From the Resource to the Business Process Risk Level

Stefan Fenz
Vienna University of Technology, A-1040 Vienna, Austria
e-mail: fenz@ifs.tuwien.ac.at

Abstract

Although a variety of information security risk management (ISRM) approaches have been proposed, well-founded methods that provide an answer to the following question are still missing: How can the risk level of a business process be determined by taking the risk levels of the involved resources into account? This paper presents our research results regarding resource-based risk analysis methods in order to assign realistic figures concerning the business process risk level. With regard to business processes the research results allow the (semiautomatic) reasoning of the current security status of an organization. In this way we can support decision makers in selecting appropriate controls to reduce risks to an acceptable level; and also in making a reasonable trade-off between investments into security and the need for protection.

Keywords

Security, Information security risk management, Business process analysis

1 Introduction

A business process is a structured and measured set of activities designed to produce a specified output supporting the business goals of the organization (Davenport, 1993). For each activity in a business process a definition regarding (i) its beginning, (ii) its end, (iii) the required input, (iv) the expected output, and (v) the resources required to conduct the activity (e.g. information technology resources) exists. Organizations heavily rely on information technology to execute their business processes to achieve their defined business goals. Therefore, we define resources in the context of this paper as hardware, software, and data which is required to execute the activities of a business process. Further resources such as human beings or legal rights are explicitly excluded.

Information security risk management (ISRM) is defined as the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data (resources) that support their organization's mission (Stoneburner et al., 2002). In the context of the ISRM process we calculate risk values for crucial resources of the organization. Each risk value is the product of an estimated threat probability and the expected impact that realizes when the threat strikes the organization (Stoneburner et al., 2002). The expected impact can be expressed in quantitative (e.g. monetary) or qualitative values. In the

context of this paper we define resource and business process risk as the potential loss of revenue a company faces in its given technical and organizational environment.

According to Baskerville (1991) the main benefit of ISRM is not its output in the form of predictive statistics. In fact, ISRM can be seen as a communication tool. It transforms and reduces highly specialized information security knowledge into fictive monetary values, which are compatible to the mindset of investment decision-makers at the management level. While operational and economic costs of protective measures are assessable, it is difficult to obtain realistic figures regarding the gains in mission capability, i.e. how business processes are protected by potential countermeasure implementations. What we need is a risk calculation model which links in the ISRM context the technology- to the business process-layer. Therefore, our research question is:

- RQ: How can the risk level of a business process be determined by taking the risk levels of the involved resources into account?

We elaborate on the research question by analyzing existing approaches in the field of business process analysis. First, we develop a method to calculate the business process risk level based on the activity and corresponding resource risk level. Second, we show a proof of concept and evaluate the underlying method by comparing its output to a traditional workshop-based risk assessment.

2 Existing Approaches

zur Muehlen and Rosemann (2005) present a process-related risk taxonomy and modeling techniques to include risks in business process models at the activity and overall process level. For modeling process-related risks they propose four model types: (i) risk structure model - to decompose risks, (ii) risk goal model - to model the impact of the risks on the goals of the process, (iii) risk state model - to capture dynamic characteristics of risks, and (iv) event-driven process chain extended with risks - to assign risks to the individual steps of a business process. While the proposed taxonomy and modeling techniques are valuable for risk-aware business process modeling they can not be used to assign concrete and comprehensible risk values to business processes.

Neiger et al. (2006) developed a framework that enables a risk-oriented process management which incorporates a multi-disciplinary view of risk. Neiger et al. propose the following steps to integrate risk and process management: (i) decomposing business values and fundamental objectives to identify relevant process risks, (ii) identifying specific risks and determine which processes and which functions within these processes contribute to these risks, (iii) developing alternative process configurations to identify the best process structure that meets the business objectives, and (iv) choosing from the alternative process configurations developed in the previous step the optimal configuration that meets risk minimization objectives in the context of the overall business requirements. To determine the best process configuration Neiger et al. calculate the utility of each alternative by combining expected costs and probabilities.

