Ontology-based Decision Support for Information Security Risk Management

Andreas Ekelhart
Secure Business Austria
Vienna, Austria
Email: ekelhart@securityresearch.ac.at

Stefan Fenz
Vienna University of Technology
Vienna, Austria
Email: fenz@ifs.tuwien.ac.at

Thomas Neubauer
Secure Business Austria
Vienna, Austria
Email: neubauer@securityresearch.ac.at

***Abstract*—As e-Business and e-Commerce applications are increasingly exposed to a variety of information security threats, corporate decision makers are increasingly forced to pay attention to security issues. Risk management provides an effective approach for measuring the security but existing risk management approaches come with major shortcomings such as the demand for very detailed knowledge about the IT security domain and the actual company environment. This paper presents the implementation of the AURUM methodology into a software solution which addresses the identified shortcomings of existing information security risk management software solutions. Thereby, the presented approach supports decision makers in risk assessment, risk mitigation, and safeguard evaluation.**

I. Introduction

Although companies consider security as one of the most important issues on their agenda, many companies are not aware how much they spend on security and if their investments in security are effective (cf. [1], [2]). Information security risk management is a crucial element for ensuring long-term business success because it provides an effective approach for measuring the security through the identification and valuation of assets, threats, and vulnerabilities and offers methods for the risk assessment, risk mitigation and evaluation. However, while existing approaches (see Section II) for implementing an adequate risk management strategy are highly accepted within the community they are requiring very detailed knowledge about the IT security domain and the actual company environment. As a consequence, organizations mostly fall back on best-practices, information security standards, or domain experts when conducting the risk assessment and are confronted with the following problems: (1) best practice guidelines such as the German IT Grundschutz Manual [3] or the French EBIOS standard [4] provide excellent knowledge about potential threats, vulnerabilities, and countermeasures, but without a domain expert the organization is usually unable to consider all the complex relationships between relevant IT security concepts, which results in a non-holistic IT security approach endangering the organization in performing its mission [5], [6], (2) to check which concrete infrastructure elements are endangered by certain threats the organization has to manually map the knowledge from best-practice guidelines to their actual infrastructure [7], (3) especially information security standards such as ISO 27001 [8] are stating only very abstract implementation suggestions for risk mitigation; concrete countermeasures or combinations thereof are mostly missing [9], (4) determining threat probabilities is mostly based on subjective perceptions, instead of objective evaluation [9], (5) while companies strive for cost-conscious solutions, they are frequently unaware of their level of IT security capital expenditure and/or, even more importantly, whether these investments are effective [10], and (6) management decision makers, such as the CPO or CIO, have to cope with a great spectrum of potential IT security investments on the one hand and the decision of selecting the most appropriate set of IT security investments on the other hand. The results of existing methods provide decision makers with inadequate or little intuitive and/or interactive decision support and, thus, do not support them in making an appropriate risk versus cost trade-off when investing in IT security solutions [11]. In order to address these reservations and demands outlined above, we developed a novel methodology for information security risk management, including objective measures of risk, risk reduction, and cost of defense, named AURUM (which is derived from "AUtomated Risk and Utility Management"). This paper presents the developed software solution for supporting the entire AURUM risk management methodology. Compared to existing approaches (e.g., CRISAM [12] and GSTool [3]), AURUM allows for automated information security risk management, including objective measures of risk and risk reduction by taking the entire setting of the organization into account.

II. Background and Requirements

Risk management in the context of information technology is not a new research domain. It was 1975 when the U.S. National Bureau of Standards proposed the Annual Loss Expectancy (ALE) as a metric for measuring computer-related risks (cf. [13]). In the 1980s it was again the U.S. National Bureau of Standards, which developed an iterative process for information security risk management. Although the information security risk management approaches of the following years provided some additional steps or different process structures, they are mainly based on this approach. A combination of qualitative and quantitative risk analysis methodologies has been proposed by [14] and comprises the identification of organizational value activities. Besides general risk management frameworks, several information

