Using Business Process Model Awareness to improve Stakeholder Participation in Information Systems Security Risk Management Processes

Christian Sillaber[1,*], Ruth Breu[1]

[1] University of Innsbruck, Institute for Computer Science, Austria
{christian.sillaber,ruth.breu}@uibk.ac.at

Abstract. The present paper examines stakeholders' business process model awareness to measure and improve stakeholder participation in information systems security risk management (ISRM) via a multi-method research study at the organizational level. Organizational stakeholders were interviewed to gain an understanding of their awareness of business processes and related security requirements in the context of an ongoing ISRM process. The research model was evaluated in four case studies. The findings indicate that stakeholders' awareness of business process models contributed to an improved ISRM process, better alignment to the business environment and improved elicitation of security requirements. Following current research that considers users as the most important resource in ISRM, this study highlights the importance of involving appropriate stakeholders at the right time during the ISRM process and provides risk managers with decision support for the prioritization of stakeholder participation during ISRM processes to improve results and reduce overhead.

Keywords: Information Systems Security Risk Management; business process model awareness; stakeholder participation; empirical information systems security risk management research

1 Introduction

Multiple studies have shown that the majority of incidents related to information systems (IS) security can be traced back to internal stakeholders (e.g. [1–3]). IS security literature moved from portraying users as the weakest link in IS security (e.g. [4, 5]) to viewing them as the solution to multiple IS security issues in recent years (e.g. [6, 7]). However, literature is still lacking empirical studies that examine more closely how users' participation positively impacts IS security risk management processes that go beyond users being viewed as "mere" executors of IS security policies. Calls for more research in this area have been made repeatedly [8, 9, 6, 7, 10].

Based on the premise that, besides focusing on the participation of stakeholders as mere subjects of IS security policies it is worthwhile to investigate their active participation in IS security risk management processes, the present paper's research question asks how user participation during IS security risk analysis phases of the risk

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Sillaber, C.; Breu, R. (2015): Using Business Process Model Awareness to improve Stakeholder Participation in Information Systems Security Risk Management Processes, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1177-1190

management process can be shaped and utilized by focusing on the underlying business processes.

User participation in IS development and its influence on the implementational success has been extensively researched and it has been repeatedly argued that the information exchange and knowledge transfer resulting from such participation is the single most important effect [11]. Accordingly, the inclusion of multiple stakeholders in the risk management process has already been included in most established IS security risk management processes [12, 13].

The objective of this paper is to examine stakeholder participation in analysis phases of the IS security risk management processes and how users' business process model awareness impacts the IS security risk management process – in particular its security requirements in both number and accuracy. In doing so, this paper answers calls for research on user participation in IS security risk processes [14] and validates the findings in several case studies at the organization under investigation.

The remainder of this paper is organized as follows. First, the concept of user participation in IS security risk analysis settings is presented and an overview on existing state-of the art research is presented. Next, the study's multi-method research design is outlined, followed by a qualitative exploratory study that examined user participation in IS security risk management processes focusing on business process awareness and its contribution to the analysis process. A theoretical model informed by IS development theories and the qualitative study is then tested in a confirmatory quantitative study. Finally, the paper concludes with a discussion of the implications of the study, limitations, and suggestions for future research.

2 Theory

IS security risk management is the continuous process to identify and assess risk and to apply methods to reduce it to an acceptable extent. The present paper distinguishes between the analysis phases where risks are identified and security requirements elicited as well as the design and implementation phases where strategies and controls are being developed and implemented respectively, based on the results of the analysis phase. The present paper focuses on the analysis phase.

The present publication builds on the theories developed on user participation in ISRM presented in [6], which in turn builds on the buy-in theory, system quality theory and emergent interactions theory.

Following an synthesis of theories explaining user participation in IS security contexts, Spears et al. [7] define user participation in ISRM as the set of behaviors, activities, and assignments undertaken by business users during risk assessment and the design and implementation of IS security controls that is expected to add value to security risk management. By focusing on the assessment (i.e. analysis) phase, we reconceptualize the success outcomes, actors, activities and hypothesized links between outcomes and activities to fit the concepts under investigation in the present paper, as suggested in [7]. In following section, the present paper examines how stakeholder's

awareness of business process models contributes to their participation in IS security risk management processes.

