Conceptual Design of a Method to Support IS Security Investment Decisions within the Context of Critical Business Processes

Heinz Lothar Grob, Gereon Strauch and Jan Hermans

European Research Center for Information Systems, University of Muenster
Leonardo-Campus 3, 48149 Muenster, Germany

Abstract. In order to safeguard the compliance of information systems, private enterprises and governmental organizations can implement a large variety of distinct measures, ranging from technical measures to organizational measures. Especially in the context of critical information system infrastructure e.g. data centers, the decision for specific safeguards is complex. An appropriate method for the profitability assessment of alternative IS security measures in the context of critical business processes has not so far been developed. With this article we propose a conceptual design for a method which enables the determination of the success of alternative security investments on the basis of a process-oriented perspective. Within the scope of a design science approach we combine established artifacts of the field of IS security management with those of the field of process management and controlling. On that basis we develop a concept that allows decision-makers to prioritize the investments for dedicated IS safeguards in the context of critical business processes.

1 Introduction

Information Systems (IS) security generally and critical business process specially raised in the past more attention of budget responsible people – visible by the above-average increase of IS security budgets compared to overall IS budgets and the increaing relevance of this research community [1]. In the meantime though, more recent works emphasis the elementary imperative of profitability analyses – despite available findings this field of research are frequently characterized as being vague, unusable or without reference to concrete recommendations for a course of action [2, 3]. In order to conceptualize a method for the decision support for IS security investments in the context of critical business processes, these special challenges need to be considered. The chosen research approach can be characterized as design-oriented, where a conceptual-deductive research method has been applied [4, 5]. A brief overview of the related work in this field shows that the suggested methods do not fit the special requirements in the context of critical processes. Most approaches in context suppose a linear exchange relationship between expected loss and the costs of security measures [6]. This procedure does not apply for information systems, which have a vital meaning for the organization [7]. Our main objective is to provide

Lothar Grob H., Strauch G. and Hermans J. (2008).
Conceptual Design of a Method to Support IS Security Investment Decisions within the Context of Critical Business Processes.
In *Proceedings of the 6th International Workshop on Security in Information Systems*, pages 113-121
DOI: 10.5220/0001741601130121

a method for decision support for security investments within critical infrastructures and to integrate this into an overall IS risk management procedure. So we define requirements in this context and offer an outlook to an approach for controlling security measures for critical business processes and information infrastructures (such as data centers) based on a configurable criteria system. To support the implementation of this method within a management information system, we develop a conceptual model and specify the formal requirements for adequate portfolios of safeguards afterwards. The article concludes with a brief summary and an outlook on future research opportunities.

2 Decision Support for Security Investment within Critical Infrastructures

2.1 Identifying Critical Processes and Aligned Information Systems

IS risk management deals with risks resulting from the usage of information systems in a company. The procedure of tasks is oriented at the general process of risk management as shown in figure 1. Focusing on business processes has been claimed repeatedly for the IS security management to keep the security compliant to the business goals [3, 8, 9]. Critical business processes should lead more the other security management policies than within the scope of "normal" risk disposition and in the same way to other instruments for decision support. Therefore, it is recommended to fulfill different safeguard planning procedures for business processes and associated information systems with normal risk disposition, critical business processes and underlying critical IS infrastructures (e.g. data center). Criticality analysis (CA) or business impact analysis (BIA) are usually carried out within the bounds of risk identification and risk analysis to identify critical business processes and the appropriate information systems (critical IS infrastructure) [10, 11]. We recommend applying established approaches from investment theory to profitability analysis based on process models [12], to information systems with normal risk disposition according to the BSI IT-Grundschutz Methodology. The procedure adjusted for regarding critical processes is shown in figure 1. The critical analysis is an approach for identification of critical business processes [11]. The "Joint Standards" are the accumulation of standards, which were published by the Business Continuity Institute (BCI) and Disaster Recovery Institute International (DRII) [10] for establishing a business impact analysis. Within this analysis, the relevance of business processes is tried to identify. If there are fatal consequences appeared, this process is considered to be critical. In case of critical analysis, business processes and each information system that is to be applied for corresponding process are assigned to different categories.

