SECRYPT 2007

INTERNATIONAL CONFERENCE ON
SECURITY AND CRYPTOGRAPHY

Proceedings

BARCELONA, SPAIN · JULY 28-31, 2007

ORGANIZED BY

TECHNICALLY CO-SPONSORED BY

IEEE Systems, Man and
Cybernetics (SMC) Society

IN COOPERATION WITH

acm SIG

IN COLLABORATION WITH

UPC UNIVERSITAT POLITÈCNICA
DE CATALUNYA

NSTICC PRESS

SECRYPT 2007

Proceedings of the
Second International Conference on
Security and Cryptography

Barcelona, Spain

July 28 – 31, 2007

Organized by
INSTICC – Institute for Systems and Technologies of Information, Control and Communication

Technically Co-Sponsored
IEEE Systems, Man, and Cybernetics (SMC) Society

Co-Sponsored
WfMC - Workflow Management Coalition

In Cooperation with
ACM Special Interest Group on Management Information Systems

In Cooperation with
Universitat Politècnica de Catalunya

Edited by Javier Hernando, Eduardo Fernández-Medina and Manu Malek

Printed in Portugal

ISBN: 978-989-8111-12-8

Depósito Legal: 261607/07

http://www.secrypt.org

secretariat@secrypt.org

BRIEF CONTENTS

INVITED SPEAKERS

Kecheng Liu

University of Reading

U.K.

Ivan Ivanov

SUNY Empire State College

U.S.A.

Tony Shan

Bank of America

USA

Franco Davoli

University of Genoa

Italy

Santanu Dutta

*n*VIDIA Corporation

U.S.A.

Mohammad S. Obaidat

Monmouth University

U.S.A.

Günther Pernul

University of Regensburg

Germany

ORGANIZING AND STEERING COMMITTEES

CONFERENCE CO-CHAIRS

Joaquim Filipe, Polytechnic Institute of Setúbal / INSTICC, Portugal

Javier Hernando, Polytechnic University of Catalonia, Spain

Mohammad S. Obaidat, Monmouth University, U.S.A.

PROGRAM CO-CHAIRS

Manu Malek, Stevens Institute of Technology, USA

Eduardo Fernández-Medina, UCLM, Spain

Javier Hernando, Polytechnic University of Catalonia, Spain

PROCEEDINGS PRODUCTION

Vera Coelho, INSTICC, Portugal

Andreia Costa, INSTICC, Portugal

Bruno Encarnação, INSTICC, Portugal

Luís Marques, INSTICC, Portugal

Vitor Pedrosa, INSTICC, Portugal

Vera Rosário, INSTICC, Portugal

CD-ROM PRODUCTION

Paulo Brito, INSTICC, Portugal

WEBDESIGNER

Marina Carvalho, INSTICC, Portugal

GRAPHICS PRODUCTION

Helder Coelhas, INSTICC, Portugal

SECRETARIAT AND WEBMASTER

Mónica Saramago, INSTICC, Portugal

PROGRAM COMMITTEE

Kamel Adi, University of Québec in Outaouais, Canada

Gordon Agnew, University of Waterloo, Canada

Jörn Altmann, School of Information Technology, Germany

Joonsang Baek, Institute for Infocomm Research, Singapore

Dan Bailey, RSA Security, U.S.A.

Lejla Batina, Katholieke Universiteit Leuven, Belgium

Anthony Bedford, RMIT Univeristy, Australia

Carlo Blundo, Università di Salerno, Italy

Emmanuel Bresson, DCSSI Crypto Lab, France

Rahmat Budiarto, National Advanced IPV6 (NAv6) Center, Malaysia

Roy Campbell, University of Illinois at Urbana-Champaign, U.S.A.

Kim-Kwang Raymond Choo, Australian Institute of Criminology, Australia

Edward Chow, University of Colorado at Colorado Springs, U.S.A.

Christophe Clavier, Gemalto, France

Debbie Cook, Alcatel-Lucent Bell Labs, U.S.A.

Rui Costa Cardoso, University of Beira interior, Portugal

Mads Dam, KTH - Royal Institute of Technology , Sweden

Paolo D'Arco, University of Salerno, Italy

Sabrina De Capitani di Vimercati, University of Milan, Italy

Breno de Medeiros, Florida State University, U.S.A.

José Neuman de Souza, Federal University of Ceará, Brazil

Falko Dressler, University of Erlangen, Germany

Orr Dunkelman, Katholieke Universitiet Leuven, Belgium

Iwan Duursma, University of Illinois at Urbana-Champaign, U.S.A.

Robert Erbacher, Utah State University, U.S.A.

Eduardo B. Fernandez, Florida Atlantic University, U.S.A.

Mário Freire, University of Beira Interior, Portugal

Steven Furnell, University of Plymouth, U.K.

David Galindo, University of Malaga, Spain

Luciano Gaspary, Universidade Federal do Rio Grande do Sul, Brazil

Paolo Giorgini, University of Trento, Italy

Juan Gonzalez Nieto, Queensland University of Technology, Australia

Carlos Goulart, Federal University of Vicosa, Brazil

Lisandro Granville, Federal University of Rio Grande do Sul, Brazil

Stefanos Gritzalis, University of the Aegean, Greece

Vic Grout, University of Wales, NEWI, U.K.

