Identifying Blind Spots in IS Security Risk Management Processes Using Qualitative Model Analysis

Christian Sillaber(✉) and Ruth Breu

University of Innsbruck, Innsbruck, Austria
{christian.sillaber,ruth.breu}@uibk.ac.at

Abstract. The present paper examines quality aspects of models created by stakeholders to identify blind spots in information systems security risk management (ISSRM) processes via a multi-method research study at the organizational level. Stakeholders were interviewed to gain an understanding of their awareness of business processes, models of the information system (IS), and related security requirements in the context of an ongoing ISSRM process. During several modeling sessions, stakeholders were asked to model various aspects of the IS under investigation in the form of component, activity and business process diagrams. We then analyzed the created models qualitatively and linked identified inconsistencies to security issues omitted during the ISSRM process (blind spots). The findings indicate that various quality aspects of models created by stakeholders that describe either the IS or related business processes can contribute to an improved ISSRM 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 ISSRM, this study highlights the importance of using and analyzing model diagrams from appropriate stakeholders at the right time during the ISSRM process to identify potential blind spots and avoid unclarity, that might be introduced by verbal communication. The research provides risk managers with a process for identifying blind spots to improve results and reduce overhead.

Keywords: Information systems security risk management · Stakeholder created models · Risk management process improvement

1 Introduction

As several studies have shown that most incidents related to IS security can be traced back to internal stakeholders (e.g. [1, 2]), IS security literature moved from portraying users as the weakest link in IS security (e.g. [3, 4]) to viewing them as the solution to multiple IS security issues in recent years (e.g. [5, 6]).

To answer calls for more empirical research in this area (e.g. [6–10]) the present paper investigates how models created by stakeholders during IS security risk analysis phases of the ISSRM process can be utilized to identify potential blind spots. The term blind spot is used in the context of this paper to denote any quality issue during the ISSRM analysis phase that might be due to omitted or miss- prioritized components,

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 252–259, 2015.
DOI: 10.1007/978-3-319-20376-8_23

overlooked security requirements, wrong assumptions about security properties and similar problems.

Based on the premise that, besides focusing on the participation of stakeholders as mere subjects of IS security policies, it is worthwhile to investigate already available artifacts, such as IS Security documentation, in ISSRM processes, the present paper's research question asks how these artifacts can bring value during analysis phases of the ISSRM process. User participation in IS development and its influence on IS 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].

The objective of this paper is to examine the utilization of models created by stakeholders in analysis phases of the IS security risk management processes and to examine how their quality impacts the ISSRM process. In doing so, this paper answers calls for empirical research on user participation in IS security risk management processes [12] and validates the findings in a case study at the organizational level.

The remainder of this paper is organized as follows. First, related work on user participation in ISSRM settings is briefly presented. Next, the study's multi- method research design is outlined, followed by the description of the exploratory study that examined model quality and its contribution to the ISSRM process. Finally, the paper concludes with a discussion of the implications of the study, limitations, and suggestions for future research.

2 Related Work

It has been repeatedly shown that the majority of incidents related to IS security can be traced back to internal stakeholders (e.g. [1, 2, 13]). IS security literature has been continuously moving from portraying users as the weakest link in IS security (e.g. [3, 4]) to viewing them as the solution to multiple IS security issues in recent years (e.g. [5, 6]). 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.

Following a synthesis of theories explaining user participation in IS security contexts, Spears et al. [6] define user participation in IS security risk management as the set of behaviors, activities, and assignments undertaken by business users during IS risk assessment and the design and implementation of IS security controls that is expected to add value to security risk management. While the value of stakeholder participation in general is backed by manifold studies, these approaches often reduce stakeholders to mere executors of business security requirements and their derived controls.

IS security risk management is the continuous process to identify and assess risk and to apply methods to reduce risks to an acceptable extent. Recent research has increasingly focused on human factors influencing the outcome of ISSRM processes, including behavioral theories [14] describing the entire ISSRM process or focusing on selected areas including security awareness [15, 16], security behavior [17], communication [18]

and the impact of audits [19] and standardization efforts [20]. In [21], the link between stakeholder knowledge on business processes and potential contributions to the ISSRM process were investigated as part of the same research project.

By focusing on the assessment (i.e. analysis) phase, we re-conceptualize 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 [15]. Therefore, the present paper examines the link between static artifacts i.e. IS security models and activities and the value they add to the ISRM process.

3 Analyzing Blind Spots in Models Created During ISSRM Processes

As this research was conducted as part of an ongoing research project at the organizational level, a mixed-method approach was chosen based on the premise that separate and dissimilar data sets from different settings would provide a richer picture and thus compensate for the fact that experimentations in IS risk management processes are difficult to conduct [22, 23]. We relied on a combination of data collection (models) and interviews with participants of the ongoing organizational IS security risk management process. Refer to [21] for an in-depth description of the research design.

3.1 Exploratory Study

During a several months lasting IS security and risk management process at the organizational level, an exploratory study was conducted to investigate the utilization of models created by stakeholders in ISSRM processes. The organization under investigation is one branch (≈100 employees) of a multinational engineering company, focusing on the development of distributed information systems within a highly regulated domain. Interview partners included employees at the project management level with a university degree in computer science or related areas. Multiple interviews with domain experts from the organization were conducted over a timespan of several months. Five semi-structured inter- views 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.

