Workshop-based Risk Assessment for the Definition of Secure Business Processes

Thomas Neubauer
Vienna University of Technology
Vienna, Austria
neubauer@ifs.tuwien.ac.at

Markus Pehn
Secure Business Austria
Vienna, Austria
pehn@securityresearch.ac.at

Abstract

Nowadays, industry and governments are faced with an increasing number of varying threats concerning the security of their valuable business processes. Due to the vast damage potential, organizations are raising their security investments, but often (i) without considering the efficiency of the investments made, (ii) neglect to involve people in order to raise security awareness and (iii) without giving decision makers a feeling about the importance of the decision problem at hand. This work provides an extension to the established risk management solution AURUM and extends its functionality by introducing the AURUM Workshop. It provides a crucial extension that allows the selection of efficient safeguards based on corporate business processes and thereby supports decision makers (i) in refining the basic infrastructure elements to the specific requirements of the corporation, (ii) focusing on the most relevant risks and (iii) in improving their awareness for the problem at hand.

1. Introduction

Security hazards such as viruses, hacker attacks or data theft pose major threats to corporate assets and may directly affect profit, shareholder value and a company's reputation. The increasing usage of Internet lead to a rise in the frequency of security breaches. Garg, Curtis and Halper [7] estimate the amount of security investments within US companies at about $30 billion by 2005. CERT estimated that about 90% of big and medium sized companies have been affected by security incidents in 2006. The New York Times reported in May 2009 a billion dollar contract the US Government signed with security specialized companies and universities with the aim of being equipped for so called "cyberwarfare". Due to this continuous increase of information technology usage and its monetary importance, a main question posed to companies' managers is how to determine the optimum value of security investments, which is related to the question which kind of measures are necessary and wise. This work provides an extension to the established risk management solution AURUM (cf. [3–6, 11–13]). AURUM is a risk management solution that allows decision makers to evaluate security investments based on their corporate business processes and infrastructure data defined in a security ontology. A Bayesian network supports the risk definition whereas an interactive multiobjective decision support approach is used for the safeguard selection. This paper extends the functionality of AURUM by introducing the AURUM Workshop. The AURUM Workshop provides the missing link between the ontology comprising corporate business processes and infrastructure, the Bayesian network and the decision support module that allows the selection of efficient safeguards. It takes typical psychological and sociological influence factors from literature into consideration and thereby supports decision makers (i) in refining the basic infrastructure elements to the specific requirements of the corporation, (ii) focusing on the most important risks (risks with a high frequency or a high impact or both) and (iii) in improving their awareness for the problem (risks) at hand.

2 Psychological and Sociological Influence Factors

Decision makers, no matter if they act on their own or as a part of a group, are usually confronted with a variety of psychological and sociological issues that have a major influence on their decisions (cf. [1]). *Confirmation trap*: Humans aspire towards consistency, which induces them to force the correctness of their actions and to ignore, eliminate or distort contrary information. *Insist on belief effect:* Works similarly to the confirmation trap discussed above; humans are trying to keep up their belief of the world through ignoring, eliminating or distorting of contrary information. *Hindsight bias:* This phenomenon states that people afterwards always think that they have predicted an event correctly. *Availability heuristic:* Humans are able to remember some things better than others (cf. [16]). Pos-

