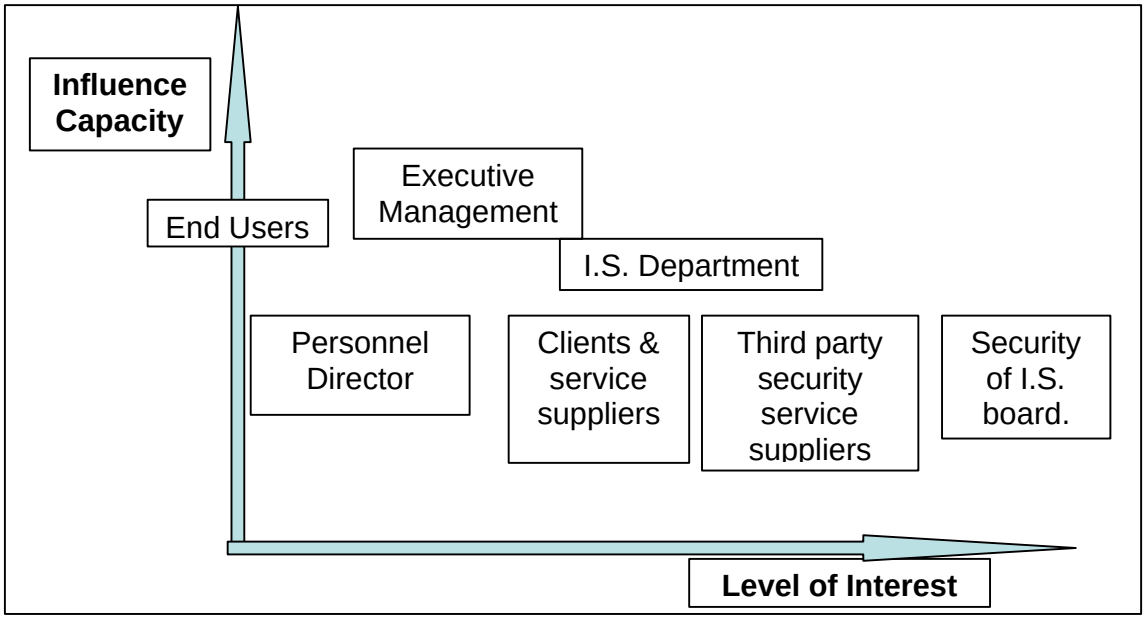

Figure 2: Analysis of stakeholders

The possible security policies were identified based on the requirements of the ISO 17799 norm and they were grouped according to the following policy clusters:

- Hiring and subcontracting (Corresponding to the point 2 of the norm). Include the possibility of recruiting new workforce for the security department.
- Assets management and risks analysis (Corresponding to the point 3 of the norm). Consists of the processes to develop and maintain a permanently updated control of the assets to be protected.
- Training, communication and awareness (Corresponding to the point 4 of the norm). Here we can found all the informal efforts to increase commitment and for developing a security culture.
- Design and Implementation of Physical-Logic Protection Controls (PLPC) (Corresponding to the points 5, 6, 7, 8, 10 and 11 of the norm). These policies

comprise the design, acquisition and implementation of some technical controls, such as, physical and logic access control or backup and recovery mechanisms.

- Management of the PLPC. This cluster of policies contains all the formal efforts oriented to maintain the PLPC working properly.
- Incidents Management (Corresponding to the point 9 of the norm). Include the management of incidents to make possible learning from them.

These clusters were built keeping in mind the similarity of the dynamics of the variables. The ISO norm contains several physical or logical measures used to protect the system, such as the physical accesses control or the logical accesses control. These controls present similar dynamics and they are grouped, at least in this first version of the model.

4.3 Behavior over time diagrams

During the project several temporary behavior diagrams were developed to describe the different behaviors that can arise during the implementation of a security management system, including both, successful and unsuccessful projects.

Figure 3 shows the evolution of the efforts in design, installation, management, risks analysis, training, audit and certification of the team in charge of the implementation of a security management system in a company.

