Economic Aspects and Needs in IT-Security Risk Management for SMEs

Markus Klemen Stefan Biffl
Institute of Software Technology and Interactive Systems
Vienna University of Technology, Karlsplatz 13, A-1040, Austria
{klemen, biffl}@ifs.tuwien.ac.at

Abstract

Business success depends increasingly on reliable IT-Infrastructure. IT-Security risk management aims at an optimal allocation of security resources regarding an "affordable" IT-Security level.
In comparison to large corporations small and medium-sized enterprises (SMEs) typically have few resources and little expertise in IT-Security risk management. Therefore, they need SME-focused framework processes and methods for strategic planning and operational tool support. Long-term goal is to improve the general security level of SME IT–Infrastructure.
In this position paper, we argue for a closer tie between economical and technical aspects of IT-Security Risk Management. Based on the RiskIt risk management process we propose empirical investigations to tackle SME-specific data needs for risk analysis and multi-objective optimization for risk-countermeasure resource allocation.

1. Current Interests

Markus Klemen is on a Ph.D. track at the Vienna University of Technology, where he focuses on economic issues of IT-Security risk management specifically customized to the requirements of small and medium-sized enterprises which may be addressed by means of multi-objective decision support methods (see also [20]). Other areas of his interest include Honeynet projects, IPv6 security aspects and information security procedures.

Stefan Biffl is an associate professor of software engineering at the Vienna University of Technology. His research interests include Empirical Software Engineering, economic models for software engineering processes, project management, quality management, software inspection, reading techniques for software inspection.

2. Past Work

During our cooperation with SMEs over the past years, we found a profound need for solid, scientific support for SME-specific IT-Security. We began to address this field, first in a diploma thesis (IT-Security in SMEs). Based on early work of Raiffa and Schlaifer dating back to 1961 [1] with considerable refinement by Howard in 1966 [2] we adapt the RiskIt process for systematic risk management to IT-Security requirements [3][4][5].

For economic evaluation of decision options we have used classic approaches towards the financial quantification of IT-related risks like ALE (Annual Loss Expectancy) [6] enhanced in Kevin SooHoo's Ph.D. thesis [7]. As IT-Security countermeasure planning is often a multi-objective problem, we came across the concept of Quadtrees developed by Habenicht [8] and Sun and Steuer [9]. For further research we want to build on an application of the theory of multi-objective decision support to IT-Security by Stummer and Strauss [11].

3. Issue Statement

Competitive and efficient organizations increasingly rely on networks and computer-based information systems [12][13]. IT-Security risk management is a strategic contribution to enable a secure and reliable IT-infrastructure. To be effective, it needs to be tied to guidelines for daily operations and should help to determine a most economic allocation of resources for either investments (e.g., setting up a new firewall) or process assessment and improvement (e.g., analyzing event logs on a daily basis, changing administrator passwords monthly).

Large corporations can maintain an IT department with a chief security officer (CSO) for strategic security planning and tactical implementation. SMEs usu-

ally have flat management hierarchies and most smaller companies are not able or willing to afford a CSO person. Therefore, either upper management or operative administrators have to make IT-Security related decisions on top of their primary responsibilities. Management often lacks the technical expertise and the administrators the time to properly deal with IT-Security issues.

IT-Security is generally plagued with unanticipated problems. While these problems cannot be eliminated totally, some of them can be controlled well by taking appropriate preventive action. These actions require financial and/or human resources. Therefore, an efficient balance between the costs of preventing risks and the costs of accepting risks must be found. Risk management is an area of project management that deals with these issues before they cause unanticipated problems. Organizations may be able to avoid a large number of problems if they use systematic risk management procedures and techniques preemptively.

Risk management approaches contain the following actions [14][15][16][17] – some of them are often conducted as group activities of project stakeholders:

- *Risk identification* produces a list of the security-specific risk items likely to endanger normal business operations. Elicitation methods for this activity are brainstorming, checklists, taxonomies and decomposition [18] .
- *Analysis of the identified risks* assesses the probability and size of loss for each risk item. Typical techniques include performance models, cost models, and network analysis [16] .
- *Risk prioritization* produces a ranked order of the risk items identified and analyzed. Typical techniques include risk reduction leverage analysis (particularly involving cost-benefit analysis) or group consensus techniques.