978-0-7695-3956-0/10 $26.00 © 2010 IEEE
DOI 10.1109/eKNOW.2010.8

sible reasons are emotional involvement time, spaciously, and sensory closeness [14], yielding to an incorrect interpretation of these events in the form of putting them into superlatives (more frequent, most important, etc.). *Anchoring and adjustment:* Based on the persons experience the anchor represents a basis for classifying new information (cf. [15]). Often caused by reasons of information lacking, an arbitrarily anchor is used which yields to a miss classification toward the anchor. *Distortion by reasons of process variation:* People are typically inconsistent in their behavior. Lichtenstein and Slovic [15] as well as Tversky and Kahneman [17] have shown that this relation is not universally valid, thus logical procedure orientation and inductive behavior is only partly given. *Question structure:* The formulation of the question has vital importance to the processing and argumentation process inside respondents mind (cf. [15, 17]). *Prospect theory:* The frame in which a situation is embedded in terms of winning or losing situation dictates the expectations of this situation. If a loss is expected a small benefit will be handled as a gain, unlike if a high benefit is expected a small benefit will be handled as a loss (cf. [1]). *Presentation of information:* Auer-Rizzi [1] illustrates the importance of good presentation of information on the subjects performance to remember and categorize information better. Important are differences between numerical and verbal presented information, structuring, and completeness.

People are ready to take higher risks at group level due to (cf. [18]) : (i) Allocation of responsibility: The risk level of group decisions increases with the number of liable participants. Also certain grade of anonymity arises, thus the risk adversity decreases with the grade of individual liability. (ii) A Person which is willing to take higher risks has more influence: Individuals, which are tending to risky decisions are arguing more convincingly and persuade others more successfully. (iii) Social comparison: Risky decisions are preferred because of the social phenomenon, that persons willing to take higher risks are reputed more positively. (iv) Strong arguments: Group members are influenced by arguments which seem to be cogent [2]. Individual preferences as well as the characterization of the person who raises the argument can influence the rating of the argument.

Studies show that "In certain circumstances, groups of sensible, smart, even shrewd men and women think and act in a way that can only be described with the term 'collective stupidity' " [9], which can be referred to as "groupthink" (cf. [10]).

3 Overview of the AURUM Workshop

The AURUM Workshop is a process supporting risk management. It is used to determine, refine and review security relevant data needed as input for the AURUM risk management framework. The main characteristics of the AURUM Workshop are:

- Moderated: The workshop comprises three methods including Brainstorming/Discussion, Evaluation and Selection that are used by the moderator to get objective results from the workshop participants.
- Role based: Each workshop participant carries out a specific role which determines his tasks.
- Group based: Each workshop participant is part in a small group of about three people. This approach aims to avoid psychological problems by splitting one big group into several small groups.
- Clear voting structures: The workshop process provides a way to model consensus of meanings, which is founded on the characterization of voting acts.
- Awareness building: The AURUM workshop aims to improve security awareness of its participants in order to build an understanding of relevant risks and options for their mitigation.

Figure 1 gives an overview of the AURUM risk management framework and the integration of the AURUM Workshop, whereas the gray squares denote activities and methods that are part of the workshop process. The workshop supports decision makers in going through the risk management process step by step. Thereby, the workshop supports the following risk management phases defined in AURUM: (i) Business Process Determination, (ii) Inventory, (iii) Threat Probability Determination and (iv) Control Evaluation.

4 Roles

The group configuration can yield to decision influences. In order to deal with this problem this section outlines the roles needed in the AURUM Workshop. Thereby, for each role a short description gives an overview of a role's tasks and responsibilities followed by recommended skills for the special role. We describe the main tasks of the role during the workshop, the interaction with other process participants.

4.1 Moderator

Typically a security consultant familiar with the AURUM process and the business area should be selected as moderator. It is highly recommended that the role of the moderator is taken by an external consultant familiar with the process and its' typical problems. The moderator leads and instructs the participants through the workshop. The