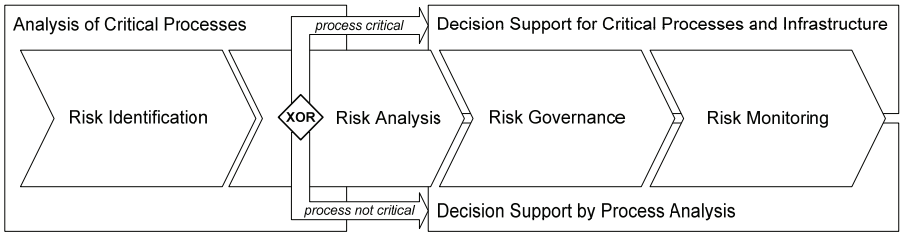

Fig. 1. Procedure model for IS risk management regarding critical infrastructures.

Seibold proposes the classification of processes in 3 to 6 groups [11], it complies with established approaches from theory and practice like IT-Grundschutz-Methodology and BIA [10, 13-17]. In his example he classifies the processes into four classes A-D, where the processes of A class cause fatal consequences in one day, class B – in 3 days and the processes of D class have no fatal consequences at all. The information systems accompanying the critical business processes are called here as critical IS infrastructures [7]. In this context, frameworks for decision support usually do not support differentiated endangerment scenarios. So the selection of safeguards should be supported by a configurable criteria system. The procedure of the configuration, system analysis and the selection of adequate measure are introduced in the following.

2.2 Procedure Model for Decision Support in the Context of Critical IS Infrastructure

The core idea is to select different safeguards with a criteria system that can be configured for the isolated case and its specific context. The criteria system should help selecting necessary safeguards as well as controlling the compliance to a required security level. The use of the criteria catalogue follows itself to a procedure model. The procedural model follows the procedure model of the IT-Grundschutz Methodology and the advanced risk analysis based on BSI standard 100-3 and state of the art risk assessment approaches [14, 15, 18]. One very important extension to common standards is that particular criteria can be defined as absolutely necessary (so-called lethal criteria). In the case of non-fulfilment one of these criteria, the necessary protection of the critical infrastructure as a whole is not guaranteed. At first an analysis of requirements, technical context and specific endangerments should be carried out, in order to adapt the criteria system. On this Base an as-is analysis of the existing systems should be executed in order to identify the unaccomplished criteria with a certain focus to lethal criteria. Thereafter it is possible to identify the possible bundles of actions to fulfil all (necessary) lethal criteria. The procedure model is shown in figure 2.

Having discussed how to identify critical IS infrastructure, we focus now on the subsequent phases of the procedure model, especially the requirements and the configuration processes that both deal with the adaptability of the criteria system. The application of a uniform, monolithic criteria system would not ensure the heterogeneity of the different application contexts. It is also not suitable for different scenarios to define only a scale of varied levels: not the level of security can differ but

specific security requirements will result from application context. E.g. highly availability can be archived by highest reliable systems or massive redundancy. The first solution fits the needs of a core banking system, focusing the integrity of even every transaction, the second approach of "peer production of suitable infrastructures" [19] is e.g. used for the critical business process of Google [20]. So the criteria should be adapted complying with the relevant environmental factors (requirements and endangerments) and constitution parameters of the critical IS infrastructure. On this occasion, threat scenarios classified as relevant and the enterprise-related application context should be considered. Table 1 contains examples for different endangerments that should lead to different (lethal) criteria for evaluating the critical IS infrastructure.

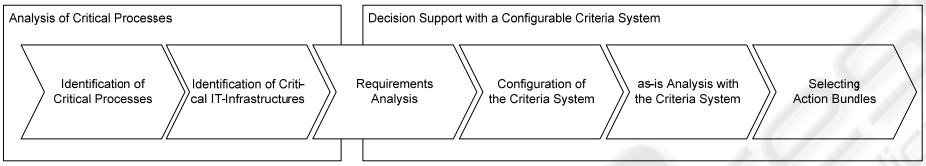

Fig. 2. Procedure model for IS risk management regarding critical infrastructures.