3 Multi-Method Research Design

A combination of data collection and analysis methods were used on separate samples to examine business process model awareness in the analysis phase of IS security risk management. Interviews were conducted with one sample, followed by a qualitative analysis on a different sample with professionals who participate in an organizational IS security risk management process.

This multi-method or mixed-method approach was chosen based on the premise that separate and dissimilar data sets would provide a richer picture and thus compensate for the fact that experimentations in IS risk management processes are difficult to conduct [15, 16]. A sequential design was used in that the qualitative exploratory study informed a subsequent confirmatory study.

Qualitative methods were appropriate as they provide a rich understanding of the activities, behaviors and assignments that define user participation in the context of this study [15]. Furthermore, they allow for the construction of a framework for analysis. As the theories were used as a framework of analysis, data collection for the qualitative study was not based on any *a-priori* theories and can therefore be considered as an exploratory study.

Quantitative methods were then employed to test the theoretical framework derived from the quantitative study based on the researchers' understanding. Hypotheses that were constructed from the qualitative study formed a model that examined the degree to which user awareness of business process models explained variation in prespecified outcome variables (number and quality of elicited security requirements). Thus, combining qualitative and quantitative methods provided both a rich context and testability to the study.

4 Exploratory Study of Business Process Model Awareness and User Participation in IS Security Management

An exploratory study was conducted to better understand the connection between business process model awareness and stakeholder participation in IS security risk management and to investigate its outcomes. The exploratory study was conducted during an ongoing action design research [17] project seeking to improve the IS security risk management process currently used by the organization. The organization under investigation is one local branch (≈ 100 employees) of a multinational engineering company, focusing on the development of distributed information systems within a highly regulated domain.

4.1 Data Collection

To conduct the exploratory study, informants currently involved in the IS security risk management process were identified within the organization.

Five semi-structured interviews were conducted with five informants including three product managers, one deputy chief information security manager and one technological executive. This convenience sample included three employees with a degree in computer science and one with a specialization in IS security.

Each interview lasted approximately 45 minutes and was recorded. The informants were granted anonymity. The interviews were conducted as part of an ongoing action design research project and informants were told the purpose of the study was to gain a better understanding of the fit between business needs and the IS security risk management process. They were asked to recall information on the business processes under investigation in the security risk analysis and to identify security requirements and risks accordingly. The business processes were obtained from an internal knowledge base documenting IS development and IS usage for development purposes. The following processes were selected: bug management, feature selection for the next release, customer approval management, and change management.

4.2 Analysis

An iterative process of three manually performed coding techniques was applied to interview transcriptions. First, selective coding was used to develop an initial code list that contained stakeholder participation, awareness of the business process model and risks. Next, open-ended coding was used to identify new codes as they emerged from interview transcripts. Finally, relationships between business process awareness, stakeholder participation and risks were identified.

As informants described the business process currently under risk analysis, they were asked which parts of the business process relate to which risks and to describe their knowledge on different aspects of the business process model. They were afterwards presented with results from an earlier IS security risk analysis and were asked to relate the described risks to the business process model.

Once the data had been collected, segments of interview transcripts were coded as business process model awareness when informants recalled specific aspects of the underlying business process model when elicitating risks or security requirements. These coded segments were subsequently grouped and assigned new codes that categorized the activities in which users participated. Relationships among codes were then analyzed.

4.3 Results

Informants described their roles and activities in relationship to different parts of the business process model under investigation during the risk analysis process. They de- scribed their awareness of business process elements and their possible contribution to the IS security risk management process in terms of identified risks, elicited security requirements and business needs from their perspective. Each of these aspects is described below, providing contextual detail of stakeholder awareness and the derived benefit to the IS security risk management process.

