Workshop-based Multiobjective Security Safeguard Selection

Thomas Neubauer
Institute of Software Technology
and Interactive Systems
Vienna University of Technology, Austria
Email: neubauer@ifs.tuwien.ac.at

Christian Stummer
School of Business, Economics,
and Statistics
University of Vienna, Austria
Email: christian.stummer@univie.ac.at

Edgar Weippl
Institute of Software Technology
and Interactive Systems
Vienna University of Technology, Austria
Email: weippl@ifs.tuwien.ac.at

Abstract— **Companies spend considerable amounts of resources on minimizing security breaches but often neglect efficient security measures and/or are not aware whether their investments are effective. While security safeguards traditionally are evaluated through a single (aggregated) criterion such as the return on investment, this may not suffice any longer as economic and legal requirements force top management to pay more attention to security issues. Thus, there is a demand for decision support tools that assist decision makers in allocating security safeguards with respect to multiple objectives of the involved stakeholders. This paper proposes a tool called MOS^3T (Multi-Objective Security Safeguard Selection Tool), that integrates ideas from multiobjective decision making in a workshop environment. The stepwise procedure for the assessment and interactive selection of sets of security safeguards improves security awareness of top management while minimizing the resources required for implementing a proper security environment that meets a corporate's needs.**

I. Introduction

Security hazards such as viruses, hacker attacks or data theft pose major threats to corporate assets and may directly effect profit, shareholder value and/or a company's reputation [1], [2], [3]. Therefore computer systems, networks, and confidential data need to be protected by proper security safeguards such as access control, firewalls or virus scans. This particularly holds for IT-driven companies like banks and insurance companies. Recent virus attacks revealed the vulnerability of professional e-business environments where the Love Bug virus provides an illustrative example with an estimated economic impact of up to $ 8.7 billions [4]. Hackers, on the other hand, not only cause costs for theft, for recovery and for loss of business value, but are also responsible for a considerable decline of a firm's reputation and its customers' confidence. Companies therefore spend significant amounts of resources on security (note that the worldwide revenue for security product and service vendors is assumed to reach $ 21.1 billions in 2005), but more often than not neglect to seriously engage in developing holistic security measures [5]. Corporate decision makers such as the CSO, CPO or CIO are faced with a wide spectrum of potential risks on the one hand and a plenitude of security safeguards on the other hand. By selecting the most appropriate set of measures and, thus, setting the right level of security-investments, they have to take into consideration

- multiple objectives that are often mutually exclusive such as the minimization of costs and the maximization of protection,
- different and changing preferences of several stakeholders,
- the necessity of maintaining existing business processes,
- a cost-efficient usage of the available resources, and
- the maximization of shareholder value and of their trust in the company.

In addition, managers are confronted with new legal requirements such as those imposed by the Sarbanes-Oxley Act [34] or the Gramm-Leach-Bliley Act [6]. The latter demands the security and confidentiality of customer records and information, the protection against any anticipated threats or hazards to the security or integrity of such records and the protection against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. Further, companies strive for cost-conscious solutions, but nevertheless they frequently are not aware of their level of spending on security and/or, even more important, whether their investments into security are effective. Since safeguards more often than not are triggered by immediate local needs, potential synergy effects are neglected and the efficiency of the installed measures turns out to be questionable at least. That may be the reason why IT security is sometimes seen only as an expense that brings little tangible benefit and is assumed to add no value to the business [3], [7]. The resulting lack of security awareness and poor commitment of the top management [8] may be addressed by expressing concepts of IT security in ways managers can relate to [7] and to provide professional support and structured methods; for an overview of the practice in risk management in small and medium enterprises (SME) cf. Weippl and Klemen [9].

Project evaluation traditionally aims at evaluating security safeguard candidates through a single (aggregated) indicator criterion such as the return on investment. However, it is not always practicable to aggregate measures from different dimensions and, moreover, stakeholders usually differ considerably in their preference functions, i.e. in their individual perception of the value of an additional unit of criterion "A" when trading it for one or more units of a criterion "B".

Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)
0-7695-2567-9/06 $20.00 © 2006 IEEE

IEEE COMPUTER SOCIETY

In this situation stakeholders need much better support to deal with the complex matter. Existing approaches mainly consider quite specific, “local” problems: Methods from risk management [10], for example, provide support to assess security infrastructure whereas workshop environments are focused on elaborating expertise of decision makers, e.g. for defining requirements [11]. Further, many available cost-benefit approaches primarily consider cost issues but often neglect benefits. And finally, interesting methods based on decision theory may support decision makers in selecting portfolios of measures with respect to resource constraints [12], but lack the required insight in security safeguard selection.

This paper proposes an approach that combines the advantages of the above-mentioned approaches within a workshop environment. It provides a structured and repeatable process that includes

- defining evaluation criteria according to the corporate strategy,
- assessing and/or refining the existing IT security infrastructure (assets, threats, vulnerabilities and potential safeguards),
- identifying the stakeholders preferences (risks, boundaries),
- determining the solution space of all efficient (Pareto-optimal) safeguard portfolios, and
- interactively selecting the individually “best” safeguard portfolio.

The approach further takes into account interdependencies between security safeguards, provides an environment for multiple users and is repeatable due to its straightforward structure. The integration of existing approaches from risk management to a moderated workshop environment provides a method for cooperatively selecting an optimal set of safeguards according to company-specific objectives. The moderator provides advice and professional support during the workshop and, thus, contributes to increase the level of security awareness of the participants. And the interactive selection allows decision makers to “playfully” explore the solution space of efficient portfolios until they find one that matches their preferences.