Javier Herranz, IIIA-CSIC, Spain

Amir Herzberg, Bar Ilan University, Israel

Alejandro Hevia, Universidad de Chile, Chile

Min-Shiang Hwang, National Chung Hsing University, Taiwan, Province Of China

Cynthia Irvine, Naval Postgraduate School, U.S.A.

Hamid Jahankhani, University Of East London, U.K.

Christian Damsgaard Jensen, Technical University of Denmark, Denmark

Willem Jonker, Philips Research, The Netherlands

Dong Seong Kim, University of Maryland College Park, U.S.A.

Kwangjo Kim, ICU, Korea, Republic Of

Seungjoo Kim, Sungkyunkwan University, Korea, Republic Of

Paris Kitsos, Hellenic Open University (HOU) , Greece

Cetin Kaya Koc, Istanbul Commerce University, Turkey

Steve Kremer, ENS Cachan & CNRS & INRIA Futurs, France

Christopher Kruegel, Technical University Vienna, Austria

PROGRAM COMMITTEE (CONT.)

Ralf Kuesters, ETH Zurich, Switzerland

Tanja Lange, Eindhoven University of Technology, The Netherlands

Albert Levi, Sabanci University, Turkey

Yingjiu Li, Singapore Management University, Singapore

Chae Hoon Lim, Sejong University, Korea, Republic Of

Javier Lopez, University of Malaga, Spain

Olivier Markowitch, Université Libre de Bruxelles, Belgium

Alexander May, TU Darmstadt, Germany

Madjid Merabti, Liverpool John Moores University, U.K.

Ali Miri, University of Ottawa, Canada

Atsuko Miyaji, Japan Advaned Institute of Science and Technology, Japan

Edmundo Monteiro, University of Coimbra, Portugal

Haralambos Mouratidis, University of East London, U.K.

Yi Mu, University of Wollongong, Australia

Volker Müller, University of Luxembourg, Luxembourg

José Luis Oliveira, University of Aveiro, Portugal

Martin Olivier, University of Pretoria, South Africa

Rolf Oppliger, eSECURITY Technologies, Switzerland

Elisabeth Oswald, University of Bristol, U.K.

Carles Padro, Universitat Politecnica de Catalunya, Spain

Daniel Page, University of Bristol, U.K.

Victor Peral Lecha, France Telecom R&D UK Ltd, U.K.

Günther Pernul, University of Regensburg, Germany

Luiz Carlos Pessoa Albini, Federal University of Parana , Brazil

Raphael C.-W. Phan, EPFL, Switzerland

George Polyzos, AUEB, Greece

Joachim Posegga, University of Hamburg, Germany

Atul Prakash, University of Michigan, U.S.A.

Indrakshi Ray, Colorado State University, U.S.A.

Indrajit Ray, Colorado State University, U.S.A.

Srinivas Sampalli, Dalhousie University, Canada

David Samyde, Intel, U.S.A.

Aldri Santos, Federal University of Paraná, Brazil

Susana Sargento, Instituto de Telecomunicações - Universidade de Aveiro, Portugal

Damien Sauveron, XLIM, UMR CNRS 6172 -- University of Limoges, France

Erkay Savas, Sabanci University, Turkey

Berry Schoenmakers, Technical University of Eindhoven, The Netherlands

Bruno Schulze, LNCC, Brazil

Alice Silverberg, University of California, Irvine, U.S.A.

Nicolas Sklavos, Technological Educational Institute of Messolonghi, Greece

Mario Spremic, University of Zagreb, Graduate School of Economics and Business, Croatia

Mark Stamp, San Jose State University, U.S.A.

Aaron Striegel, University of Notre Dame, U.S.A.

Lily Sun, The University of Reading, U.K.

Willy Susilo, University of Wollongong, Australia

Michael Szydlo, RSA security division of EMC, U.S.A.

Tsuyoshi Takagi, Future University Hakodate, Japan

Ferucio Laurentiu Tiplea, "Al.I.Cuza" University of Iasi, Romania

Ambrosio Toval, Universidad de Murcia, Spain

Wade Trappe, Rutgers University, U.S.A.

Wen-Guey Tzeng, National Chiao Tung University, Taiwan, Province Of China

Ulrich Ultes-Nitsche, University of Fribourg, Switzerland

Dominique Unruh, Saarland University, Germany

PROGRAM COMMITTEE (CONT.)

Guillaume Urvoy-Keller, Institut Eurecom, France

Yongge Wang, University of North Carolina, U.S.A.

Susanne Wetzel, Stevens Institute of Technology, U.S.A.

Duminda Wijesekera, George Mason University, U.S.A.

S. Felix Wu, University of California, Davis, U.S.A.

Chaoping Xing, National University of singapore, Singapore

Shouhuai Xu, UTSA, U.S.A.

Mariemma I. Yagüe, University of Malaga, Spain

Alec Yasinsac, Florida State University, U.S.A.

Sung-Ming Yen, National Central University, Taiwan, Province Of China

Meng Yu, Monmouth University, U.S.A.

Moti Yung, RSA Labs. and Columbia University, U.S.A.