Further steps in the IT-Security risk management process are preparation for detection, reaction, and reflection procedures in case of security incidents [19]. Over time, a number of specific risk management approaches have been developed. In this paper we use the Kontio's RiskIt process [5], a systematic procedure for risk management consisting of the above-mentioned steps with some further refinements.

In general, managers are not only expected to allocate resources and manage them in a cost-conscious manner, but they are also held accountable for making certain that these resources are implemented as intended. This is especially true for security management in the IT sector [12][13] and in SMEs.

Thus it is important to provide a set of operative threat scenarios as part of a strategic risk management process specifically adapted to SME requirements. Those threat scenarios should consist of a comprehensive list of threat sources (e.g., intruder hacking firewall, employee stealing data, thunderstorm destroying hardware), assets to be protected (such as servers, confidential information, network access), likelihood of occurrences and an estimated damage range. Real-world tools are to provide means and methods which can be relatively easily implemented and customized.

There are three economic IT-Security related tasks that need to be addressed:

1 – Given a predetermined target level of IT-Security, determine a minimal sufficient budget for achieving this level from the current situation;

2 – Given a fixed budget for IT-Security safeguards, determine the optimum safeguard portfolio for a specific enterprise context;

3 – Given the *status quo* of budget and security level, determine changes in the processes (e.g., patching servers, evaluating log-files, preparing installation images) or hardware/software configuration that improve the level of security without increasing the financial burden.

4. Proposed Approach

The approach we suggest in this position paper can assist risk managers in their work by helping them to define "affordable security" for their context: by presenting a variety of different security scenarios and evaluating the utility, costs, and diversification of entire bundles of security measures.

One of the main problems of economic analysis of IT-Security areas is the poor availability of raw data. Interestingly, although most authors of analysis techniques recognize this as the major inhibitor to applicable IT-Security Risk Management, few concepts have so far been developed to tackle this issue. We suggest addressing it by using a portfolio of techniques to collect and assess data:

To evaluate the probability of security incidents and costs of IT-Security safeguards and countermeasures, we suggest empirical studies to establish proper frameworks. In contrast, the benefits of security improvements depend heavily on the perspective of various stakeholders (e.g. administrators, decision-makers, employees, partners). We will therefore adapt existing collaborative tools and methods [21][22]which will enable us to analyze different utility functions and their

impact on the benefit of IT-Security measures in financial terms.

We propose to conduct empirical studies and adjust existing IT-Security risk management approaches to SMEs in order to addresses five specific areas:

1 – *Multiobjective risk-countermeasure budget optimization* based on interactive tool support – as proposed in [11] – will ease the process of determining the "affordable" level of security for a specific organization in the face of non-monetary constraints on budget allocation. This interactive collaboration process will improve the quality of the threat scenarios and will enable different views from different stakeholders within an organisation.

2 – *Determine cost/benefit ratios of IT-Security safeguards, countermeasures and procedures*. Traditionally IT-Security is only seen as a cost factor. We want to elicit the potential benefits of IT-Security in financial terms which will allow for a more differentiated view on this topic.

3 – *Enterprise-specific context awareness:* Case studies that apply the risk management process, analysis and optimization methods with industry practitioners will help to find the balance between generic aspects applicable for most SMEs and specific peculiarities of certain industry sectors, branches, or types of SME.

4 – *Data base for the assessment of security scenarios in general.* There is a need for data on security incidents in a range of company contexts to calibrate models for the probability of threat scenarios. Sensitive empirical surveys with interested companies as well as studies with government large-scale threat response centers (such as various *Computer Emergency Response Teams* or the Austrian CIRCA initiative) can help to provide a data collection that improves models for the deduction of realistic threat scenarios.

5 – *Investigate impact of context (large and small corporations) on applicable IT-Security risk management methods.* Since most existing approaches – like the German IT-Base Protection Manual, Cobit, ISO 17799 or GMITS – were developed for governmental institutions and large corporations, applicable methodologies for SMEs need to be developed which allow specific risk management packages: a framework process, risk analysis and countermeasure planning methods, elaboration of improved sets of typical threat scenarios, and tool support for individual adaptation to corporate context.

