A Systematic Review of Methodologies and Models for the Analysis and Management of Associative and Hierarchical Risk in SMEs

Antonio Santos-Olmo[1], Luis Enrique Sánchez [1], Eduardo Fernández-Medina[2] and Mario Piattini[2]

[1] SICAMAN Nuevas Tecnologías. Departament R+D,
Ave Maria, 5. Tomelloso, Ciudad Real, Spain

[2] ALARCOS & GSyA Research Group. Universidad de Castilla-La Mancha,
Paseo de la Universidad, 4, 13071 Ciudad Real, Spain

Abstract. As a result of the growing dependence of information society on ICTs, the need to know the risks that can affect information is enormously increasing with the purpose of protecting it. This article shows advances in the identification and management of risks in ICTs, particularly in the case of SMEs, along with the first proposal of a methodology for management and analysis of the associative risk in SMEs taking into account not only internal risks derived from SMEs but also other external risks derived from other enterprises in the same sector or collaborating with them. Thus, we will obtain a high quality risk analysis at low cost using advanced concepts such as "associative algorithms" and "enterprise social networks". In the era of globalization, SMEs no longer work as independent companies but share more and more services, even facilities, with other companies. Therefore, we cannot obtain an adequate risk analysis without considering the risks associated with these collaborations. In this article we present rhe results of a systematic review of methodologies and models for the analysis and management of associative and hierarchical risk in SMEs.

1 Introduction

From the point of view of enterprises, it is of utmost importance to put security controls in place that would enable them to be aware of the risks to which they may be subject, while at the same time controlling these risks carefully [1]. Nevertheless, the majority of firms have chaotic security systems which have been created with no proper guides, no documentation and insufficient resources [2].

The truth is that the actual extent to which these systems have been put in place is really low. This is in spite of the fact that reality has shown that for enterprises to be able to use information and communication technology with some guarantee, there needs to be availability of guides, measures and tools that would make it possible for them to know at any given time what their security level is, as well as to find out the points of vulnerability not yet covered [3].

Santos-Olmo A., Sánchez L., Fernández-Medina E. and Piattini M..
A Systematic Review of Methodologies and Models for the Analysis and Management of Associative and Hierarchical Risk in SMEs.
DOI: 10.5220/0004102601170124
In *Proceedings of the 9th International Workshop on Security in Information Systems* (WOSIS-2012), pages 117-124
ISBN: 978-989-8565-15-0

Some authors [4] suggest that a risk analysis should be carried out as a fundamental part of the SME. Other authors [5] propose the need to develop a new model of risk analysis, directly addressing SMEs, considering that the use of techniques of analysis and risk management, as well as the role of third parties, are essential if the security of SME information systems is to be guaranteed.

It should also be said that in an age where collaboration is vital, with the present state of the market being as it is, it is also essential to take a close look at the risk coming about from the relationship of the company with its environment, as well as with its circumstances (ever-changing) and other enterprises. These latter may be third parties in some kind of service which the firm carries out, or they might be co-participants in multi-enterprise projects.

In addition to this type of risk, those risks that are vertical in kind need to be managed in the company hierarchy, where a subsidiary's activity may affect the parent firm, and vice-versa.

The main objective of this work, therefore, is to carry out a systematic review of the models and methodologies which are either already in existence or in development, for analyzing and managing risk. We take a look at associative and hierarchical risk, as pertinent to SMEs.

2 Planning the Review

In the first place, at this stage we identify the need for the review, pointing out what its objectives are, which sources will be used to find the primary studies, and whether there were any restrictions. We also clarify what the inclusion and exclusion criteria are, as well as which criteria will be used to assess the quality of the primary studies and how the data from the studies will be extracted and synthesized.

2.1 Formulating the Question

In this section, the research question is defined; the goal here is to make the focus of interest of the work clear and to settle the nature of the problem to be dealt with and its main characteristics. This being the case, the research question can be defined as follows:

> *What work has been carried out to develop systems of risk analysis, which takes into account hierarchical and associative risk, as well as application in SMEs?*

Within the context of the planned systematic review, the existing proposals on models and methodologies of risk analysis are going to be observed. Special emphasis is going to be placed on those models and methodologies addressing work on associative risk, hierarchical risk and/or directed at SMEs. The most important ones are extracted, and a subsequent analysis and comparison of them is undertaken.

2.2 Selecting the Sources

This phase takes as its objective the selection of the sources that will be used to carry out the search for primary studies. The criterion for the selection of search sources will be the possibility of consulting the documents on the Internet or in the digital library of the University of Castilla La Mancha. This latter facility contains studies in English, as well as inclusion search engines which make it possible to look up whatever interests us with more advanced parameters, as well as to search using a key word.