Rieke and Winkelmann (2008) propose a risk modeling approach developed on the basis of the event-driven process chain (EPC). The proposed method provides visualization and documentation mechanisms for process-oriented risks, enabling a more efficient risk identification by a focused presentation and a lower model complexity. While the presented approach provides risk-oriented modeling techniques it is not designed to assign

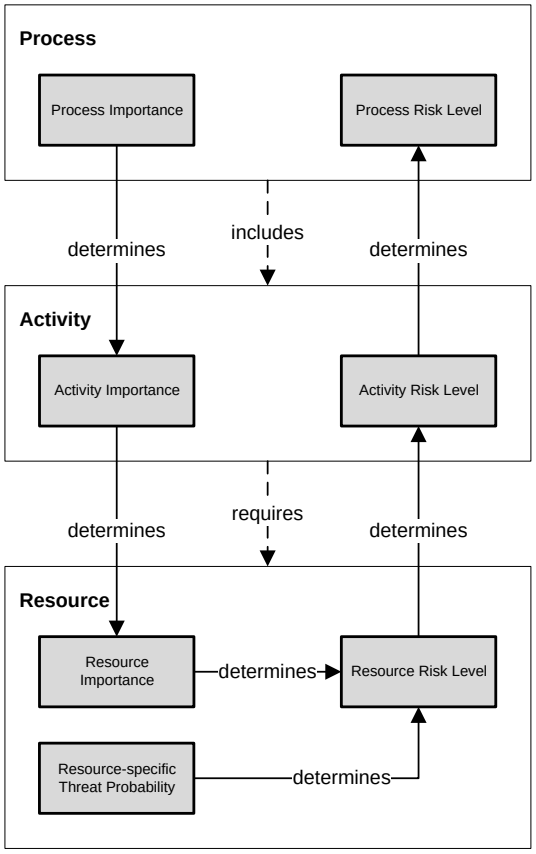

Figure 1: Overview

risk levels to entire business processes or identify specific resource risks within a business process.

3 Overview

Figure 1 shows a brief overview of our business process risk calculation model. Basically, each business process includes activities that require resources to fulfill designated tasks. In the context of this paper we consider hardware, software, and data as resources. Further resources such as legal rights, human beings or external services are currently not considered. Fenz et al. (2009) showed how to calculate the business process-based importance of resources. The importance indicates the organizational impact if the considered resource is not longer able to conduct its designated tasks (we focus on the availability aspect). Fenz and Neubauer (2009) presented an approach to determine resource-specific threat probabilities by using ontologies and Bayesian networks. Based on this work we present in this paper an approach to determine the process risk level based on activity and resource risk levels. The final process risk level incorporates (i) the overall importance of the business process, (ii) the importance of the involved resources calculated based on the structure of the business process, and (iii) a resource-specific threat probability regarding high level threats such as data loss or asset loss.

4 Business Process Risk Determination

Based on any given business process structure, we developed a method to determine the business process risk level taking the organizational context and risk levels of involved resources into account. As we consider hardware, software, and data as resources the final business process risk level reflects the risk level of those resource types.

The unit which is used to express the process risk depends on the unit used to describe the importance of the overall business process and the required resources. Monetary (e.g. Euros per hour) or qualitative (e.g. high, medium, and low) scales are amongst others an option to express the importance (i.e. value) of the business processes and resources.

4.1 Assumptions

As this paper builds on previous research and because of page limitations, we have to make some assumptions: (i) the business process is available in a machine-readable form, (ii) for each resource required by the activities of the business process a local, i.e. business process-specific and global, i.e. organization-wide importance value and a resource-specific threat probability is available. To determine the resource importance values based on the business process structure we use the approach presented in Fenz et al. (2009). To calculate resource-specific threat probabilities we use the approach presented in Fenz and Neubauer (2009) that is based on the ontological information security base presented in Fenz and Ekelhart (2009). To summarize the assumptions: for each resource A_i we have (i) a business process-specific (local) importance value $I_{P_j}(A_i)$ in the context of process P_j, (ii) an organization-wide (global) importance value $I_G(A_i)$ derived from its involvement in the business processes of the organizations, and (iii) a resource-specific threat probability $TP(A_i)$. The components are used to determine the local and global resource risk level and in the end the risk level of the considered business processes.

