PRACTICAL APPLICATION OF A SECURITY MANAGEMENT MATURITY MODEL FOR SMES BASED ON PREDEFINED SCHEMAS

Luís Enrique Sánchez, Daniel Villafranca
SICAMAN NT. Departament of R+D, Juan José Rodrigo, 4. Tomelloso, Ciudad Real, Spain

Eduardo Fernández-Medina, Mario Piattini
ALARCOS Research Group. TSI Department. University of Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain

Keywords: ISMS, SME, Maturity Level, ISO27001, Security System, Information Security Management System, Small-Medium Size Enterprise.

Abstract: For enterprises to be able to use information technologies and communications with guarantees, it is necessary to have an adequate security management system and tools which allow them to manage it. In small and medium-sized enterprises, the application of security standards has an additional problem, which is the fact that they do not have enough resources to carry out an appropriate management. This security management system must have highly reduced costs for its implementation and maintenance in small and medium-sized enterprises (from here on refered to as SMEs) to be feasible. In this paper we show the practical application of our proposal for a maturity model with which to manage the security in SMEs, centring upon the phase which determines the state of the enterprise and some of the mechanisms which allow the security level to be kept up to date without the need for continuous audits. This focus is continuously refined through its application to real cases, the results of which are shown in this paper.

1 INTRODUCTION

The availability of an information management system is fundamental to the enterprises stability, and is the principal differentiating factor in its evolution. Its assets are subjected to a great variety of risks, which may have a critical effect on the enterprises, but the main risk which an enterprises faces is that of being unable to manage those assets. Innumerable sources exist which show the magnitude of the problems caused by a lack of appropriate security measures (Wood, 2000; Hyder and Heston et al., 2004; Biever, 2005; Telang and Wattal, 2005; Goldfarb, 2006).

In this paper our proposal for a maturity and security management model oriented towards SMEs (Sánchez and Villafranca et al., 2007a) is applied to actual case studies, and its benefits are presented. The aim of this model is to solve problems detected in classic models which are proving to be inefficient when implanted in SMEs owing to their complexity or to another series of factors which have been analysed in previous papers (Sánchez and Villafranca et al., 2007b). Our earlier works have presented the current situation of security management systems for information systems, and various versions of our maturity model which have evolved as a result of this, such as the tool developed to provide automatic support and the metrics which help to improve its efficiency and to reduce costs (Sánchez and Villafranca et al., 2007c). In this paper the phase related to the model in charge of establishing the enterprises current situation has been studied in greater depth, and we have analysed the results obtained from 11 real case studies after applying this phase of our model to them. We also show the differences that appear in this model after updating the schema, which formerly took ISO17799:2000 (ISO/IEC17799, 2000) as its base and which now takes la ISO27002 (previously ISO27002) (ISO/IEC17799, 2005; ISO/IEC27002, 2007). Finally, we show the functioning of one of the system's principal procedures which allows the level of the security system initially obtained to

Enrique Sánchez L., Villafranca D., Fernández-Medina E. and Piattini M. (2008).
PRACTICAL APPLICATION OF A SECURITY MANAGEMENT MATURITY MODEL FOR SMES BASED ON PREDEFINED SCHEMAS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 391-398
DOI: 10.5220/0001923803910398

evolve, instantaneously altering the data from the scoreboard, and thus permitting the enterprises management to be aware of the situation and to make decisions in a reasonable amount of time.

The remainder of this paper is organized as follows: Section 2 very briefly describes existing maturity models, their current tendencies and some of the new proposals that are appearing. Section 3, introduces our proposal for a maturity model orientated towards SMEs. Section 4 we show some of the results obtained after applying our model to real practical cases, centring on the results obtained to date in the phase which permits the establishment of the enterprises current situation with regard to the security management level. Finally, in Section 5, we shall conclude by discussing our future work on this subject.