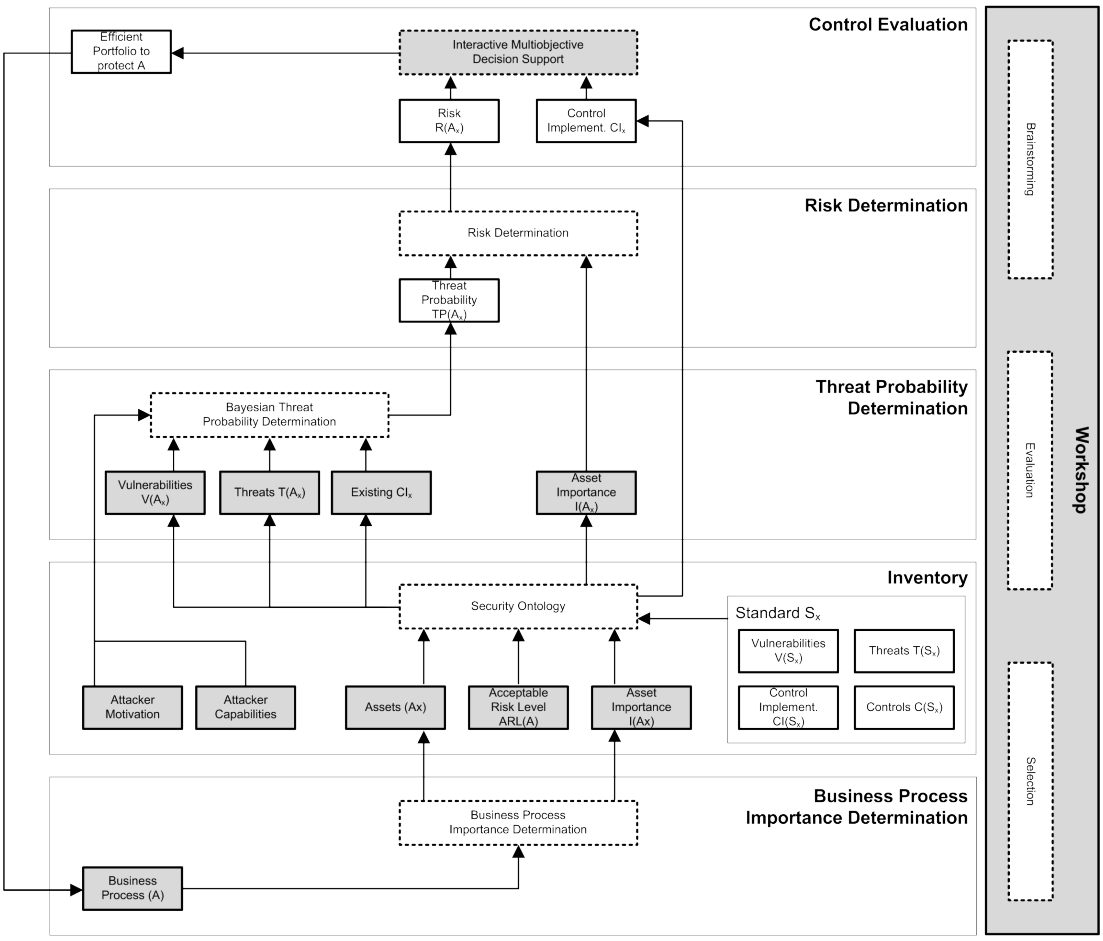

Figure 1. The AURUM Workshop Process

moderator represents one of the main roles of the AURUM workshop. (i) He defines small groups, creates user accounts and assesses roles to all process participants. (ii) He manages data input, e.g., resulting from brainstorming sessions, resolves naming divergences and handles merging and deleting tasks. (iii) The AURUM workshop is characterized by highly interactive tasks where the moderator is the main interaction controller.

4.2 Management Member

This role should be represented by members of middle or high level management, which enhance the group with structural and process knowledge. Before process execution, it is essential to ensure management support and therefore sufficient presence of management members. Each management member is directly integrated in exactly one group. Each management member is involved in all group decisions and executes the leading role at category evaluation. He should be aware of the strategic goals of internal or external business processes as not to lose sight of integration problems possibly caused by new security controls. The inclusion of cost problems from the first moment of task execution can eliminate unrealistic economical security control estimations. The ability to present decisions and their costs at management level is indispensable for the adoption of accepted solutions.

