Developing a Maturity Model for Information System Security Management within Small and Medium Size Enterprises

Luis Enrique Sánchez[1], Daniel Villafranca[1], Eduardo Fernández-Medina[2] and Mario Piattini[2]

[1] SICAMAN Nuevas Tecnologías. Departament I+D
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, Spain

[2] Castilla-La Mancha, ALARCOS Research Group,
TSI Department, UCLM-Soluziona Research and Development Institute.
University of Castilla-La Mancha, Paseo de la Universidad 4, Ciudad Real, Spain

Abstract. For enterprises to be able to use information and communication technologies with guarantees, it is necessary to have an adequate security management available. This requires that enterprises always know their current maturity level and to what extend their security must evolve. Current maturity models are showing us that they are inefficient in small and medium size enterprises since these enterprises have a series of additional problems when implementing security management systems. In this paper, we will make an analysis of the maturity models oriented to security existing in the market by analysing their main disadvantages regarding small and medium size enterprises using as a reference framework ISO17799. This approach is being directly applied to real cases, thus obtaining a constant improvement in its application.

1 Introduction

Information and processes supporting systems and nets are the most important assets for any organization [1], and they are the main differentiation factor in a company's evolution. These assets are submitted to a great variety of risks that can critically affect enterprises. There are many sources that provide us with figures that show the importance of the problems caused by the lack of adequate security measures [2]. In this way, the CGI/FBI Computer Crime and Security Survey [3] estimates that the total losses in the US in 2004 as a result of security breaches was 141.496.560$. However, the majority of the losses are unknown since the lack of adequate controls to carry out the information tracking avoids that enterprises know the existence of information leaks and therefore they cannot quantify their cost. Organizations, independently of their size or activity, need to implement an Information Security Management System (ISMS) to protect their most sensitive assets [4][5]. However, to develop these ISMS not only we have to face technological aspects [6] but also we have to develop management as well as legal and ethical aspects.

Enrique Sánchez L., Villafranca D., Fernández-Medina E. and Piattini M. (2006).
Developing a Maturity Model for Information System Security Management within Small and Medium Size Enterprises.
In *Proceedings of the 4th International Workshop on Security in Information Systems*, pages 256-266

Anyway, although many new rules are appearing, the current tendency [7] to face an ISMS consists of homogenizing some of its basic aspects such as maturity models and best practices guides into a stable set that let us face each particular case with the ISMS model that better adapts to it.

As a core of the new security orientation as a management system, security policies containing sets of rules and regulations to determine how an organization must protect itself have been created [8]. Thus, Cabrera Martin [9] puts forward that the way to planify security within an organization must always start from the definition of a Security Policy that determines the organization's objectives in the security field and from this determination, we could decide through an adequate implementation plan how the fixed objectives will be reached.

Before starting a project for implementing an information security management system within an enterprise, it is necessary to determine the level of the Information Security Governance of the company since the absence of it guarantees the failure of the security management. It is not viable to start implementing a security management system with the absence of a stable and defined information security governance. [10]. The following step for the implementation of an ISMS is to establish the security maturity level of the enterprise and to where it should evolve although these maturity levels can be established in different ways. Thus, Von Solms [11] defines security as a discipline of multiple dimensions that must be covered to obtain a security plan, through an incremental certification of security, and for Von Solms, the most important phase of the plan is to determine the maturity level of the company ISMS and compare that level to the losses that it can cause to the business. The maturity model that we propose states an evolution of the maturity levels similar in some aspects to that stated by Von Solms, in a way that enterprises will be able to certify themselves in the different levels of the maturity model. This will let them face projects with a shorter temporary vision as well as analyse the results of the plan earlier.

Nowadays, it is very complex for a small or medium size enterprise to face the implementation of a security management system. Concerning security, the enterprises' tendency is to slowly migrate their culture to the creation of an ISMS, although this progression is very slow in such a way that René Sant-Germain [3] estimates that with the current models, in 2009, only a 35% of the enterprises with more than 2000 employees in the world will have an ISMS implemented and figures regarding small and medium size enterprises will be much worse.

