Case Study Role Play for Risk Analysis Research and Training

Lisa Rajbhandari and Einar Arthur Snekkenes

Norwegian Information Security Laboratory, Gjøvik University College, Gjøvik, Norway

Abstract. Typically, a risk analysis may identify and document sensitive and confidential information regarding threats, vulnerabilities, assets and their valuation, etc. The intrusive nature of the risk analysis process makes it difficult for researchers (or students) to gain access to scenarios from operational organizations for evaluating (or training on) risk analysis methods. In order to resolve these issues, we propose Case Study Role Play (CSRP). We elaborate the use of CSRP in combination with the Conflicting Incentives Risk Analysis (CIRA) method to analyze privacy risks to an end-user from using the eGovernment service. This paper contributes by demonstrating how CSRP helps to establish a platform for doing risk management related research and training in a 'reasonably' realistic environment, where confidentiality, sensitivity issues, red tape and the need for permissions do not create roadblocks. Furthermore, CSRP ensures that the time and resources needed to set up the required environment is low and predictable.

1 Introduction

Risk analysis helps to identify and estimate risks, and to provide insight suitable for deciding if risk exposure needs to be changed. That is, if a treatment action is needed, or a high risk exposure is more cost effective. Here, we focus on risk analysis in the context of information security and privacy management.

Typically, an information security risk analysis may identify and document sensitive and confidential information regarding threats, vulnerabilities, assets and their valuation, etc. Most of the risk analysis method evaluations are usually presented with a toy example. In [13], Kotulic et al. state that due to the sensitivity issues, they faced difficultly in validating their model. Their study was declined by majority of the organizations they had contacted. They write "we learned, the hard way, that developing a research stream in an emerging, organization-sensitive area requires major personal, financial and professional commitments far beyond what most researchers can afford to expend". Information Security Management (ISM) is about people rather than technology. Training students in core ISM skills requires access to a representative teaching environment, for e.g., an operational business setting. However, in the context of information security risk management, researchers/ students (referred to as *practitioners* from here on, in situations where it fits both) cannot usually be cleared for access to sensitive information and will not be permitted to perform representative vulnerability discovery activities. These issues create a blockage for public research or training on risk analysis methods.

Rajbhandari L. and Arthur Snekkenes E..
Case Study Role Play for Risk Analysis Research and Training.
DOI: 10.5220/0004599500120023
In *Proceedings of the 10th International Workshop on Security in Information Systems* (WOSIS-2013), pages 12-23
ISBN: 978-989-8565-64-8

Risk analysis case study research may have multiple objectives such as discovering new unknown vulnerabilities, validating a method (checking how well it performs, if it is usable, scalable) and for providing a real life like training platform. In this paper, we focus on the latter two stated objectives. We can use case study research in two settings: non-interventive and interventive. In a non-interventive case study, the practitioner is basing his work on information that can be obtained without interacting with the organization in question. In most cases, the bulk of the information will be from written sources. In an interventive case study, individuals from the organization in question will participate in activities initiated by the practitioner. This typically includes answering questions or following procedures prescribed by the practitioner.

These two approaches have very different performance characteristics. The interventive case study may give rise to increased costs for the organization in terms of lost time. Furthermore, sensitive information regarding members of staff, technology, procedures, plans etc. may be disclosed to a third party (the practitioner). For example, the construction of psychologic profiles of a large number of members of staff to be used in a risk analysis will in general be time consuming, intrusive and sensitive. Kotulic et al. [13] state that information security research is highly intrusive in nature, thus it is hard for the organizations and individuals to trust an outsider trying to gain data about their security strategies or practices. Unless the researcher is able to convince the organization that he is providing significant value, there is no reason for the organization to consider offering access - not even conditioned on the signing on an NDA (Non- Disclosure Agreement). When security is at stake, access will be even more restricted. There is always the possibility that the parties involved will not respect the NDA. Clearly, a prudent organization will take this risk into account when deciding if a third party is to be offered access.