2 RELATED WORK

Security maturity models (Eloff and Eloff, 2003; Lee and Lee et al., 2003; Aceituno, 2005) seek to establish a standardized validation with which the state of the information security within an organisation can be determined, and which will allow us to plan the route which must be followed if we are to attain the desired security goals.

Among the information security maturity models which are most frequently applied in enterprises at present, those which are most outstanding are the SSE-CMM (Systems Security Engineering Capability Maturity Model), COBIT and ISM3 (Walton, 2002), and although research has been carried out to develop new models (Eloff and Eloff, 2003; Lee and Lee et al., 2003), none has been able to solve the current problems which occur when these models are applied in SMEs.

Other proposals take Risk Analysis as being the central nucleus of ISMS (Information Security Management System). As opposed to these models, in our case, although Risk Analysis is highly important, it is still only another piece in the system. Siegel (Siegel and Sagalow et al., 2002) point out that the information security models which centre exclusively upon risk elimination models are not sufficient, and Garigue (Garigue and Stefaniu, 2003) furthermore note that at present managers not only wish to know what has been done to mitigate these risks, but that they should also be able to discover, in an efficient manner, that this task has been carried out and that costs have been reduced.

The main problem with the majority of the maturity models mentioned is that they are not successful when implanted in SMEs, mainly due to the fact that they were developed for large organisations and their associated organisational structure. Their structures are, therefore, rigid, complex and costly to implement, which makes them unsuitable for an SME environment.

The vision of how to tackle these maturity levels varies according to the authors who confront the problem. Some authors therefore insist upon using the ISO/IEC17799 international standard in security management models, but always do so in an incremental manner, considering the particular security needs (Von Solms and Von Solms, 2001; Walton, 2002; Eloff and Eloff, 2003; Barrientos and Areiza, 2005).

The proposal that we have developed is also based on the ISO27002 International Standard, but its application is SME oriented, thus avoiding the problems detected in current models, which require more resources then the enterprise is able to provide, which in its turn leads to a higher risk of failure in implantation and maintenance, which is unacceptable for this type of companies.

3 MODEL

Earlier versions of the model have been presented in previous papers (Sánchez and Villafranca et al., 2007a). Therefore, in this section we present a highly resumed description of the models principal phases.

The Information Security Maturity Model that we propose allows any organisation to evaluate the state of its security, but is mainly oriented towards SMEs through the development of security management models which are simple, economical, rapid, automated, progressive and sustainable, these being the main requirements of this type of companies when implanting these models.

One of the objectives in the development of the entire process is that of obtaining the greatest possible level of automation with the minimum amount of information collected in the shortest possible time. In our system we have prioritized speed and cost reduction, thus sacrificing the precision offered by other models, which is to say that our model seeks one of the best security configurations, but not that which is optimum, and time and cost reduction are always prioritized.

Another of the major contributions of our model is a set of matrices which allows us to relate the different components of the ISMS that the system uses to automatically generate a great part of the necessary information, thus notably reducing the time needed to develop and implant the ISMS.

However, the limited nature of this paper prevents us from showing an analysis of the results of these matrices here.

The security management model is made up of three phases, and the results of each of the previous phases are necessary for the following phase:

- *Phase I: Establishment of Maturity Level:* The main objective of this phase is to discover both the company's current security level, and that which is desirable, through two sub-phases which can be carried out in parallel. In the first sub-phase we determine what the company's desirable level of security is, whilst in the second sub-phase we determine what the company's present level of security management is. For the first sub-phase our starting point was information from the (The National Institute of Statistics) which is relative to the current state of Spanish SMEs with regard to technological enterprises indicators, while for the second our base was the ISO27002 standard.
- *Phase II: Risk Analysis:* One of the most importatnt aspects of the Risk Analysis that we have developed are the Association Matrices which allow us to minimize the risk analysis cost and produce the maximum results and information for the company with the least amount of effort. A series of matrices have been developed which permit the association of the various components of the risk analysis (active-threat-vulnerability), which are in their turn associated with the results produced in Phase I (controls).
- *Phase III: Generation of ISMS:* Our objective in this phase was to ensure that the ISMS was manageable, focused on the domains of the Standard which were of greatest interest to the organisation and that it contained a number of reduced metrics in order to obtain rapid results and feedback the process in each cycle, until we obtained the maturity level initially designated. One of the most important aspects in this generation phase of the ISMS are the Association Matrices which permit the association of all the objects in these library. These matrices use the system internally to recommend an initial ISMS plan for the SME according to the information obtained in the earlier phases. The final result of this phase is a set of rules and procedures which should be fulfilled to obtain a greater level of security in the company, and which will be colour-coded to provide the user with a rapid visual indication of where the greatest effort must be applied.