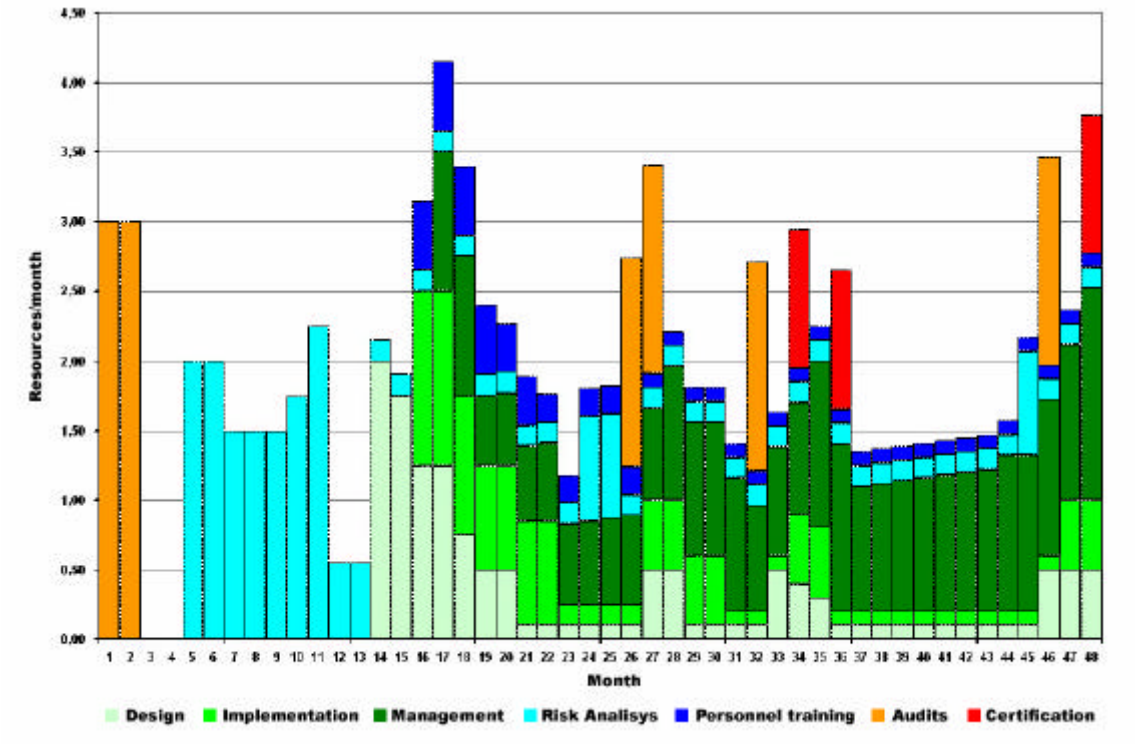

Figure 3: Resources needed for implementing a Security Management System

4.4 Causal loop diagram

The main variables of the model were also represented in a causal loop diagram (Figure 4). This model includes four core balancing loops which allow the accomplishment of the desired security level. These balancing loops correspond to:

- the development of a security culture (B1).
- their formal management (B2)
- the implementation of the PLPC (B3) and,
- the efforts allocated to the risk analysis activities (B4),