The list of sources that was obtained and used to execute the systematic review is the following: Science Direct, ACM digital library, IEEE digital library, SCOPUS, Scholar Google, y DBLP.

2.3 Selecting the Studies

Once the sources have been established, the process has to be described, along with the criterion that we are going to follow in executing the review to choose and assess the studies.

First of all, the key words chosen were combined with connectors AND and OR, obtaining the abstract search string shown below.

Methodology ***OR*** *model* ***AND*** *associative* ***OR*** *hierarchical* ***AND*** *"risk analysis"* ***OR*** *"risk management"* ***OR*** *"risk assessment"****AND*** *SMB* ***OR*** *SME* ***OR*** *PYME*

The procedure for the choice of studies begins by adapting the search string to each source search engine and the execution of the search, with the latter limited to work published in the last 7 years. The inclusion criterion acts upon the results obtained when the search is run on the source, allowing us to make an initial selection of documents which, in the context of the review, will be considered as candidates to become primary studies.

The exclusion criterion operates on the sub-set of relevant studies obtained and allows us to get the set of primary studies. As primary studies we choose those which, for example, focus on the application of some standard such as ISO 27001 to risk analysis in SMEs, or work that defines agile risk management methodology, or which takes associative or environmental risk into account.

3 Carrying out the Selection and Information Extraction

Under this point, the systematic review is run on each one of the sources selected, applying all the criteria and procedure specified.

The information extracted from the studies should contain the techniques, methods, processes, measures, strategies or any type of initiative for the adaptation of the analysis, management or assessment of risk that is within the reach of SMEs, or that handles associative or hierarchical risk.

At this point we will give an overview of each of the studies chosen and presented

above, according to the information extracted by means of the Information forms created:

- *Nachtigal, S. "E-business Information Systems Security Design Paradigm and Model" [6]:* The author proposes an Information Systems security model focusing on organizations based on e-commerce, covering the design and management of Information Security in this type of businesses.
- *Abdullah, H. "A Risk Analysis and Risk Management Methodology for Mitigating Wireless Local Area Networks (WLANs) Intrusion Security Risks" [7]:* In this work, the author proposes a Methodology of analysis and management of risk in WLAN networks. The methodology proposed is based on the risk analysis methodology known as OCTAVE, although it takes it only as a basis, since a large amount of time is needed to apply this methodology.
- *Bagheri, E. et al. "Astrolabe: A Collaborative Multiperspective Goal-Oriented Risk Analysis Methodology" [8]:* In this work, the authors present a risk analysis methodology called Astrolabe. It is based on an analysis of the causes of risks in Information Systems.
- *Alhawari, S. et al. "Knowledge-Based Risk Management framework for Information Technology project" [9]:* These authors have a proposal for a conceptual Framework called Knowledge-Based Risk Management (KBRM), which uses Knowledge Management (KM) to improve the efficiency of risk management and increase the probability of success in Information Technology (IT) Projects.
- *Strecker, S et al. "RiskM: A multi-perspective modeling method for IT risk assessment" [10]:* In this work, its authors propose a conceptual modeling method known as RiskM, aiming to meet the essential requirements in the sphere of risk evaluation in IT.
- *Ma, Wei-Ming. "Study on Architecture-Oriented Information Security Risk Assessment Model" [11]:* This author develops an architecture-oriented information security risk assessment model (AOISRAM).
- *Feng, Nan et al. "An information systems security risk assessment model under uncertain environment" [12]:* What is proposed here is a model for the assessment of security risks in Information Systems based on the evidence theory (a generalization of the Bayesian theory of subjective probability).
- *Abraham, A. "Nature Inspired Online Real Risk Assessment Models for Security Systems" [13]:* This author of this work explains and discusses the advantages of using fuzzy inference methods to develop intelligent online risk assessment models.
- *Chang, She-I et al. "The development of audit detection risk assessment system: Using the fuzzy theory and audit risk model" [14]:* In this research work the authors set forth a system for risk detection in auditing. The system is put into operation using fuzzy theory and the audit risk model to establish with the greatest possible accuracy the amount of auditory evidence available.
- *Yang, Fu-Hong et al. "A Risk Assessment Model for Enterprise Network Security" [15]:* The authors suggest a conceptual modeling proposal for risk analysis in Information Systems Security, focusing on the scope of local networks of the enterprise under threat of infection and propagation of computing viruses. The main advantage of the model proposed is that it can depict the state of risk on the network in graphic

form.