978-0-7695-3551-7/09 $25.00 © 2009 IEEE
DOI 10.1109/ICONS.2009.8

security investment decision support methods, which are an integral part of existing information security risk management methodologies, have been proposed (cf. [16], [17]). In 2008, the PCR (perceived composite risk) metric was introduced by [18]. Their approach extends the traditional ALE by combining it with the expected severe loss and the standard deviation of the loss, and provides organizations with an additional decision support tool for information security investments. To make these academic approaches usable to organizations, some of them have been used as a foundation for todays information security risk management methods, standards and best-practice guidelines (e.g., CRAMM [19], NIST SP 800-30 [20], OCTAVE [21], EBIOS [4], and recently ISO 27005 [22]). Software solutions supporting entire information security risk management methodologies support users in preparing, administrating, and updating information security concepts that meet the requirements of the corresponding methodology. After having modeled the organization's assets relevant to information security, the solutions offer predefined threats and connected controls for the various asset classes. Although these approaches are sophisticated, their underlying data structures are proprietary and thus difficult to apply in different contexts, hindering standardized and collaborative information security risk management. We assessed CRISAM Explorer by Calpana, GSTool by the German Federal Office for Information Security, CRAMM by Insight Consulting and EBIOS by the French DCSSI and identified the following shortcomings, which may result in an inadequate implementation of the corresponding information security risk management strategy:

- Manual and unguided inventory of the organization's assets and no support for an automatic or semi-automatic inventory of IT assets. Problem: important assets may be simply forgotten.
- No vulnerability catalog is provided to support the identification of vulnerabilities. Problem: the existence and severity of vulnerabilities determines the threat exploitation probability and therefore the risk level.
- The control implementation inventory is conducted by control questions which have to be answered by the user. Problem: potential side-effects of control implementations are not considered and hinder therefore a sound cost/benefit analysis of the control implementations.
- There are no sound calculation schemes for the threat probability determination. Problem: besides the potential impact the risk calculation relies on realistic threat probability values. Since the calculated risk is fundamental for the subsequent control implementation selection, wrong risk values render the entire information security risk management efforts useless.
- Insufficient or no cost/benefit analysis support regarding potential control implementations. Problem: management is not aware about what to implement in order to decrease the risk to an acceptable level.

III. The AURUM Process

This chapter provides the reader with a short description of each step in the AURUM process. For each of those steps we show the user interfaces used for communicating with the system and describe how we realized those steps in the AURUM software solution. The AURUM tool was designed to minimize the interaction necessary between user and system and to provide decision makers with an intuitive solution that can be used without extensive knowledge about the information security domain. However, the solution is capable of providing expert users with detailed information on different levels of granularity. Figure 1 demonstrates the schematic layout of the working area. The left section summarizes information on (a) the business processes and its dependence on assets, and (b) the assets's physical locations in the organization. The middle section provides the decision maker with (a) a graphical representation of the selected business process together with the assets needed for the execution of the selected business process, (b) the graphical representation of the physical location model together with assets, and (c) an interface for the interactive selection of control implementations. Information provided in the middle section depends on the selection the decision maker made in the left section (the same holds analogously for the dependence between the middle and the right section). The right section displays detailed information for selected assets. This area includes (a) a risk level for the selected asset, (b) a list of threats and their calculated probabilities, and (c) implemented and not implemented controls with their calculated effectiveness figures. The tool was implemented in C# using the Protege OWL API for incorporating the security ontology[1], the Netica C# API for the Bayesian threat probability determination, and the Windows Presentation Foundation Framework for the graphical user interface. The interface was build in consideration of common usability guidelines (e.g., http://www.usability.gov).

A. Inventory of the Organization

The AURUM approach is based on a security ontology that provides a highly granular physical infrastructure model. The basic version of the ontology provides the user with an extensive set of initial information on the security infrastructure that is usually needed in organizations. A company that decides on using the security ontology as a basis for information security risk management has to initialize the ontology once with company specific information. A typical physical infrastructure modeling process is conducted as follows: (1) definition of the organization, (2) definition of site concepts and relating them to appropriate location concepts, (3) definition of building concepts, (4) definition of level concepts (including information about their vertical position within the building), (5) if necessary, definition of areas, (6) definition of sections and section connectors (e.g., doors or windows), (7) modeling tangible assets (including ratings for acceptable risk levels and importance for the organization's mission) and