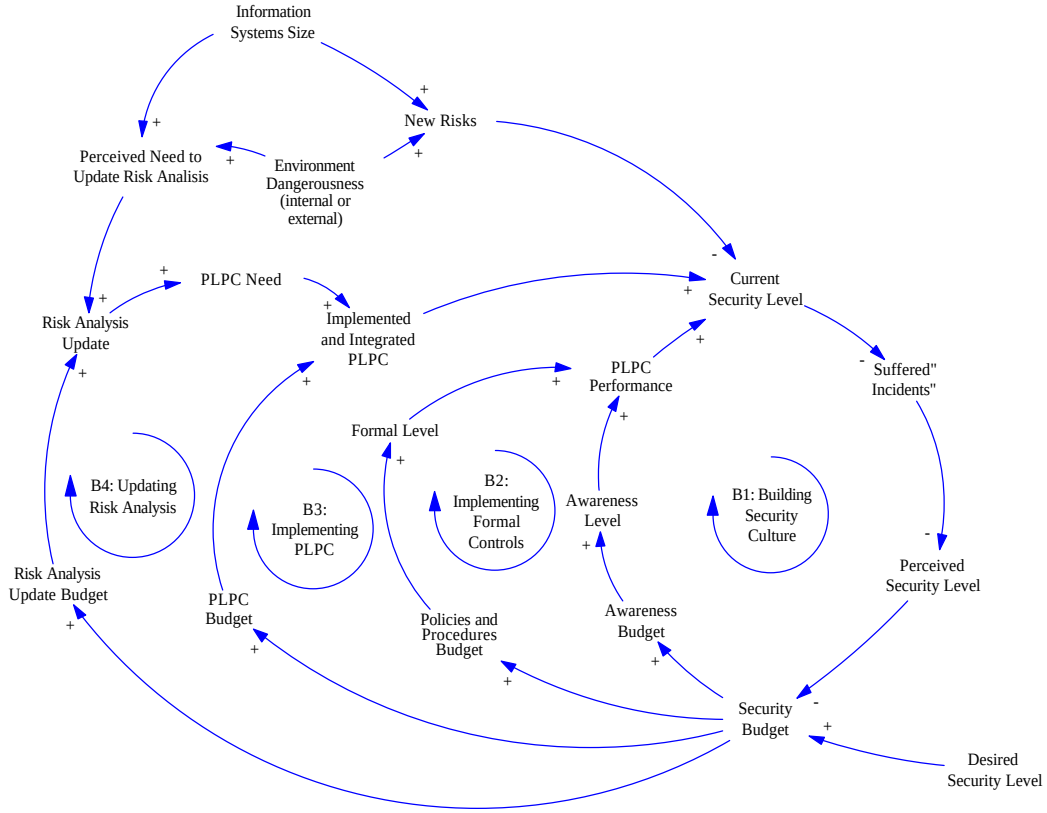

Figure 4: Causal Loop Diagram

Some of these loops had already been identified while explaining security management of information systems (Sarriegi et al., 2005b). The behavior of the system depends on the correct dynamic balance between these loops.

4.5 Levels and flows diagram

Figure 5 represents the model developed in the project. The main purpose of this model has been to make explicit the benefits of the modeling process. Thus, people without previous knowledge about modeling and system dynamics have better understood modeling concepts and also have acquired skills to interrelate structure and behaviour.