Interview partners were repeatedly asked to draw models of various aspects of the IS under investigation. These models included component diagrams, activity diagrams and business processes related to the IS. While the research results regarding models related to business processes are presented in [21], component diagrams and associated system models will be at the focus of interest in the remainder of this paper. Models created by the stakeholders were converted to UML compatible models (component diagrams and class diagrams) to enable further comparison and analysis.

3.2 Data Collection and Measurement Setting

We devised the measurement setting as shown in Fig. 1 to perform the investigation. The four step process was executed for each component of the IS under investigation:

- **Step 1: Stakeholder interview:** In this step, we asked stakeholders to describe the component under investigation and its security properties.
- **Step 2: Stakeholder created models:** In this step, we asked stakeholders to model the component under investigation.
- **Step 3: Creation of models for comparison:** Using the information gathered in step 1 and the model produced in step 2, we digitally created a sanitized model to remove ambiguity.
- **Step 4: Identification of blind spots:** We compared the models from step 3 and identified blind spots (i.e. differences in the models) in both the component model as well as the security requirements elicited by identifying differences in the models.

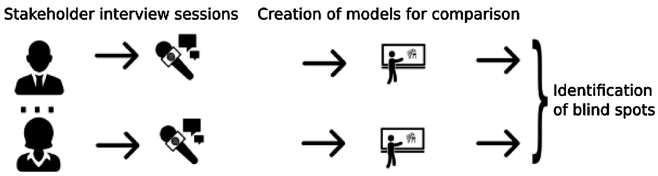

Fig. 1. Overview of the measurement setting (Icons made by Freepik from flaticon.com licensed under CC BY 3.0.).

Content Validity: We made an effort to ensure that the tasks were clearly understood by the participating stakeholders and that they responded to questions that we intended to ask. The entire process was conducted verbally and clarifications were provided by the researchers if needed. All stakeholders that participated in the study could access any organizational knowledge source that is normally available to them (internal documentation, internal wiki, etc.). They could draft their models on paper and/or a whiteboard.

Setting: We conducted each modeling session 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 components of the IS under investigation. All stakeholders were promised anonymity and the organization was promised confidentiality regarding specific security risk related results and the architecture of their IS.

Model Creation: Based on the input received from stakeholders during the sessions, models were sanitized and digitally recreated. All participants were IS professionals and were product managers 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.

3.3 Analysis

The descriptive results are provided in Table 1. We identified in total four types of potential blind spots. To analyze the resulting models and elicited security requirements in terms of quantity and quality, we validated whether the elicited security requirements had an understandable description and were linked to at least one component of the IS. Then we compared both the security requirements and the models created by each stakeholder against the models created for the same component by the other stakeholders.

Table 1. Model issues and identified blind spots in the ISSRM process.

Issue in model	# Identified	Blind spot found	Example
Omitted model element	18	Overlooked security requirements	A system component was omitted
Omitted association (to security requirement)	14	Wrong security requirements chosen	An insecure protocol was used for data exchange
Differently modeled components	7	Components with unclear security requirements	Stakeholders had a different understanding of several components of the IS and their security requirements
Omitted association (to component)	3	Missing stakeholder awareness	Several stakeholders did not select security requirements, contradicting organizational policies

As a result, we were able to identify several security requirements that were either not reflected in the IS under investigation or contradicted organizational policies. Furthermore, we were able to identify several components that were currently not aligned with organizational security requirements.

While most stakeholders were able to model the components correctly and elicit the correct security requirements for them (and vice versa), the majority of identified blind spots, as shown in Table 1 were overlooked security requirements. The second largest number of blind spots were omitted associations from either components to security requirements or vice versa. Examples for this category include valid components not linked to valid security requirements or valid security requirements linked to valid (but wrong) components.

By comparing the identified blind spots to the results of the ongoing ISSRM process, we found that all security issues identified during the ISSRM process were also identified by using our approach. A majority of blind spots (27/42) was identified after interviewing only two stakeholders and all blind spots were identified after interviewing four stakeholders - which lead to quicker results than the ISSRM process which required 9 interviews each.

4 Discussion

The present paper examined blind spots in IS security risk management processes using qualitative model analysis. In a mixed-method research study we assessed the models created by stakeholders during an ongoing IS security risk management process and used these models to identify potential blind spots.

Investigation of omitted model elements was found to improve the security risk management process by identifying security issues faster. Thus, qualitatively analyzing models created by stakeholders was found to add value to an organization's IS security risk management process.

4.1 Research Contribution and Implications for Practice

In extension to existing research on user participation in IS security risk management, the present study examined how artifacts created by stakeholders can improve the IS security risk analysis process. We found evidence that the analysis of models created by the stakeholders involved in the IS security risk management process contributes to the overall performance. This study contributes towards the growing body of knowledge on user behavior and stakeholder contribution to the IS security risk management process.