The majority of enterprises have found many problems at the time of implementing systems such as BS7799 certification and UNE71502 since they are total certifications and this avoids that enterprises have intermediate points to focus the reach of their objectives. It also avoids that system departments obtain intermediate success that allow them to obtain the support of the Direction Board. The maturity model that we state allows us to obtain intermediate certification, being able to face each maturity level in 1 or 2 years periods instead of the 3 to 6 years that are currently needed in a medium size enterprise. Audit, certification and accreditation of the management system is important to provide the security environment, customers and providers with credibility. For this reason, our proposed maturity model is based on the certification by levels instead of an only total certification. Our maturity level proposes to divide UNE71502 certification and ISO27001 into three certification levels [1 to 3], each one having a subset of controls extracted from ISO17799.

This paper proposes a maturity model oriented to small and medium size enterprises with the purpose of solving the problems detected in the classic maturity models which are shown not to be efficient at the time of implementing them into small and medium size enterprises due to their complexity and other series of factors that will be analysed in a detailed way in the following sections of this paper. The paper continues with Section 2, in which the existing maturity models, their current tendency and the new proposals that are emerging will be described. In Section 3, our proposal of a maturity model oriented to small and medium size enterprises is introduced. Finally, in Section 4, we will conclude by indicating our future work.

2 Related Work

Security Maturity Models have the aim of establishing a standardized valoration with which it can be determined the state of information security within an organization and that allows us to be able to planify the way to reach the desired security goals. These maturity levels will be progressive in such a way that the implemented information increases as the maturity levels increase. These levels are the ideal mechanisms to know the security of the enterprises to be analysed and that of third companies with which these enterprises have to interact. The problem is that although there are maturity models in the market, they are only total security certifications and this fact avoids that many companies can have a valoration of their current maturity level. Therefore, our model suggests the certification by maturity levels instead of the unique certification existing today, this certification will be periodically revised and the company could increase or decrease its maturity level. This model is similar to the appreciations by Eloff and Eloff [5] that suggest a progressive controls implementation that allows the enterprise to adapt itself to the security evolution in a non-traumatic way.

The vision of how to face these maturity levels differs regarding the authors taken as a reference. In this way, some authors insist on using ISO17799 in security management models but always in an incremental way, taking into consideration the particular security needs [11], by using maturity models. Other models such as that proposed by the Information Security Institute of South Africa (ISIZA) [11] put forward a progressive increase of security. ISIZA Level 1 consists of selecting a basic level of a small subset of ISO17799 controls related to security policy, virus control and personnel security. Following the model proposed by ISIZA, time reductions when certifying companies according to the BS7799 regulation [11] have been achieved.

For our maturity model, we have used the standard ISO17799 as a starting point, coinciding with the research being carried out by Pittsburgh University for the development and putting into practice of a comprehensive standard of security based on the guides provided by ISO17799 [12]. Other studies consider the regulation important but they complement it in some way with other aspects [13], such as Endorf [14], that incorporates the American HIPAA requirements into a security program complementing ISO17799; or Von Solms [15], that considers a whole and complementary application of COBITs and the regulation; or even Masacci that apart

from the regulation, considers controls related to the fulfilment of the Italian legislation in the field of data protection and privacy.

Other aspects that are being studied for their application to the maturity models is the management of costs associated to security management since they can influence model dimensioning. Thus, Rebecca Mercuri [16] proposes to associate the cost-benefit analysis(CBA) as a fundamental part of ISMS development in the risk analysis phase; Kim&Choi [17] analyses a methodology oriented to processes models and criteria of analysis of cost and benefit factors that support the economic justification of the investment in security and that can be applied to estimate the maximum level of maturity that the enterprise can face; and Peltier [13] states that controls must be selected regarding the cost-efficiency in relation to the risk that they reduce and the potential losses that security breaches can cause.