All informants indicated that they had participated in the past in documenting business processes to determine information use throughout a business process - at least at an informal level, thus confirming the observations made in [6]. They also confirmed that the information flow within the business process model is a main source of information for the risk assessment process. Following the flow of information, stakeholders elicited security requirements for different parts of the business process.

The informants (except the for the chief information security manager) stated the effort for the IS security risk management process is normally led by other roles within the organization and that they have already provided input to it in the past based on their in-depth knowledge of business needs.

Following the categorization of the CIA (Confidentiality, Integrity, Availability) triad [18], we could observe that all informants were able to elicit at least one confidentiality, integrity or availability security requirement for each part of the business process model under investigation.

As for the awareness of the business process model in relation to the IS security risk process, we could elicit the following classification:

- *Complete awareness*: the stakeholder could describe the entire business process as defined at the organizational level.
- *Partial awareness*: the stakeholder could describe several parts of the business process as defined at the organizational level. We did not differentiate between incomplete or wrong assertions made by the stakeholder and utilized the taxonomy introduced in [19].
- *Referential awareness*: the stakeholder could not describe the business process as defined at the organizational level but knew whom to ask or where a descriptive document could be found.
- *No awareness*: the stakeholder could not describe the business process and was not able to refer to a further knowledge source.

Regarding the participation of stakeholders during the risk management process, stakeholders reported their past involvement during (1) the analysis (2) the risk mitigation strategy creation (3) control design and (4) control implementation phase, which seems to fit the IS security risk management model (albeit differences in nomenclature) proposed in [6]. The informants reported their contribution during all stages in all implemented business processes they either had claimed complete or at least partial awareness.

All informants reported that they felt most confident when talking about risks related to business processes they had complete awareness of. All but two informants insisted on referring to an external source when inquiring about risks related to a business process they had partial awareness of. This finding is further examined in the confirmatory study by testing the hypothesis:

H1: Including stakeholder with complete awareness of business processes in IS security risk management processes positively contributes to the risk analysis process.

During the interviews we could identify one business process where all informants but the deputy chief information security manager had no awareness of the business process model. However, when asked to elicit security requirements for this business process, which had the term "customer data processing" in its description, we could observe all informants trying to recall security requirements elicited for a known business process with a similar name. For example, Anton (all names changed for anonymity), a product manager said:

[The same scenario] happened during a risk assessment when I started in my first year [at XY organization]. Due to my name being the same as [a stakeholder from a different business unit], the risk manager inquired me about "my" business process and activities. I was not aware of the mix-up until much later and thought that I had to come up with security requirements [...]. I provided him with those of a related business process I was aware of.

This observation is further examined in the confirmatory study by testing the hypothesis:

H2: Stakeholders with no awareness of the business processes will re-use security requirements from business processes they are familiar with.

If informants only had referential awareness of a business process under investigation, we validated their references to other informants (two references were made to stakeholders not in the sample group). We found that all references to other informants were either correct (i.e. the referenced stakeholder had complete awareness) or could point to a stakeholder that had complete awareness. The therefrom generated directed graph was acyclic.

We found that stakeholders with partial business process awareness can be categorized according to the following scheme:

- *business process stakeholder deficit awareness*: the informants failed to recall responsible stakeholders (7 times)
- *business process information flow deficit awareness*: the informants failed to recall the correct flow of information between different stages of the business process (4 times)

- *business process documentation artefact deficit awareness*: the informants failed to recall documentation artefacts that were created during or as a result of the business process (9 times)
- *general business process deficit awareness*: the informants failed to recall aspects of the business process not related to the previous categories. We observed one case where an informant described an outdated business process and one case where an informant falsely claimed that this particular business process has no instantiations within the organization.

Informant answers, if categorized into one of the three first groups were found to omit risks related to the awareness lacking area as well as the other two, but to a lesser degree. Low documentation artefact awareness seemed to correspond most negatively to overall awareness of security requirements and risks related to this particular business process. Most informants that gave answers categorized in this group claimed no awareness of any documented security requirements or IS security policies applicable to that business process. The fact that business process stakeholders' awareness of documentation artefacts, created during or after the execution of a business process, seemed to correlate with the contribution to the risk management process (i.e. the fewer documentation artefacts the informant could recall, the more incomplete the elicited security requirements were), we formulated the following hypothesis:

H3: Stakeholder awareness of business process documentation influences the stakeholder's contribution to the IS security risk management process.