Fangguo Zhang, Sun Yat-sen University, China

André Zúquete, University of Aveiro, Portugal

AUXILIARY REVIEWERS

Alfonso Rodríguez, Universidad del Bio Bio, Chile

Aniello Castiglione, University of Salerno - D.I.A, Italy

Ayca A. Hintoglu, Sabanci University, Turkey

Ayse G. Karatop, Sabanci University, Turkey

Barbara Masucci, University of Salerno - D.I.A., Italy

Benoit Chevallier-Mames, Gemalto, France

Bo-Ching Wu, National Central University, Taiwan

Bogdan Warinschi, University of Bristol, U.K.

Carlos Gutiérrez, Correos Telecom , Spain

Chen-Kang Chu, National Chiao Tung University, Taiwan

Chien-Ning Chen, National Central University, Taiwan

Daniel J. Bernstein, University of Illinois at Chicago, U.S.A.

Eleftherios Stefanis, Athens University of Economics and Business, Greece

Fan Zhang, Singapore Management University, Singapore

Flavio Garcia, University of Nijmegen, The Netherlands

Francisco Javier Lucas Martínez, Universidad de Murcia, Spain

Frederic Valette, CELAR , France

Giannis F. Marias, Athens University of Economics and Business, Greece

Hsi-Chung Lin, National Central, Taiwan

Ivan Visconti, University of Salerno - D.I.A., Italy

Izuru Kitamura, Sony, Japan

Jean-Rene Reinhard, DCSSI , France

Jheng-Hong Tu, National Central University, Taiwan

Joaquin Lasheras Velasco, Universidad de Murcia, Spain

Johann Barbier, CELAR, France

Jordi Nin, IIIA-CSIC, Spain

Junji Shikata, Yokohama National University, Japan

Kazuto Ogawa, Japan Broadcasting Corporation, Japan

Liu Yang, Stevens Institute of Technology, U.S.A.

Martijn Stam, EFPL, Switzerland

Masakazu Soshi, Hiroshima City University, Japan

Miguel Ángel Martinez Aguilar, Universidad de Murcia, Spain

Nigel Smart, University of Bristol, U.K.

Norbert Meckl, University of Regensburg, Germany

Pantelis A. Frangoudis, Athens University of Economics and Business, Greece

SELECTED PAPERS BOOK

A number of selected papers presented at ICETE 2007 will be published by Springer, in a book entitled e-Business and Telecommunications IV. This selection will be done by the conference co-chairs and program co-chairs, among the papers actually presented at the joint conference, based on a rigorous review by the ICETE 2007 program committee members.

TECHNICALLY CO-SPONSORED BY

Workflow Management Coalition

WfMC

IEEE

Systems, Man, and Cybernetics Society

CONTENTS

INVITED SPEAKERS

KEYNOTE LECTURES

ACCESS CONTROL AND INTRUSION DETECTION

FULL PAPERS

SHORT PAPERS

POSTERS

NETWORK SECURITY AND PROTOCOLS

FULL PAPERS

SHORT PAPERS

POSTERS

CRYPTOGRAPHIC TECHNIQUES AND KEY MANAGEMENT

FULL PAPERS

SHORT PAPERS

POSTERS

INFORMATION ASSURANCE

SHORT PAPERS

POSTERS

SECURITY IN INFORMATION SYSTEMS

FULL PAPERS

SHORT PAPERS

POSTERS

DEVELOPING A MODEL AND A TOOL TO MANAGE THE INFORMATION SECURITY IN SMALL AND MEDIUM ENTERPRISES

Luís Enrique Sánchez, Daniel Villafranca
SICAMAN NT. Departamento de I+D, Juan José Rodrigo, 4. Tomelloso, Ciudad Real, Spain
{lesanchez, dvillafranca} @sicaman-nt.com

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

Keywords: ISMS, SME, Maturity Model, Risk Analysis.

Abstract: The maturity and security management systems are essential in order to guarantee the continuity and stability of the companies in the current market situation. However, this requires that enterprises know in every moment their security maturity level and to what extend their information security system must evolve. 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 will put forward our proposal of a maturity model for security management in SMEs and we will briefly analyse other models that exist in the market. 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 (Dhillon and Backhouse 2000) and they suppose the main differentiating factor in the evolution of an enterprise. These assets are exposed to a great variety of risks that may critically affect enterprises. There are many sources that provide us with figures showing the importance of the problems caused by a lack of adequate security measures (Wood 2000; CSI 2002; Hyder et al. 2004; Biever 2005; Telang and Wattal 2005; Goldfarb 2006).

At present, tackling the implementation of a security management system is extremely complex for a small or medium-sized enterprise (Pertier 2003; Kim and I.Choi 2005). The tendency in the field of enterprise security is that of gradually migrating their culture towards the creation of a security management system (ISMS), despite the fact that this progression is very slow. Thus, studies such as that of René Sant-Germain (Sant-Germain 2005) estimate that with the current models, by 2009 only 35% of the enterprises in the world which employ more than 2000 people will have implemented an ISMS, and that the figures for SMEs will be much worse.

