ISAHP 2003, Bali, Indonesia, August 7-9, 2003

DECISION MODELING BASED APPROACH TO THE BS 7799 DEPLOYMENT

Tomas Feglar
Vondrousova 1199, 163 00 Prague 6, Czech Republic
feglar@czn.cz

Abstract

Key words: BS 7799,Decision modeling, AHP hierarchy, resource allocation, risk driven, hypotheses.

The paper describes decision modeling based approach to the BS 7799 deployment. First we briefly introduce why BS 7799 is important as common security framework in the age of Electronic Commerce. Then we identify limitations that characterize risk driven approach to the BS 7799 deployment. We argue that these limitations can be overcome with decision modeling based approach using AHP hierarchy. This hierarchy includes two types of criteria levels – static and dynamic. Decision making model that uses this hierarchy includes three particular processes: BS 7799 Deployment Modeling, Risk Driven Countermeasure (RDC) generation and Human Resource Allocation Alternatives (HRAA) generation process. Our approach is supported with three powerful tools to achieve appropriate quality of decisions and performance. BS 7799 Deployment Modeling uses EC 2000, RDC process uses CRAMM and HRAA generation is based on GUHA. Proposed decision modeling approach controls interactions between all three tools and generates final objective – optimal BS 7799 deployment.

More and more companies become dependent on information systems that introduce additional risks that can seriously damage core business activities. Security Standard BS 7799 was developed to help companies to minimize these risks. BS 7799 deployment becomes one of the strategic business decisions. This deployment is currently based on risk driven approach that is different from a framework usually used for decision making.

The first difference concerns of a gap between decisions oriented categories typical for managers and very specialized reports generated by risk analysis tools. The second difference concerns of a gap between BS 7799 security profile (set of countermeasures recommended on the base of risk analysis) and decisions in terms of manpower and cost.

We suggest overcoming risk driven deployment limitations of BS 7799 with new approach that is based on decision modeling and human resource allocation alternatives generation.
AHP Hierarchy for a BS 7799 Optimal Deployment was developed as the basement of Decision Making

Model (DMM). This hierarchy includes:

- Strategic criteria. Hierarchical levels L1, L2 and L3 describe “static” criteria that are easily understandable for the top management. L1 criteria serve for finding of a compromise between “internal motivation” (Efficiency, Internal Assurance) and “External Image” (Customer Trust, Business Partner Trust). L2 and L3 levels relate to the BS 7799 structuring.
- Operational criteria. Hierarchical levels L4 and L5 describe “dynamic” criteria that depend on Risks and Responsibility Assignment. Risks and Responsibilities become known only on the base of the Risk Analysis Process. “Dynamic” criteria are difficult to understand without very good information technology security background. L4 criteria describe countermeasure groups (CG). Each Security Category (L3) can be represented as a cluster of countermeasure groups. L5 Criteria describe relationships between particular responsibility and countermeasure groups (sub-groups).
- Hypotheses about Human Resource Allocation Alternatives. At the bottom of our hierarchy we place four Allocation Scenarios (AS). Each AS represents security concept with some kind of preference. Scenario 1 prefers BS 7799 deployment strongly on the base of internal staff (company employees).

Scenario 2 uses service providers to cover BS 7799 requirements. Scenario 3 is similar but it prefers to hire third party. Scenario 4 prefers to cover all BS 7799 deployment effort within one contract with Computer Services Business Center (CSBC). Real situation requires a combination of scenarios in dependency on final structure of the levels L4 and L5. HR Allocation Alternatives are generated on the database data (HR pool, contracts, costs) with respect of a particular AS. The generation process is hypotheses driven.

Decision process that uses AHP Hierarchy just described requires high expertise at least in the' areas of decision making, risk analysis and information security. It is not easy to put together so different experts. We overcome this problem using three powerful tools:

- Expert Choice 2000 (EC 2000) for a development of the AHP hierarchy and for BS 7799 Decision modeling.
- CRAMM for dynamic creation of the criteria at the levels L4 and L5.
- GUHA for Human Resource Allocation Alternatives (HRAA) hypotheses generation.

Smart functionality of our model requires careful planning of key processes that interact each other.

The first process is the BS 7799 Deployment Modeling. This process includes all steps necessary for building of the AHP hierarchy. Criteria levels L1, L2 and L3 are built on the base of a Business and IT Strategy and Security Policy. Bottom criteria levels – L4 and L5 are synthesized on the base of outputs from the Risk Driven Generation process. Alternatives are synthesized on the base of outputs from the HRAA Generation process. This process is supported by EC 2000.

The second process is the Risk Driven Countermeasure Generation process. It includes all steps that are necessary for creation of a set of risk driven countermeasures and for responsibility types assignment. This process is supported by CRAMM.

The third process is the Human Resource Allocation Alternatives (HRAA) Generation process. This process is supported by GUHA.

Information security was understood as something mysterious for a long time. Last decade changed significantly overall picture. BS 7799 allows including information security as integral part of business processes. This new opportunity requires changes in the area of decision making. The approach presented in this paper completely covers three most critical parts of the BS 7799 deployment. AHP hierarchy including static and dynamic set of criteria is the core of decision making modeling. Dynamic criteria are generated in dependency on risks – risk driven countermeasure generation is the second part. Finally human resource allocation alternatives are pre-prepared using automatic hypotheses generation and testing.

Topics for further research include:

- Verification of the approach at least on two different types of companies
- More detailed research of human resource allocation in dependency on various scenarios.

Research described in this paper is the subject of Czech participation in the EU COST 274 – Theory and Applications of Relational Structures as Knowledge Instruments (TARSKI).