2.1 Other Security Maturity Models

Among the information security maturity models [18] that are currently being most often applied within enterprises, we can highlight SSE-CMM, COBIT and ISM3 [19], although at present, new models that try to solve the problems detected in these models are being developed. Now, we will show a brief description of the main maturity models existing today and some of the most promising proposals:

- **ISO 21827/SSE-CMM:** The Capability Maturity Model in Systems Security Engineering is a model derived from the maturity model of CMM software and it is oriented to security. This model describes the essential characteristics of processes that must exist within an organization to assure a proper systems security. In Lobree 2002 [20], a comparison of the most important good practices guides with the maturity model SSE-CMM is made and they come to the conclusion that all of them basically consider the same security aspects but with different depth level.
- **ISM3 [12]:** It is oriented to define different security levels where each of them can be the final objective of an organization. In other words, it is not a model that can be used to improve but it is useful to classify the security level required by an enterprise. ISM3 defines five security maturity levels of an enterprise [0 a 4]. These levels will be associated to processes in a way that, depending on the maturity level, the enterprise will be forced to comply with a series of processes. Thus, a level 0 will imply the fact of not fulfilling any process.
- **COBIT:** The maturity model COBIT [18] offers us the basis for the understanding and evaluation of the current conditions of security and processes control of the IT environment within an organization. This model provides us with the bases for the understanding and evaluation of the main functions of IT area, through the consideration of each one of its key processes that will be assigned a value between [0-5], thus indicating the effort level ("maturity") that is suggested to invest in the activity of control of such process to guarantee a good relation cost-benefit by assuring the strictly required security level. The maturity model COBIT is based on the software development maturity model CMM-SW, and for this reason, it is not an updated model since today CMMI is the most commonly used model.

Von Solms [13] [15] has studied the coexistence and complementary use of COBIT and ISO 17799 by developing a mapping for the synchronization of both frameworks and by analysing the reasons why they are complementary. Some of ISO17799 detractors state as a disadvantage that it is a support guide but it does not reach the necessary framework for information technology governance. Its main advantage with respect to COBIT is that it is more detailed and has more guides oriented to how to do things. A recent report made by the IT Governance Institute solves the problem of synchronization by developing the mapping between COBIT´s DCO´s and ISO17799. There are plenty of scenarios [11] where we can see how ISO17799 and COBIT are complementary.

- **CC_SSE-CCM:** Common Criteria (CC) only provides us with standards to evaluate product and security systems information. On the other hand, SSE-CMM provides us with security standards for the evaluation of process engineering. Jongsook Lee [7] proposes to integrate CC and SSE-CMM to create CC-SSE-CMM that is a maturity model including the advantages of both models. This new model is divided into processes, products and environment. The advantage of this model is that it is useful when an organization that was developed with CC wants to be evaluated with SSE-CMM to improve its level with respect to the security process. CC_SSE-CMM consists of 23 process areas with 5 maturity levels. Each process area (PA) has BP (base practices) and the capacity levels have GP (generic practices).
- **Eloff and Eloff [5]:** They prefer to define four different protection classes that allow us to progressively increase the security levels, basing on the sections of ISO17799 to do so.
- **Karen & Barrientes [21]:** This proposal of maturity model consists of carrying out an analysis related to computer security to identify the vulnerability degree as well as determine the improvement aspects to be performed in the organization with the purpose of reducing risk. This model supports the evaluation of the information security and lets us determine which level the organization is at regarding security and thus, we will be able to establish its strengths and weaknesses at the time of protecting information. The proposed model has the five levels stated by CMMI adapted to agree with information security. Each level has a definition and a general description in which it is indicated the organization behaviour with respect to information security. Such behaviour determines the maturity level of information security. Practices of each level correspond to the controls defined in the international standards ISO17799 [22]. This model takes into account that organizations have different internal structures, and so, it is considered that controls defined in each level are the minimum or the most general that should be established by organizations, independently of their internal structure.

The main problem of all presented maturity models is that they are not being successful at the time of being implemented into small and medium size enterprises mainly due to the fact that they were developed thinking of big organizations and the organizative structures associated to them.