[1] Security Ontology: http://securityontology.securityresearch.at

persons, and relating them with their typical physical location (e.g., sections), (8) modeling data and software concepts and relating them with those IT and telecommunication instances on which they are stored on, (9) relating one or more roles to each modeled person, and (10) modeling organizational controls. This step is supported by a novel inventory solution (for a detailed description cf. [23], [24]) for software and IT-related infrastructure elements which is able to capture the device data automatically (operating system, IP address, patch level, etc.) independent of the used operating system. This enables us to enhance the efficiency of the system characterization step significantly, since the inventory of IT-related infrastructure elements is one of the most labor-intensive steps. Collecting such detailed device data enables, in the case of software-related threats (e.g., malware or errors in standard software), the mapping of software vulnerabilities on the current IT infrastructure in order to visualize threatened systems immediately. After being initialized once (by using a wizard we provide in the AURUM tool), the ontology serves as a knowledge base for the following step of the information security risk management process.

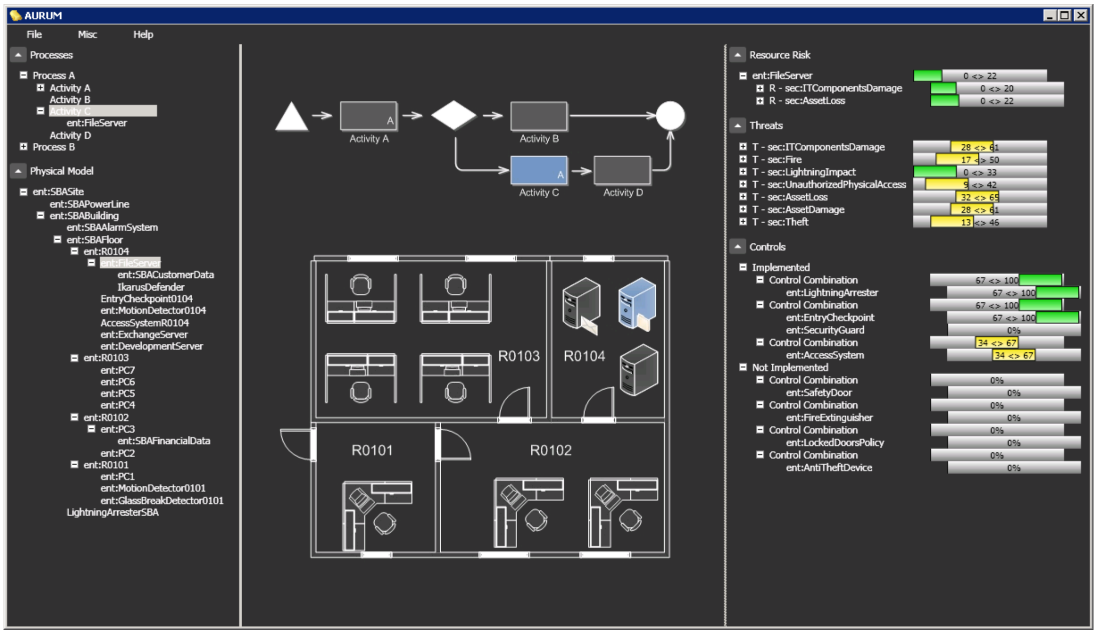
B. System Characterization

As the inventory step is carried out only once, this step is intended to update the system information before starting with the risk management. This step comprises the refinement of the system boundaries, of the assets and information used and/or required by the defined system → systematic inventory of hardware, software, existing physical and organizational controls, system interfaces, data, information, and persons who support or use the information system → determination of the acceptable risk level for each inventoried asset. The AURUM tool provides the following two options for updating information. At the same time these alternatives provide the decision maker with a fast overview:

- Process Model: AURUM allows to use business process models as a basis for identifying corporate risks. The left section provides an overview of the business processes selected for the specific risk assessment. By selecting one of these processes, the tool provides a graphical representation of the business process in the middle section. Additionally, all assets needed for executing this process are displayed. When the user selects one of those assets (File Server in this example), the tool provides further information on threats, vulnerabilities, risk levels and potential controls (cf. Section III-C) in the middle section of the AURUM user interface (cf. Figure 1). In order to support companies already using business process management tools, AURUM allows to import the business processes under consideration as well as the mapping between services and processes from such tools (e.g., Adonis or ARIS).
- Location Model: Based on the data stored in the security ontology, AURUM allows to generate a building map including the location of all assets. In return this model can be used for adding assets to the ontology and, of course, for simulating different scenarios (e.g., for identifying the optimal location for valuable assets). The left section of the AURUM user interface provides an overview of the corporate assets and their location in the building. By selecting one of those assets (or one of the rooms, buildings, sections, etc.), the tool displays a graphical representation of the assets location and connected business processes in the middle section. In analogy to the process model, clicking on one of the assets provides the user with further information on threats (and connected vulnerabilities), risk levels and potential controls (cf. Section III-C) in the right section of the AURUM user interface (cf. Figure 1).