4.3 Expert Member

An expert member fills the gap between structural and cost knowledge of management members and user experience of the key process users. Other process participants enhance expert's knowledge by providing him a view beyond his own scope. Each expert member is integrated in exactly one group. Each expert member is involved in all group decisions. He should have (i) infrastructural knowledge to handle the task asset identification. This also addresses knowledge about former incidents and their occurrence rates. (ii) The ability to identify and estimate possible

synergy effects and effectiveness of safeguard candidates. (iii) Cost knowledge, which is important to interact with the management members. Without feasible estimations about possible safeguard implementation costs the management is unable to consider cost restrictions in the evaluation process.

4.4 Key Process User

The participation of key process users should enhance the acceptance of the decided actions and its costs at employee level. The key process user should have experience with main business processes. This includes data input problems as well as experience with the use of former information security measures. Each key process user is directly integrated in exactly one group. The interaction with members of other groups happens through discussion tasks as described above. Each key process user is involved in all group decisions.

5 Workshop Methods

The workshop comprises three methods including Brainstorming/Discussion, Evaluation and Selection that are used by the moderator to generate data necessary to carry out the risk management process.

1. Brainstorming: Brainstorming enables a group of decision makers to quickly assess the data relevant for the information security of their organization. The system supports the decision makers with data input and data structuring.

2. Evaluation: Based on Grünbacher (cf. [8]) we use a border criterion voting mechanism for rating the items generated during brainstorming. Each participant decides upon the importance and ease of implementation of the so called win conditions. The system calculates a medium value and depending on the degree of consensus the voting results are underlined with a traffic light system to signal contentious points (e.g., using the colors red (<50% consensus), orange (>=50 and <=75% consensus) and green (>75% consensus)). The borders are variable and arise from task dependent mathematical methods: (i) Taking numerical values as input, the standard deviation of the input values from the different decision makers is used to determine the threshold and, thus, the grade of consensus. (ii) Taking the number of votes as input, the number of votes related to the total number of voters determines the threshold and, thus, the grad of consensus. To avoid disagreement, e.g., out of ignorance, the voters are instructed not to vote if they do not have sufficient knowledge about the issue.

3. Selection/Discussion: During a group discussion based on the ratings' analysis, the group decides which items are to be selected. If judged necessary, the brainstorming and rating steps can be repeated.

6 The AURUM Workshop Process

This section explains the phases of the AURUM workshop in detail. Each step is described according to the criteria: input, output, and sub steps.

6.1 Workshop Briefing

The first phase of the workshop includes the following tasks: (i) Definition of the risk analysis context and goals: This first step defines the scope of the workshop, its contents and goals. It is required for the workshops' strategic alignment and for the definition of criteria to measure its success. (ii) Selection of workshop participants: In order to raise the efficiency of the workshop session in terms of quality and quantity of the workshop output, the moderator must select participants according to their knowledge, their "match" and their "key user role"'. Workshop participants are selected to cover the whole spectrum of security problems and include a manager in charge of the decisions emerging from this process. (iii) Psychological problems: With knowledge about psychological tendencies in group decision making the participants are possibly able to avoid typical problems. (iv) AURUM workshop process: Participants are informed about the process steps especially input and expected output data. This has to happen in a way in which the members understand their roles and therefore their integration in the process, including voting mechanisms, group structuring, etc. (v) Terminology: It is essential for performing the workshop part of the process to impart knowledge about basic security terms and how they correspond.

6.2 Phase 1: Business Process Importance Determination

Description: This step aims to extract the most relevant business processes. For this purpose the expert group is asked to execute a brainstorming and evaluation task. Gross discrepancies (foremost red colored items) have to be discussed by the workshop members, and result in an accepted list of processes ranked by their importance.

Steps:

Business Process Selection: The decision makers select the business processes that should be evaluated. This step includes the discussion of the selected processes and their ranking if a low grade of consensus exists. In order to resolve this problem the moderator discusses the

following questions with the workshop participants: "Why have specific processes been mentioned" and "Why have specific members voted high, and others low about the importance of a business process".
Business Process Importance Determination: The decision makers determine the importance of the selected business processes within the corporation, and, thus their need for protection.