Finally, the risk manager should be able to select and prioritize stakeholders they want to include in the IS security risk analysis phase by some metric in case they need to prioritize due to limited time and budget. We therefore formulated the following hypothesis:

H4: Stakeholder selection based on business process model awareness is viable and improves data quality in early stages of the IS security risk management process.

5 A Confirmatory Study of User Participation IS Security Management

To validate the hypotheses and to further triangulate the results from the exploratory study, four case studies were conducted at the organization under investigation. Four business processes were randomly selected for conducting a IS security risk analysis. Stakeholders from the organization (including the stakeholders from the exploratory study) were asked to participate in each of the case studies. Information on the expected results from IS security risk analysis were gathered with senior risk managers.

5.1 Measures

For each business process and each stakeholder, a survey was used. The survey items used to measure the research model variables were derived from the qualitative study and all model constructs were measured with indicators as described next:

Business process awareness: Self-reported business process awareness (BPA_s): we asked stakeholders to self-assess their awareness levels regarding the business process according to the classification developed in the exploratory study. Observed business process awareness (BPA_o): we asked the stakeholders to describe or draw the business process and ranked them accordingly.

Security requirements elicitation: We asked stakeholders to elicit security requirements for the business process and evaluated (SR_n) the number of elicited security requirements, (SR_m) the number of security requirements matching the reference data set, (SR_a) the number of security requirements that are valid and had been omitted in the previous IS security risk assessment, and (SR_r) the number of reused security requirements from other business processes if stakeholders stated that they are doing so.

Business process contextual awareness: We counted the number of omitted business process stakeholders (BPC_p), omitted information flow paths (BPC_i), and omitted process documentation artefacts (BPC_d).

5.2 Data Collection

Content validity**:** We made an effort to ensure that the survey items were clearly understood by the respondents and that the informants responded to questions that we intended to ask. The survey was conducted verbally and clarifications were provided by the researchers. Participants could model their business processes on a whiteboard and were provided with access to any organizational knowledge source that is normally available to them.

We conducted each case study at the premises of the organization under investigation and told stakeholders to view the researchers as risk managers conducting an IS security risk analysis. With each stakeholder, we went through all four business processes starting with asking the survey questions and voice recording their answers. All stakeholders were promised anonymity and the organization was promised confidentiality regarding specific security risk related results and the content of their business processes.

We interviewed 9 stakeholders for at least one hour per use case. All participants were IS professionals and were product manager or senior developers. Despite the small sample size of 9 stakeholders, we are confident that we provide a reasonably adequate representation of the target population, as we are not interested in perceived effects (requiring a broad sample size) but rather objectively measurable influence in IS security risk management, which would not be gather-able in a broad fashion. A discussion of further limitations and future evaluation in a broader study is presented in the next section.

5.3 Analysis

The R Package "plsm" [20] was used to analyze the collected data. The descriptive statistics of the data are provided in Table 1 and Table 2.

We found that observed business process awareness (BPA_o – observed by researchers) explained better than the self-reported business process awareness (BPA_s – as reported by the stakeholders) the contribution to the number of elicited security requirements (0.639 vs 0.382). The more details on each business process the stakeholders omitted, the worse the elicited security requirements turned out: Number of omitted business process stakeholders, number of omitted information flow paths and number of omitted documentation artefacts could predict the number of new security requirements added during elicitation.

Out of those stakeholders that had an awareness level of 3 or 4 (partial or complete awareness), 100% of the security requirements (compared to the referential data set of security requirements elicited during the last IS security risk analysis) could be elicited by just including one stakeholder in the IS security risk analysis process. We observed that the "best" stakeholders outperformed the previous IS security risk analysis by eliciting one, two and in one case event three security requirements that were not included in the referential set, which could be explained by several awareness campaigns that happened since. This phenomena will be investigated in the future.