The company's real work begins once the ISMS have been generated. Until this moment, thanks to the use of schemas, the consultant has been able to define the management system which is most appropriate for the company and whose costs are reasonable. Now the company must begin to work with the system.

Work with the security management system proposed has been developed for simplicity, so the users must know a maximum of 50 procedures and some 250 norms. Not all users should have access to knowledge about these 50 procedures, as the majority can only be used by the person responsible for security, or members of the systems department. In general, the users should only be made aware of the existence of a small set.

4 A PRACTICAL APPLICATION OF OUR MODEL TO SME´S

In this section we show some of the results obtained after applying our model in real cases. These results are centred on the application of the first phase of the model presented in the previous section.

The model that we have developed is being validated through its application in 11 real cases (companies in the Sicaman group and their customers) whose principal data is shown in Table 1.

Table 1: Data of the customers who have taken part in the test cases.

Name	Sector
SNT	Informatics Actives
Customer2	Research and development
Customer3	Research and development
Customer4	Food and drink industry
Customer5	Manufacture of metal (not including machinery)
Customer6	Other business activities
IMP	Other business activities
ComerciaRed	Construction
Pronatec	Real Estate
Customer10	Informatics
Customer11	Manufacture of electronic materials

The following sub-section describes the main details and the application of the two sub-phases, of which the establishment phase of the maturity level is made up, in real cases.

4.1.1 Initial Security Audit

This sub-phase of Phase I consist of producing a detailed check-list which helps us to position the company's present state with regard to its security level.

The study was initially carried out on ISO17799:2000 (ISO/IEC17799, 2000), having later updated the schema and all its data to ISO27002 (ISO/IEC17799, 2005). This allowed us to compare the variations that the model underwent in both standards after evolving from the 2000 version to the 2005 standard.

Table 2: Current security level of test cases obtained from the ISO17799:2000 and ISO27002 checklist.

		ISO17799	
ISMS	**Nombre**	**2000**	**2005**
ISMS-01	ISMS Sicaman 2007	59	59
ISMS-02	ISMS Customer2 2006	28	37
ISMS-03	ISMS Customer3 2007	67	62
ISMS-04	ISMS Customer4 2007	18	23
ISMS-05	ISMS Customer5 2007	19	24
ISMS-06	ISMS Customer6 2007	50	51
ISMS-07	ISMS IMP 2007	33	38
ISMS-08	ISMS ComerciaRed 2007	40	41
ISMS-09	ISMS Pronatec 2007	34	38
ISMS-10	ISMS Customer10 2007	14	14
ISMS-11	ISMS Customer11 2007	22	23
	TOTAL:	**35**	**37**

Table 2 shows the difference in the results obtained from the check-list according to the schema applied. In the first case, a check-list of 735 sub-controls obtained from ISO17799:2000 was applied, and in the second case the ISO27002 was used as a base for 896 sub-controls. Amongst the results obtained, it is interesting to point out that in general the results obtained underwent slight variations (between 1-2%), although customers with greater imbalances (5-10%) also exist as a result of being directly affected by some of the changes.

In our current version of the model, the sub-control level is only used to obtain a value which is as close as possible to the current security level to be controlled. Once these values have been obtained, the metrics ignore this level and automatically update the security level, using the values obtained in this phase. The periodical audits carried out on the company's security management system recalculate the check-list again, using the lowest levels which are the sub-controls.