After aligning the criteria system to a specific scenario, an as-is analysis should be carried out as a weak point analysis. The criteria system contributes to identify weak points to be repaired, in which it reproaches a huge number of measures for lethal criteria, which are not fulfilled and have thus top priority. Every criterion also should have a questionnaire to raise all important parameters. In the connection, all possible action, which can be carried out to improve the level of the criteria, can be identified. Through this, only such action portfolios fulfill the defined minimum requirements in order to achieve all lethal criteria, are part of the allowed portfolios of the necessary measures. The portfolio, which shows the slightest total cost of ownership (TCO), can be selected. Other (more expensive) portfolios can be taken into consideration in the frame of a "bargaining solution" if these fulfill more non lethal criteria in higher measure to mention multiple objects [21].

3 Conceptual Design of a Decision Support System for Selecting Optimal Action Sets

3.1 Design of a configurable Criteria System for Decision Support

By the development of a criteria system, for the assessment of critical infrastructures three levels are to be regarded. In the core, the real criteria system is located itself on the two essential fields for the availability, which refer to current enterprise and the restart of the systems after an incident.
For decision support a business intelligence layer should provide different kinds of indexes, reports and dashboards and drill-down functionality to the different level of criteria aggregation. The adaptation will occur through the choice of the criteria, their scaling and the way of their settlement into an index. The base for the criteria system

is the form level. A form repository should support the evaluation of criteria with questionnaires for each one. The contents of the criteria system should be descended from the relevant standards. Criteria will be affiliated during the as-is-analysis to real existing entities to control their compliance to the security policy. Most frameworks in this context focus on technical aspects and regard organizational considerations only on the brink. Given the importance of these questions we suggest a multi-perspective design, inclosing an organizational and a process oriented dimension of every technical criterion facing the questions, how to observe the criterion and who is responsible for that [22]. The criteria simultaneously should be divided into different classes according to best practice standards to improve the transparency of this system [15, 23]. The connections or cause-effect relations between the specific criteria within the whole criteria system can be visualized analogously to the strategy map of a balanced scorecard in an area map [24]. By this multidimensional view, detailed evaluations within the particular areas are possible. So every criterion contains necessary value for all these dimensions and is associated with actions to ensure these values, which cause defined costs to implement them. The evaluation of the criteria bases on the questionnaires of the form level. At this level, it is defined, how the single criteria should be raised. In addition to the elevation way, the elevation time should also be defined at this level. In dependence of the single criterion, suitable methods should be identified and should be specified in a discipline-conceptual draft. The forms can serve as templates for the concrete arrangement of a specific criteria system. The forms should be raised and their contents should be adapted accordingly to the modeled context. This design should lead to the construction of a management information system which offers support for risk assessment and governance within critical IS infrastructures by identifying adequate portfolios of actions. To gain a deeper understanding of meeting these requirements and computing of adequate portfolios, we introduce a conceptual model in the following section.

3.2 Conceptual Model for the Computation of Action Bundles

Figure 3 depicts an entity relationship model [25, 26] that provides the basis for the computation of suitable action bundles. In the model, the entity type »Scenario« is used to describe the environment, in which security-related actions (»Action«) are to be applied. Each scenario consists of a set of criteria, that the actions in a bundle (»Action Bundle«) have to satisfy. Accordingly, instances of the entity type »Criterion« embody the requirements of scenarios. As stated above, we differentiate between lethal and non-lethal criteria by introducing the two entity types »Lethal Criterion« and »Non-lethal Criterion«. The entity type »Value« is used to create presets for the different criteria. Thereby, a value is assigned to its criterion via the relationship type »VALCRIS«. By connecting values with a scenario through »VALSCE«, we express which criteria different actions have to satisfy in order to make up a suitable bundle. We describe actions in the same way as we describe scenarios by assigning instances of the entity type »Value«. A comparison of the values that a scenario requires, and the values that an action exhibits, serves as a starting point for the computation of action bundles.