The non-interventive case study is only suitable for research where the required information is readily available and when one is not doing research into the interaction process itself. In a non-interventive case study, findings will typically be illustrated through examples rather than through aggregated data. This represents an additional challenge, since in many cases, the researcher would like to publish the results. This challenge manifests itself as a lack of published work reporting on the use of risk analysis for non-trivial scenarios.

A resolution towards the above issues is proposed by specifying and demonstrating the Case Study Role Play (CSRP) method. CSRP is developed from the integration of case study [23], persona [5] and role play [22]. In CSRP, data is collected from the individuals playing the role of the fictitious characters rather than from an operational setting. In our study, role play as a mechanism helps in mimicking behavior (that would yield sensitive output) for producing non-sensitive output. Apart from creating the persona for the users (which is normally done in user centered design), we create personas of a wide range of stakeholders e.g. CEO, IT Manager and System Administrator. Moreover, in our approach, each role as described in the persona and scenario is played by a real person. By doing this, we can extract information from the participant as required by the risk analysis method.

In this paper, we investigate- ‘Can CSRP be used as a platform for risk analysis research and training, resolving the inherent problem of risk analysis findings’ sensitiv-

ity and confidentiality?'. The Conflicting Incentives Risk Analysis (CIRA) method [19] addresses human aspects of information security. Thus, CIRA seems an ideal candidate for demonstrating CSRP. Typically, when applying CIRA in a real life risk analysis activity, it will produce sensitive information as depicted in Fig. 1(a). Note that $CIRA_1$, $CIRA_2$ and $CIRA_3$ corresponds to the structural data collection phase, numerical data collection phase and analysis phase of the CIRA method (explained in Sect. 4). However, when using CSRP with CIRA, the information extracted will be non-sensitive as illustrated in Fig. 1(b).

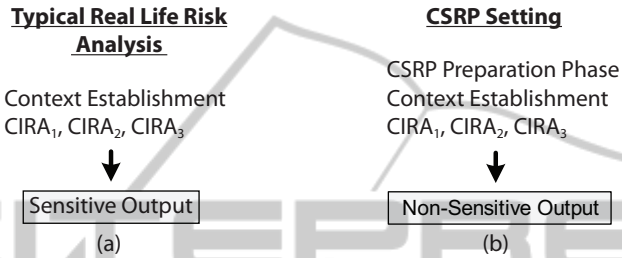

Fig. 1. Steps and output of CIRA in (a) Typical real life risk analysis and (b) CSRP setting.

This paper contributes by demonstrating how CSRP helps to establish a platform for doing risk management related research and training in a 'reasonably' realistic environment, where confidentiality, sensitivity issues, red tape and the need for permissions do not create roadblocks. CSRP can be used as a platform for improving/ gaining new knowledge about risk analysis methods. Furthermore, CSRP ensures that the time and resources needed to set up the required environment is low and predictable. However, CSRP may not be particularly well suited for discovering actual risks in an operational system unless the role play closely matches a real organization.

The remainder of this paper is organized as follows. Related work is presented in Sect. 2 followed by the explanation of CSRP approach in Sect. 3 and summary of CIRA in Sect. 4. In Sect. 5, we provide an overview of how CSRP was utilized in one of our case studies to analyze the privacy risks. In Sect. 6, we discuss the results, limitations and lessons learned from using CSRP, and provide suggestions for future work. Finally, we conclude the paper in Sect. 7.

2 Related Work

Our study is inspired by the work on the use of case studies, personas and role play. These, along with risk analysis and management methods, are briefly described and discussed below.

