A COMPARISON OF SECURITY SAFEGUARD SELECTION METHODS

Thomas Neubauer
Secure Business Austria, Favoritenstrasse 16, 1040 Vienna, Austria
neubauer@securityresearch.ac.at

Keywords: Security, Risk Management, Economics, Decision Support.

Abstract: IT security incidents pose a major threat to the efficient execution of corporate strategies and business processes. Although companies generally spend a lot of money on security companies are often not aware of their spending on security and even more important if these investments into security are effective. This paper provides decision makers with an overview of decision support techniques, describes pros and cons of these methodologies.

1 INTRODUCTION

Companies are often not aware of their spending on security and even more important if the investments into security are effective. The definition of security safeguards is often a result of current needs or influenced by security problems that may go public. When seeking to select the most appropriate set of measures and, thus, the right level of security investments, decision makers are challenged by (i) having to concentrate resources on value-generating and supplementary business processes while (ii) having to consider multiple strategic objectives that are often conflicting as well as (iii) the cost-efficient usage of the available resources and interdependencies between the systems and (iv) a variety of potential technologies and potential systems. As a consequence security decisions provide only punctual solutions and are made without considering the costs and benefits of introducing theses measures. Accordingly, a variety of approaches have been introduced that aim to support decision makers in identifying the “right” investment candidates. This paper provides decision makers with an overview of common methods for the evaluation and selection of security safeguards and describes pros and cons of these methodologies. One major focus of this evaluation lies on identifying the method’s capabilities in (i) considering business processes for aligning expenditure to actual business needs and (ii) integrating multiple objectives in order to properly consider financial, technical and/or further types of objectives. Thereby this paper supports decision makers in their decision which methods to choose when having to evaluate security investments.

2 COMPARISON

The *Analytic Hierarchy Process (AHP)* developed by Saaty (Saaty, 1980) is a tool for solving multi-criteria decision making problems and is based on the principles of hierarchy, pairwise comparison, and weight synthesizing for prioritizing criteria and the evaluation of alternatives. Specifically, the process consists of the following steps: Structuring a Hierarchy, Prioritizing the Criteria, Evaluating the Alternatives, and Calculating the Global Priorities. The Analytic Hierarchy Process (AHP) is a widespread and easy to use decision support tool for evaluating different alternatives that can be applied to solve security safeguard selection problems. Its strength is the analysis of the alternatives’ properties in different categories, or in other words, the evaluation of alternatives with respect to multiple objectives. The pairwise comparison technique however requires (i) the direct comparability of alternatives and (ii) may result in a major effort. As security safeguards are not limited to technical solutions but also include organizational measures and operational procedures, comparing them directly may be problematic, e.g., comparing a packet filtering firewall with a fire extinguisher. Therefore, it may be beneficial not to use the AHP as a standalone tool for solving information security-related problems, but to integrate it with other methods. Regarding the effort, Maiden (Maiden and Ncube, 1998) illustrates this fact by means of a case study of a project with about 130 requirements: because it would have required an estimated 42,000+ individual paired comparison scores, applying AHP was impossible in this and similar cases due to the time constraint involved.

Another framework that takes multiple objectives into consideration when determining suitable security safeguards is the cost/benefit-based *Security Attribute Evaluation Method (SAEM)* (Butler, 2002). As the risk assessment process is tasked with prioritizing threats, a benefit assessment determines the safeguard effectiveness, and a cost analysis determines the expenses associated with the security measures. The SAEM process involves the following four steps: Risk Assessment, Benefit Analysis, Coverage Analysis, and Security Technology Tradeoff Analysis. Unlike AHP, it was developed specifically for solving information security evaluation problems and therefore particularly addresses security-related concepts such as threats and safeguard effectiveness. Multiobjectivity is considered in the multiattribute risk assessment where threats are ranked according to their likelihood of occurrence and impact on attack outcome attributes. The resulting threat index values and the effectiveness values of the security technologies under consideration are then used to calculate their risk reduction impact. The coverage analysis ensures that no security gap is overlooked when arranging the safeguard portfolio, and the tradeoff analysis compares the risk reduction impact and other benefits of security measures with their costs like implementation or maintenance costs. The SAEM approach is a very detailed and structured process to evaluate information security and safeguards. The risk assessment process ensures that specific threats are addressed, and the benefit and tradeoff analysis consider the multiobjectivity of threat consequences and safeguard effectiveness. The normalization of threat and safeguard values also allows the concurrent usage of qualitative and quantitative data. But, as the SAEM method is quite detailed and extensive, it is also rather complex to conduct. Each phase requires relatively much work and, without automation of certain steps, this work can be quite tedious. Although this method allows the definition of multiple objectives, the outcome is still aggregated into a single scalar value used for the evaluation, i.e., the threats and safeguards cannot be evaluated subject to the attributes 'independently'. Also, SAEM does not consider the business processes and the safeguards' influence on them.