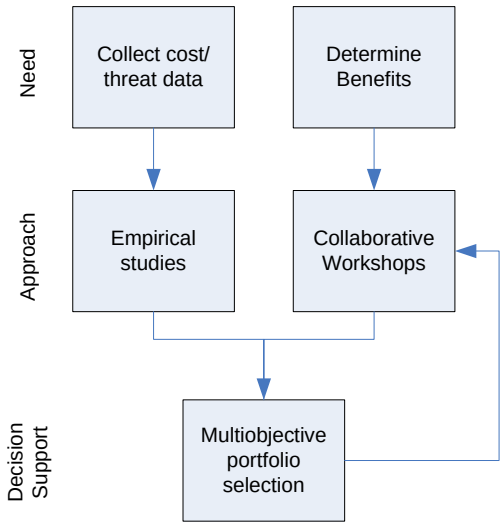

Figure 1: The different needs for data for establishing applicable cost/benefits models are addressed by a dual approach.

These areas result in three parallel research tracks:

The first research track establishes methods for collecting valuable quantitative data for better calibrated threat scenarios and cost models. It is a set of empirical studies collecting, analyzing, and calibrating input to establish realistic initial threat scenarios and countermeasure costs. Currently, no statistically significant publicly available threat scenario or threat ranking exists that would list the likelihood and magnitude of IT-Security risks backed by real-world data.
In our approach, the amount of damage will be measured not only in monetary units but also in multiple loss criteria which are too difficult to determine in financial terms (e.g. loss of reputation, bad press, embarrassment).

The second track develops methods for determining the benefits of IT-Security investments and safeguards using collaborative workshops. These workshops will help to better understand soft and stakeholder-specific factors.

The third track utilizes the generated data and insights from the empirical studies and the workshops for multiobjective portfolio selection, which can also be used in the workshops as an important additional tool.

5. Results, Status, Prospects, and Needs

Stummer and Strauss [11] presented a multi-objective decision support methodology for IT-Security. Since the current shortage of real-world data reduces the immediate usability of their approach (and all other approaches in this area in general), we plan to gather empirical data for designing realistic threat scenarios as a basis for cost-benefit analysis and subsequent investment optimization.

The two most essential input parameters are the probability of occurrence and the magnitude of damage caused by a specific threat (i.e., the expected value of harm). Providing useful data at least for an important subset of real-world contexts would be a huge contribution towards assessing and improving the IT-Security level in general.

This will be greatly facilitated by extending concepts like the Stummer multiobjective approach by interactive collaboration processes like **CIDECS**, which is a successor of the Hermes research initiative on value-based software engineering management **Error! Reference source not found.**.

Collecting data for IT-Security risk analysis for a single company is too costly and too inefficient. Therefore, chambers or other associations should conduct such studies for their members. Following this idea, we have submitted an EU research project. One part of this project addresses the imminent shortage of data and the specific requirements of IT-Security for SMEs in Europe. This project involves various industry associations in four member states.

6. Open Issues

An important open issue is the *investigation of valid valuation methods for determining expected losses and probabilities of risks* as well as perspectives from different stakeholders and the modeling of uncertainty aspects (see also [20]).

Currently, there is *no operative concept of how to gather and analyze the data for creating threat scenarios*, which would also have to be updated on a regular basis. Although many institutions exist that collect IT-Security related data, they are usually not publicly available apart from aggregated abstracts with limited use for IT-risk management.

A new area will be the combination of multiobjective support models with interactive collaboration tools. This combination is not limited to the area of IT-Security and might prove useful for other areas, where decisions have to take hard and soft criteria into consideration.

7. References

[1] Raiffa, H., and Schlaifer, R., Applied Statistical Decision Theory, Boston, Harvard University, 1961.

[2] Howard, Ronald A., Decision Analysis: Applied Decision Theory, *Proc. of the Fourth International Conference on Operational Research*, David B. Hertz and Jacques Melese, editors, New York: Wiley-Interscience, 1966.

[3] Kontio, J., Basili, V.R., Empirical Evaluation of a Risk Management Method, *Proceedings of the SEI Conference on Risk Management*, SEI Software Engineering Institute, 1997.

[4] Kontio, J., Basili, V.R., Empirical Evaluation of a Risk Management Method, *Proc. of the SEI Conference on Risk Management*, SEI Software Engineering Institute, 1997.