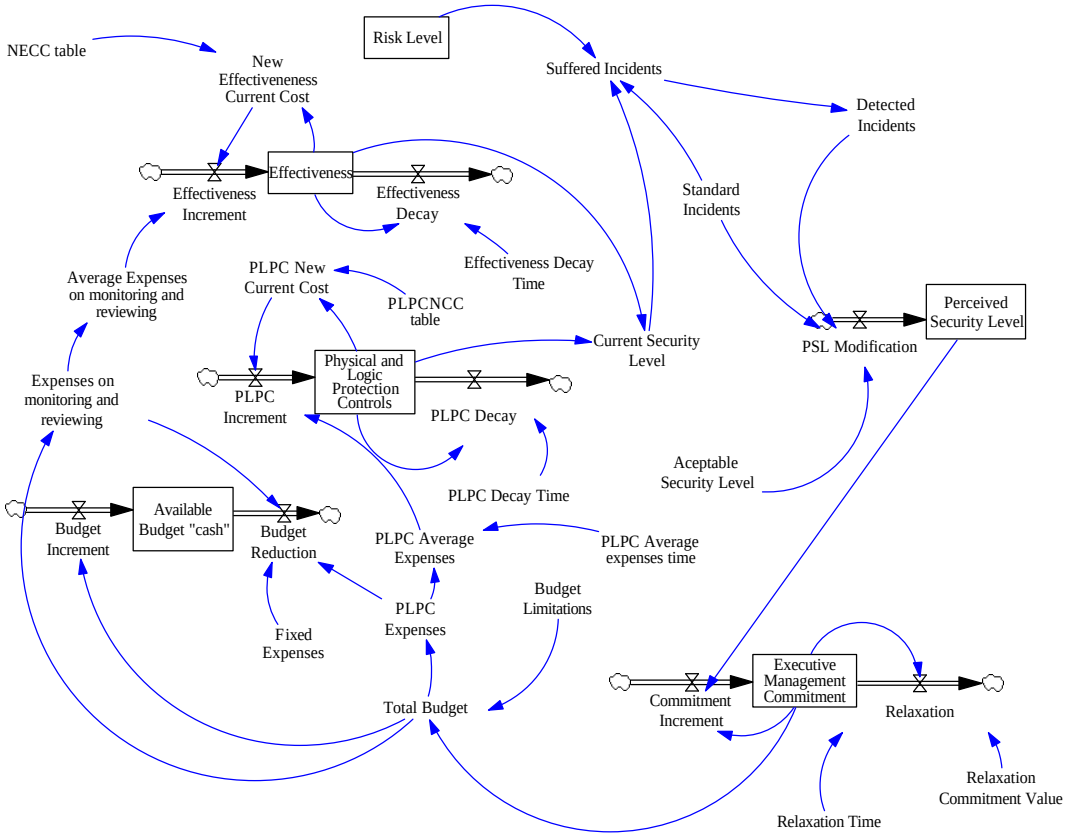

Figure 5: Simulation Model

The model includes variables to measure the implemented PLPC (Physical and Logic Protection Controls), formal controls (Effectiveness), and also security culture variables (Executive Management Commitment).

The model allows assigning resources to two different types of security controls: PLPC and Formal Controls (Effectiveness). The obtained current security level is a combination of these two levels.

Current security level determines the suffered incidents rate, which establishes the perceived security level after de delay.

The perceived security level controls the current Executive Management Commitment, which is responsible for allocating new resources.