The Central Computer and Telecommunications Agency (CCTA) *Risk Analysis and Management Method (CRAMM)* (InsightConsulting, 2007) is a commercial qualitative risk analysis methodology developed by the UK government's Central Computer and Telecommunications Agency in full compliance with BS7799. CRAMM is divided into the three stages Asset Identification and Valuation, Threat and Vulnerability Assessment, and Countermeasure Selection and Recommendation. The CRAMM process includes the following steps: Assets, Threats, Vulnerabilities, Risks, Countermeasures, Implementation, and Audit. The framework is intended for large governmental and commercial organizations. It provides a structural method to identify relevant assets (arranged into asset groups), possible vulnerabilities, and threats, to combine them to risks that are measured according to the assets' values and vulnerability and threat levels, and to recommend suitable countermeasures. The process is considered as rather complex and considerable experience is required in order to produce meaningful and correct results. Therefore, organizations often rely on external qualified CRAMM practitioners to conduct the analysis instead of letting internal analysts undergo the extensive training to gain the necessary expertise. This reduces the organization's internal staff's involvement in the assessment phase and therefore also does not improve their insight into security matters. The outcome is often quite extensive and a full review may last up to several months. The framework neither offers the flexibility to customize it to the organizations characteristics, nor does it provide an evaluation of business process related issues. Grouping the assets into asset groups may also prove to be unfavorable, as all assets have their own properties and security requirements. And finally, CRAMM does not calculate economic indicators, such as implementation costs of the recommended safeguards and whether they fit into the security budget.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (CERT, 2007) is a risk-based strategic assessment and planning technique for security developed by the Carnegie Mellon University. Essentially, the OCTAVE framework is a set of criteria containing guidelines and requirements for implementing process steps, instead of pre-specified techniques. These criteria must be fulfilled in order to correctly implement the OCTAVE framework.

Unlike other frameworks, the OCTAVE approach focuses on organizational risks instead of technological ones and is structured into three phases: Build Asset-based Threat Profiles, Identify Infrastructure Vulnerabilities, and Develop Security Strategy and Plans. OCTAVE is quite different to CRAMM: On the one hand, the actual OCTAVE framework does not provide a step by step procedure as CRAMM, but a set of criteria that has to be met to conform to the OCTAVE methodology. This provides great adaptability and more flexibility than CRAMM to address specific organizational needs. For easier access, three specific application methods have been developed to choose from, suited for different sizes of organizations. On the other hand, it is self-directed, meaning that the OCTAVE methodology has to be wholly exercisable by the organization's internal staff in a workshop environment, thus not relying on external experts. Finally, OCTAVE is focused on organizational risks, whereas CRAMM concentrates more on technical issues, and OCTAVE generally does not take threat likelihood into consideration (except for OCTAVE S which provides basic means for including threat likelihood in the evaluation).

While the risk assessment methodologies evaluate security technologies on their effectiveness to mitigate risks, the POSeM framework deals with information security in a different way. The *Process-Oriented Security Model (POSeM)* framework developed at the University of Zürich by Röhrig (Röhrig, 2002) is a methodology to define security requirements and to derive security measures by using process models as the basis for the analysis. In this proposal, the four security objectives confidentiality, integrity, availability, and accountability are used to measure the security levels of each process component (actor, artifact, activity), and suitable security measures are derived via rule bases. It takes into consideration that assets do not generate business value themselves, but participate in business processes that produce utility, and therefore the methodologies rely on business processes as the basis for their analysis. It also ignores specific harmful events (e.g., threats), but concentrate on eliciting security requirements and deriving appropriate security measures. The POSeM approach consists of five steps: Definition of General Security Objectives, SEPL Model, Consistency Analysis, Derivation of Generic Security Measures, and an optional Implementation Phase. The strengths of the POSeM approach lie in the usage of business process models as the basis for the security evaluation and the definition of organization specific rule sets for the consistency checks and safeguard derivation. Using process models seems to be a logical step in today's process-centered world. As processes are continually improved (or completely restructured with BPR techniques), the security status should be evaluated and improved in line with the business processes. Relying on the well established CIA properties also enhances the insight into security-related matters of processes, especially by assigning them to the individual process components (participant, data, activity). By defining organization-specific rules, the particularities of the organization and its main processes can be taken into consideration, thus reaching a high level of adaptability of the POSeM process. These rules can be specified once and stored for further uses, which significantly reduces the amount of time needed for the (re-)evaluation. And the formal description methods of SPEL, SMDL, and SCRL allow a high degree of automation, thus further reducing the workload. As emphasized by Röhrig, this framework is mainly intended to elicit the requirements for safeguards, but not to decide which specific safeguards to choose. As a matter of fact, it is not suited as a standalone decision making method. The outcome of the evaluation is solely a list that is suitable for implementing the required security levels of the process components. This is underpinned by the fact that the economical factors of safeguards, namely their costs in monetary or time units, are completely neglected and only the technical aspect of security measures are evaluated. Furthermore, POSeM ignores any specific negative factors influencing business processes such as threats and vulnerabilities, which are integral parts of risk assessment practices. No harmful events (such as a viral infection of the information system) are considered and therefore no safeguards can be defined to counter that specific problem. This is a major disadvantage of a framework that is specifically designed to be a security evaluation process.