At present, the market demands that enterprises are able to guarantee that technologies for computer assets and information are secure, fast and easy to interact with (Corti et al. 2005). However, in order to fulfill these requirements, the system administrators have discovered two problems with no satisfactory solution: a lack of tools to allow them to confront the management of information system security in a centralized, simple way and (according to the size of the enterprises) a lack of information security (Pertier 2003; Kim and I.Choi 2005).

The first problem is still unsolved, but we believe that by solving the second problem we shall be able to solve the first. With regard to the second problem, not only national organizations but also international ones have gone to great lengths to elaborate a set of rules and specifications related to the security of information and communication technologies. These rules are above all focused on the definition of security controls through codes of good practices, rules defining security management systems and rules with criteria to certify security. Nevertheless, the situation is complex, and for a small or medium-sized enterprise it is an extremely difficult task to implement a security management system which may have several levels of exigency, and with their limited resources. In addition, the process almost always gives rise to the situation of the enterprise being forced to take the risk of not having a security management system because it is not able to implement it.

In this paper, we shall describe a new proposal for a maturity model and security management orientated towards SMEs, aimed at solving the problems detected in classical models which are proving to be inefficient when implemented in SMEs due to both their complexity and another series of factors that will be analysed in detail in the following sections of the paper.

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. Finally, in Section 4, we shall conclude by discussing our future work on this subject.

2 RELATED WORK

Security Maturity Models (COBIT 2000; Eloff and Eloff 2003; Lee et al. 2003; Aceituno 2005; Areiza et al. 2005; Barrientos and Areiza 2005) are designed with the intention of establishing a standardized valuation which can not only be used to determine the state of security information in an organization but which also allows us to plan the means by which to attain the desired security goals. These maturity levels will be progressive, meaning that the information security implemented increases at the same time as maturity levels rise.

Almost all the defined maturity models, have common domains, and matrixes have been developed (Institute; Eloff and Eloff 2003; Jimmy Heschl 2006) which make it possible to interconnect and relate maturity models to each other, so that they can be compared and interconnected with each other.

Among the information security models (Areiza et al. 2005) that are most frequently applied to enterprises nowadays, we can highlight SSE-CMM (Systems Security Engineering Capability and Maturity Model), COBIT (COBIT 2000) and ISM3 (Walton 2002), Moreover, although research to develop new models has been carried out, none of it has been able to solve the current problems that occur at the time of applying those models to SMEs. Among these new proposals we can highlight CC_SSE-CCM developed by Jongsook Lee (Lee et al. 2003), which is based on the Common Criteria (CC), and the SSE-CMM model developed by Eloff and Eloff (Eloff and Eloff 2003), which defines four different classes of protection allowing a progressive increase in security levels.

Other proposals see risk analysis as being the central concept of ISMS. Among these, we can highlight the proposal by Karen & Barrientes (Barrientos and Areiza 2005) and UE CORAS (IST-2000-25031) (Lund et al. 2003).

The majority of the current models based on risks use the Magerit v2 risk analysis (MageritV2 2005) as a methodology. The problem with the Magerit is that as it is the most complete and efficient risk analysis that exists in the market, it is not useful for SMEs since it implies both an enormous complexity when collecting data and the direct involvement of users.

As opposed to those models which see risk analysis as being the nucleus of ISMS, in our case, and although we consider it to be very important, it is only seen as one more piece in the system. Siegel (Siegel et al. 2002) points out that computer security models that are exclusively centred upon risk elimination models are not enough. On the other hand, Garigue (Garigue and Stefaniu 2003) highlights that nowadays managers wish to know not only what has been done to mitigate risks but also that this task has been effectively carried out and whether its performance has allowed the company to save money.

We must take into account that risk analysis is an expensive process which cannot be repeated any time a modification is performed. Hence, it is important to develop specific methodologies which allow the maintenance of risk analysis results. UE Coras' (Lund et al. 2003) project makes this risk analysis maintenance the main point of its model.

The way in which to confront these maturity levels differs according to the authors taken as a reference. Thus, some authors insist on using

ISO/IEC 17799 international regulation in security management models but always in an incremental manner which takes the particular security needs into consideration (Von Solms and Von Solms 2001; Walton 2002; Eloff and Eloff 2003; Barrientos and Areiza 2005).

The proposal presented in this paper is also based on the ISO/IEC 17799 international regulation but has been orientated towards its application in SMEs and an avoidance of the problems detected in current models.

3 SMM-SME: SPYRAL MATURITY MODEL FOR ISMS

The Information Security Maturity Model that we propose allows any organization to evaluate the state of its security but is mainly orientated towards SMEs since it develops simple, cheap, rapid, automated, progressive and maintainable security management models, which are the main requirements of these enterprises when implementing these models. 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 the following: i) it has three security levels (1 to 3) instead of the 5-6 levels proposed by the classical models, ii) we propose that each level is certifiable instead of the total certification that exists at present, and finally, iii) the maturity level is associated with the characteristics of the enterprise.

In this way, and by using the information obtained from customers who use SICAMAN, we have developed a spirally structured maturity model (see Figure 1). This model has the aim of facilitating the performance of fast and economic cycles which allow us to create a security culture within the organization, in a constant and progressive way. The purpose of our model is, initially, to carry out an estimation of the enterprise maturity level at a low cost and in a short period of time, so as to determine a project plan which can be presented the company's board of directors. 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.