The remainder of this paper is organized as follows. After a brief discussion of related work in Section II and an overview of the proposed workshop procedure in Section III, we provide a step-by-step description of the process in Section IV. This is followed by the formulation of the underlying mathematical programming model in Section V and a numerical example in Section VI. The paper finishes with conclusions and an outlook to further research.

II. Related Work

A. Security Risk Management

The basis for risk management is the definition of a security policy by the management. A security policy is *a set of security-motivated constraints, that are to be adhered to by, for example, an organization or a computer system* [13]. In many application scenarios dependability is equally important as security. Dependability comprises five attributes (availability, reliability, safety, integrity and maintainability) [13], whereas security is usually defined as CIA (confidentiality, integrity and availability) [13], [14], [15], [16]. The process of risk management consists of five steps [17]: Security Policy Definition; Risk Assessment, Safeguard Selection, Safeguard Implementation, Monitoring (cf. Figure 1). The first step after defining the corporate security policy is the risk assessment whereby the

- assets worth protecting, threats and vulnerabilities are defined,
- all potential safeguard are identified and listed,
- the risk is quantified by analyzing the probability of occurrence and the consequence (impact) of occurrence, and, finally,
- ways to handle the risk are evaluated (i.e., they can be reduced, avoided, transferred, or accepted [18]).

This process allows to model the existing security infrastructure and therefore the existing degree of protection [10].

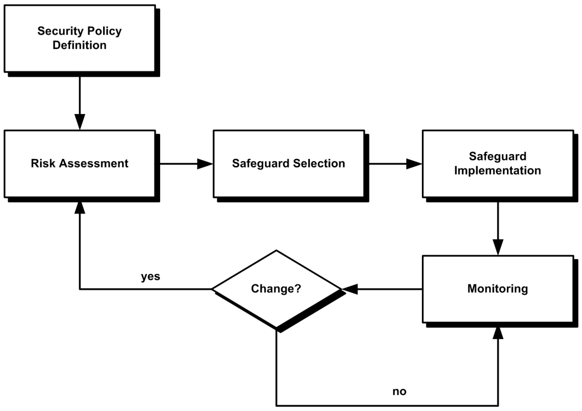


Fig. 1. Risk Management Life Cycle

The data collected during risk assessment serves as the basis for the selection of appropriate safeguards. Finally, the selected safeguards must be implemented and additional methods for monitoring the operational use of the safeguards must be introduced. This allows the continuous improvement of the implemented safeguards. Adaptations of the existing environment will take place after a re-assessment.

B. Decision Support for Security

Literature on approaches applying methods from decision theory to security management is rather rare. Many existing approaches focus on the application of decision making processes to intrusion detection systems (IDS) or intrusion prevention systems (IPS). This also holds for Gao et al. [19] whose IDS focuses on the prediction of attacks. They combine the prediction data from the hidden Markov model with a fuzzy algorithm and deliver the prediction for various attack types. A game theoretic approach is presented by Alpcan and Basar [20] who use cooperative game theory for analysis and configuration purposes and, additionally, bring a two-person finite game into play when modeling the interaction between the IDS and the attacker. Next, Cuppens et al. [21], [22] present a data-based approach using logical representations of intrusions and countermeasures. Their LAMBDA (Language to Model a database for Detection of Attacks) aims at building libraries of attacks and countermeasures in order to later-on use anti-correlation when searching for a proper combination of responses to a given threat. And Mu et al. [23] propose the use of fuzzy cognitive maps (FCM) for selecting countermeasures in an IDS where FCMs are knowledge networks that combine fuzzy logic with neural networks and cognitive maps thus allowing the computation of imprecise information and also the memorizing of attack patterns.

Other approaches focus on the development of methods for selecting (portfolios of) security safeguards where Butler et al. [24] provide a typical example. Note that their procedure was initially intended for software testing purposes and not before later extended to selecting and combining countermeasures (cf. [25]). Improving security architectures is strived for by Liu et al. [26] who for this purpose use a neural networks as well as data from previous security incidents. For the Security Attribute Evaluation Method (SAEM) as a means for cost-benefit analysis of security and selection of risk-mitigating steps confer to Butler [27]. And Fahramand et al. [28] introduce a model for managing vulnerabilities of information systems with the focus on the classification of threats and the management of confidentiality, integrity and availability. Further approaches stem from Guan et al. [29], who apply methods from multicriteria decision support to risk management, Gupta et al. [30], who propose a decision support approach based on a genetic algorithm for security portfolio selection, and Strauss and Stummer [31], who introduce a two-step interactive multiobjective decision support approach for selecting portfolios of measures in IT-risk management.

III. Overview of MOS^3T

This paper proposes a workshop procedure for the risk assessment and the selection of security safeguards called MOS^3T (Multi-Objective Security Safeguard Selection Tool). MOS^3T is an integral part of a research roadmap defining “Secure Business Process Management” [32]. The structured and systematic process of a workshop is used to define the need and scope of IT security measures and to reduce the decision complexity. The workshop is designed as a full day meeting being split into two parts. The first part consists of the assessment of the existing security environment and the subsequent generation of promising safeguards portfolios. In the second part of the workshop the number of these portfolios is iteratively reduced until the portfolio is identified that best fits the stakeholders’ notions. The entire workshop is supported by a tool we have implemented. Details on how the tool supports the process are provided in the next section. An additional benefit lies in the fact that the entire process is automatically documented as required by various standards such as ISO17799 [33]. Note that prior to starting with the workshop the following prerequisites must be fulfilled:

- Based on the corporate strategy and the security policy the focus of the workshop has to be defined. This step includes the pre-selection of objectives that are used for valuating security safeguards.
- To the end of ensuring multidisciplinarity, security experts from different areas of the company should be involved in the workshop process. In addition the management must show its commitment by participating in the workshop as well. Potential further participants are process managers, security managers, human resource managers and key users.