Main Question: What should be protected?
Output: An accepted list of business processes ranked by their importance.

6.3 Phase 2: Inventory

Description: This step aims to extract the most relevant assets. For this purpose the expert group is asked to execute a brainstorming and evaluation task. Note, that this phase can be supported by the AURUM security ontology that already contains a wide selection of assets. Thus, decision makers just have to review the assets proposed by the ontology and the discussion can focus on the issues where low consensus exists.
Steps:
Assets: This step includes the discussion of the assets corresponding to the selected business processes.
Asset Importance Determination: The decision makers determine the importance of the selected assets, and, thus their need for protection. The decision makers can use a suggestion made by the system that is calculated based on the importance of the business processes (cf. [6]).
Acceptable Risk Level: Level of risk judged to be outweighed by corresponding benefits or one that is of such a degree that it is considered to pose minimal potential for adverse effects.
Attacker Capabilities: This step aims to evaluate and define the capabilities of potential attackers.
Attacker Motivation: This step aims to evaluate and define the motivation of potential attackers.

Main Question: Which assets exist, and which of them are really worth to protect?
Output: An accepted list of assets ranked by their importance. The acceptable risk level for each business process, the attacker's capabilities and the attacker's motivation.

6.4 Phase 3: Threat Probability Determination

Description: This step aims to review and determine vulnerabilities, threats and existing countermeasures. This step evaluates possible dangers and their causes. At first the potential threats are determined for each asset, which happens by performing a group voting session. The result is a list of threats. Each threat is associated with relevant vulnerabilities (also by using group voting), which results in a list of vulnerabilities per threat. The vulnerability and the threat determination are finalized by a discussion task based on the determined consensus grade of the two voting steps. For this purpose the expert group is asked to execute a brainstorming and evaluation task. Gross discrepancies are discussed by the workshop members. The result are accepted lists of vulnerabilities and threats ranked by their importance. Note, that this phase can be supported by the AURUM security ontology that already contains a wide selection of vulnerabilities and threats based on established security standards such as ISO 27001 or NIST SP 800. Thus, decision makers just have to review the given vulnerabilities and threats proposed by the ontology and discussion can focus on the issues where low consensus exists. In this case voting is reducible to selection tasks, the vulnerabilities are determined automatically and only have to be attuned to the specific business needs.
Steps:
Threats: This sub step evaluates a set of corresponding threats per asset. After moderator's data aggregation a list of threats per asset represents the output of this sub step.
Vulnerabilities: Based on the list of threats this step deals with the determination of causes per threat.
Existing countermeasures: This step aims to review and evaluate existing countermeasures.

Main Question: Which threats/vulnerabilities correspond to each single asset?
Output: Accepted lists of threats and corresponding vulnerabilities.

6.5 Phase 4: Control Evaluation

Description: Based on the risk evaluation the set of possible administrative, technical and physical controls to avoid such incidents are determined. In order to solve this problem a voting task followed by a discussion is carried out. The output represents a set of controls for each risk. Alternatively, the participants can define the requirements for each control. Concrete products can be determined in the post workshop valuation step.
Steps:
Criteria Definition: This step defines a set of criteria respecting business conditions and eventually related enterprise wide controlling mechanisms.
Interactive Selection: This step supports the decision maker in making a final determination of the solution that best fits his notions out of the possibly hundreds (or even thousands) of Pareto-efficient alternatives of countermeasure portfo-

lios identified before. The procedure starts from an efficient portfolio and allows the decision maker to iteratively move in the solution space towards more attractive alternatives until no "better" portfolio can be found. The system provides immediate feedback about the consequences of different choices in terms of the remaining alternatives and, thereby, allows the decision maker to evaluate different investment scenarios. The system provides the decision maker with ample information on the specific selection problem and ensures that the final solution will be an optimal (i.e., Pareto-efficient) one.

Main Question: Which countermeasures are imaginable?

Output: Accepted lists of countermeasure portfolios for protecting the selected business processes.