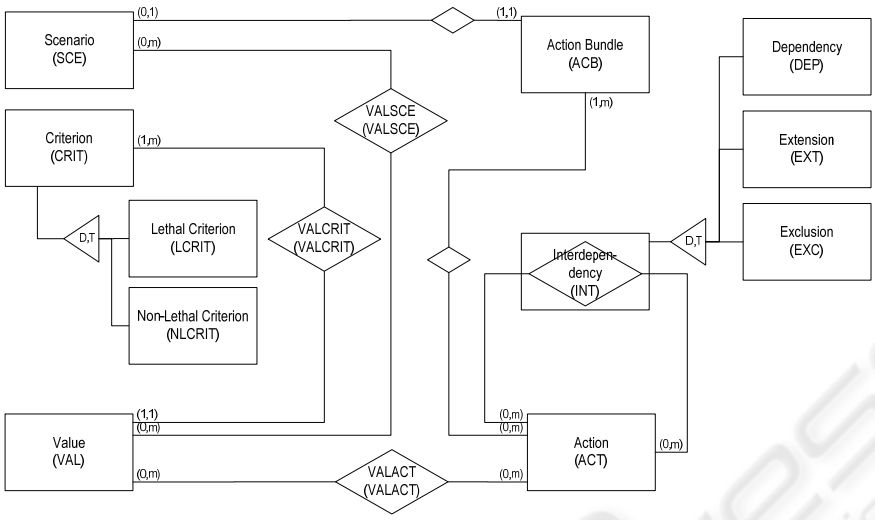

Fig. 3. Conceptual Model for Computing Action Bundles.

Due to space restrictions however, the conceptual model cannot be elaborated in greater detail at this point, especially in respect to the trivial modellizing of the attributes like different perspectives and the costs of the affiliated actions for a single criterion. The relationship type »Interdependency« allows combining different actions. As different types of interdependencies, we distinguish between (1) the simple dependency (»Dependency«), (2) the extension (»Extension«), and (3) the exclusion (»Exclusion«):

1. If action a depends on action b, a bundle covering action a also has to contain action b.
2. If action a extends action b, action a also satisfies the criteria that are fulfilled by action b.
3. If action a excludes action b, a bundle covering action a must not contain action b.

3.3 Formalizing the Computation of Action Bundles

In order to explain how to compute suitable action bundles, we express some of the conceptual model elements by sets. In the following, let ACT be the set of all actions, SCE the set of all scenarios, and VAL the set of all values. The subset $VALSCE \subseteq VAL \times SCE$ expresses the values which describe a scenario, while the subset $VALSCE \subseteq VAL \times SCE$ depicts the values which characterize an action. Furthermore, a certain action bundle acb consists of a set of actions. Hence, the power set of ACT describes the set of all (theoretically) possible action bundles viz. ACB. The subset $INT \subseteq ACT \times ACT$ of the Cartesian product of two action sets expresses interdependencies. Dependencies, extensions, and exclusions are defined as subsets of INT, so that $INT = DEP \cap EXT \cap EXC$ holds. Next, we introduce the function

dep: ACT → $\wp$(ACT). By this function, we compute the set of all actions required by a certain action act in order to satisfy the dependency relation:

$$\mathrm{dep}(\mathrm{act}) = \{\mathrm{dep} \in \mathrm{ACT} \mid (\mathrm{act}, \mathrm{dep}) \in \mathrm{DEP}\} \tag{1}$$

With ACBdep we define the set, which contains all action bundles, whose actions satisfy all dependencies required within the bundle:

$$\mathrm{ACB}_{\mathrm{dep}} = \{\mathrm{acb} \in \wp(\mathrm{ACT}) \mid \forall \mathrm{act} \in \mathrm{acb}, \forall \mathrm{act}_{\mathrm{dep}} \in \mathrm{dep}(\mathrm{act}) : \mathrm{act}_{\mathrm{dep}} \in \mathrm{acb}\} \tag{2}$$

Next, we introduce the function exc: ACT → $\wp$(ACT), by which we compute the set of all actions excluded by a certain action act:

$$\mathrm{exc}(\mathrm{act}) = \{\mathrm{exc} \in \mathrm{ACT} \mid (\mathrm{act}, \mathrm{exc}) \in \mathrm{EXC}\} \tag{3}$$

With ACBexc, we denote the set, which contains all action bundles, whose actions do not violate any exclusion required within the bundle:

$$\mathrm{ACB}_{\mathrm{exc}} = \{\mathrm{acb} \in \wp(\mathrm{ACT}) \mid \forall \mathrm{act} \in \mathrm{acb}, \forall \mathrm{act}_{\mathrm{exc}} \in \mathrm{exc}(\mathrm{act}) : \mathrm{act}_{\mathrm{exc}} \notin \mathrm{acb}\} \tag{4}$$