IV. The MOS^3T Workshop Process

In this section the workshop process is described in more detail. Figure 2 shows an overview of the six steps of the workshop each with three phases, where all values marked with an asterisk are estimates. In step “Risk compilation” in the third Phase and in all steps of Phase 6 the workshop moderator is supported by our system. All ”Selection” steps are performed by the moderator in cooperation with the workshop team whereas the workshop team goes through the remaining steps by itself (but once again being supported by our tool).

A. Step 1: Definition of Benefit and Resource Categories

In the *first step* of the workshop the stakeholders have to appoint benefit and resource categories. The definition of these categories relate to the preferences of the stakeholders and the intended output of the workshop. Especially in the context of IT-systems the attainment of the security attributes (CIA) will be a major goal of the management. For example, a hacker who attacks and crashes a server reduces the availability of this server. If there is no appropriate backup system the crash of the server will have a major impact on the efficiency of the department or even the whole company. The loss resulting from a stop of the business process that is supported by the crashed server will affect the decision to buy a backup system. On the other hand, the server might be used for less important tasks and thus be of no importance for the reliable execution of an essential corporate business process. In this case the costs of implementing a backup system might exceed the potential benefits resulting from a reduced loss. The proposed workshop supports decision makers in defining an optimal set of security safeguards according to the corporate strategy and the security policy. Therefore, benefit and resource categories have to be derived from the given corporate strategy. A company in the financial sector might focus on maximizing confidentiality and availability whereas a low cost company will rather focus on the minimization of the resource categories such as costs. Thus the output of this phase are the definition of relevant resource and benefit categories. The existing security infrastructure has to be valued according to the defined categories. Therefore, the number of categories should also correspond with the resources (particularly time and budget) that are available for the workshop. A basic scenario can already be performed by using two traditional criteria such as cost and benefit that are