6.6 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 leading to the demand to carry out risk assessment on a regular basis. This paper proposed an approach called AURUM workshop for integrating the advantages of workshops into the established risk management solution AURUM. It provides decision makers with a stepwise methodology for the risk assessment by taking into account and mitigating typical psychological and sociological influence factors that usually occur in (group) decision processes. 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. AURUM workshop is intended to not only evaluate data, but also impart a sense for security awareness in the participants' minds in order to build an understanding of relevant risks and options for their mitigation. It supports decision makers in identifying and focusing on the most important risks and provides intuitive interactive decision support for evaluating different protection scenarios. Whereas this paper focused on introducing the workshop extension of AURUM, future research will provide real-world case studies to prove the effectiveness of the proposed approach.

References

[1] W. Auer-Rizzi. *Entscheidungsprozesse in Gruppen - kognitive und soziale Verzerrungstendenzen*. Wiesbaden, DUV, 1999.

[2] E. Burnstein and A. Vinokur Testing two classes of thories about group-induced shifts in individual choice. *J. Exp. Social Psychology*, 13:315–332, 1973.

[3] A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for supporting information security risk management. In *Proceedings of the 42nd Hawaii International Conference on System Sciences, HICSS2009*, 2009. IEEE Computer Society.

[4] A. Ekelhart, S. Fenz, and T. Neubauer. Ontology-based decision support for information security risk management. In *International Conference on Systems, 2009. ICONS 2009.*, pages 80–85. IEEE Computer Society, March 2009.

[5] A. Ekelhart, T. Neubauer, and S. Fenz. Automated risk and utility management. In *2009 Sixth International Conference on Information Technology: New Generations*, pages 393–398. IEEE Computer Society, 2009.

[6] S. Fenz, A. Ekelhart, and T. Neubauer. Business process-based resource importance determination. In *Proceedings of the 7th International Conference on Business Process Management (BPM'2009)*, pages 113–127. Springer, 2009.

[7] A. Garg, J. Curtis, and H. Halper. Quantifying the financial impact of it security breaches. *Information Management & Computer Security*, 11/2:74–83, 2003.

[8] P. Gruenbacher and R. Briggs. Surfacing tacit knowledge in requirements negotiation: Experiences using EasyWinWin. *Proceedings of the 34th Hawaii International Conference on System Sciences*, 34:1–8, 2001.

[9] P. Hart. Psychological Studies of Policy Decisions and Fiascoes. *Boston: Houghton Mufflin*, 1982.

[10] I. Janis. Groupthink in government: A study of small groups and policy failure. *Swets & Zeitlinger*, 1990.

[11] T. Neubauer, A. Ekelhart, and S. Fenz. Interactive selection of iso 27001 controls under multiple objectives. In *Proceedings of the Ifip Tc 11 23rd International Information Security Conference, IFIPSec 2008*, volume 278/2008, pages 477–492, Boston, July 2008. Springer.

[12] T. Neubauer and C. Stummer. Extending Business Process Management to Determine Efficient IT Investments. In *Proceedings of the 2007 ACM Symposium on Applied Computing*, pages 1250–1256, 2007.

[13] T. Neubauer and C. Stummer. Interactive selection of Web services under multiple objectives. *Information Technology and Management*, Springer, 2009.

[14] R. Nisbett and L. Ross. *Human Inference: Strategies and Shortcomings of Social Judgement.* Prentice Hall, 1980.

[15] P. Slovic and S. Lichtenstein. Comparison of bayesian and regression approaches in the study of information processing in judgement. *Organizational Behavior and Human Performance*, 6:649 – 744, 1971.

[16] A. Tversky and D. Kahneman. Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, 5:207–232, 1973.

[17] A. Tversky and D. Kahneman. The framing of decisions and the psychology of choice. *Science*, 211:453 – 458, 1981.

[18] M. Wallach, N. Kogan and D. Bem. Group influence on individual risk taking. *J. Abnorm. Soc. Psychology*, 65:75–86, 1962.