3 SSE-PYME: Security Maturity Model Oriented to Small and Medium size Enterprises

The Information Security Maturity Model that we propose allows any organization to evaluate the state of its security but it is mainly oriented to small and medium size enterprise since they are experiencing the greater failure rate and also they are the enterprises where the existing maturity models are being less successful. Furthermore, small and medium size companies represent more than 95% of Spanish companies and for this reason, we could not consider the Spanish set of enterprises mature from a technological viewpoint until we could not achieve an adequate security level in small and medium size enterprises. The most outstanding characteristics of our model are that it has three security levels [1 to 3] instead of the 5-6 levels proposed by classic models and that it proposes that each level can be certified instead of the total certification existing today. Finally, in our model, the maturity level is associated to the characteristics of the enterprise and it is not compulsory (and sometimes not even advisable) that all companies reach level 3.

In this way and from the information obtained through the SICAMAN implementation into customers, we have developed a maturity model following the spiral structure showed in Fig. 1. This model has the aim of facilitating the performance of fast and economic cycles that let us create a security culture within the organization, in a constant and progressive way. Our model proposes to carry out, in the first place, an estimation of the enterprise maturity level in a way that, with a low cost and in a short period of time, a project planning could be determined to present it to the direction board. Other characteristic of our model is that it has the purpose of carrying out the proposed plans in a short term instead of the plans derived from the current models that have a long duration and this fact makes them totally inadequate for the current changing structure of small and medium size enterprises. Through this model, we could estimate, in a minimum period of time, the maturity level of the enterprise ISMS as well as identify the set of rules that better adapt themselves to it. Thus, we could propose short-term realistic goals of the expected evolution of the company for each spiral cycle. Once we have identified the current maturity level of the enterprise, an improvement plan will be created and will be presented to the direction board. Its main objective will be that of complementing the current maturity level to reach the following maturity level.

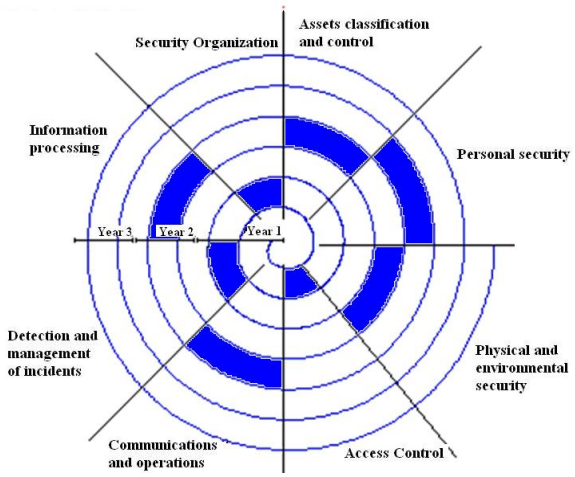

Fig. 1. Spiral model for ISMS maturity.

Although in Fig. 1, the maturity model only presents eight sections of ISO17799, our final maturity model is being developed over the ten sections of this regulation. Nowadays, we are analysing the possibilities of migrating the obtained results through the action research method to the new version of ISO17799:2005. In addition, although the main core of the model that we have developed is based on ISO17799, we have not refused to complement it with other kind of standards and recommendations in the field of security and security management that can solve the lack detected in ISO17799 and that have been analysed in the section 2 of this paper.

Our model defines three maturity levels to value the state of the information system security of the enterprise. In this way, an enterprise that, according to the employees and turnover parameters is considered small, it should only apply the maturity level ISO17799-1 that is a subset of the controls recommended by ISO17799 (Table 1). Any of the other two versions of the regulation would suppose over-dimensioning the enterprise security. This would give place to an increase in the risk of the fact that the implemented controls are not maintainable and it would produce a continuous degradation of the controls and the maturity level. Other factors to be taken into account is that even though the different sections could advance in an independent way, the most logical thing to do is to planify to improve those aspects that need lower security.

As a first step to put into practice our model within a company, we will determine what level of regulations we should applied regarding the characteristics of the company. Once we have identified the appropriate level, we will carry out an analysis of controls to determine the plan that allows us to complement this maturity level. In our model, the security level of the company will evolve in an interval from 0 to 100 %, for each one of the three proposed maturity levels that in turn, will be divided into six sublevels to help the direction board in the monitoring of the project.

Table 1. Proposed models according to the type of enterprise and maturity level.