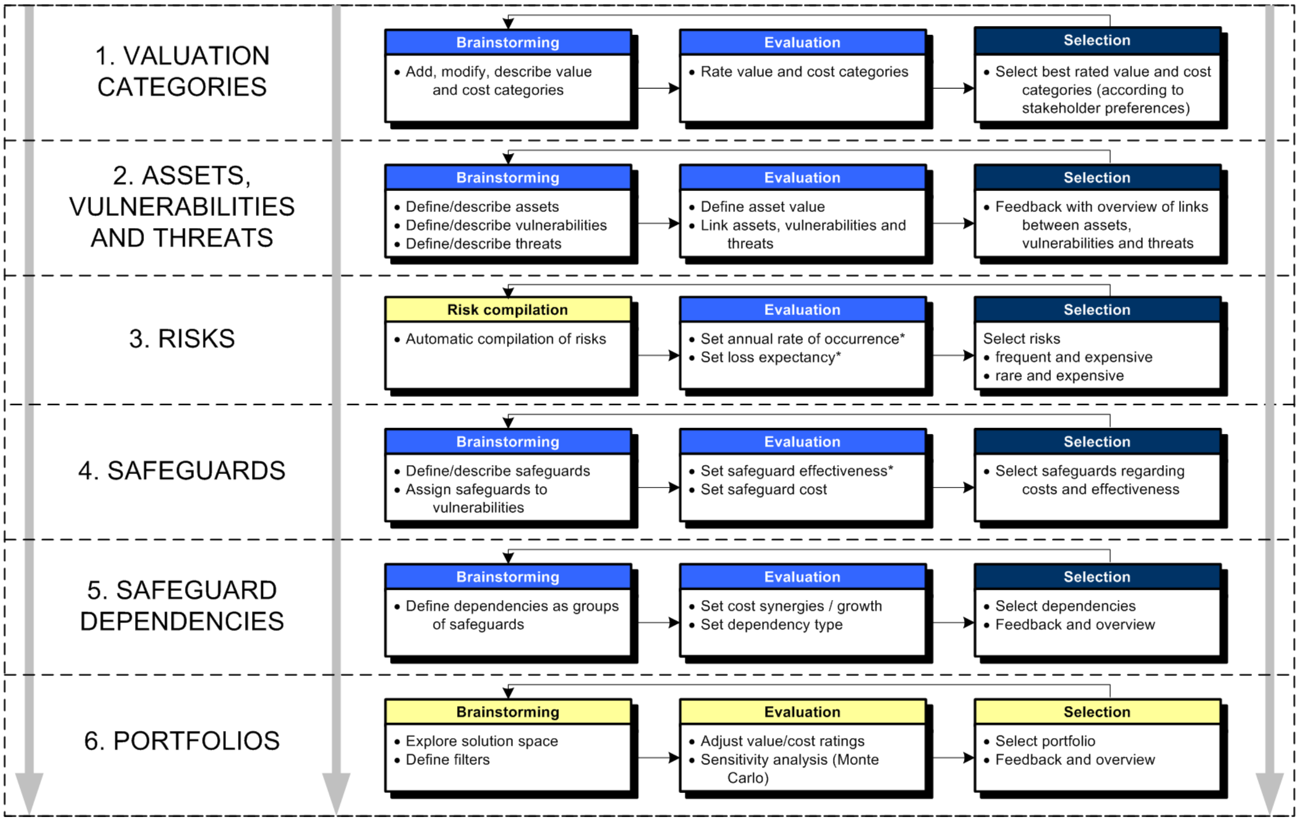

1. VALUATION CATEGORIES
Brainstorming
• Add, modify, describe value and cost categories
Evaluation
• Rate value and cost categories
Selection
• Select best rated value and cost categories (according to stakeholder preferences)
2. ASSETS, VULNERABILITIES AND THREATS
Brainstorming
• Define/describe assets
• Define/describe vulnerabilities
• Define/describe threats
Evaluation
• Define asset value
• Link assets, vulnerabilities and threats
Selection
• Feedback with overview of links between assets, vulnerabilities and threats
3. RISKS
Risk compilation
• Automatic compilation of risks
Evaluation
• Set annual rate of occurrence*
• Set loss expectancy*
Selection
Select risks
• frequent and expensive
• rare and expensive
4. SAFEGUARDS
Brainstorming
• Define/describe safeguards
• Assign safeguards to vulnerabilities
Evaluation
• Set safeguard effectiveness*
• Set safeguard cost
Selection
• Select safeguards regarding costs and effectiveness
5. SAFEGUARD DEPENDENCIES
Brainstorming
• Define dependencies as groups of safeguards
Evaluation
• Set cost synergies / growth
• Set dependency type
Selection
• Select dependencies
• Feedback and overview
6. PORTFOLIOS
Brainstorming
• Explore solution space
• Define filters
Evaluation
• Adjust value/cost ratings
• Sensitivity analysis (Monte Carlo)
Selection
• Select portfolio
• Feedback and overview

Fig. 2. The MOS^3T Workshop

measured in terms of monetary units. Note that categories are not limited to monetary value and can also comprise non-monetary aspects such as a company's image or manpower.

B. Step 2: Assets, Vulnerabilities and Threats

Based on the benefit categories defined in the first step of the workshop the assets worth being protected as well as potential threats must be identified in the *second step*. Usually this data is collected prior to the workshop and refined and prioritized in this step of the workshop. Assets such as servers, confidential information or business processes can be affected by threats or sequences of threats. Therefore, the value of an asset might be reduced by the occurrence of a threat. A threat such as a hacker, a virus or a thief exploits vulnerabilities for compromising assets, e.g. a server can be attacked by a hacker if ports are left open. Therefore threats *and* vulnerabilities must be considered in the risk assessment process because a security breach can only arise if both threats and vulnerabilities exist. A computer without access to the Internet is not exposed to the threat of an outside hacker attack because there is no related vulnerability. For defining a threat scenario a particular asset has to be related to a particular vulnerability and a particular threat. In the proposed workshop approach assets and threats as well as vulnerabilities are assessed independently where assets are connected with potential security threats through vulnerabilities.

C. Step 3: Risk Generation and Quantification

After completing the above assessment all asset-threat-vulnerability combinations are generated. A security risk corresponds to the potential that a given threat will exploit vulnerabilities to cause damage to an asset or a group of assets. The formal definition of risk can be calculated as the Cartesian product of assets, threats and vulnerabilities. It has to be considered that not all combinations are possible, e.g. the theft of a server by exploiting weak passwords. The latter combinations are therefore discarded. Each risk is assigned an annual rate of occurrence (ARO) representing the estimated number of times a threat on a single asset is estimated to occur. A rate of 0.1 describes a risk occurring once in 10 years while a rate of 10 means that a risk is supposed to occur ten times a year.

D. Step 4: Safeguards

In this step the potential safeguards are defined. Safeguards consume resources but also reduce the potential damage when a vulnerability is exploited by a threat. The benefits of safeguards are implicitly calculated by considering the saved costs that arise in each benefit category as a result of the installation of safeguards. Nevertheless, only few safeguards provide absolute security; usually they only reduce the rate of occurrence and/or the impact. Naturally the effectiveness of different safeguards varies, e.g. a corporate fire brigade will have a higher effectiveness than the installation of fire extinguishers. Therefore their efficiency needs to be defined independently for each safeguard. Note that we take into consideration only efficient safeguard, i.e. those for which the resulting benefits of risk reduction exceed the implementation cost. Risk can be handled by reducing, avoiding, transferring or accepting it [18]. The MOS^3T model does not explicitly differentiate between these types of risk handling; this distinction is addressed implicitly by the choice of the safeguard. For instance, the safeguard of installing a firewall would reduce the risk, an insurance would transfer the risk.

E. Step 5: Safeguard Interactions

In this step, interactions between safeguards are defined. Thus, decision makers can model that certain safeguards should only be applied in combination (e.g. firewall and virus scan) and/or that their combination yields synergy effects (e.g. the implementation of a combined anti virus and firewall tool might reduce the costs compared to the separate implementation of these safeguards). Other safeguards are mutually exclusive (e.g. in general a combined anti virus and firewall tool will not be implemented in parallel to another anti virus tool) or cause cannibalism effects. In the proposed model four different types of dependencies and interactions are defined:

- Interaction (min): Based on a given number of safeguards a portfolio has to include *at least* the specified number of safeguards.
- Interaction (max): Based on a given number of safeguards a portfolio has to include *at most* the specified number of safeguards.
- Interdependency (min): If a portfolio contains *at least* a specified number of safeguards synergy effects can be realized. For this purpose the values of each cost and benefit category can be adapted.
- Interdependency (max): If a portfolio contains *at most* a specified number of safeguards synergy effects can be realized. For this purpose the values of each cost and benefit category can be adapted.