The *CORAS Framework* is a tool-supported and model-based risk analysis methodology, the result of the EU-funded CORAS project. The framework is founded on four pillars: Risk Documentation Framework, Risk Management Process, Integrated Risk Management Process and System Development Process, and Platform for Tool Inclusion. The CORAS framework that also applies UML for modeling security-related issues, is centered around a traditional risk assessment process with asset, vulnerability, threat identification and evaluation and safeguard derivation. In order to model the risk entities, a UML profile has been developed. Unlike the other methods, CORAS incorporates techniques of other frameworks to realize its risk identification process (e.g., HAZard and OPerability study (HazOp) and Fault Tree Analysis). This ensures a thorough analysis of the problem, but also requires participants proficient with these techniques to pick the most appropriate. The main pillar of interest, the risk management process, is based on the Australian/New Zealand Standard AS/NZS 4360:1999: Risk Management and ISO/IEC 17799: 2000 Information technology - Code of practice for information security management. In contrast to specifying its own methods, the CORAS risk management process relies on techniques of other frameworks for each of the steps including HAZard and OPerability study (HazOp), Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA), Markov analysis, and the CCTA Risk Analysis and Management Methodology (CRAMM). To provide a framework for modeling all risk-related aspects, a UML profile was developed to act as a graphical reference and communication method between the different stakeholders. The risk management process consists of the following steps: Establish Context, Identify Risks, Analyze Risks, Risk Evaluation, and Risk Treatment. The CORAS risk management process represents a holistic framework for the evaluation of information security of different application areas. It inherits all strengths and weaknesses of the assessment methods it incorporates, and the graphical models are used for describing the target system, its context, and all security features, and therefore provide a valuable insight into the subject and facilitates communication between the stakeholders. The combination of different analysis methods also reduces the individual weaknesses and therefore enhances the overall quality of the risk assessment outcome. This integration also poses a considerable drawback of the CORAS approach. As it is recommended to rely on multiple methods in the same process step to get a more complete result, this also means an increased demand for time. Generally, the CORAS methodology is very time consuming, and the participants need experience in the multiple methods to be able to select and apply them efficiently.

3 CONCLUSIONS

Today many companies are not aware of their spending on security and if their investments into security are effective. Decision makers are increasingly challenged by having to define an optimal set of security safeguards in line with the corporate business processes as well as multiple strategic objectives. This paper gave an overview of common methods for the evaluation of security safeguards identified the method's capabilities in considering business processes for aligning expenditure to actual business needs and integrating multiple objectives. This comparison reveals that all methodologies focus on certain aspects of information security only and neglect others, thus not being able to provide a complete security evaluation of a business process and multiobjective safeguard selection. The risk-based approaches take assets and threats into account and therefore consider specific risks in the analysis, but neglect business processes. POSeM in turn is process-based, but ignores specific threats and risks. None of these frameworks consider multiple criteria when evaluating the safeguards, except for AHP and SAEM. But AHP is not specifically developed to deal with security-related issues, thus lacking information security specific functionality. And SAEM can be considered as a hybrid, including methods for multiobjective optimization and risk determination, but not as thorough as the other risk-based methods, and also lacks business process support.

REFERENCES

Butler, S. A. (2002). Security attribute evaluation method: a cost-benefit approach. In *ICSE '02: Proceedings of the 24th International Conference on Software Engineering*, pages 232–240, New York, NY, USA. ACM Press.

CERT (2007). Octave. Online at http://www.cert.org/octave/index.html.

InsightConsulting (Access in May 2007). Cramm. Online at http://www.cramm.com.

Maiden, N. A. and Ncube, C. (1998). Acquiring COTS software selection requirements. *IEEE Software*, 15(2):46–56.

Röhrig, S. (2002). Using process models to analyze health care security requirements. In *International Conference Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet*, Italy.

Saaty, T. L. (1980). *The Analytic Hierarchy Process*. McGraw-Hill.