C. Threat and Vulnerability Assessment

A threat requires a threat source and an existing vulnerability to become effective. The threat source can exploit a vulnerability either intentionally or accidentally. The goal of the threat identification step is to determine potential threats and their corresponding threat sources. Common threat sources are natural threats (e.g., earthquakes, floods, wild fire, etc.), human threats (e.g., active network attacks, theft, unintentional data alternation, etc.), and environmental threats (e.g., power failure, water leakage, ...). This step compiles a comprehensive list of potential threats (e.g., as recommended in [20], [4], [3]) that are taken as input for the risk mitigation strategy. In contrast to existing tools, AURUM supports the decision maker to answer the following questions: Which threats threaten critical assets? Which threat is a multiplier (i.e. which threat gives rise to other threats)? Which vulnerabilities have to be exploited by a threat to become effective? The threat tree (located in the right section of Figure 1) shows the potential threats to the selected asset (File Server in our example), including a priori threat probabilities based on the physical location of the organization. By selecting a threat from the tree representation, valuable information such as a threat description in natural language is displayed. Furthermore, affected security attributes (confidentiality, integrity, and availability) are provided. In addition, a threat can be a consequence of other threats (e.g., unauthorized physical access can be the result of a break in or missing key management) and can itself potentate other threats (e.g., break-in gives rise to unauthorized physical access or asset damage). Note, that this step only shows those threats to the risk manager, which are - based on the formal threat descriptions - relevant for the organization. For each threat highly granular vulnerabilities, which a threat could exploit, have been defined and modeled in the ontology. A description of each vulnerability in natural language complements the vulnerability presentation. For each of the vulnerabilities a mitigation control is assigned, thus implementing a control closes a vulnerability. To enhance the understanding, each control is enriched by a natural language description. With these functions in place, a user knows exactly how to protect his organization from specific threats: mitigating vulnerabilities by implementing recommended controls. Up to the current point the decision



ent:FileServer	0 <> 22
R - sec:ITComponentsDamage	0 <> 20
R - sec:AssetLoss	0 <> 22
T - sec:ITComponentsDamage	28 <> 61
T - sec:Fire	17 <> 50
T - sec:LightningImpact	0 <> 33
T - sec:UnauthorizedPhysicalAccess	9 <> 42
T - sec:AssetLoss	32 <> 65
T - sec:AssetDamage	28 <> 61
T - sec:Theft	13 <> 46
Control Combination	67 <> 100
ent:LightningArrester	67 <> 100
Control Combination	67 <> 100
ent:EntryCheckpoint	67 <> 100
ent:SecurityGuard	0%
Control Combination	34 <> 67
ent:AccessSystem	34 <> 67
Control Combination	0%
ent:SafetyDoor	0%
Control Combination	0%
ent:FireExtinguisher	0%
Control Combination	0%
ent:LockedDoorsPolicy	0%
Control Combination	0%
ent:AntiTheftDevice	0%

Fig. 1. Side-by-Side View: Process Model and Physical Model

maker is aware of the considered system, potential threats and corresponding vulnerabilities, which allow threats to become effective. The control analysis step determines which controls (either technical such as encryption mechanisms, or nontechnical controls such as security policies) are already in place and which controls exist to mitigate the probability that a threat exploits a certain vulnerability (e.g., the threat *break-in* exploits the vulnerability *No Intrusion Alarm System* which could be mitigated by the installation of an *intrusion alarm system* and an *intrusion detector* (motion detector, glass break sensor, or heat detector) in every section). To facilitate the aspect of automatic compliance checks regarding our defined mitigation controls, each control further incorporates formal implementation descriptions. The implementation area shows the actual implementation measures for a control. The underlying formal control descriptions can be executed as rules against the organizations concrete modeled environment to identify which parts of the building are in compliance. The compliant parts of the building are displayed using the location model (cf. Section III-B).