These audits work like a scoreboard readjustment system to update the levels of security, in a similar way to a clock which we wish to put to the correct time. The imbalance produced by each control between two audits serves to adjust the model and make it more efficient.

Table 3: Results obtained for the test cases using the ISO17799:2000 checklist.

Domain	**Cust2**	**SNT**	**Cust 3**	**Cust 4**	**Cust 5**	**Cust 6**	**IMP**	**CMR**	**PRO**	**Cust 10**	**Cust 11**
3	50	88	88	25	25	50	13	63	25	13	0
4	16	59	75	9	14	43	32	43	32	6	31
5	22	31	51	0	0	17	8	13	8	0	28
6	25	89	87	7	7	34	33	33	34	8	17
7	43	60	45	26	29	62	57	57	61	47	64
8	30	63	72	26	26	68	51	51	50	20	21
9	44	63	65	25	24	76	54	54	54	19	20
10	29	56	63	18	18	45	35	35	35	12	12
11	2	32	68	5	4	50	5	5	5	0	1
12	15	52	56	40	39	61	44	44	38	18	29
	28	**59**	**67**	**18**	**19**	**50**	**33**	**40**	**34**	**14**	**22**

Table 3 shows the results obtained for the domain of the ISO17799:2000 standard. Note that some companies have totally ignored aspects such as Business Continuity, considering it to be superfluous to their company.

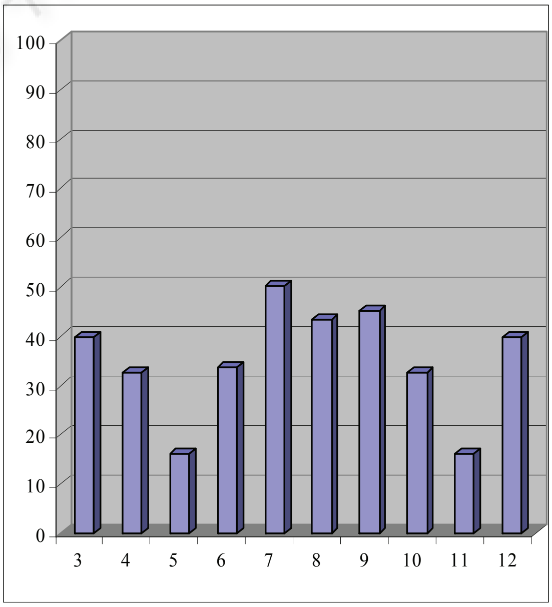

Figure 1: Average fulfilment level of ISO17799:2000 domains.

Figure 1 shows the average results per domain of the 11 cases analysed in the previous table. It is notable that none of the domains exceeds 50% of fulfilment and those two cases, “Classification of Activities” and “Business Continuity”, in which companies have a very low level of compliance.

Table 4: Results obtained for test cases from the ISO27002 check-list.

Domain	**Cust2**	**SNT**	**Cust 3**	**Cust 4**	**Cust 5**	**Cust 6**	**IMP**	**CMR**	**PRO**	**Cust 10**	**Cust 11**
5	30	55	55	25	25	30	14	39	14	0	0
6	49	64	55	23	28	41	40	48	40	3	23
7	52	57	68	28	28	48	43	46	43	18	45
8	48	77	64	11	11	38	42	40	43	5	15
9	47	61	48	30	33	66	59	58	61	48	68
10	46	46	49	28	29	56	42	44	42	18	20
11	51	68	71	28	29	86	65	65	68	25	26
12	41	66	74	21	21	49	42	42	39	11	11
13	29	64	68	14	14	36	21	21	22	2	15
14	2	32	68	5	4	50	5	5	5	0	1
15	16	54	58	41	41	63	46	47	39	20	32
	37	**59**	**62**	**23**	**24**	**51**	**38**	**41**	**38**	**14**	**23**

Table 4 shows the results obtained per domain from the ISO17799:2000 standard. As we can see, almost all the companies have considered “Business Continuation” to be a superfluous point in the business model, which demonstrates that in some companies the root of the problem is cultural and is not precise.