- *Wawrzyniak, D. "Information Security Risk Assessment Model for Risk Management" [16]:* This author proposes an assessment and management model for risk in Information Systems, setting out to make it above all as flexible and as simple as possible to use.
- *Lin, Mengquan et al. "Methodology of Quantitative Risk Assessment for Information System Security" [17]:* These authors put forward their proposal for a methodology for assessing security risks in Information Systems; it is based on quantitative methods for obtaining the respective criteria that indicate the way to assess the general security of the Information System.
- *Hewett, R. et al. "A Risk Assessment Model of Embedded Software Systems" [18]:* In this work we see a proposal for a technique for representing and assessing risks associated with software that is embedded in given systems. The representation technique proposed is based on dynamic flow-graphs.
- *Patel, S.C. et al. "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements" [19]:* The method which these authors have come up with has the goal of assessing the vulnerability of an organization when faced with breaches in its systems of information security.

4 Analysis of Results

In Table 1 below, a comparison of the different proposals analyzed may be seen, with respect to the future proposal that is hoped to be undertaken. The aspects assessed may be considered to have been fulfilled completely, or partially, or not tackled at all in the model.

Each one of these aspects analyzed is described as: i) Scope of Application: If the model is applied in a company comprehensively- i.e., to the security of all the Information Systems, or if is applied to only a subset of these; ii) Metrics: The guide includes mechanisms for measuring the clear criteria of risk, giving detailed information on its application and assessment; iii) Qualitative techniques: The model includes qualitative measurement techniques; iv) Quantitative techniques: The model includes quantitative measurement techniques; v) Associative: The model takes risk distribution into account (for example, in outsourced activity, or in activity undertaken by the company in partnership with other firms) and it also considers the interrelationship between the firm and its particular setting; vi) Hierarchical: The model takes the hierarchical relationship between related companies into account; vii) SME-oriented: The model has been developed to address the particular principles involved in SMEs; viii) Knowledge reuse: The guide gathers knowledge as regards how the model is put into operation, and information is collected throughout its use, so that when the model is installed on subsequent occasions, this knowledge may be reused.

These features that are desirable for a model of analysis and management of associative and hierarchical risks for SMEs have been obtained using the application of the "action-research" method to real-life cases. It is deemed that each one of these characteristics can be completely fulfilled, partially fulfilled or not taken into account at all by the model.

Table 1. Comparison of the proposal selected.

Name	Global scope	Metrics	Qualitative Techniques	Quantitative Techniques	Associative	Hierarchical	SME-oriented	Knowledge Reuse
Nachtigal, S.	No	Part.	No	No	Part.	No	Part.	No
Abdullah, H	No	No	Yes	No	No	No	Yes	No
Bagheri, E. et al.	Yes	Yes	Yes	No	No	No	No	No
Alhawari, S. et al.	No	No	No	No	No	No	No	Yes
Strecker, S et al.	Yes	No	Part.	Part.	No	No	No	No
Ma, Wei-Ming	Yes	No	No	No	Part.	Part.	Part.	No
Feng, Nan et al.	Yes	No	Yes	Yes	Part.	No	No	No
Abraham, A.	No	No	No	No	Part.	No	No	Yes
Chang, She-I et al.	No	Part.	Part.	No	Part.	No	No	No
Ngai, E.W.T. et al.	No	Part.	Yes	No	Part.	No	No	No
Yang, Fu-Hong	No	No	No	No	Part.	No	No	No
Wawrzyniak, D.	Yes	No	Yes	No	No	No	No	No
Lin, Mengquan et al.	Yes	Part.	No	Yes	No	No	No	No
Hewett, R. et al.	No	No	No	No	Part.	No	No	Yes
Patel, S.C. et al.	Yes	Part.	No	Yes	No	No	No	No

5 Conclusions and Future Work

In this paper a systematic review of the different models and methodologies for risk analysis and management has been carried out. The goal has been to study the SME-oriented proposals that focus on associative and hierarchical risk. As a result of this review, it has been possible to establish how important risk management and analysis of Information System security is as part of any enterprise's effort to sustain performance and growth, aspects that are basic to that firm's being able to fulfill its mission and reach its organizational goals in a highly competitive environment.

There are numerous sources in the literature that point to and underline the difficulty SMEs have in using traditional methodologies and models of risk analysis. These were designed for large enterprises and their application in SMEs is difficult and costly. [20, 21].

The main reasons why existing models of analysis and management are not enjoying success when implemented in SMEs are the following:

- Some of them were developed with large organizations in mind (Major standards such as CRAMM, ISO/IEC 27005, MAGERIT, OCTAVE, NIST SP 800-39, Mehari, COBIT o ERMF), as well as in the organizational structures associated with these.