By the function ext: act → $\wp$(ACT), we compute all actions that extend a certain action act:

$$\mathrm{ext}(\mathrm{act}) = \{\mathrm{ext} \in \mathrm{ACT} \mid (\mathrm{act}, \mathrm{ext}) \in \mathrm{EXT}\} \tag{5}$$

Based on eq. 5, we introduce the function actval: ACT → $\wp$(VAL) to calculate all values covered by a certain action act:

$$\begin{aligned} \mathrm{actval}(\mathrm{act}) = \{&\mathrm{val} \in \mathrm{VAL} \mid (\mathrm{val}, \mathrm{act}) \in \mathrm{VALACT} \\ &\vee \exists \mathrm{act}_{\mathrm{ext}} \in \mathrm{ext}(\mathrm{act}) : (\mathrm{val}, \mathrm{act}_{\mathrm{ext}}) \in \mathrm{VALACT}\} \end{aligned} \tag{6}$$

In order to compute all values of lethal criteria for a scenario sce, we use the function letval:

$$\begin{aligned} \mathrm{letval}(\mathrm{sce}) = \{&\mathrm{val} \in \mathrm{VAL} \mid (\mathrm{val}, \mathrm{sce}) \in \mathrm{VALSCE} \\ &\wedge (\mathrm{val}, \mathrm{crit}) \in \mathrm{VALCRIT} \wedge \mathrm{crit} \in \mathrm{LCRIT}\} \end{aligned} \tag{7}$$

Based on eq. 6 and eq. 7, we define the function ACBval: SCE → $\wp$(ACT), by which we compute all action bundles that satisfy the requirements of a certain scenario sce:

$$\begin{aligned} \mathrm{ACB}_{\mathrm{val}}(\mathrm{sce}) = \{&\mathrm{acb} \in \wp(\mathrm{ACT}) \mid \forall \mathrm{val} \in \mathrm{letval}(\mathrm{sce}) \\ &\exists \mathrm{act} \in \mathrm{acb} : \mathrm{val} \in \mathrm{actval}(\mathrm{act})\} \end{aligned} \tag{8}$$

By computing the intersection of the sets defined in eq. 2, eq. 4, and eq. 8, we establish all action bundles which are suitable for a certain scenario sce:

$$\mathrm{ACB}(\mathrm{sce}) = \mathrm{ACB}_{\mathrm{dep}} \cap \mathrm{ACB}_{\mathrm{ext}} \cap \mathrm{ACB}_{\mathrm{val}} \tag{9}$$

In order to select the optimal bundle, we take the cost of the action bundles into account. Therefore, we assume, that the cost caused by a certain action act is given by the function cost: ACT → ℜ. Based on this assumption, we can compute the cost of a certain action bundle acb:

$$\text{cost}(\text{acb}) = \sum_{\text{act} \in \text{acb}} \text{cost}(\text{act}) \tag{10}$$

By applying eq. 10 to each element of eq. 9, we can compute the cost optimal action bundle.

4 Summary and Outlook

With this paper, a procedure model for the decision support of IS safeguards in the context of critical business processes has been introduced. Since then IS security investments have been primarily exhibiting a direct impact on the organizational processes, the latter are in the focus of the suggested method. Therefore, we suggested identifying the most important processes, the critical processes by a criticality analysis. Existing approaches were integrated into a generic proceeding model for IS risk management in the case of regular risk disposition. In addition, the necessity of a distinction between such methods for regular and critical business processes was shown. After a refinement of the procedure for critical business process requirements for decision support in this context were developed. For that purpose we recommend the development of a management information system to handle different criteria resulting from the multitude of relevant standards e.g. for data center security. Thereafter, the necessary structure of a criteria system for critical infrastructure and the procedure model to apply this to existing business information systems were shown. Afterwards, we formalized the necessary conditions to identify cost optimal bundles of actions to provide a basis for our proof of concept. Further research demand lies in parameterizing the criteria system with relevant norms. At this time several countries in Europe joined their efforts conforming their standards and frameworks to a common base. So we expect in the near future detailed common criteria catalogues for critical information system, which can be applied with the presented approach