Another of the main contributions presented by the model that we have developed is a set of matrixes which allow us to relate the various components of ISMS (controls, assets, threats, vulnerabilities, risk, procedures, registers, templates, technical instructions, regulations and metrics) and which the system uses to automatically generate a large amount of the necessary information, noticably reducing the necessary period of time for ISMS development and implementation. This set of interrelations between all of the ISMS components means that if there is any change in these components in any of those objects, the measurement value of the rest of the objects in the system is altered so that we can always have an updated valuation of how the security system of the company evolves.

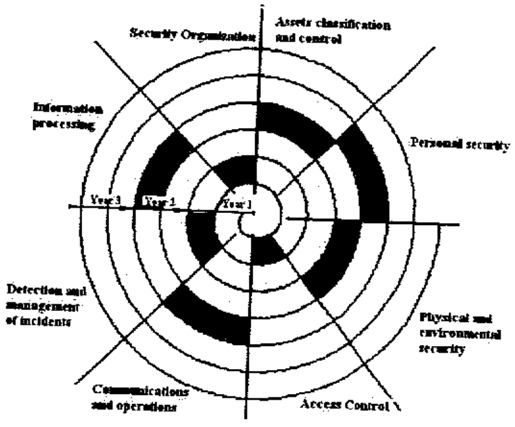
Security Organization
Assets classification and control
Information processing
Personal security
Year 3
Year 2
Year 1
Detection and management of incidents
Physical and environmental security
Communications and operations
Access Control

Figure 1: Simplified Diagram of the spiral model phases.

By using this model, we are always able to estimate, in a minimum period of time, the maturity level of the enterprise's ISMS and are also able to identify the set of rules that best adapt themselves to it. We are thus able to propose realistic short-term goals for the company's expected evolution 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 board of directors. The main objective of this will be that of complementing the current maturity level in order to reach the following maturity level.

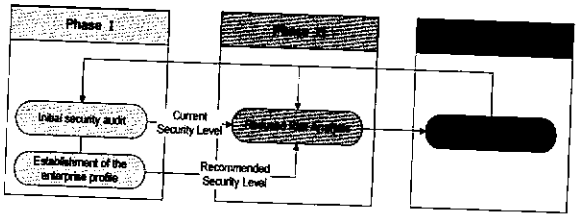
Phase 1
Initial security audit
Establishment of the enterprise profile
Current Security Level
Recommended Security Level

Figure 2: Simplified Diagram of the spiral model phases.

The security management model is formed of three phases and the results of each of the previous phases are necessary for the following phase (see Figure 2). At the same time, there is information feedback from Phase III to Phases I and II which allows the system to modify its parameters if necessary, and to adapt itself to the new circumstances.

In the following section, we will give a summerized analysis of the functioning of each phase of the model by reviewing and analysing the algorithms that the system uses to generate adequate information for the enterprise with minimum effort. At the end of the section, we will briefly present the tool used to automate the model.

3.1 Phase I: Establishment of the Current and Desired Maturity Level

The main objective of this phase is the establishment of the security level desirable for the enterprise and later, the current security level will be obtained through the audit. Moreover, vital information for Phases II and III will be obtained.

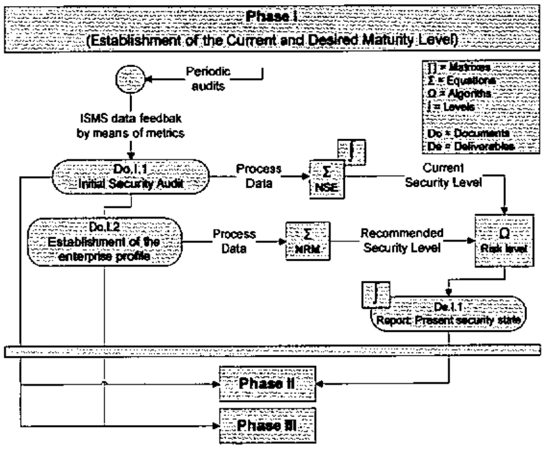
Phase I
(Establishment of the Current and Desired Maturity Level)
Periodic audits
ISMS data feedbak by means of metrics
[] = Matrices
Σ = Equations
Ω = Algoriths
| = Levels
Do = Documents
De = Deliverables
Do.I.1 Initial Security Audit
Process Data
Σ NSE
Current Security Level
Do.I.2 Establishment of the enterprise profile
Process Data
Σ NRM
Recommended Security Level
Ω Risk level
De.I.1 Report: Present security state
Phase II
Phase III

Figure 3: Diagram of the Spiral Model Phase I.

This section is composed of two sub-phases (see Figure 3):

- ***Establishment of the enterprise profile:*** The model that we propose uses a set of characteristics intrinsic to the enterprise in order to define the maximum maturity level to which the enterprise must evolve taking into account the current situation. Each of these parameters is translated into a value and the normalized sum of these values determines the maximum maturity level that the system considers appropriate for the enterprise.