Maturity Level (According pre-audit performed about ISO17799)		**Enterprise type (according to number of employees and turnover)**		
Security Evaluation	**Maturity Level**	**Small**	**Medium**	**Big**
		0 – 25 Employees	25 – 250 Employees	>250 Employees
		0 – 1 Million €	1 – 100 Million €	>100 Million €
0 – 100%	Low	ISO17799-1 (100)	ISO17799-1 (100)	ISO17799-1 (100)
100% - 200%	Medium	ISO17799-1 (100)	ISO17799-2 (300)	ISO17799-2 (300)
200 - 300%	High	ISO17799-1 (100)	ISO17799-2 (300)	ISO17799-3 (500)

Some of the main and most valuable conclusions obtained from the feedback of SICAMAN customers in which these models have been analysed are listed below:

- The overdimensioning of the security level of an enterprise with respect to its size finishes generating a degradation of the overdimensioned controls until they reach their natural balance. The final consequence is that the enterprise invests more resources than the strictly necessary that will not provide any value. In Fig. 2, we can see a simulation of how, according to the size of the company, security systems have a natural tendency to find their balance.

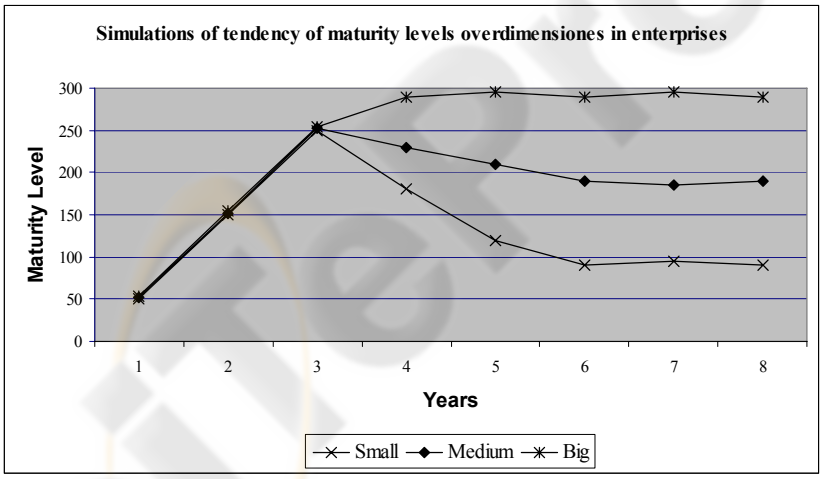

Fig. 2. Simulation of tendency of overdimensioned maturity levels.

In Fig. 2, the percentage from 0 to100 % represents maturity level 1, the percentage from 100 to 200% represents maturity level 2 and the percentage from 200 to 300% represents maturity level 3. There are some exceptions in some sectors and types of enterprises where this tendency is not fulfilled and therefore, the model is being improved by adding it variables.

- Enterprises are more receptive to short-term implementation plans (1 to 2 years) than to long-term plans (4 to 6 years). The certification by levels offers us a guarantee for the valoration of the short-term project evolution.

We are currently working on other models that include new factors that can affect when deciding about the fulfilment level that must be applied: the enterprise's type of activity, the dependency on departments (such as Research and Development), etc.

4 Conclusions and Future Work

In spite of the enormous efforts that are being made to create maturity models appropriate for mediating and managing security in small and medium size enterprises, these models do not fit properly with the environment where they must be implemented yet. The most probable reason is the lack of maturity of enterprises and the fact that we have tried to make too general and ambitious models. Sometimes, this makes that companies do not know the objective they must fulfil or how to start to perform their systems reestructuration or that the stated goals seem very far away and the direction board becomes discouraged. One of the documents generated by the standardization international group considered most important worldwide is the code of good practices ISO17799, that defines a very vast set of security controls and that it is being used in some of the most innovating maturity models in the market. Nevertheless, this code of good practices does not offer a global solution and must be complemented with other regulations and management mechanisms more appropriate, although it means a very good starting point for the development of new maturity models.

In this paper, we have presented from our practical experience, a first approximation to the development of a new maturity model oriented to small and medium size enter that takes as a basis the regulation that we have mentioned so many times in this paper and adapts it to adjust it to the size of the company in which we want to implement it as well as to its maturity level. This model is being developed taking as a basis the currently existing maturity models analysing their main disadvantages and testing them in our customers to determine the success and failure factors of the model.