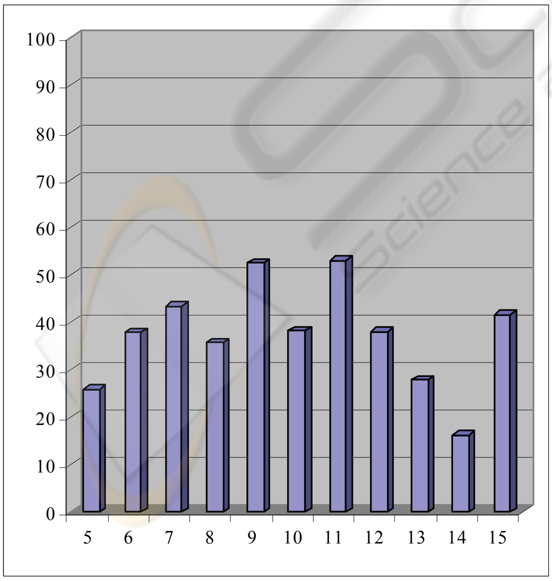

Figure 2: Average level of fulfilment of ISO27002 domains

Figure 2 shows that although “Business Continuation” continues to be one of the pending subjects, “Classification of Activities” undergoes an improvement upon being measured with the new standard, owing to the fact that some controls have moved to other domains and have taken into account certain factors which were not previously evaluated. In general, the results obtained ISO27002 have proved to be much more precise than those obtained with ISO17799:2000. Finally, some of the distortions produced among the results of the models are due to the fact that ISO27002 takes updated factors into account which ISO17799:2000 ignored.

To sum up, Figure 3 shows a comparison of the global security level for each test case ISO17799:2000 as opposed to ISO27002 was applied.

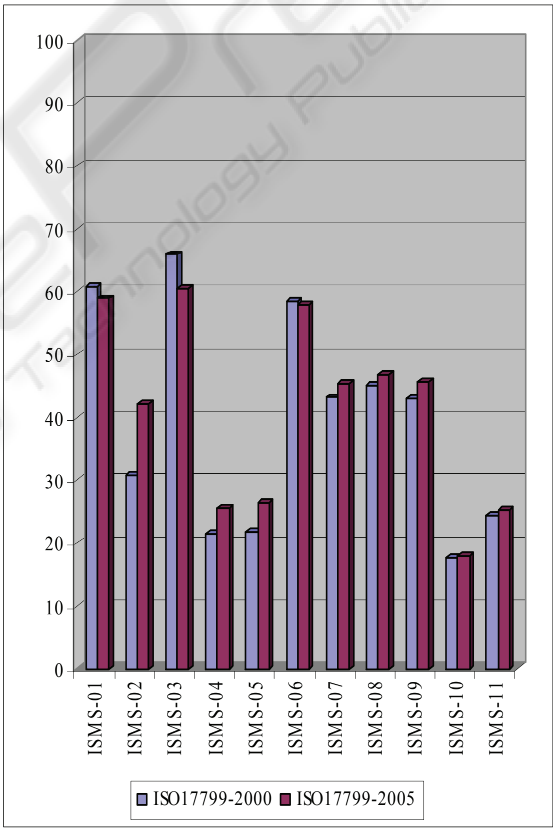

Figure 3: Comparison of fulfilment levels of 11 real cases between ISO27002 and ISO27002.

3.1.2 Establishing the Company’s Profile

The model that we propose uses a set of characteristics which are intrinsic to the company, in order to define the maximum maturity level to which the company should evolve in its current situation.