F. Step 6: Portfolio Selection

Data collected during security assessment in Steps 1 through 5 is used in Step 6 as input for determining efficient safeguard portfolios. To this end, a complete enumeration procedure is applied that for each potential portfolios (i.e., each combination of safeguards) aggregates total costs and benefits for each category, e.g. the total installation costs of all safeguards in a certain portfolio or the total benefits realized by installing all safeguards of a certain portfolio. If the portfolio is feasible (i.e., it does not require more resources than being available and it does not violate a critical dependency between safeguards), it will be checked whether it is Pareto-optimal (nondominated) with respect to all other feasible portfolios. Note that this procedure may become time-consuming if a high number of safeguards are involved. In the latter case, the usage of proper meta-heuristic procedures is recommended (cf. [35]). The final selection of an optimal portfolio is made through an interactive module similar to that developed by Stummer and Heidenberger [12] that supports the decision makers in exploiting the solution space of all identified efficient portfolios.

V. The Formal Model

In the following we first describe the formal data representation and then provide an overview on the calculation routine. This model is used in Step 6 for the generation of efficient portfolios.

A. Basic Data

Decision makers have to provide information (definitions) on benefit categories for assets

$$B = \{b_1, \ldots, b_{n1}\},$$

resource (cost) categories for safeguards

$$C = \{c_1, \ldots, c_{n2}\},$$

the sets of assets

$$A = \{a_1, \ldots, a_{n3}\},$$

vulnerabilities

$$V = \{v_1, \ldots, v_{n4}\},$$

threats

$$T = \{t_1, \ldots, t_{n5}\},$$

and potential safeguards

$$S = \{s_1, \ldots, s_{n6}\}.$$

For each defined benefit category of each asset as well as for each defined cost category of each safeguard input data has to be given.
Function VAL then shows the value of asset a in category b

$$VAL(a, b) : A \times B \rightarrow \mathbb{R}^+$$

while COST stands for the costs of safeguard s in category c

$$COST(s, c) : S \times C \rightarrow \mathbb{R}^+.$$

By building the Cartesian product of assets, vulnerabilities and threats the set of risks can be generated

$$R = A \times V \times T.$$

A risk (defined as a tupel)

$$r = (a, v, t)$$

is assigned with an annual rate of occurrence

$$ARO(r) : R \rightarrow \mathbb{R}^+$$

and an exposure factor

$$EXF(r, b) : R \times B \rightarrow \mathbb{R}^+$$

that estimates the exposure of the compromised asset with respect to a benefit category b. Note that function values may differ between these categories, e.g. the attack of an hacker might affect the category "corporate image" with 10% and the category "availability" with 50%. A safeguard s can confine multiple vulnerabilities v. Therefore, the effectiveness of each safeguard is determined through a factor for each of these vulnerabilities and each benefit category b that refers to the potential of reducing an exposure:

$$EFF(s, v, b) : S \times V \times B \rightarrow \mathbb{R}$$

The annual rate of occurrence must take a value greater or equal zero

$$ARO(r) \geq 0$$

and the exposure factor must lie between a value of zero (the asset value is not affected at all) and one (the asset value is completely affected):

$$0 \leq EXF(r, b) \leq 1$$

The effectiveness of a safeguard may reach its maximum value of 1 which indicates that a safeguard completely closes the existing vulnerability. However, it can also take a negative value in case the safeguard is ineffective and even raises the risk for the corresponding benefit category:

$$EFF(s, v, b) \leq 1$$

B. Calculation

The above described data is collected during the risk assessment phase and entered into the system. As a next step the data is used for the calculation of efficient safeguard portfolios. A portfolio can be written as a binary vector

$$\vec{x} = (x_1, \ldots, x_{n6})$$

where $x_i = 1$ if safeguard s_i is included in the portfolio and $x_i = 0$ otherwise. Firstly, for each asset a the expected annual loss (Annual Loss Expectancy: ALE) for each category b before the implementation of safeguards is calculated as

$$ALE(a, b) = VAL(a, b) \cdot \sum_r (EXF(r, b) \cdot ARO(r))$$

by summing up the products of the exposures and the annual rate of occurrence (i.e. the "expected damage potential") for all risks (i.e., combinations of vulnerabilities and threats for a given asset) and multiplying it with the value of the asset.

After the implementation of the safeguards of a specific portfolio $\vec{x}$ the ALE is typically reduced. It is calculated as

$$\begin{aligned}\overline{ALE}(a, b, \vec{x}) = VAL(a, b) \cdot \sum_r (&EXF(r, b) \cdot ARO(r) \cdot \\ &\cdot AEFF(\vec{x}, v, b)),\end{aligned}$$

where function

$$AEFF(\vec{x}, v, b) = 1 - \prod_i (1 - EFF(s_i, v, b) \cdot x_i)$$

stands for the aggregated effectiveness of all safeguards of portfolio $\vec{x}$ for vulnerability v and benefit category b. Note that $EFF(s_i, v, b) = 0$ for all categories b if the safeguard s_i does not hold for the vulnerability. Further, if $EFF(s_i, v, b) < 0$ the safeguard is not efficient and the aggregated effectiveness will be decreased.