To analyze the resulting security requirements in terms of quantity and quality, we validated whether the elicited security requirements a) had an understandable description, b) were linked to at least one artefact of the underlying business process, and c) were linked to at least one business source (e.g. customer contract, law) that establishes the business need for each security requirement (c.f. the taxonomy we proposed in [19]). If all three conditions were met, we counted the security requirement as properly elicited. Then those security requirements were matched to the set of already elicited security requirements from a previous IS security risk analysis.

As a result, we could confirm the hypothesized relationship between stakeholders' awareness of business processes and their possible contribution to the IS security risk management process. Furthermore, we could confirm the hypothesized possibility to prioritize and select stakeholders based on their business process model awareness for participation in the IS security risk management process. The following section discusses the results in more detail and presents contributions to research and industry.

	Business Process 1									Business Process 2								
Stakeholder	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**
BPA_s	4	1	2	1	3	4	4	4	1	4	3	1	2	4	3	3	3	4
BPA_o	4	1	1	1	3	3	4	3	2	4	4	1	1	4	3	3	3	3
SR_n	13	2	2	3	10	10	15	11	5	8	11	2	6	7	11	5	2	11
% match	1.08	0.17	0.17	0.25	0.83	0.83	1.25	0.92	0.42	0.89	1.22	0.22	0.67	0.78	1.22	0.56	0.22	1.22
SR_m	12	1	2	2	9	8	12	9	5	8	9	1	4	7	8	2	2	7
% match	1.00	0.08	0.17	0.17	0.75	0.67	1.00	0.75	0.42	0.89	1.00	0.11	0.44	0.78	0.89	0.22	0.22	0.78
SR_a	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1
SR_r	1	2	2	1	0	2	2	2	3	0	3	2	2	0	2	3	0	1
BPC_p	0	3	4	5	1	1	0	3	3	0	0	4	2	0	3	2	4	1
%match	0.00	0.60	0.80	1.00	0.20	0.20	0.00	0.60	0.60	0.00	0.00	1.00	0.50	0.00	0.75	0.50	1.00	0.25
BPC_i	0	9	20	21	6	3	0	8	20	2	0	12	8	0	1	7	11	2
% match	0.00	0.43	0.95	1.00	0.29	0.14	0.00	0.38	0.95	0.17	0.00	1.00	0.67	0.0	0.08	0.58	0.92	0.17
BPCd	0	7	6	6	1	2	0	0	6	0	0	3	2	0	0	0	1	0
% match	0.00	1.00	0.86	0.86	0.14	0.29	0.00	0.00	0.86	0.00	0.00	1.00	0.67	0.00	0.00	0.00	0.33	0.00

Table 1. Results from the case studies (Business processes 1 and 2)

6 Discussion

The present paper examined stakeholder participation in IS security risk management processes. In a multi-method research study we assessed the impact stakeholders' business process model awareness had on the stakeholders' contribution to the IS security risk management process. Stakeholders' awareness of business process models was found to improve the elicited security requirements in both number and accuracy. Thus, stake- holder awareness of business process models was found to add value to an organization's IS security risk management process.

Self-assessment of stakeholders' business process model awareness was found to be a good indicator of a stakeholder's potential contribution to the IS security risk management process. Objective assessment of stakeholders' awareness of business process models outperformed self-assessment.