[5] Kontio, J., The RiskIt Method for Software Risk Management, *Tech. report CS-TR-3782*, University of Maryland, 1997.

[6] Hoffman, J. Lance and Hung, T. Brian: A Pictorial Representation and Validation of the Emerging Computer System Security Risk Management Framework, *Proc. Computer Security Risk Management Model Builders Workshop*, Ottawa, Canada, June 20–22, 1989.

[7] SooHoo, K., How Much is enough? A Risk-Management Approach to Computer Security, *Consortium for Research on Information Security and Policy (CRISP)*, June 2000.

[8] Habenicht, W., ENUQUAD: A DSS for discrete vector optimization problems, eds. M. Cerny, D. Glueckaufova and D. Loula, *Multicriteria Decision Making: Methods; Algorithms; and Applications, Institute of Economics*, Czechoslovak Academy of Sciences, Prague, 1992, 66-74.

[9] Sun, M., and Steuer, R.E., InterQuad: An interactive quad tree based procedure for solving the discrete alternative multiple criteria problem, *Euro. J. Oper. Res.* 89, 3 (1996) 462-472.

[10] Sun, M., and Steuer, R.E., Quad tree data structures for use in large-scale discrete alternative multiple criteria problems, eds. Y. Shi and M. Zeleny, *New Frontiers of Decision Making for the Information Technology Era*, World Scientifc, Singapore, 2000, p. 48-71.

[11] Stummer, C., Strauss, C., Multiobjective Decision Support in IT-Risk Management, *Int. Journal of Information Technology & Decision Making* Vol. 1, No. 2 (2002) 251-268.

[12] Cash Jr., J.I., McFarlan, W.F., and McKenney, J.L., Corporate Information Systems Management: The Issues Facing Senior Executives Irwin, *Homewood*, 1992.
[13] Elo, M.M., von Solms, S.H., Information security management: An approach to combine process certification and product evaluation, *Comput. Security* 19, 8 (2000) 698-709.
[14] Boehm, B. Software Risk Management: Principles and Practices, *IEEE Software*, Jan. 1991, p.32-41.
[15] Biffl, S., et al., "Tool Support for a Risk Management Process – An empirical study on effectiveness and efficiency", *Proc. IASTED Software Engineering Conf.*, February 2004, Innsbruck, Austria.
[16] Charette, R., *Software Engineering Risk Analysis and Management*, McGraw-Hill, 1989.
[17] Hillson, D., Developing Effective Risk Responses, *Proc. 30th Annual PMI Seminars & Symposium*, Philadelphia, 1999.
[18] Carr, M.J., Konda, S.L., Monarch, I.A., Ulrich, F.C., Walker, C.F., *Taxonomy-Based Risk Identification, SEI Technical Report SEI-93-TR-006*, SEI Software Engineering Institute, 1993.
[19] Pipkin, D., *Information Security*, Prentice Hall PTR, New Jersey, 2000.
[20] Biffl, S., et al., Economic Risk-Based Management in Software Engineering: The HERMES Initiative, *(http://qse.ifs.tuwien.ac.at/research/hermes/-overview.htm).*
[21] Boehm, B.W., P. Grünbacher, and R.O. Briggs, *Developing Groupware for Requirements Negotiation: Lessons Learned*. IEEE Software, 2001(May/June).
[22] Briggs, R.O. and P. Grünbacher. EasyWinWin: Managing Complexity in Requirements Negotiation with GSS. *In 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 1. 2002.* Big Island, Hawaii.

8. Biography

Markus Klemen has studied International Business Economics at the University of Vienna. He worked for 10 years self-employed in the area of customized business software development as well as IT-Security consulting and Network services. He is currently employed at the Vienna University of Technology. He is working on his Ph.D. thesis. The research focuses on economic issues of IT-Security risk management in small and medium-sized enterprises and multi-objective decision support methods.

Stefan Biffl is an associate professor of software engineering at the Vienna University of Technology.
In addition to academic lecturing and publishing he offers software engineering consulting services to industrial projects.
He received an MS and PhD in computer science from the Vienna University of Technology and an MS in social and economic sciences from the University of Vienna. He is a member of the ACM and IEEE.