2.1 Risk Analysis and Management Methods

There are many classical risk analysis and management approaches and guidelines in the context of information security such as the ISO/IEC 27005:2008 standard [12] (its new version ISO/IEC 27005:2011), the ISO 31000 standard [11] (that supersedes

AS/NZS 4360:2004 [2]), NIST 800-39 [16] (that supersedes NIST SP 800-30 [21]; its revised version NIST 800-30 Rev. 1 [17] is a supporting document to NIST 800-39), CORAS [14], TVRA [6], Risk IT [10] and OCTAVE [1]. For conducting an effective risk analysis and management, the inputs from the stakeholders need to be considered and the results need to be communicated.

Depending on the depth of the analysis to be conducted, these methods involve gathering of sensitive and confidential data. For e.g., in the ISO/IEC 27005:2008 standard [12], when defining the scope of risk management, information about the organization is collected so as to determine its operational setting/ environment. The information includes the organization's strategic business objectives, strategies and policies, business processes, the organization's functions and structure, information assets, constraints affecting the organization, etc. Besides these, other relevant information necessary for conducting risk analysis is collected throughout the process. According to the ISO 31000 standard [11] risk management relies on the foundation of the best available information. The information sources as per the ISO 31000 standard include historical data, experience, stakeholder feedback, observation, forecasts and expert judgment. In Risk IT [10], the 'collect data' process under risk evaluation domain is dedicated to gathering data on the organization's operating environment and risk events in order "to enable effective IT related risk identification, analysis and reporting".

2.2 Case Study

According to Yin [23], a case study is "an empirical inquiry that investigates a contemporary phenomenon in depth and within its real life context, especially when the boundaries between phenomenon and context are not clearly evident". Case study is a method that is widely used in research but many view it as being subjective, lacking rigor, requiring less effort than other research methods e.g. experiments. Yin [23] and Flyvbjerg [7] have pointed out and clarified these misunderstandings about case studies by providing relevant examples and explanation. Even though they emphasize these in relation to social science, we think their explanations are relevant for our area of focus. Flyvbjerg further states that the benefit of a case study is that "it can close in on real-life situations and test views directly in relation to phenomena as they unfold in practice" [7].

2.3 Persona

Persona [5] is typically employed in user centered design for system development projects. Persona are fictitious characters that are built to represent the users' needs and goals. It was used by Cooper [5] in order to remove biases of the programmers that resulted in their own assumptions and opinions about the 'user' for which the system was being designed. He phrased this act as "designing for the elastic user". For him, persona should be believable with specific details and each persona should be distinct by their descriptions and scenarios in relation to their respective goals. Personas are designed based on empirical data collected from representative users. Typically, data is collected using methods such as interviews, ethnography, workshops and observations to create good description of the user. However, when the empirical data might not be

easily elicitable, e.g. in the case of an attacker, an assumption persona can be used [3]. According to Atzeni et al. [3], the assumptions may be derived from different sources of data for the type of individuals that are known to attack the systems.

Nielsen [15] explains how to write a good description of the user i.e. how to describe the 'user' as a character in a way that engages the readers. She states that it is important to consider the users' environment, character traits, goals and tasks. A persona is brought to life by giving it "a name, a life, a personality as well as a portrait" [9]. Pruitt et al. [18] states that persona is not a science but a powerful tool that helps to engage people in an effective way. After all, one of the incentives behind using persona is to use it as a means for communication or discussion.

2.4 Role Play

Role play has been used in entertainment (theater/ movies), research, education, clinical training and therapies. Role play is the way of "deliberately constructing an approximation of aspects of a real life episode or experience" which is controlled (initiated and/ or defined) by the investigator [22]. According to Greenberg et al., role play is used in organizational research to learn about attitudes and behaviors of individuals in organizations and to understand about the basic psychological processes [8]. Even though role play can be conducted for various studies, they point out that in all of the cases, it differs in three dimensions: level of involvement, role being played (self/ other) and degree of response specificity provided.