D. Risk Determination

This phase comprises the determination of the probability of a threat exploiting a certain vulnerability in the given system. The subsequent impact analysis determines the impact on the organization's ability to perform its mission, if a threat should successfully exploit a certain vulnerability. By combining the threat probability with the magnitude of the impact the organization is able to determine the risk level and thus to plan the necessary actions. In contrast to other approaches (cf. [20], [25]), our approach focuses on an automated support utilizing the developed knowledge base and the defined relationships. Probability determination is concerned with the probability that a threat exploits a certain vulnerability within the given system. Therefore, the organization has to deal with the following factors: (1) motivation and capability of the threat agent in the case of deliberate threat origin, (2) nature of the vulnerability, and (3) effectiveness of existing control implementations. We utilized the following algorithm to establish - based on the security ontology - a Bayesian threat probability determination net to obtain asset- and organization-specific threat probabilities: (1) the security ontology is queried to obtain those threats which directly threaten the considered asset, (2) to generate an asset-specific threat net we obtain for each threat recursively its predecessors, (3) for each threat in the established threat net we determine the corresponding vulnerabilities, (4) for each vulnerability we determine those controls which are able to mitigate the considered vulnerability, and (5) for each control we determine those inventoried assets which are able to protect the considered asset regarding the formal control implementation specification. After setting up the threat probability determination net the asset-specific threat probability of a specific threat can be calculated by the following calculation schema (bottom-up): (1) to determine the exploitation probability of each vulnerability two contrasting factors are taken into consideration: (a) the a priori probability of the corresponding threat (in the case of accidental threat sources) or the effectiveness of a potential attacker (in the case of deliberate threat sources), and (b) the effectiveness of existing control implementations which lower the original a priori vulnerability exploitation probability (e.g., an implemented fire extinguishing system which protects the considered asset against the fire threat), and (2) the vulnerability exploitation probabilities are combined together with the predecessor threat probabilities to the final posterior threat probability. The state of each node in the Bayesian network is determined by the numerical state of its predecessors and their corresponding weights. Except for the control combination effectiveness nodes, the state of each node in the network is represented by a distribution among a qualitative state set (e.g., High, Medium, and Low) represented by positive numerical values (e.g., 1, 2, and 3). To express their contradictory effect the states of control combination effectiveness nodes are represented by negative numerical values (e.g., -1, -2, and -3). Note that each threat probability is calculated for each asset, since the determination of already implemented controls is always bound to the considered asset. To get a specific threat probability over the entire organization, the individual threat probabilities per asset are aggregated. Thus, our approach enables the risk manager to deal with an overall and asset-specific risk, if necessary. The AURUM tool provides information on an asset's risk when the decision maker selects a certain assets in the process model or the location model. In the next step we focus on the impact: instead of rating the impact of each threat directly, which includes understanding the threat in detail, knowing the threatened assets and all implications on business processes and then deciding on the aggregated impact, we reduced the problem to rating the impact for each asset independent of specific threats. Thus, for each asset the impact in case of loss of availability, loss of confidentiality and loss of integrity are rated separately by the information and technology owners in terms of High, Medium and Low (cf. [20] for a detailed description of these categories). Due to the semantic relations between a threat and threatened asset classes, we automatically obtain a collection of concrete threatened assets in an organization (taken from the inventoried assets, cf. Section III-B). As each threat targets specific security attributes, we gather the affected impact values of the threatened assets. By iterating all threats, we calculate the individual risk for each threatened asset by multiplying the probability with the impact. These asset bound risk levels (cf. Figure 1) are required in the subsequent control recommendation step as countermeasures could be required individually for each asset.