Based on the calculation of the ALE before and after the implementation of the security safeguards the total benefit of a security portfolio $\vec{x}$ in a benefit category b can be aggregated over all assets to

$$AGGBEN(\vec{x}, b) = \sum_j \left(ALE(a_j, b) - \overline{ALE}(a_j, b, \vec{x})\right).$$

Analogously total costs of a portfolio $\vec{x}$ in a given cost category are determined as

$$AGGCOST(\vec{x}, c) = \sum_i COST(s_i, c) \cdot x_i.$$

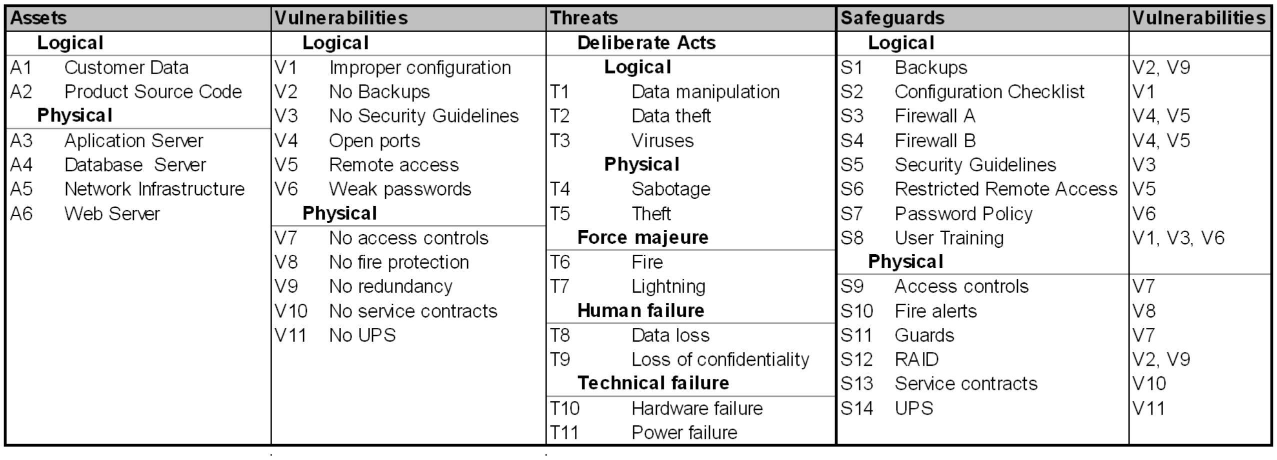
A portfolio is characterized by its vector of safeguards $\vec{x}$ and the aggregated costs and benefits for each category. Based on this data all portfolios that do not meet the defined ranges of minimal benefits or maximal costs are excluded from further consideration. The same holds for portfolios that violate one of the additional constraints defined by the decision makers (e.g., if two mutually exclusive safeguards are both included in a portfolio). Thereafter the complete enumeration procedure is started in order to identify the Pareto-optimal portfolios. They then serve as the basis for the interactive selection of the individually "best" compromise portfolio according to the decision makers preferences (cf. [12]).

VI. Example

We define two benefit categories, namely image value (measured in points) and monetary value (measured in monetary units), as well as the five resource categories of acceptance costs (in points), setup manpower (in persons), running costs (in monetary units), setup time (in hours), and setup costs (in monetary units). Figure 3 provides on overview of the assets, vulnerabilities and threats. In addition, it shows the potential safeguards assigned to the vulnerabilities they reduce.

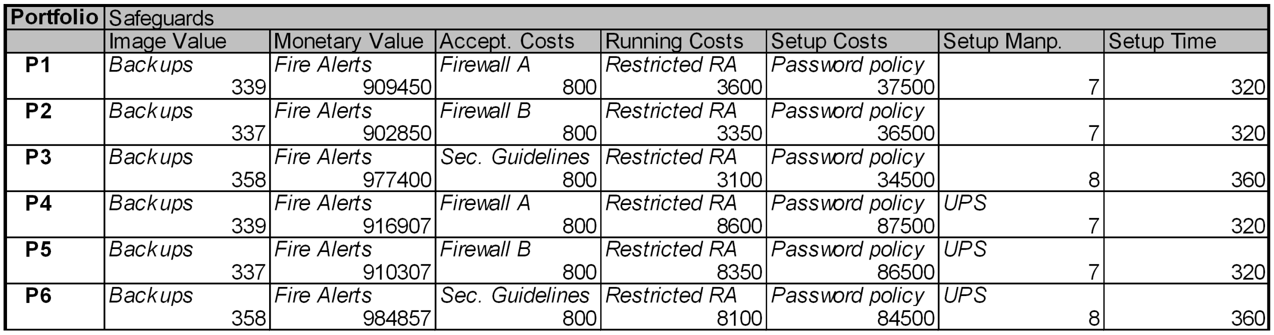
For each risk the annual rate of occurrence and the exposure factors have to be provided. The latter is defined for each benefit category that is affected, e.g. one valid risk is the occurrence of the threat "data manipulation" due to the vulnerability "no access control". The affected asset would be the "database server". In this example we set the ARO for this risk to 1 and the exposure factor for the benefit category "monetary value" to 1000 units (20%) and for the benefit category "image value" to 10 points (10%). After the valuation of the risks the potential safeguards are assigned to the vulnerabilities they affect with a certain effectiveness, e.g. the vulnerability "no backups" can be protected by implementing the safeguard "backups". The safeguard "backups" has an effectiveness of 99% on both benefit categories. Thus, this safeguard can accordingly reduce the potential damage. Finally, the Pareto-optimal portfolios are generated.