3 Case Study Role Play

CSRP is obtained from the integration of case study [23], persona [5] and role play [22]. In CSRP, data is collected from the individuals playing the role of the fictitious characters rather than from an operational setting. In our study, role play as a mechanism helps in mimicking behavior (that would yield sensitive output) for producing non-sensitive output. The CSRP preparation phase consists of the following steps:

Determine the Objective of the Activity. We first decide the objective of the activity e.g. whether it is to mimic an operational setting for the purpose of gaining knowledge about the performance of a risk analysis method or to provide a real life like training platform.

Select the Organization. We then select the organization that would be appropriate for the above identified activity e.g. bank, software company.

Familiarization with the Method. The practitioner needs to get familiar with the risk analysis method to be used for the analysis. The information and procedural requirements of the risk analysis method need to be identified.

Design and Build the Organization. We design an abstract form of the selected organization considering all information and procedural requirements required to carry out the risk analysis activities. The requirements may include identifying the objective of the organization, stakeholders, service architecture, process flow, etc. To capture the essential features of that context, experimental setting with equipments may also be set up. After the stakeholders are identified, it is followed by persona and scenario construction, role play selection and guidance as given below.

Persona and Scenario Construction. For each of the identified stakeholders, we design the personas and develop the scenarios. The intention behind constructing persona is to communicate who the stakeholders are, what they are like, what their roles/ tasks are, what their needs are, etc. Attributes such as name, age and gender are assigned to the personas. The possible behavioral variable types proposed by Cooper [5] are used where applicable which includes activities, attitudes, aptitudes, motivation and skills. These are derived from the empirical data or assumptions of stakeholders in a certain situation or from existing data sources.

In our case, scenarios are written to provide the background information of the role to the participants. The background information includes the goals, needs of an individual and how one can accomplish it. Besides that, it also includes the details of the company or the system a person is working on for which the risk analysis is being conducted. While developing the scenario to be provided to the participant, the narrative is written such that it helps the participant to be able to imagine her/ himself in that position as required by the persona. The narrative makes the technological knowledge about the system and process/ flow easier to comprehend for a non-expert.

Role Play Selection and Guidance. The participants are selected to play the role of each persona. At first, the initial approval for participation needs to be gathered. It should be made clear that as the participants are playing a role/ character, the personal data of the participant will not be collected. Moreover, the participation should be voluntary and the results completely anonymous.

Each of the players are provided with a set of instructions explaining how to play the role that he has been assigned. For instance, when doing the risk analysis of an information system, the role of the user can be played by someone who is using a similar system or has some knowledge about it and hence should be representative of general users. However, in cases where a close match is not available, for instance, in the case of the hacker, someone who has knowledge or has done research about the hackers can be selected. Alternatively, the data can simply be collected based on research work about hackers.

Finally, the selected risk analysis method is applied and data as required by the method are gathered from the participants by conducting interviews, through questionnaires, etc.

4 Summary of the Conflicting Incentives Risk Analysis Method

CIRA [19] identifies the stakeholders, their actions and perceived expected consequences that characterize the risk situation. There are two classes of stakeholders: the

strategy owner and the risk owner. The strategy owner is the stakeholder who is capable of triggering an action that will influence the risk owner. Typically, each stakeholder is associated with a collection of actions that he owns. The risk taker is the stakeholder whose perspective is taken when performing the risk analysis, that is, he is the stakeholder at risk. Utility is the benefit as perceived by the corresponding stakeholder and it comprises of utility factors. Chulef et. al. [4] identify utility factors relevant for our work. Each utility factor captures a specific aspect of utility, for e.g., prospect of wealth, reputation, social relationship. The procedure in CIRA consists of context establishment and three phases as shown in Fig. 1(b), which are explained below:

$CIRA_1$ **(Structural Data Collection).** This phase consists of the identification of stakeholders, their utility factors and actions. Based on the case description, the risk taker and his key utility factors are identified. Note that these utility factors are informally identified by the risk analyst from the case description and later finalized by interviewing the respective stakeholders. Secondly, the actions that can influence the risk taker's utility factors are identified. Then, the roles that may have the opportunities/ capabilities to perform these actions are identified. Finally, the strategy owners that can take on these roles and their utility factors are determined.