E. Control Evaluation and Implementation

This step involves the evaluation of the identified controls or combinations thereof regarding their cost/benefit ratio. Those controls which are suitable to mitigate the risk to an acceptable level at the lowest possible costs are incorporated in the control implementation plan. At this point management knows which risks are not acceptable for the organization and therefore, measures have to be taken (in terms of controls which could mitigate or eliminate the identified risks). For each vulnerability, appropriate controls are identified, taken from best practice standards such as the German IT Grundschutz Manual. Offering these controls equips the decision makers with effective countermeasures to lower the risk level and thereby protect their business. As controls only provide information on the class of safeguards that should be used (e.g., Fire Extinguisher), instances must be identified that are finally implemented into the organization. Therefore, potential control implementations are evaluated according to a set of defined resource- and benefit categories (e.g., costs, effectiveness, reliability) in order to precisely target the company's specific business needs in line with economic demands. This analysis does not only consider cost and benefit in monetary terms but includes non-financial objectives. All potential controls identified in the previous step are rated against the chosen criteria using data from the security ontology. Using the potential controls and their ratings in each category as input, all Pareto-efficient combinations of safeguards are determined (i.e., there is no other solution with equally good or better values in all objectives and a strictly better value in at least one objective). All solutions taken into consideration have to be feasible with respect to two sets of constraints: The first set relates to limited resources (e.g., development costs or maintenance costs). The second set ensures that at most a maximum – or at least a minimum – number of safeguards from given subsets (e.g., from a certain type of safeguards such as firewalls) is included in the feasible solutions. Decision makers are often overwhelmed with the high number of solution alternatives and are often not aware if their investments into security are appropriate or effective at all. Therefore, AURUM provides an interactive interface that offers the decision maker information on the specific selection problem while the system ensures that the final solution will be an efficient one. The decision makers learn about the consequences of their decisions and get information on the gap (in each category) between the existing solution and the potential solutions. We are using a search based procedure, which starts from an efficient portfolio and allows the decision maker to iteratively "move" in solution space towards more attractive alternatives until no "better" portfolio can be found (cf. [26]). Our approach is based on interactive modifications of lower and upper bounds for one or more objectives. The tool starts with displaying bars representing resource and benefit categories that are assigned with units. Whereas, the bars needed for the interactive selection are shown in the middle section of the AURUM user interface, information on the selected criteria, dependencies between controls, limits and the safeguards contained in the currently selected portfolio are presented to the decision maker in the right section. Two movable horizontal lines with small arrows at one side represent lower and upper bounds and are intended to restrict the set of remaining solutions in a step-by-step manner (e.g., by raising the minimum bound in one of the objectives) or for expanding it (e.g., by once again relaxing some bounds) according to the decision makers' preferences. In all of these cases, the system provides immediate feedback about the consequences of such choices in terms of the remaining alternatives. In further iterations, the decision maker continues playing with minimum and maximum bounds and by doing so can learn about the consequences of his decisions and, thus, gain a much better "feeling" for the problem in terms of what can be achieved in some objectives at what "price" in terms of opportunity costs in other objectives. After several cycles of restricting and once again expanding the opportunity set, the decision maker will finally end up with a solution alternative that offers an individually satisfying compromise between the relevant objectives. Note that he does not need to explicitly specify weights for objectives nor to specify the form of his preference function or to state how much one solution is better than another during any stage of the whole procedure. Instead, ample information on the specific selection problem is provided to him and the system ensures that the final solution will be an optimal (i.e., Pareto-efficient) one, with no other feasible solution available that is "better" from an objective point of view.

IV. Conclusions

Companies consider security as one of the most important issues on their agenda, because the increasing number of security breaches poses a major threat to the reliable execution of corporate strategies and may have negative effects on business value. Risk management ensures the consideration of a broad range of possible threats and vulnerabilities, as well as the valuable assets. Existing approaches such as best-practice guidelines, information security standards, or domain experts but also risk management approaches that are highly accepted within the community come with shortcomings. This paper presented a methodology for supporting information security risk management and provides, compared to existing solutions the following benefits: (1) the ontological information security knowledge base ensures that the information security knowledge is provided in a consistent and comprehensive way to the risk manager, (2) modeling the organization's assets within our ontological framework ensures that assets are modeled in a consistent way, (3) the incorporation of existing best-practice guidelines and information security standards ensures that only widely accepted information security knowledge is used for threat/vulnerability identification and control recommendations, (4) the proposed Bayesian threat probability determination ensures that the threat probability determination is based on a more objective level, compared to existing approaches, (5) threat impacts can be automatically calculated after assets have been rated initially, (6) controls to reduce risks to an acceptable level are offered automatically, (7) the use of interactive decision support allows decision makers (e.g., the risk manager) to investigate various scenarios and, thus, to learn about the characteristics of the underlying problem, while the system guarantees that only efficient solution can be selected, and (8) by considering multiple objectives and providing a gap analysis we support decision makers in getting a much better "feeling" for the problem in terms of what can be achieved in some objectives at what "price" in terms of opportunity costs in other objectives.