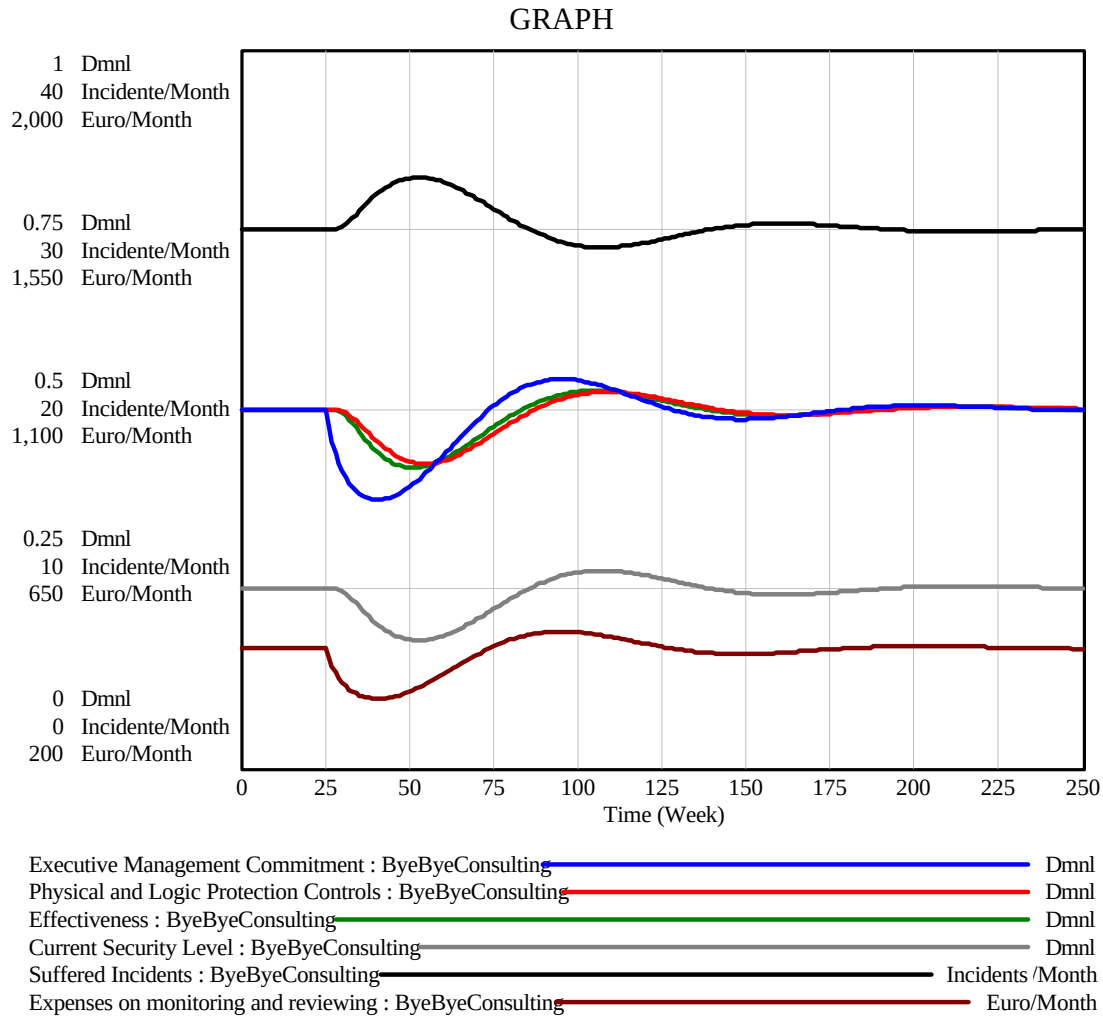

Figure 6: Behavior of the model

Figure 6 shows the behavior obtained in a scenario where the consulting firm helping the company to implement the Security management system left the project, which decreased the commitment to security and caused an oscillation of the main variables of the model.

In this case, 70% of the budget is constantly devoted to PLPC while 30% is spent in Formal Controls.

This simulation, among others, has been useful to explain to the modeling process team members the strong relationship between structure and behavior.

4.6 Validation of the Model

A model is valid if it is useful for the purpose it has been created for. A valid model does not mean an exact model. The model built in this stage of the project should still be improved but it has been very helpful so far to demonstrate the usefulness of the modeling process for gaining a better understanding about how to maintain a dynamic equilibrium between the variables involved in the information systems security management.

The validation of the current model also presents the difficulty of not having historical data for the variables of the model. To solve this difficulty the team is already working in the design of a group of indicators that allow capturing reliable information of the evolution of this type of systems in different companies. The outlined indicators are referred to:

- Training: Activities and programs to boost employees' information security knowledge and skills.
- Awareness: the appreciation, at all levels within the organization, about the needs and benefits of information security.
- Physical and logical preventive countermeasures implemented: Set of technical controls to avoid unauthorized physical and logic access to critical assets or areas.
- Risk Analysis: Activities for having an accurate identification, classification and prioritization of critical assets, vulnerabilities, threats, their impacts, and probability of happening.
- Procedures Implemented: Set of policies and procedures designed, approved and documented.

Security expert of the team accepted the results of the model and qualify them as very reasonable, although they suggest the necessity of adding more variables to the model in order to satisfy its pedagogical purposes.

4.7 Pending tasks

The model should be built in an iterative way, adding the needed variables to reproduce in a realistic way the behavior of the observed system. Therefore, some other variables considered significant might be included in the model.

Once a reliable model is developed a simulation game that allows its use by people without modeling knowledge will be built. In the game, when "players" make decisions the model answers generating a behavior that forces the player to make new decisions.

Finally, it is also necessary to advance in the validation process of the model. It should be necessary to design the appropriate mechanisms to capture the required information and contrast the behavior generated by the model with the real one.

5 Conclusions

Security management of information systems is a dynamic and complex problem that includes a large number of variables of very different nature and multiply interrelated. An efficient security management needs a dynamic equilibrium between several factors. Managing this dynamic equilibrium, which includes several factors difficult to measure, supposes a challenge for security managers.

A modeling process allows advancing in the best understanding of the complex systems, since it facilitates the dialogue and the integration of agents' perspectives who initially have different perspectives. The modeling process has resulted useful dealing with security management.

The experience with a real case has allowed obtaining some valuable results that reinforces the theoretical benefits of the modeling process. Companies without previous system dynamics modeling experience have decided to go on with the project and increment their modeling efforts. Consequently, the main objective has been reached and the validity of the methodology has been demonstrated.