4.2 Risk Determination

When it comes to the risk determination we always focus on risks regarding availability (e.g. data loss or asset loss). Although confidentiality and integrity risks are currently not handled by the used resource importance determination approach and we are therefore not addressing these security attributes in this contribution, the approach can be extended to the confidentiality and integrity level.

The global, i.e. organization-wide risk $R_G(A_i)$ for resource A_i is calculated by multiplying its organization-wide importance $I_G(A_i)$ and the corresponding threat probability $TP(A_i)$ (e.g. data loss or asset loss).

$$R_G(A_i) = I_G(A_i) * TP(A_i) \tag{1}$$

The local, i.e.business process-specific risk $R_{P_j}(A)$ for resource A_i and business process P_j is calculated by multiplying its local importance $I_{P_j}(A_i)$ and the corresponding threat probability $TP(A_i)$ (e.g. data loss or asset loss).

$$R_{P_j}(A) = I_{P_j}(A_i) * TP(A_i) \tag{2}$$

Assuming that RL_{P_j} holds the local risk levels of the resources which are required by business process P_j, the risk level $R(P_j)$ of business process P_j equals the risk level of the resource with the highest risk level included in RL_{P_j}.

$$R(P_i) = max\{R_{P_j}(A_i)|A_i \in RL_{P_j}\} \quad (3)$$

Explanation: The risk level of each resource is the product of its importance and threat probability. While the importance depends on the organization's business needs and the business process layout, the threat probability varies with countermeasure implementations or changes in the threat environment. If we would simply sum up the resource risk levels to get the overall business process risk level we would mix different resource importance values and a business process with several low risk resources might have a higher risk than a business process with only one high risk resource. The subsequent risk mitigation would concentrate their efforts on the process with the several low risk resources and not on the one with the crucial high risk resource. To reliably identify high risk business processes we have to calculate their risk level as shown in Equation 3. In its underlying worst case assumption the business process risk level can only be mitigated if we mitigate the highest resource risk level.

5 Proof of Concept

For the proof of concept we use the following three fictitious business processes, which partly require the same resources for their correct execution: (i) process Register Damage (P_{RD}) generates 300 Euros per hour and requires the resources PC-Consultant, Notification-Server, Employee-Data, Client-Data, Police-Data, and Historical-Data, (ii) process Conclusion of Contract (P_{CC}) generates 200 Euros per hour and requires the resources Notification-Server, PC-Consultant, Client-Data, and Printer-Consultant, and (iii) process Consultant Assignment (P_{CA}) generates 100 Euros per hour and requires the resources PC-Reception, Appointment-Data, Client-Data, Historical-Data, Employee-Data, and Notification-Server.

We use a machine-readable representation of these business processes and the resource importance determination approach by Fenz et al. (2009) to determine the process-specific (local) organization-wide (global) importance of each resource. I.e., how is the entire organization affected if the considered resource is no longer able to fulfill its designated tasks. The used resource importance determination approach analyzes the business process structure, potential execution flows, and the required resources of each activity to determine the importance of the considered resource. As we use monetary units to express the importance of the processes the resource importance is also expressed in monetary units (see Table 1). The global, i.e. organization-wide importance $I_G(A_i)$ is the sum of all process-specific importance values $I_{P_j}(A_i)$ of the resource A_i.

Depending on the physical and organizational environment (a priori threat probabilities, attacker profile, and implemented countermeasures) of the considered resource we calculate the threat probability regarding availability threats (data or asset loss) for each of the listed resources. The used Bayesian threat probability determination model (see Fenz and Neubauer (2009) for a detailed model description) is based on the information security ontology presented in Fenz and Ekelhart (2009) and assumes that the entire physical and organizational environment is mapped to the ontology (e.g. attacker capability and motivation, IT components such as server or clients, implemented security policies, installed fire-walls or fire extinguishing systems, etc.). Based on that organization-specific knowledge and formal information security control definitions reasoning engines determine the compliance degree of each control and transfer this information