The equation (1) to calculate the maturity level associated with the company is as follows:

$$\Sigma(SectWeight*(ValFactor/MaxValFactor)/\ \Sigma(SectWeight) \quad (1)$$

According to that expression and our practical experience with our customers, we have considered three maturity levels (see Figure 4):

- 1: If the result is between 0-0.25.
- 2: If the result is between 0.25–0.75.
- 3: If the result is between 0.75–1.

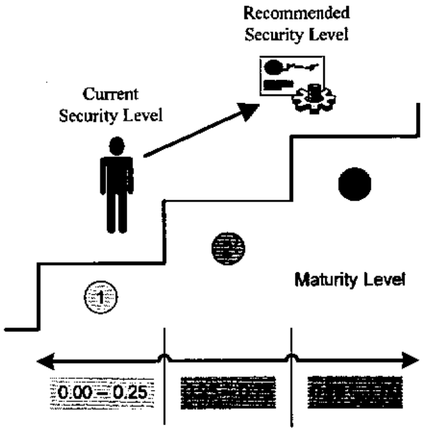

Figure 4: Phase I – Maturity Levels.

The different elements of this expression are shown below:

- o ***Factors:*** Factors represent a set of parameters that we have selected and that have an effect upon determining the security dimensioning which is adequate for the enterprise. In the current version, the following parameters have been considered: 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.
  These factors have values ranges associated that are determined depending on the characteristics of the enterprise.
- o ***WeightFactor:*** This is a correct parameter extracted from a matrix which assigns values to the factor—sector pair. This parameter of the equation allows us to control the deviations that the special characteristics of enterprises belonging to certain sectors may produce.

- ***Initial Security Audit:*** This subphase, included in Phase I, consists of performing a detailed check-list that helps us position the current state of the company with regard to its maturity level. The 735 subcontrols can belong to different maturity levels, although in the initial configuration that we recommend all subcontrols belong to a same level.

3.2 Phase II: Risk Analysis

Once we have carried out the first phase to position the enterprise at a Maturity Level and to decide to what extend the ISMS implementation must be developed, we must perform a risk analysis of the enterprise assets (see Figure 5).

This phase is extremely delicate due to the high cost that it may suppose and the importance of its results in the success of the ISMS.

The risk analysis model that we have developed is based on the models proposed by Stephenson (Stephenson 2004) which are centered upon the synergy between technical testing and risk analysis, taking ISO17799 and the Magerit v2 risk analysis methodology (MageritV2 2005) as a reference. These models have not proved to be adequate for SMEs for the following reasons: Firstly, they are enormously complex, in the second place, they require an enormous effort of involvement from the members of the enterprise, and finally the costs associated with them are not acceptable to this type of enterprises.

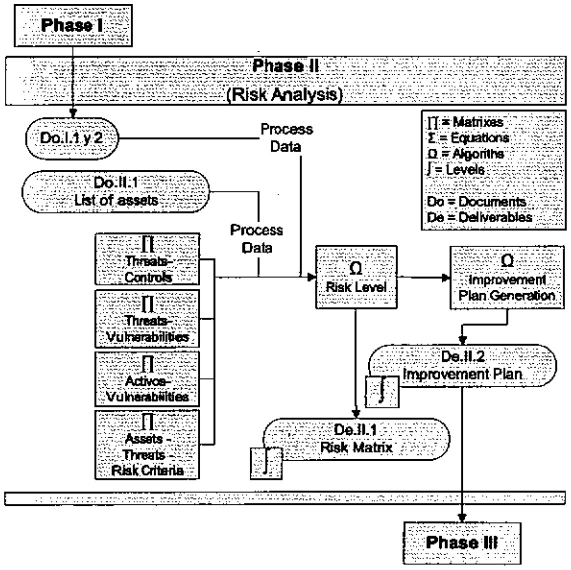

Figure 5: Diagram of the Spiral Model Phase II.

For this reason, in our model we have tried at all times to simplify the previous models in order to make them adequate for use in SMEs. The main bases on which our methodology is defined are: Flexibility, Simplicity and Cost Efficiency (both human and temporal). It is, therefore, a methodology aimed at identifying enterprise assets and their associated risks at the lowest possible cost, by using the results generated in Phase I and some simple algorithms.

This risk analysis will be formed of different objects (Assets, Threats, Vulnerabilities, Impacts and Risks) which interact with each other.

One of the most important aspects of the risk analysis that we have developed is that of **Association Matrixes** which allow us to minimize the cost of risk analysis and to produce the maximum result and information for the enterprise with the minimum effort. There have been performed a series of matrixes that allow us to associate the different components of the risk analysis (assets-threats-vulnerabilities) and at the same time, these components with the results produced in Phase I (controls). These matrixes are of great importance due to the fact that they help us both to simplify risk analysis and to obtain a valoration of the level of coverage of an asset with regard to ISO/IEC 17999 controls. These matrixes are static although the consultant may decide to modify them in other to make them more adequate for the company's needs:

- ***Assets vs vulnerabilities Matrix:*** This allows us to associate assets with the vulnerabilities that may affect them.
- ***Threats vs vulnerabilities Matrix:*** This allows us to associate vulnerabilities to each type of threat.
- ***ISO17799 threats vs controls Matrix:*** This makes it possible to associate threats with the ISO17799 controls which affect them, and thanks to the previous matrixes; it also allows us to give a security level to an asset from the controls associated with it.
- ***Assets-Threats vs Risk Criteria:*** This matrix makes it possible to associate the assets and threats of a company with regard to the risk criteria we have defined (Confidentiality, Integrity, Availability y Legality). Although in the current version, the risk generation algorithm doesn't use this matrix for the improvement plan, it is used for the report generation.