In our example the total number of possible portfolios is 16384 (i.e., 2^{14} because 14 potential safeguards are taken into consideration), the number of feasible portfolios turns out to be 4096 while the number of Pareto-optimal portfolios is



Assets		Vulnerabilities		Threats		Safeguards		Vulnerabilities
Logical		**Logical**		**Deliberate Acts**		**Logical**		
A1	Customer Data	V1	Improper configuration	**Logical**		S1	Backups	V2, V9
A2	Product Source Code	V2	No Backups	T1	Data manipulation	S2	Configuration Checklist	V1
Physical		V3	No Security Guidelines	T2	Data theft	S3	Firewall A	V4, V5
A3	Aplication Server	V4	Open ports	T3	Viruses	S4	Firewall B	V4, V5
A4	Database Server	V5	Remote access	**Physical**		S5	Security Guidelines	V3
A5	Network Infrastructure	V6	Weak passwords	T4	Sabotage	S6	Restricted Remote Access	V5
A6	Web Server	**Physical**		T5	Theft	S7	Password Policy	V6
		V7	No access controls	**Force majeure**		S8	User Training	V1, V3, V6
		V8	No fire protection	T6	Fire	**Physical**		
		V9	No redundancy	T7	Lightning	S9	Access controls	V7
		V10	No service contracts	**Human failure**		S10	Fire alerts	V8
		V11	No UPS	T8	Data loss	S11	Guards	V7
				T9	Loss of confidentiality	S12	RAID	V2, V9
				Technical failure		S13	Service contracts	V10
				T10	Hardware failure	S14	UPS	V11
				T11	Power failure			

Fig. 3. Assets, Vulnerabilities, Threats and Safeguards



Portfolio	Safeguards						
	Image Value	Monetary Value	Accept. Costs	Running Costs	Setup Costs	Setup Manp.	Setup Time
P1	*Backups* 339	*Fire Alerts* 909450	*Firewall A* 800	*Restricted RA* 3600	*Password policy* 37500	7	320
P2	*Backups* 337	*Fire Alerts* 902850	*Firewall B* 800	*Restricted RA* 3350	*Password policy* 36500	7	320
P3	*Backups* 358	*Fire Alerts* 977400	*Sec. Guidelines* 800	*Restricted RA* 3100	*Password policy* 34500	8	360
P4	*Backups* 339	*Fire Alerts* 916907	*Firewall A* 800	*Restricted RA* 8600	*Password policy* 87500	*UPS* 7	320
P5	*Backups* 337	*Fire Alerts* 910307	*Firewall B* 800	*Restricted RA* 8350	*Password policy* 86500	*UPS* 7	320
P6	*Backups* 358	*Fire Alerts* 984857	*Sec. Guidelines* 800	*Restricted RA* 8100	*Password policy* 84500	*UPS* 8	360

Fig. 4. Resulting Portfolios

1244. After playing with the system and requiring an image value higher than 320, running costs lower than 20000 and a setup time of less than 400 hours, only six efficient portfolios remain. Decision makers now can investigate them one by one in detail and compare them to each other.

Figure 4 shows the following data for each of the remaining portfolios:

- The safeguards that are included in the portfolio, e.g. Backups, Fire Alerts, Firewall A, Restricted Remote Access and Password Policy in the case of Portfolio 1 (P1).
- The calculated values for each benefit and resource category defined at the beginning of the Workshop, e.g. the costs for implementing the security safeguards of Portfolio 1 (Setup Costs) are 37500.

Although the compositions of remaining portfolios are quite similar, there are considerable differences regarding the costs and the benefits of implementing one of these portfolios. Comparing portfolios P3 and P6 shows a major difference in the categories “Running Costs” and “Setup Costs” when decision makers decide to implement an Uninterruptible Power Supply (UPS). The implementation of portfolio P6 results in costs about 261% higher in category “Running Costs” and about 245% higher in category “Setup Costs” compared to portfolio P3. The resulting benefits of this decision are rather negligible with less than one percent of additional benefit in category “Monetary Value”.

VII. Conclusion

Managers regularly have to cope with a wide spectrum of potential risks and, thus, the decision of selecting the most appropriate set of security safeguards. Moreover, they are challenged by legal and economic requirements. The complexity of finding an “optimal” security level is further increased as decision makers have to deal with multiple, often opposing, objectives, as well as differing preferences of several stakeholders. Workshop approaches have proven to efficiently support stakeholders in decision making. This paper has proposed an approach (MOS^3T) for combining the advantages of workshops with multiobjective decision support and, thus, providing decision makers with a stepwise methodology for the assessment and interactive selection of sets of security safeguards. Due to its straightforward structure the repeatability of the process is ensured. Decision makers are supported by a moderator who provides professional advice during the whole process and reduces the influence of single opinions on the whole decision. And finally, our approach may serve as a valuable tool to improve security awareness of top management as decision makers can run through different scenarios and potential solutions which should decrease the probability to overlook relevant risks.

Further research will be directed to accepting function coefficients that are random variables with approximated probability distributions. Thus, our mathematical program will need to incorporate the concept of stochastic dominance (cf. [36]) which will be achieved by introducing percentiles as additional objectives. This extension will allow to not only take into consideration point estimates or expected values but also uncertain outcomes that are typical for complex environments.

REFERENCES

[1] K. Campbell, L.A. Gordon, M.P. Loeb, and L. Zhou, “The economic cost of publicly announced information security breaches: empirical evidence from the stock market”, *Journal of Computer Security*, vol. 11, pp. 431-448, 2003.

[2] M. Ettredge and V.J. Richardson, “Assessing the risk in e-commerce”, *Proceedings of the 35th Annual Hawaii International Conference on System Sciences, HICSS*, 2002.

[3] W. Alms, “Viren, Würmer, kriminelle Mitarbeiter: Deutschland hat Nachholbedarf bei IT-Security”, *Information Management & Consulting*, vol. 17, 2002.