References

1. Anderson, R., Moore, T.: The Economics of Information Security. Science 314 (2006) 610–613
2. Sonnenreich, W., Albanese, J., Stout, B.: Return on security investment (ROSI). A practical quantitative model. In: Fernández-Medina, E., Hernández, J.C., García, L.J. (eds.): Security in Information Systems, 3rd Int. Workshop on Security in Information Systems (WOSIS'05), In conjunction with ICEIS'05 (2005), New York (2005) 239-252
3. Neubauer, T., Klemen, M., Biffl, S.: Business process-based valuation of IT-security. In: Sullivan, K. (ed.): Seventh international workshop on Economics-driven software engineering research, St. Louis (2005) 1- 5

4. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly 28 (2004) 75-105
5. Becker, J., Niehaves, B.: Epistemological Perspectives on IS Research - A Framework for Analyzing and Systematizing Epistemological Assumptions. Information Systems Journal 17 (2007) 197-214
6. Le Veque, V.: Information Security - a Strategic Approach. Wiley, Hoboken (2006)
7. Hyslop, M.: Critical Information Infrastructures: Resilience and Protection. Springer, New York (2007)
8. Röhrig, S.: Using Process Models to Analyse IT Security Requirements. Zürich (2003)
9. Jakoubi, S., Tjoa, S., Quirchmayr, G.: Rope: A Methodology for Enabling the Risk-Aware Modelling and Simulation of Business Processes. In: Österle, H., Schelp, J., Winter, R. (eds.): Fifteenth European Conference on Information Systems, St. Gallen (2007) 1596-1607
10. Business Continuity Institute: Business Continuity Management - Good Practice. In: Institute, T.B.C. (ed.): (2005)
11. Seibold, H.: It-Risikomanagement, München (2006)
12. Grob, H.L., Strauch, G., Buddendick, C.: Conceptual Design of a Method to Support IS Security Investment Decisions. In: Kop, C., Kaschek, R. (eds.): International Conference on Information Systems Technology and its Applications (ISTA 08), Klagenfurt (2008)
13. BSI: BSI-Standard 100-2: IT-Baseline Protection Methodology. (2005)
14. BSI: BSI-Standards 100-3: Risk Analysis based on IT-Baseline Protection. (2005) 19
15. BSI: IT-Baseline Protection Catalogues. Bonn (2007)
16. von Rössing, R.: Betriebliches Kontinuitätsmanagement. mitp Verlag, Bonn (2005)
17. Kairab, S.: A Practical Guide to Security Assesments. Auerbach, Boca Raton (2005)
18. Vidalis, S., Blyth, A.: Understanding and Developing a Threat Assessment Model. 2nd European Conference on Information Warefare, London (2002)
19. Benkler, Y.: Peer Production of Survivable Critical Infrastructures. In: Grady, M.F., Parisi, F. (eds.): The Law and Economics of Cybersecurity. Cambridge University Press, Cambridge (2006) 73-114
20. Barroso, L.A., Dean, J., Hölzle, U.: Web Search for a Planet: The Google Cluster Architecture. IEEE Micro 23 (2003) 22-28
21. Neubauer, T., Heurix, J.: Defining Secure Business Processes with Respect to Multiple Targets. In: Jakoubi, S., Tjoa, S., Weipel, E.R. (eds.): Third International Conference on Availability, Reliability and Security (ARES 2008). IEEE Computer Society, Barcelona, Spain (2008) 758-764
22. Asnar, Y., Giorgini, P.: Modelling Risk and Indentifiying Countermeasure in Organisations. In: Lopez, J. (ed.): Critical Information Infrastructures Security: First International Workshop, Critis 2006, Vol. 4347. Springer, LNCS, Samos Island, Greece (2006) 79-90
23. BITKOM: Reliable Data Centers Guideline. (2006)
24. Kaplan, R.S., Norton, D.P.: The Balanced Scorecard-Measures that Drive Performance. Harvard Business Review 70 (1992) 71-79
25. Chen, P.P.: Entity-Relationship Model: Towards a Unified View of Data. ACM Transactions on Database Systems 1 (1976) 9-36
26. Scheer, A.-W.: ARIS - Business Process Modeling. Springer, Berlin (1998)