Another of the aspects provided in our risk model is that **of Level of fulfilment of a control** subjected to an unacceptable risk. The level of fulfilment of a control is of vital importance at the time of prioritizing the system improvement plan because it permits us to determine the level of current coverage of a particular asset. In the case of an asset whose risk is high because of the impact that a security error might have upon the organization and which, at the same time, has low control coverage, we must prioritize the increase of such coverage in order to raise its level of protection.

Finally, the risk analysis will be based on two algorithms:

- ***Risk Level Algorithm:*** The definition of risk level (RN) will be given by the combination of the probability (P) of occurrence (vulnerabilities) with the threat level (TL).
- ***Improvement Plan Generation Algorithm.*** For the current phase of the project, the improvement plan generation algorithm that has been developed is very basic and it is only generated by taking as a reference the assets that have obtained a high risk and ordering them from highest to lowest according to the control coverage. With the results obtained, the system achieves the controls, and issues a report indicating the control that must be improved and those factors that will improve.

3.3 Phase III: ISMS Generation

In this phase, we have tried to make ISMS manageable, orientated towards the dominions of the most interesting regulation for the organization and to reduce the number of metrics, thus obtaining rapid results and feeding back the process in each cycle with the purpose of achieving the initially indicated maturity level.

In the previous phases, we have obtained the enterprise profile, its current maturity level, its maximum advisable maturity level, the state of its controls, its assets, the risks associated with it and the improvement plan. With all this information, the system is now ready to automatically prepare an information system management plan for the enterprise, using a series of matrixes associated with the previous results to do so (see Figure 6).

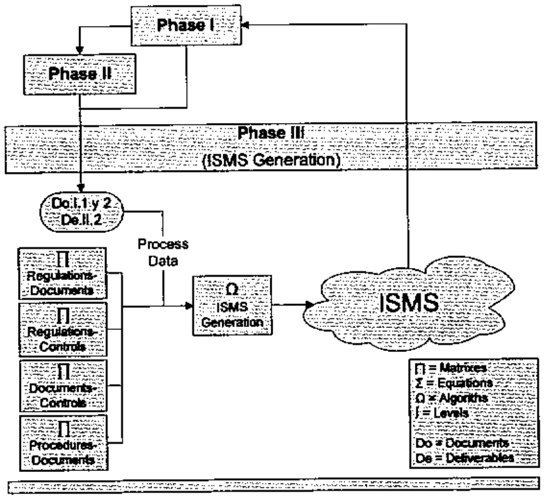

Figure 6: Diagram of the Spiral Model Phase III.

This set of matrixes which, together with those shown in Phases I and II, are the main contributions of our model will be internally used by the system to determine which procedures, technical instructions, registers, etc. must be activated for the enterprise.

The objects library of which the ISMS application is composed will steadily grow, so for this reason we have preferred to generate the first version of the model with a single library composed of the following set of objects (4 technical instructions, 25 regulations, 65 patterns, 50 procedures, 35 register).

In this phase of ISMS generation, one of the most important aspects is that of the ***Association Matrixes*** which allow us to associate all the objects in these libraries. These matrixes are internally used by the system to recommend an ISMS initial plan for the SME according to the information obtained in previous phases. There are four types of matrixes:

- ***Relationship between regulation and documents:*** The regulation defines the rules that must be fulfilled in an ISMS concrete subject. The violation of a rule of this regulation is normally associated with the non-fulfilment of other objects (procedures, patterns, registers and so on).
- ***Relationship between regulation and ISO17779:*** This matrix allows us to associate the regulation rules with ISO17799 controls in a way in which we can measure the non-fulfilment of ISO17799 controls.
- ***Relationship between documents and ISO17799 controls:*** This is the most important matrix since it allows us to

associate the documents by composing our model with ISO17799 controls.

- ***Relationship between procedures and their associated documents:*** This matrix is at present used as a reference by which to determine which documents are input/output and which are only input or only output.

Matrixes associated with ISO17799 are vitally important in the design of our system since they are used by the algorithm for the selection of those documents and procedures which are considered vitally important not only for the ISMS design but also for its subsequent follow-up.

To finish this phase, an ***ISMS generation Algorithm*** is used. Given the enormous scope of the research, the ISMS generation Algorithm has been developed by seeking the simplicity principle. This algorithm is composed of the following steps: ISMS objects Selection and Application of colour codes.

The final result of this phase will be a set of regulations and procedures that must be fulfilled if the security level of the enterprise is to improve. They will have a colour code which will visually and rapidly indicate to its users where a greater effort must be made. ISMS will be dynamic; adapting it self to the changes in control coverage levels along with those in the security levels, depending upon how the system evolves. The evolution of the system will be measured through a set of metrics defined upon the ISMS set of objects.