Resource A_i	$I_{P_{RD}}(A_i)$	$I_{P_{CC}}(A_i)$	$I_{P_{CA}}(A_i)$	$I_G(A_i)$
Notification Server	300 €/h	200 €/h	100 €/h	600 €/h
PC Consultant	300 €/h	200 €/h	-	500 €/h
PC Reception	-	-	100 €/h	100 €/h
Printer Consultant	-	100 €/h	-	100 €/h
Client Data	300 €/h	200 €/h	100 €/h	600 €/h
Appointment Data	-	-	50 €/h	50 €/h
Historical Data	150 €/h	-	25 €/h	175 €/h
Employee Data	300 €/h	-	100 €/h	400 €/h
Police Data	150 €/h	-	-	150 €/h

Table 1: Business processes, required resources and their local and global importance values

together with information on the attacker profile and a priori threat probabilities to the Bayesian threat probability determination model. Based on that information the model generates a resource-specific threat probability (e.g. for the data loss threat if it is a data resource). Table 2 shows the availability threat probability $TP(A_i)$, the process-specific risk $R_{P_j}(A_i)$, and the organization-wide (global) risk $R_G(A_i)$ of resource A_i. The high threat probability is due to the weak security program of our exemplary organization and the high a priori threat probabilities.

Resource A_i	$TP(A_i)$	$R_{P_{RD}}(A_i)$	$R_{P_{CC}}(A_i)$	$R_{P_{CA}}(A_i)$	$R_G(A_i)$
Notification Server	54%	162 €/h	108 €/h	54 €/h	324 €/h
PC Consultant	77%	231 €/h	154 €/h	-	385 €/h
PC Reception	79%	-	-	79 €/h	79 €/h
Printer Consultant	63%	-	63 €/h	-	63 €/h
Client Data	75%	225 €/h	150 €/h	75 €/h	450 €/h
Appointment Data	67%	-	-	34 €/h	34 €/h
Historical Data	71%	107 €/h	-	18 €/h	125 €/h
Employee Data	69%	207 €/h	-	69 €/h	276 €/h
Police Data	57%	86 €/h	-	-	86 €/h

Table 2: Resources, their threat probabilities and process-specific and organization-wide risk levels

Applying the proposed risk determination formula $R(P_i) = max\{R_{P_j}(A_i)|A_i \in RL_{P_j}\}$ reveals the final process risk levels (see Table 3). Each business process inherits its final risk level from the resource with the highest risk level in the context of the resources that are required to execute the considered business process. This seems obvious as the process-specific resource risk reflects the importance of the resource in the context of the process and the resource-specific threat probability. The process-specific importance of the resource incorporates the structure of the process and its organization-wide importance. I.e., changing the business process structure, the business process importance, or the resource-specific threat levels by implementing additional countermeasures changes the business process risk level.

With these figures on hand the organization is able to concentrate their IT security efforts on the business processes with the highest risk level. At each process our approach shows which resources are responsible for the current risk level. Two options to decrease the resource and therefore the process risk level exist: (i) lowering the importance of

Process P_j	**Process-specific Risk** $R(P_j)$
Register Damage P_{RD}	231 €/h
Conclusion of Contract P_{CC}	154 €/h
Consultant Assignment P_{CA}	79 €/h

Table 3: Final process risk levels

the required resources (e.g. detecting and mitigating single points of failure), and (ii) decreasing the threat probability by implementing additional countermeasures (e.g. virus scanner, back up policies, access control mechanisms, etc.).

6 Evaluation

A workshop-based assessment has been conducted to evaluate the risk level results of the proposed approach. Three business processes, the involved resources, their process-specific and organization-wide importance values, and threat probabilities for each resource as described in Section 5 have been provided to the workshop participants. Each of the three participants has been working in the information security risk management and business continuity domain for several years. To guarantee correct evaluation conditions the following steps have been performed at the assessment: (i) definition of the workshop goal → calculating business process risk levels based on resource importance values and threat probabilities, (ii) definition of the risk term as the product of importance and threat probability, (iii) manual resource risk determination by workshop participants - each participant is required to determine the risk level of each business process based on the given data, and (iv) manual business process risk determination by workshop participants.