The presented maturity model reduces the systems implementation costs and improves the success percentage of implementations.

As this proposal is very preliminary, our short and long term objective is that of studying in depth maturity models to carry out the complete development of a new maturity model that means a bigger percentage of success in small and medium size companies. Through the research method, "action research" and with the help of the feedback directly obtained from our customers, we hope to achieve a continuous improvement of these implementations.

This maturity model and the methodology which it belongs to will be complemented with a security systems management tool, mainly oriented to the direction board, to facilitate decision making when performing security systems planning.

Acknowledgements

This research is part of the following projects: DIMENSIONS, partially financed by FEDER and the Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha (PBC-05-012-1), CALIPO (TIC2003-07804-C05-03) and RETISTIC (TIC2002-12487-E) financed by "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (España).

References

1. Dhillon, G. y Backhouse, J. Information System Security Management in the New Millennium, Communications of the ACM, (2000) 43(7).
2. Computer Security Institute – CSI. Computer Crime and Security Survey. (2002)
3. René Sant-Germain. Information Security Management Best Practice Based on ISO17799. Setting Standars, The information Management Journal – July/August 2005.
4. María Eugenia Corti, Gustavo Betarte, and Reynaldo de la Fuente. Hacia una implementación Exitosa de un SGSI. 3er Congreso Iberoamericano de seguridad Informática, Nov, (2005).
5. Eloff, J. y Eloff, M. Information Security Management – A New Paradigm. Proc. of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT´03, (2003) 130-136.
6. Tsujii, S. Paradigm of Information Security as Interdisciplinary Comprehensive Science. Proc. of the 2004 International Conference on Cyberworlds (CW'04), IEEE Computer Society, (2004) 1-12.
7. Jongsook Lee, Jieun Lee, Seunghee Lee and Byoungju Choi. A CC-based Security Engineering Process Evaluation Model. Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC`03)
8. Rodriguez, Luis Ángel. Seguridad de la Información en Sistemas de Computo. Ventura Ediciones, México, (1995).
9. Cabrera Martin, Álvaro. Políticas de Seguridad. Boletín del Criptonomicón #71.Madrid, (2000).
10. Isg, Information Security Governance a call to action, Abril 2004.
11. Von Solms, B. y Von Solms, R. Incremental Information Security Certification. Computers & Security 20, (2001) 308-310.
12. Walton, J.P. Developing an Enterprise Information Security Policy. Proc. of the 30th annual ACM SIGUCCS conference on User services, (2002) 153-156.
13. Peltier, T.R. Preparing for ISO 17799. Security Management Practices, jan/feb, (2003) 21-28.
14. Endorf, C. Outsourcing Security: The Nedd, the Risks, the Providers, and the Process. Information Security Management, (2004) 17-23.
15. Von Solms, B. Information Security governance: COBIT or ISO 17799 or both? Computers & Security 24, (2005) 99-104.
16. Rebecca T. Mercuri. Analysing Security Costs. Communications of the ACM, June 2003/vol.46, nº 6.
17. S. Kim and I.Choi. Cost-Benefit Análisis of Security Investments: Methodology and Case Study. P. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3482, pp. 1239 – 1248, 2005.

18. Karen A. Areiza, Andrea M. Barrientos, Rafael Rincón, and Juan G. Lalinde-Pulido. Hacia un modelo de madurez para la seguridad de la información. 3er Congreso Iberoamericano de seguridad Informática, Nov, (2005).
19. Vicente Aceituno. Ism3 1.0: Information security management matury model, 2005. 12 Karen A. Areiza et al.
20. Bruce A. Lobree, CISSP. Impact of legislation and information security management. Security Management Practices, November/December 2002
21. Andrea M. Barrientos Karen A. Areiza. Integración de un sistema de gestión de seguridad de la información conun sistema de gestión de calidad. Master's thesis, Universidad EAFIT, 2005.
22. ISO/IEC. International standard ISO17799 (2000). information technology - code of practice for information security management, 2000.