4 CONCLUSIONS AND FUTURE WORK

Despite the enormous efforts that are being made to create adequate maturity models to manage security in SMEs, these do not yet fit properly with the environment in which they must be implemented. The most probable reason for this is the lack of maturity of the enterprises as well as the fact that they have tried to implement models which are too general and ambitious.

In this paper, we have presented a proposal for a new maturity and security management model orientated towards SMEs which allows us to reconfigure and adapt existing models in order to guarantee the security and the stability of their management system with regard to the dimension of each enterprise. To do so, we have defined a methodology and a tool able to support the results that have been generated during the research (the tool has not been described in this paper due to space restrictions). We have clearly defined how this new maturity model must be used and the improvements that it offers with regard to the classical models.

Some of the main and most valuable conclusions obtained from the feedback of the participant enterprises in which several models have been analysed are shown below:

- The majority of the SMEs have very similar security structures. This characteristic makes it possible to develop automated security systems by means of the definition of static matrixes, which can later be reconfigured.
- If we over-dimension the security level of an enterprise with regard to its size, a degradation of the controls that we have over-dimensioned will be produced until they reach their natural balance.
- Enterprises are shown to be more receptive to very short-term implementation plans than to long- term ones.

The maturity model presented reduces the system's implementation costs and also improves the percentage of success of its implementation in SMEs. For these reasons, as the majority of our customers are SMEs, our proposal is being well received and its application is being very positive because it allows this type of enterprises access to the use of security maturity models which, until now, has only been possible for large enterprises.

As this proposal is under constant development, our short and long term objective is that of studying maturity models to a greater depth so as to refine both our model and the tool that is being developed at the same time as the model.

Among the model improvements that we intend to work on in the future, it is worth highlighting that we wish:

- To improve the algorithms of which the system is composed in order to increase their effectiveness in decision making.
- To include a planner of the time and the resources that the company wants to spend on the project, so that the system will be able to estimate time-milestones in the improvement plan.
- In Phase III, to include a library with the subprojects that should be worked on to improve the security management system globally.

With the help of the “action research” research method and the feedback directly obtained from our customers, we hope to achieve a continuous improvement in these implementations.

ACKNOWLEDGEMENTS

This research is part of the following projects: DIMENSIONS (PBC-05-012-1) and MISTICO (PBC-06-0082), both supported by the FEDER and the “Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha”, RETISTRUST (TIN2006-26885-E) granted by the “Ministerio de Educación y Ciencia” (Spain), 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."

Areiza, K. A., A. M. Barrientos, et al. (2005). Hacia un modelo de madurez para la seguridad de la información. IV Congreso Internacional de Auditoría y Seguridad de la Información.

Areiza, K. A., A. M. Barrientos, et al. (2005). Hacia un modelo de madurez para la seguridad de la información. 3er Congreso Iberoamericano de seguridad Informática.

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.

COBIT (2000). Cobit Guidelines, Information Security Audit and Control Association.

Corti, M. E., G. Betarte, et al. (2005). Hacia una implementación Exitosa de un SGSI. IV Congreso Internacional de Auditoría y Seguridad de la Información.

CSI (2002). Computer Security Institute, Computer Crime and Security Survey.

Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM 43(7): 125-128.

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.

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.

Institute, I. G. "COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT." IT Governance Institute, from http://www.itgi.org.

Jimmy Heschl, C., CISM. (2006). "COBIT Mapping: Mapping of ISO/IEC 17799:2005 with COBIT." IT Governance Institute, from http://www.itgi.org.

Kim, S. and I.Choi (2005). Cost-Benefit Análisis of Security Investments: Methodology and Case Study. ICCSA 2005, LNCS 3482.

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).

Lund, M. S., F. d. Braber, et al. (2003). "Proceedings of the Seventh European Conference On Software Maintenance And Reengineering (CSMR’03)." IEEE.

MageritV2 (2005). Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2.

Pertier, T. R. (2003). "Preparing for ISO 17799." Security Management Practices jan/feb: 21-28.

Sant-Germain, R. (2005). "Information Security Management Best Practice Based on ISO/IEC 17799." Setting Standars, The information Management JournaL 39(4): 60-62, 64-66.

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.

Stephenson, P. (2004). "Forensic Análisis of Risks in Enterprise Systems." Law, Investigation and Ethics sep/oct: 20-21.

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.

AUXILIARY REVIEWERS (CONT.)

Pierre Loidreau, CELAR, France

Pooya Farshim, University of Bristol, U.K.

Rolf Schillinger, University of Regensburg, Germany

Sebastien Kunz-Jacques, DCSSI , France

Shiao-Ying Lin, National Chiao Tung University, Taiwan

Srdjan Capkun, ETH Zurich, Switzerland

Stefan Dürbeck, University of Regensburg, Germany

Takeshi Ishihara, NTT Docomo, Japan

Theodoulos Garefalakis, Department of Mathematics, University of Crete, Greece

Toshiaki Tanaka, KDDI, Japan

Wanyu Zang, Department of Computer Science Western Illinois University, U.S.A.

Wolfgang Dobmeier, University of Regensburg, Germany

Xinyi Huang, University of Wollongong, Australia

Proceedings of SECRYPT 2007
International Conference on Security and Cryptography
ISBN: 978-989-8111-12-8
http://www.icete.org