	Business Process 3									Business Process 4								
Stakeholder	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**
BPA_s	4	2	3	3	4	4	3	2	4	4	3	1	2	3	2	1	2	2
BPA_o	4	1	3	2	3	3	4	1	4	4	4	1	1	3	2	1	2	2
SR_n	14	3	4	10	11	12	11	1	16	7	8	2	1	1	3	1	5	6
% match	1.00	0.21	0.29	0.71	0.79	0.86	0.79	0.07	1.14	1.75	2.00	0.50	0.25	0.25	0.75	0.25	1.25	1.50
SR_m	4	3	3	7	10	12	10	0	14	10	4	2	0	0	3	0	3	0
% match	1.00	0.21	0.21	0.50	0.71	0.86	0.71	0.00	1.00	0.00	1.00	0.50	0.00	0.00	0.75	0.00	0.75	0.00
SR_a	0	0	0	0	0	0	0	0	2	3	3	0	0	0	0	0	1	1
SR_r	1	3	4	4	1	1	0	1	1	0	0	2	1	3	3	1	5	3
BPC_p	0	0	0	2	2	0	0	4	1	0	0	2	1	1	0	3	3	1
%match	0.00	0.00	0.00	0.40	0.40	0.00	0.00	0.80	0.20	0.00	0.00	0.67	0.33	0.33	0.00	1.00	1.00	0.33
BPC_i	1	1	3	3	1	6	0	5	1	0	0	9	10	9	10	11	9	8
% match	0.14	0.14	0.43	0.43	0.14	0.86	0	0.71	0.14	0.00	0.00	0.82	0.91	0.82	0.91	1.00	0.82	0.73
BPC_d	0	6	5	1	0	1	0	5	0	0	0	1	2	1	0	2	1	2
% match	0.00	1.00	0.83	0.17	0.00	0.17	0.00	0.83	0.00	0.00	0.00	0.50	1.00	0.50	0.00	1.00	0.50	1.00

Table 2. Results from the case studies (Business processes 3 and 4)

We found that awareness of documentation artefacts that are produced during or after a business process executes (e.g. checklists, protocols, requirement specifications), was the most important predictor for stakeholders' ability to contribute to the IS security requirements process.

6.1 Research Contribution

In extension to existing research on user participation in IS security risk management (e.g. [21, 12]), the present study examined how stakeholder awareness of business process models impacts the IS security risk analysis process. Both the qualitative and quantitative studies found evidence that the better the stakeholders involved in the IS security risk management process are aware of the business process under investigation, the better their contribution to the IS security risk management processes was. This study provides a first step towards the analysis of user behavior and stakeholder contribution to the IS security risk management process. Secondly, the multi-method research design of the study contributed a first classification scheme of business process model awareness for the assessment of stakeholders within IS security risk management process.

6.2 Implications for Practice

The results of the present study suggest that the IS security risk managers can prioritize user participation in the security risk process according to stakeholders' awareness of the underlying business process. Existing literature recommends to mostly focus on business process owners as a main source for the risk management process - which, without further differentiation, might lead to quality deficits as our study has shown. Instead, an objective assessment of stakeholders' awareness of business process models is a better strategy to select stakeholders for participation.

A second implication of the study is the call for increased business process transparency and better documentation of security requirements related to the business processes. Study findings suggest that there is a benefit from making business process knowledge available to all stakeholders. In particular it seems to be desirable to include IS security risk analysis results in the business process documentation as stakeholders remembering results outperformed stakeholders that had not been involved during the last analysis and had no available documentation (i.e. they could defer security requirements from an existing set of security requirements covering a business process known to them).

Finally, study findings suggest that user participation in the IS security risk management process is highly desirable and that this participation can lead to a better fit of IS security risk analysis results to the business needs.

6.3 Study Limitations

Several limitations of the study need to be acknowledged. First, stakeholder awareness of business processes was measured using both a self-reported assessment as well as an assessment based on the stakeholder's ability to recreate the business process model. Both measurements contain subjective errors and should be used with caution. In particular, the comparison between the self-reported and the observed

levels of awareness confirmed that the self-reported awareness levels must receive special attention.

A second limitation of the study is that it was conducted within the relatively low population of one organization. This limitation is applicable to all surveys with an in-depth focus on a problem from industry, where objective experimentation or broad surveys are not possible. To limit the threat to generalizability of the findings, we did not include industry-specific business processes in the investigation and made sure that the IS security risk analysis process did not require industry-specific knowledge.

A third limitation of the present study stems from the fact that stakeholder awareness of the business process was measured in individual settings. Due to organizational constraints at the organization under investigation, it was not possible to conduct group interviews or group modeling sessions. We tried to mitigate this by allowing stakeholders to access any organizational knowledge source (also call other stakeholders) to gather information if the stakeholder lacked complete business process awareness.