6 References

Andersen, D., Richardson, G. 1997. Scripts for Group Model Building, *System Dynamics Review 13*.

Andersen D., Rich E., Cappelli C., Moore A., Shimeall T., Sarriegi J. M.,. Gonzalez J. J., Mojtahedzadeh M., Stanton J., Weaver E., Zagonel A. 2004. Preliminary System Dynamic Maps of the Insider Cyber-Threat Problem. 22rd International Conference of the System Dynamics Society, Oxford, UK.

Andersen D., Rich E,. Martinez.-Moyano I.., Conrad, S., Cappelli D., Ellison R., Stewart T., Moore A., Lipson H., Torres J. M., Shimeall T., Mundie D., Weaver E., Sarriegi J. M., Wiik J., Gonzalez J. J., Sawicka A. 2005. Simulating insider cyber-threat risks: a model based case and a case based model. 23rd International Conference of the System Dynamics Society, Boston.

Anderson R. 2001. Why Information Security is hard; An economic Perspective, Proceedings of the,

Chung, L, Nixon B. 1995. Dealing with non-functional requirements: Three experimental studies of a process-oriented approach,.

Conrad S., W. B., Thomas R., Corbet T., Brown T., Hirsch G., Hatzi C. 2003. How do we increase port security without imperiling maritime commerce? Using flight simulators and workshops to begin the discussion. 21st International Conference of the System Dynamics Society, New York.

Dhillon, G, Backhouse, J. 2000. Information System Security Management in the New Millennium. *Communication of the ACM*. 43 (7)

Dhillon, G. and Moore, S. 2001.Computer crimes: theorizing about the enemy within. *Computer & Security* 20 (8) 715-723

Firesmith, D.G. 2003.*Common concepts underlying safety, security and survivability engineering*. CMU/SEI-2003-TN-033

Gonzalez J. J, Sawicka A. 2003. The role of learning and risk perception in compliance. 21st International Conference of the System Dynamics Society, New York.

Gordon, L, Loeb, M. 2006. *Managing cyber security resources. A cost-benefit analysis.* New York, NY: McGraw-Hill

Melara, C, Sarriegui, J.M., Gonzalez, J..J, Sawicka, A, Cooke, D.L. 2003. A System Dynamics Model of an Insider Attack on an Information System. From Modeling to Managing Security: A System Dynamics Approach, Norwegian Academic Press. (Kristians and, Norway).Ed. by Gonzalez, Jose J.

Mitnick K., Simon W. L. 2002. The art of deception: controlling the human element of security. Wiley. New York.

Nielsen, J. 2004. User education is not the answer to security problems. Jakob Nielsen's Alertbox, Oct 25, www.useit.com/alertbox

OECD, 2002.Guidelines for the Security of Information Systems and Networks. Towards a culture of security,

Reason, J. 1997.*Managing the Risk of Organizational Accidents.*: Ashgate Publishing Ltd, Hants, UK

Richardson, G, Andersen, D. 1995. Teamwork in Group Model Building, *System Dynamics Review 10*

Sarriegi, J M, Eceiza, E, Torres, J M, Santos J. 2005a. Security Management of Information Systems Report.

Sarriegi, J. M., Torres, J. M., Santos, J. 2005b. Explaining security management evolution through the analysis of CIOs' mental models. 23rd International Conference of the System Dynamics Society, Boston.

Sveiby K. E. 1997. *The new organizacional wealth.* Berret-Koehler Publishers, San Francisco

Torres, J. M., Sarriegui J. M. 2004. Dynamic aspects of the security management of information systems. 22nd International Conference of the System Dynamics Society, Oxford.

Treck, D. 2004. Business dynamics supported security policy management. 22nd International Conference of the System Dynamics Society, Oxford.

Venter, H. S. and J. H. P. Eloff. 2003. A taxonomy for information security technologies. *Computers & Security* 22(4): 299-307.

Yee K.P. 2004. Aligning security and usability. *IEEE Security & Privacy* 2 (5) 48-55.