V. Acknowledgments

This work was supported by grants of the Austrian Government's FIT-IT Research Initiative on Trust in IT Systems under the contract 813701 and was performed at the Research Center Secure Business Austria funded by the Federal Ministry of Economics and Labor of the Republic of Austria (BMWA) and the City of Vienna.

References

[1] L. Gordon, M. Loeb, W. Lucyshyn, and R. Richardson, "CSI/FBI Computer Crime and Security Survey," September 2006.

[2] M. Bishop, "What is computer security?" *IEEE Sec. Priv. Mag.*, vol. 1, no. 1, pp. 67–69, Jan.-Feb. 2003.

[3] BSI, "IT Grundschutz Manual," 2004. [Online]. Available: http://www.bsi.de/english/gshb/manual/download/index.html

[4] DCSSI, "Expression des Besoins et Identification des Objectifs de Scurit (EBIOS) - Section 2 - Approach," General Secretariat of National Defence Central Information Systems Security Division (DCSSI), 2004.

[5] M. Vitale, "The growing risks of information systems success," *MIS Quarterly*, vol. 10, no. 4, pp. 327–334, December 1986.

[6] W. Baker and L. Wallace, "Is information security under control?: Investigating quality in information security management," *IEEE Security and Privacy*, vol. 5, no. 1, pp. 36–44, 2007.

[7] R. Baskerville, "Information systems security design methods: Implications for information systems development," *ACM Computing Surveys*, vol. 25, no. 4, pp. 375–414, December 1993.

[8] ISO/IEC "27001:2005, Information technology - Security techniques - Information security management systems - Requirements," 2005.

[9] W. Baker, L. Rees, and P. Tippett, "Necessary measures: metric-driven information security risk assessment and decision making," *Communications of the ACM*, vol. 50, no. 10, pp. 101–106, 2007.

[10] C. D. Ittner and D. F. Larcker, "Coming Up Short On Financial Measurement," *Havard Business Review*, vol. 81, no. 11, 2003.

[11] D. M. Lander and G. E. Pinches, "Challenges to the practical implementation of modelling and valuing real options," *The Quarterly Review of Economics and Finance*, vol. 38, pp. 537–567, 1998.

[12] M. Stallinger, "IT-Governance im Kontext Risikomanagement," Ph.D. dissertation, Johannes Kepler Universitt Linz, 2007.

[13] FIPS, "Guideline for automatic data processing risk analysis," National Bureau of Standards, Federal Information Processing Standards Publications (FIPS PUB) 65, August 1975.

[14] R. Rainer, C. Snyder, and H. Carr, "Risk analysis for information technology," *Journal of Management Information Systems*, vol. 8, no. 1, pp. 129–147, Summer 1991.

[15] T. Finne, "A conceptual framework for information security management," *Computers & Security*, vol. 17, pp. 303–307, 1998.

[16] L. Gordon and M. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, November 2002.

[17] H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating it security investments," *Communications of the ACM*, vol. 47, no. 7, pp. 87–92, 2004.

[18] L. Bodin, L. Gordon, and M. Loeb, "Information security and risk management," *Communications of the ACM*, vol. 51, no. 4, pp. 64–68, April 2008.

[19] B. Farquhar, "One approach to risk assessment," *Computers and Security*, vol. 10, no. 10, pp. 21–23, February 1991.

[20] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930, NIST Special Publication 800-30, July 2002.

[21] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE approach," Carnegie Mellon - Software Engineering Institute, Pittsburgh, PA 15213-3890, Tech. Rep., August 2003.

[22] ISO/IEC "27005:2007, Information technology - Security techniques - Information security risk management," 2007.

[23] A. Ekelhart, S. Fenz, T. Neubauer, and E. Weippl, "Formal threat descriptions for enhancing governmental risk assessment," in *Proceedings of the First International Conference on Theory and Practice of Electronic Governance*. ACM Press, 2007.

[24] T. Neubauer, A. Ekelhart, and S. fenz, "Interactive selection of iso 27001 controls under multiple objectives," in *Proceedings of the 23rd International Information Security Conference*, 2008.

[25] T. R. Peltier, *Information Security Risk Analysis*, 2nd ed. Auerbach Publications, 2005.

[26] T. Neubauer and C. Stummer, "Interactive decision support for multiobjective cots selection," in *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, no. 01, 2007.