The solution posed for this sub-phase is simple, as at all times we have attempted to ensure that the model is agile, cheap and rapid. Nevertheless, despite its cheapness it has proved to be effective and has produced highly accurate results. In the current version we have only considered as parameters a reduced set of what we consider to be the companies' most outstanding characteristics: i) Number of employees, ii) Annual turnover, iii) Dependency on I+D Department, iv) Number of employees using the Information System, v) Number of people directly associated with the Systems Department, vi) Level of enterprise dependency on I.S. outsourcing.

In (1) we show the equation which allows us to calculate the company's DML (Desirable Maturity Level). This level may change according to the changes undergone by the company's profile.

$$\text{DML} = \Sigma(\text{WeightFactor}*(\text{RatingFactor}/\text{ValueMaximFactor}))/\text{NumberFactors} \qquad (1)$$

According to the expression in (1) and the practical experience obtained from the study of Sicaman Group customers, we have considered 3 security levels: i) Level 1 if the result is between 0–0.25; ii) Level 2 if it is between 0.25–0.75; iii) Level 3 if it is between 0.75–1.

The choice and refinement of the statistical data was carried out by taking the following factors into consideration: i) Economic Data; ii) Technological Data; iii) Statistical reports by sector; iv) Statistical reports by number of employee.

Table 6 shows the results obtained from the case study used to establish the company's current security maturity level (CML) which, when applied to equation (1), allow us to obtain the company's Desirable Maturity Level (DML). The current maturity level columns for the ISO17799:2000 and ISO27002 version are obtained in the first part of Phase I (Initial Security Audit). Finally, the table shows the imbalance that is produced between the current and the desirable maturity levels.

If the result of applying equation (1) is that it returns a value which coincides with the limit of both levels, we always tend towards normalizing said value to the upper maturity level.

Table 6 shows how the values which were close to the limit of two levels have passed to the upper level upon changing the version of the schema ISO17799:2000 to ISO27002.

Even when this formula gives us an indication of the current level, this does not mean to say that the security is correct. For example, in the case of SNT the current security level coincides with that which is desirable, but it may be that the load distribution of the domains is not appropriate and that we therefore require a plan which will be generated in other phases. An advance in the prototype is obviously necessary to solve this problem, and the results obtained must be refined.

Table 5: Current and desired maturity levels of test cases.

		Maturity Level				
ISMS	**DML**	**Current 2000**	**Current 2005**	**Desirable**	**Different 2000**	**Different 2005**
SNT	0.67	2	2	2	0	0
Cust2	0.78	2	2	3	1	1
Cust 3	0.78	2	2	3	1	1
Cust 4	0.47	**1**	**2**	2	1	0
Cust 5	0.47	**1**	**2**	2	1	0
Cust 6	0.75	2	2	3	1	1
IMP	0.28	2	2	2	0	0
CMR	0.50	2	2	2	0	0
PRO	0.25	2	2	3	1	1
Cust 10	0.56	1	1	2	1	1
Cust 11	0.50	**1**	**2**	2	1	0

4 CONCLUSIONS AND FUTURE WORK

In this paper we have presented our model and the tool supporting the maturity and security management model for SMEs which was developed during our research. This tool allows companies to adapt to change with a minimum of cost, guaranteeing the security and stability of their information system. We have clearly defined how the application uses the model developed to achieve goals, and the improvements which are offered with regard to classic systems.

We have also presented some of the results obtained during the research process which, owing to space limitations, are centred on those obtained in the first phase and the evolution undergone by the prototype schema when a change was made from using the ISO17799:2000 standard as a base as opposed to using ISO27002.

The developed application reduces the system's implantation costs and improves the percentage of success of implantations in SMEs. As the majority of our customers are SMEs, our proposal has been well received and its application is proving to be very positive since it gives this type of businesses access to security maturity models, a privilege which has until now been reserved for large companies.

Moreover, this model allows us to obtain short-term results and to reduce the costs which the use of other models supposes, thus attaining a higher level of satisfaction from the businesses in question.

Given that this proposal is under constant development, our medium and long term objective is to study the maturity models in greater depth in order to refine our model, thus improving the tool's level of automation.