Manual Resource Risk Determination: Based on the given data the workshop participants calculated the process-specific risk of each resource. The participants intuitively used, by multiplying the process-specific resource importance with the given threat probability, the traditional risk determination formula. Each participant came up with the process-specific resource risk levels presented in Table 2.

Manual Business Process Risk Determination: Based on the resource risk levels the participants determined the risk level of the given business processes. Similar to the proposed approach, each participant used the maximum resource risk to derive the final process risk level as presented in Table 3.

At the resource and business process risk determination the participants obtained the same results as the proposed approach. The subsequent discussion was basically focused on two issues: (i) while availability risks are addressed, risks regarding confidentiality and integrity are not covered, and (ii) the approach requires detailed quantitative input data which is hardly available in small- and medium-sized enterprises. Further research will address both limitations by (i) developing and incorporating novel methods to determine the confidentiality and integrity requirements of resources and processes, and (ii) evaluating the proposed approach by using qualitative input data and corresponding numerical mapping schemes. After addressing these limitations a further evaluation will also include business process experts of selected partner companies.

7 Conclusion

Organizations rely on realistic and comprehensible business process risk figures to efficiently address those risks which endanger their most important processes. Therefore, the research question of this paper was: How can the risk level of a business process be determined by taking the risk levels of the involved resources into account? Based on local and global importance values and threat probabilities we calculate process-specific and organization-wide resource risk levels and use these levels to determine the risk level of business processes.

The advantages of the approach are: (i) assuming that the required input data is available the business process risk level is automatically calculated based on resource importance values and threat probabilities, (ii) changes in the resource risk level due to additional countermeasures or different threat environments are reflected immediately on the process layer, (iii) management is provided with a comprehensible methodology which transforms technical facts such as countermeasure implementations or attacker profiles to monetary values on the business process layer, and (iv) resource single points of failure are reflected in the business process risk level. The conducted evaluation reveals a few limitations: (i) the approach focuses only on availability threat probabilities, and (ii) the quantitative approach (i.e. dealing with monetary values) is not always applicable as not every company is able to deliver such detailed data for their business processes. While the first limitation will be addressed in further research we stress that the presented approach is also applicable with qualitative rating systems and corresponding numerical values.

Empirical tests and large scale case studies to further improve the proposed approach will be the main focus of our further research. As the current approach only supports the availability perspective we will also research on extensions to determine business process risks regarding confidentiality and integrity. The next research question will be: How can the confidentiality and integrity risk level of a business process be determined by taking the characteristics of involved resources into account?

Acknowledgment

This work was supported by grants of the Austrian Government's FIT-IT Research Initiative on Trust in IT Systems under the contract 813701 and was performed at the research center SBA Research funded by the Federal Ministry of Economy, Family and Youth of the Republic of Austria and the City of Vienna.

References

Baskerville, R. (1991). Risk analysis as a source of professional knowledge. *Computers & Security*, 10:749–764.

Davenport, T. (1993). *Process innovation: reengineering work through information technology*. Harvard Business School Press.

Fenz, S. and Ekelhart, A. (2009). Formalizing information security knowledge. In *Proceedings of the 4th ACM Symposium on Information, Computer, and Communications Security*, pages 183–194, New York, NY, USA. ACM. 978-1-60558-394-5.

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

Fenz, S. and Neubauer, T. (2009). How to determine threat probabilities using ontologies and bayesian networks. In *CSIIRW '09: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research*. ACM.

Neiger, D., Churilov, L., zur Muehlen, M., and Rosemann, M. (2006). Integrating risks in business process models with value focused process engineering. In *Proceedings of the 14th European Conference on Information Systems*.

Rieke, T. and Winkelmann, A. (2008). Modellierung und management von risiken - ein prozessorientierter risikomanagement-ansatz zur identifikation und behandlung von risiken in geschäftsprozessen. *Wirtschaftsinformatik*, 5:346–356.

Stoneburner, G., Goguen, A., and Feringa, A. (2002). Risk management guide for information technology systems. NIST Special Publication 800-30, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930.

zur Muehlen, M. and Rosemann, M. (2005). Integrating risks in business process models. In *Proceedings of the 16th Australasian Conference on Information Systems*.