Others (Abdullah, Wei-Ming Ma, Nachtigal) have attempted to simplify the model to make it suitable for companies with limited means. These researchers, however, either produce incomplete models which tackle only part of the issue, or try to provide basic guides for the steps to be taken, without going into how to really assess and manage risk in such a way that the technical personnel of the firm can be involved in the process. Furthermore, most of these proposals are theoretical and are still in development.

- The majority of the proposals do not take into account the need to address hierarchical and associative risks, which are crucial factors in the present structure and work of enterprises (in which Cloud systems are becoming more and more widely-employed). All this is especially true in the case of SMEs.

It may be concluded, then, that it is justifiable to produce a new model for implementation in SMEs, which would allow us to include all those features considered as desirable which have been mentioned above.

All of the standards and proposals for assessing and managing risk studied in this paper are significant ones, and their contributions will be taken into account in the development of a methodology that will incorporate all the characteristics desired.

Acknowledgements

This research is part of the following projects: MEDUSAS (IDI-20090557), financed by the Centre for Industrial Technological Development (CDTI), ORIGIN (IDI-2010043(1-5)) financed by the CDTI and the FEDER, BUSINESS (PET2008-0136) awarded by the Spanish Ministry for Science and Technology and MARISMA (HITO-2010-28) and SISTEMAS (PII2I09-0150-3135) financed by the Council of Education and Science of the Castilla-La Mancha Regional Government.

References

1. Kluge, D. Formal Information Security Standards in German Medium Enterprises. in CONISAR: The Conference on Information Systems Applied Research. 2008.
2. Wiander, T. and J. Holappa, Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method., in Technical Report, V.T.R.C.o. Finland, Editor 2006.
3. Wiander, T. Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases. in AISC '08: Proceedings of the sixth Australasian conference on Information security. 2008. Wollongong, Australia.
4. Volonino, L. and S. Robinson. Principles and Practice of Information Security. in 1 edition, Anderson, Natalie E. 2004. New Jersey, EEUU.
5. Spinellis, D. and D. Gritzalis. nformation Security Best Practise Dissemination: The ISA-EUNET Approach. in WISE 1:First World Conference on Information Security Education. 1999.
6. Nachtigal, S., E-business Information Systems Security Design Paradigm and Model. Royal Holloway, University of London, Technical Report, 2009: p. 347.
7. Abdullah, H., A Risk Analysis and Risk Management Methodology for Mitigating Wireless

Local Area Networks Intrusion Security Risks. University of Pretoria, 2006: p. 219.
8. Bagheri, E. and A. A. Ghorbani, Astrolabe: A Collaborative Multiperspective Goal-Oriented Risk Analysis Methodology. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, 2009. 39(1): p. 66-85.
9. Alhawari, S. et al., Knowledge-Based Risk Management framework for Information Technology project. International Journal of Information Management, 2012. 32(1): p. 50-65.
10. Strecker, S., D. Heise, and U. Frank, RiskM: A multi-perspective modeling method for IT risk assessment. Inf Syst Front, 2010(13): p. 595–611.
11. Ma, W.-M., Study on Architecture-Oriented Information Security Risk Assessment Model. ICCCI 2010, Part III, LNAI 6423, 2010: p. 18–226.
12. Feng, N. and M. Li, An information systems security risk assessment model under uncertain environment. Applied Soft Computing, 2011. 11(7): p. 4332-4340.
13. Abraham, A., Nature Inspired Online Real Risk Assessment Models for Security Systems. EuroISI 2008, LNCS 5376, 2008.
14. Chang, S.-I., et al., The development of audit detection risk assessment system: Using the fuzzy theory and audit risk model. Expert Systems with Applications, 2008. 35(3): p. 1053-1067.
15. Yang, F.-H., C.-H. Chi, and L. Liu, A Risk Assessment Model for Enterprise Network Security. ATC 2006, LNCS 4158, 2006: p. 293 – 301.
16. Wawrzyniak, D., Information Security Risk Assessment Model for Risk Management. TrustBus 2006, LNCS 4083, 2006: p. 21–30.
17. Lin, M., Q. Wang, and J. Li, Methodology of Quantitative Risk Assessment for Information System Security. CIS 2005, Part II, LNAI 3802, 2005: p. 526 – 531.
18. Hewett, R. and R. Seker, A Risk Assessment Model of Embedded Software Systems. 29th Annual IEEE/NASA Software Engineering Workshop (SEW'05), 2005: p. 8.
19. Patel, S. C., J. H. Graham, and P. A. S. Ralston, Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. International Journal of Information Management, 2008. 28(6): p. 483-491.
20. Calvo-Manzano, J. A. et al., Experiences in the Application of Software Process Improvement in SMES. Software Quality Journal., 2004. 10(3): p. 261-273.
21. Mekelburg, D., Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. Software Quality Professional, 2005. 7(3): p. 4-13.