The most outstanding improvements to the model upon which were working are:

- The inclusion of a new array which will allow us to obtain the desirable maturity level at the control level in order to be able to compare these levels with the current security levels of each control.
- The improvement of the system's algorithms in order to maximize its efficiency in decision-making.
- The inclusion of a resource planner in which the company is willing to invest over a period of time so that the system is able to apply these resources to its improvement plan.
- The inclusion in Phase III of an archive with sub-projects which should be met in order to globally improve the security management system.
- The inclusion of new objects in Phase III which will allow us to continue adjusting the model to the new version of the scheme based on
- The obtaining of new statistical reports concerning the imbalances produced between two audits using the model, to synchronize the instrument panel's recalibration mechanism.

Through the "research in action" research method, and with the help of the feedback obtained directly from our customers, we have achieved a continuous improvement in these implantations.

ACKNOWLEDGEMENTS

This research is part of the following projects: MISTICO (PBC-06-0082), and QUASIMODO (PAC08-0157-0668) both supported by the FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", and Proyect SCMM-PYME (FIT-360000-2006-73) supported by the PROFIT granted by the "Ministerio de Industria, Turismo y Comercio).

REFERENCES

Aceituno, V. (2005). "Ism3 1.0: Information security management matury model."

Barrientos, A. M. and K. A. Areiza (2005). Integración de un sistema de gestión de seguridad de la información conun sistema de gestión de calidad. Master's thesis, Universidad EAFIT.

Biever, C. (2005). Revealed: the true cost of computer crime. Computer Crime Research Center.

Eloff, J. and M. Eloff (2003). "Information Security Management - A New Paradigm." Annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT´03: 130-136.

Garigue, R. and M. Stefaniu (2003). "Information Security Governance Reporting." Information Systems Security sept/oct: 36-40.

Goldfarb, A. (2006). "The medium-term effects of unavailability " Journal Quantitative Marketing and Economics 4(2): 143-171

Hyder, E. B., K. M. Heston, et al. (2004). The eSCM-SP v2: The eSourcing Capability Model For Service Providers (eSCM-SP) v2. Pittsburh, Pennsylvania, USA. 19 May.

ISO/IEC17799 (2000). ISO/IEC 17799. Information Technology - Security techniques - Code of practice for information security management.

ISO/IEC17799 (2005). ISO/IEC 17799. Information Technology - Security techniques - Code of practice for information security management.

ISO/IEC27002 (2007). "ISO/IEC 27002:2005, the international standard Code of Practice for Information Security Management (en desarrollo)."

Lee, J., J. Lee, et al. (2003). A CC-based Security Engineering Process Evaluation Model. Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC).

Sánchez, L. E., D. Villafranca, et al. (2007a). Developing a model and a tool to manage the information security in Small and Medium Enterprises. International Conference on Security and Cryptography (SECRYPT'07). Barcelona. Spain., Junio.

Sánchez, L. E., D. Villafranca, et al. (2007b). MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. 9th International Conference on Enterprise Information Systems (WOSIS'07). Funchal, Madeira (Portugal). June.

Sánchez, L. E., D. Villafranca, et al. (2007c). SCMM-TOOL: Tool for computer automation of the Information Security Management Systems. 2nd International conference on Software and Data Technologies (ICSOFT'07). , Barcelona-España Septiembre.

Siegel, C. A., T. R. Sagalow, et al. (2002). "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security." Security Management Practices sept/oct: 33-49.

Telang, R. and S. Wattal (2005). Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis. 4h Workshop on Economics and Information Security, Boston.

Von Solms, B. and R. Von Solms (2001). "Incremental Information Security Certification." Computers & Security 20: 308-310.

Walton, J. P. (2002). Developing an Enterprise Information Security Policy. 30th annual ACM SIGUCCS conference on User services.

Wood, C. C. (2000). Researchers Must Disclose All Sponsors And Potential Conflicts. Computer Security Alert, San Francisco, CA, Computer Security Institute.