[4] Computereconomics [online]. Available: www.computereconomics.com

[5] CSO Magazine, “E-crime watch survey 2004”, Carnegie Mellon University Software Engineering Institutes CERT Coordination Center [Online]. Available: www.cert.org

[6] Gramm-Leach-Bliley Act; 15 usc, subchapter i, sec. 6801-6809, 1999.

[7] S. Thorne, “A new vision for IT security in the 90s”, *Sicherheit in Informationssystemen; Proceedings der Fachtagung SIS*, 1994.

[8] F. Romeike, “Integration von e-Business und Internet in das Risk Management des Unternehmens”, *Kommunikation & Recht*, vol. 8, 2001.

[9] E. Weippl and M. Klemen, “Implementing IT security for small and medium-sized enterprises”, *Practice and Experience in Applied Enterprise Information Assurance and Computer Security*, Idea Group, forthcoming, 2006.

[10] T.R. Peltier, *Information Security Risk Analysis*, Auerbach Publications, 2001.

[11] P. Gruenbacher, “Collaborative requirements negotiation with easywinwin”, *IEEE*, pp. 954-985, 2000.

[12] C. Stummer and K. Heidenberger, “Interactive R&D portfolio analysis with project interdependencies and time profiles of multiple objectives”, *IEEE Transactions on Engineering Management*, vol. 50, pp. 175-183, 2003.

[13] A. Avizienis, J.C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing”, *IEEE Transactions of Dependable and Secure Computing*, vol. 1, pp. 11-33, 2004.

[14] M. Bishop, *Computer Security: Art and Science*, Addison-Wesley-Longman, 2002.

[15] C.P. Pfleeger, *Security in Computing*, 2nd ed., Wiley, 1996.

[16] C. Landwehr, A. Bull, J. McDermott, and W. Choi, “A taxonomy of computer program security flaws”, *ACM Computing Surveys*, vol. 26, pp. 211-254, 1994.

[17] C. Strauss, *Informatik-Sicherheitsmanagement*, Teubner, 1991.

[18] D.L. Pipkin, *Information Security: Protecting the Global Enterprise*, Prentice Hall, 2000.

[19] F. Gao, J. Sun, and Z. Wei, “The prediction role of hidden markov model in intrusion detection”, *IEEE Canadian Conference on Electrical and Computer Engineering*, pp. 893-896, 2003.

[20] T. Alpcan and T. Basar, “A game theoretic approach to decision and analysis in network intrusion detection”, *Proceedings of the 42nd IEEE Conference on Decision and Control*, 2003.

[21] C. Cuppens, S. Gombault, and T. Sans, “Selecting appropriate countermeasures in an intrusion detection framework”, *17th IEEE Computer Security Foundations Workshop, CSFW-17*, pp. 78-87, 2004.

[22] F. Cuppens and R. Ortalo, “Lambda: A language to model a database for detection of attacks”, *Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection RAID ’00*, Springer, pp. 197-216, 2000.

[23] C.P. Mu, H.K. Huang, and S.F. Tian, “Fuzzy cognitive maps for decision support in an automatic intrusion detection response mechanism”, *IEEE Cyber Learning and Cybernetics*, 2004.

[24] S. Butler, P. Chalasaniy, S. Jha, O. Raz, and M. Shaw, “The potential of portfolio analysis in guiding software decisions”, *Proceedings of the 21st International Conference on Software Engineering (Workshop on Economics-Driven Software Engineering Research)*, 1999.

[25] S.A. Butler, “Improving security technology selections with decision theory”, *Proceedings of the 23rd International Conference on Software Engineering (Workshop on Economics-Driven Software Engineering Research)*, 2001.

[26] F. Liu, K. Dai, and Z. Wang, “Applying multiple criteria decision making to improve security architecture development”, *ACM Proceedings of the 3rd international conference on Information security*, pp. 244-246, 2004.

[27] S.A. Butler, “Security attribute evaluation method: A cost-benefit approach”, *ACM Proceedings of the 24th International Conference on Software Engineering*, pp. 232-240, 2002.

[28] F. Fahramand, S.B. Navathe, P.H. Enslow, and G.P. Sharp, “Managing vulnerabilities of information systems to security incidents”, *ACM Proceedings of the 5th international conference on Electronic commerce*, pp. 348-354, 2003.

[29] B.C. Guan, C.C. Lo, and P. Wang, “Evaluation of information security related risks of an organization - The application of multi-criteria decision-making method, *IEEE 37th International Carnahan Conference on Security Technology (ICCST)*, 2003.

[30] M. Gupta, J. Rees, A. Chaturvedi, and J. Chi, “Matching information security vulnerabilities to organisational security profiles: a genetic algorithm approach”, *Decision Support Systems*, forthcoming, 2006.

[31] C. Strauss and C. Stummer, “Multiobjective decision support in IT-risk management”, *International Journal of Information Technology and Decision Making*, vol. 1, pp. 251-268, 2002.

[32] T. Neubauer, S. Biffl, Secure Business Process Management: A Roadmap; *Proceedings of the First International Conference on Availability, Reliability and Security ARES 2006*, IEEE CS, 2006.

[33] BS7799 [Online]. Available: http://www.bs7799-iso17799.com

[34] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (July 30, 2002), is a United States federal law also known as the Public Company Accounting Reform and Investor Protection Act of 2002.

[35] C. Stummer and M. Sun, “New multiobjective metaheuristic solution procedures for capital investment planning”, *Journal of Heuristics*, vol. 11, pp. 183-199, 2005.

[36] S.B. Graves and J.L. Ringuest, *Models & Methods for Project Selection*, Kluwer Academic Publishers, 2002.

IEEE COMPUTER SOCIETY