$CIRA_2$ **(Numerical Data Collection).** This phase consists of determining how the utility factors can be operationalized, how the stakeholders weigh the utility factors and how the various actions result in changes to the utility factors for each of the stakeholders.

$CIRA_3$ **(Analysis).** The risks to the risk owner are determined and evaluated.

5 Using CSRP for CIRA Research and Training

In this section, we explain how CSRP is utilized for evaluating the performance of CIRA and to provide a real life like CIRA training platform. We used CSRP in one of our studies, to analyze the privacy risks facing the end-user of an eGovernment service. The details on the case and the overall application are provided in [20]. Below, we provide an overview of the procedure as depicted in Fig. 1(b).

CSRP Preparation Phase. The objective of using CSRP was to mimic an operational setting for the purpose of gaining knowledge about the performance of the CIRA method. We selected A-SOLUTIONS (that manages an Identity Management System) as an organization to carry out the study. The process of eliciting the data from the stakeholders involved in the actual operational setting using the CIRA method gave rise to sensitivity and confidentiality issues. This is because, when analyzing real life scenarios, personal information of the stakeholders such as their preferences, goals, actions and information about their wealth, reputation, status, etc. may need to be collected. In our case, this data is sensitive and data collection is considered intrusive.

We then created an abstraction of the fictitious organization anticipating information required by CIRA. We assumed A-SOLUTIONS manages an authentication system called NorgID and a portal (ID-Portal). Their goal is to provide secure access to digital public services. NorgID is one of the identity providers which provides authentication for logging on to a federation called 'ID-portal'. It provides the end-user cross-domain Single Sign-On (SSO), i.e., the end-user needs to authenticate only once and can gain access to many services by using the portal for eGovernment services such as tax, health care and pension. The stakeholders were identified followed by the persona and scenario construction, participants' selection as explained below.

Persona and Scenario Construction. During the study, we created the persona "Bob" to represent an end-user, based on the assumption that he is concerned about privacy. The synopsis of the persona for Bob is given in Table 1.

Table 1. Personas of the stakeholders.

Role	Name	Description
End-user	Bob	30 years old, local school teacher, regular user of NorgID with general IT knowledge; aware of some privacy issues mainly due to the media coverage of data breaches.
CEO	John	50 years old, ensures the overall development and relationship with its stakeholders; has motivation to increase the company's service delivery capacity.
System Admin	Nora	29 years old, known for her friendly behavior and highly trusts her co-workers; ensures the system is functioning properly and secure; manages the access permission for internal staffs to the server; in her absence to assure that co-workers get proper system function, she usually lets them access servers and even shares important credentials to the server.

Instead of having someone that represents the general population of users, Bob portrays a specific end-user. Apart from Bob, we can construct personas, for e.g., for individuals that are concerned about privacy but use the service rarely or never as shown in Fig. 2. We considered Bob as the primary persona i.e. the individual with the main focus in our analysis.

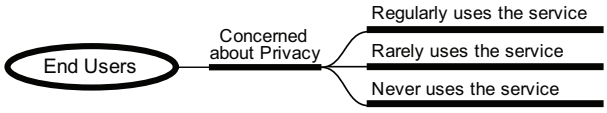

Fig. 2. Categories of end-users for which the personas can be constructed.

Similarly, for other stakeholders, the personas were created. The synopsis of the personas are given in Table. 1. Due to space constraint, we leave out the description of the hacker that was included in the study [20]. Then, for each of the stakeholders, the scenario was written to provide background information. For example, the scenario description for Bob included the brief description of the eGovernment service, for what purpose he uses it, how it works and what personal information is collected by the service. The scenario description for the other two stakeholders included the description of the company and the functionality of the system.