The results of the present study suggest that the IS security risk managers can and should utilize artifacts produced by stakeholders participating in IS security risk management processes. The findings of our study suggest that there is a benefit from making high quality documentation of the security of the IS available to all IS stakeholders (improving awareness). In particular, it seems to be desirable to properly document the security attributes of each component.

Finally, study findings suggest that active 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.

4.2 Study Limitations and Future Work

Several limitations of the study need to be acknowledged. First, the process of model creation was subjective and might depends on the stakeholder's ability to recreate the IS under investigation and might contain subjective errors.

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 minimized the number of industry-specific components 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 the modeling process was conducted in individual settings. Due to organizational constraints at the organization under investigation, it was not possible to conduct extensive group interviews or group modeling sessions. We tried to mitigate this by allowing stakeholders to access any organizational knowledge source (also contact other stakeholders) to gather information.

To improve the generalizability of this research in the future, we plan to apply the proposed research model at other organizations and compare against an objective ISSRM conducted by independent auditors, to remove subjective bias. Furthermore, we seek to refine the process model to include formalized methods of comparing stakeholder created models.

5 Conclusion

We analyzed models created by stakeholders as part of an ongoing IS security risk management process and compared them against models from other stakeholders and reference models (if available). We identified differences in the models and linked them to potential security issues. We identified several patterns and quality issues in models that correlate to blind spots in the ongoing ISSRM process.

The present study provides evidence that models created by stakeholders in ISSRM processes can be utilized to identify and remove potential blind spots and eliminate risks during early stages of the ISSRM process. IS security risk managers can utilize the results of the present study to identify potential blind spots quickly and efficiently prioritize efforts in ISSRM processes without sacrificing quality of the results.

Acknowledgements. This work was supported by the Austrian Federal Ministry of. Economy (BMWFW), QE LaB - Living Models for Open Systems (FFG 822740).

References

1. Ernst and Young's, Into the cloud, out of the fog; Global Information Security Survey, Young, Ernst. Technical report, November 2011
2. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
3. Wade, J.: The weak link in IT security. Risk Manag. **51**(7), 32–37 (2004)
4. Siponen, M.T.: Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. Inf. Manag. Comput. Secur. **8**(5), 197–209 (2000)
5. Stanton, J., Stam, K., Mastrangelo, P., Jolton, J.: Behavioral information security. In: Human-Computer Interaction and Management Information Systems: Foundations, p. 262. M.E. Sharpe, New York (2006)
6. Spears, J., Barki, H.: User participation in information systems security risk management. MIS Q. **34**(3), 503–522 (2010)
7. Vance, A.: Neutralizaiton: new insights into the problem of employee information systems security. MIS Q. **34**(3), 487–502 (2010)
8. Benbasat, I.: An empirical study of rationality-based beliefs in information systems security. MIS Q. **34**(3), 523–548 (2010)
9. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS Q. **34**(4), 757–778 (2010)
10. Siponen, M., Oinas-Kukkonen, H.: A review of information security issues and respective research contributions. ACM Sigmis Database **38**(1), 60–80 (2007)

11. Locke, E.A., Alavi, M., Wagner III, J.A.: Participation in decision making: an information exchange perspective. Res. Pers. Hum. Resour. Manag.: A Res. Ann. **15**, 293–332 (1997)
12. Markus, M.L., Mao, J.-Y.: Participation in development and implementation- updating an old, tired concept for today's IS contexts. J. Assoc. Inf. Syst. **5**(11), 14 (2004)
13. CSI, CSI Computer Crime & Security Survey, Computer Security Institute. Technical report (2008)
14. Alavi, R., Islam, S., Mouratidis, H.: A conceptual framework to analyze human factors of information security management system (ISMS) in organizations. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 297–305. Springer, Heidelberg (2014)
15. Spears, J.L., Barki, H.: User participation in information systems security risk management. MIS Q. **34**(3), 503–522 (2010)
16. Mejias, R.: An integrative model of information security awareness for assessing information systems security risk. In: 2012 45th Hawaii International Conference on System Science (HICSS), pp. 3258–3267 (2012)
17. Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E.: Understanding nonmali- cious security violations in the workplace: a composite behavior model. J. Manag. Inf. Syst. **28**(2), 203–236 (2011)
18. Heath, R.L., O'Hair, H.D.: Handbook of Risk and Crisis Communication. Routledge, London (2010)
19. Steinbart, P.J., Raschke, R.L., Gal, G., Dilla, W.N.: The relationship between internal audit and information security: an exploratory investigation. Int. J. Account. Inf. Syst., Research Symposium on Information Integrity and Information Systems Assurance **13**(3), 228–243 (2011)
20. Peltier, T.R.: Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press, Abingdon (2013)
21. Sillaber, C. Breu, R.: Using business process model awareness to improve stakeholder participation in information systems security risk management processes. In: Conference on Wirtschaftsinformatik (2015, in press)
22. Kohlbacher, F.: "The Use of Qualitative Content Analysis in Case Study Research", Forum Qual. Soc. Res. **7**, 31 (2006)
23. Verendel, V.: Quantified security is a weak hypothesis. In: Proceedings of the 2009 workshop on New security paradigms workshop - NSPW 2009, p. 37 (2009)