6.4 Suggestions for Future Research

The present study suggests two areas where future research would be valuable. First, a broad examination of individual user participation in IS security risks management and the impact of business process awareness would increase our understanding of stakeholder contribution in such settings. The present study examined business process model awareness from a rather high and abstract point of view. Particular aspects of the business process model might be worthwhile to investigate in further studies, including learning effects related to different modeling strategies and conventions as well as knowledge sharing effects between IS security risk management process stakeholders.

Given, that documentation artefact awareness was found to be an important indicator of potential stakeholder contributions to the IS security risk process it seems worthwhile to investigate security requirements documentation further. For example, how can the documentation of security requirements contribute to the alignment of business needs and IS security risk needs? Are creators of such documents better skilled for the IS security risk analysis process? How can information systems be used to improve the communication of security requirements?

7 Conclusions

The present study provides evidence that stakeholder participation in IS security risk management processes is not only desirable but the potential contribution of different stakeholders can be predicted by their respective awareness of the business process under analysis. IS security risk managers can utilize the results of the present study to prioritize the involvement of different stakeholders in the IS security risk management process without sacrificing quality of the results.

Acknowledgment This work was supported by the Austrian Federal Ministry of Economy (BMWFW), QE LaB - Living Models for Open Systems (FFG 822740), the Tyrolean business development agency through the Stiftungsassistenz QE-Lab, and partially funded by the European Commission under the FP7 project "PoSecCo" (IST 257129).

References

1. Peters S 2009 CSI computer crime and security survey. Computer Security Institute
2. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1): 1–11
3. Ernst Young (2011) Into the cloud, out of the fog; Global Information Security Survey. http://www.de.ey.com/GL/en/Services/Advisory/2011-Global-Information-Security-Survey---Into-the-cloud--out-of-the-fog. Accessed 25 Nov 2014
4. Siponen MT (2000) Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. Information Management & Computer Security 8(5): 197–209
5. Wade J (2004) The weak link in IT security. Risk Management 51(7): 32–37
6. Siponen MT, Oinas-Kukkonen H (2007) A review of information security issues and respective research contributions. ACM Sigmis Database 38(1): 60–80
7. Spears JL, Barki H (2010) User participation in information systems security risk management. MIS quarterly 34(3): 503–522
8. Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly 34(3): 523–548
9. Puhakainen P, Siponen M (2010) Improving employees' compliance through information systems security training: an action research study. MIS quarterly 34(4): 757–778
10. Siponen M, Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly 34(3): 487
11. Locke EA, Alavi M, Wagner III, John A (1997) Participation in decision making: An information exchange perspective
12. Ryan JJ, Mazzuchi TA, Ryan DJ et al. (2012) Quantifying information security risks using expert judgment elicitation. Computers & Operations Research 39(4): 774–784
13. Susanto12 H, Almunawar MN, Tuan YC (2011) Information security management system standards: A comparative study of the big five
14. Markus ML, Mao J (2004) Participation in development and implementation-updating an old, tired concept for today's IS contexts. Journal of the Association for Information Systems 5(11): 14

15. Kohlbacher F The use of qualitative content analysis in case study research. In: 7th Qualitative Social Research Forum, vol 7, pp 31–52
16. Vilhelm V Quantified security is a weak hypothesis: a critical survey of results and assumptions. In: 2009 Workshop on new Security Paradigms, pp 37–50
17. Maung K. Sein, Ola Henfridsson, Sandeep Purao et al. (2011) Action design research. MIS Q 35(1): 37–56
18. Parker DB (1981) Computer security management. Reston Publishing Company
19. Sillaber C, Breu R Quality Matters: Systematizing Quality Deficiencies in the Documentation of Business Security Requirements. In: Availability, Reliability and Security (ARES), 2014 Ninth International Conference on, pp in print
20. Sanchez G (2013) PLS path modeling with R. Online, January
21. Kirlappos I, Parkin S, Sasse Ma Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. In: 2014 Workshop on Usable Security, pp 21–37