Role Play Selection and Guidance. The participants were selected for each of the persona. All the participants were IT literate. At first the initial approval for participation was gathered. Then, each of the participants were introduced to the persona and the scenario description was explained. The participants were also given an explanation about the process of data collection for the study.

Context Establishment. CIRA is implemented starting with context establishment which includes defining the scope and boundaries of risk analysis, objectives of the organization, etc.

$CIRA_1$ **(Structural Data Collection).** In our scenario, the risk taker is the end-user (Bob). We identified the key utility factors for Bob which were privacy, satisfaction from using the service and usability. Then, the actions that can influence Bob's utility factors were identified. Here, we focused on the actions that cause privacy risks to Bob such as secondary use (*SecUse*) and breach of confidentiality of his information caused by sharing credential (*ShareCred*) by the other stakeholder. We identified the roles that may have the opportunities to perform these actions and the stakeholders (i.e. the strategy owners) in those particular positions. We considered the strategy owners as the CEO (John) and the System Administrator (Nora) of the company operating the eGovernment service in the position to execute the SecUse and ShareCred strategies respectively. Then, we identified the utility factors of interest to these strategy owners.

$CIRA_2$ **(Numerical Data Collection).** In our case, the necessary data (e.g. weights for the utility factors) as required by CIRA were collected through interviews and surveys from the participants representing Bob, John and Nora. In this way, data can be collected through role play from participants rather than from those in an operational setting.

$CIRA_3$ **(Analysis).** Finally, the risks to Bob were determined and evaluated. It was determined that Bob faced higher risk in terms of breach of confidentiality of his information than that of his information being used for secondary purpose. This is because when John (CEO) executed the *SecUse* strategy, it resulted in negative utility for both himself and Bob. However, when Nora (System Administrator) executed the *ShareCred* strategy, it resulted in positive gain for Nora and loss for Bob.

6 Discussion

In this section, we include (a) results that are beneficial to the practitioners, (b) explain limitations and lessons learned from using CSRP and (c) provide suggestions for further work.

Results. The application of CSRP proved beneficial as it helped to analyze the risks faced by an end-user when using the eGovernment service without having to worry about the intrusive nature of the study and the hassle of getting access to an operational case study and the stakeholders in an operational setting [20]. It was easy to communicate the details to the participants using CSRP because of the narrative nature of persona and scenario.

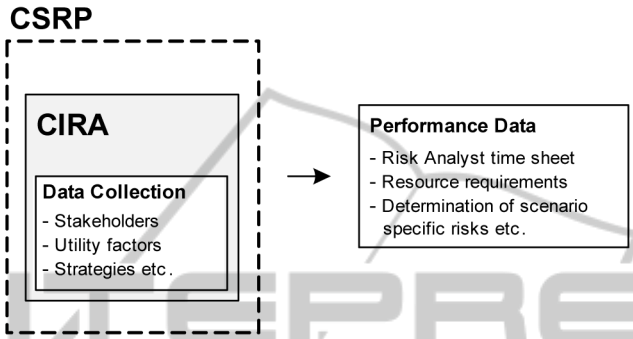

Fig. 3. Samples of data collected to assess CIRA performance using CSRP.

Fig. 3 depicts data collected using CSRP to assess the performance of CIRA. The data collection in CIRA includes the structural data (e.g. stakeholders, their utility factors) and numerical data (e.g. values of the utility factors) as explained above. By using CSRP, we were able to collect CIRA performance data such as the approximate time required for the analysis, determination of scenario specific risks and resource requirements.

Limitations and Lessons Learned. CSRP is an approach with a primary focus on method specific research with the objectives of validating a method or for providing a real life like training platform. It can also be used for discovering new unknown vulnerabilities of a system. However, it may not be particularly well suited for discovering actual risks in an operational system unless the role play closely matches a real organization.

One of the issue identified was- 'What happens if participants deviate from their roles (e.g. provide wrong information) ?'. This issue may or may not have an impact depending on the objective of using CSRP. If one is using CSRP for training the students to use a risk analysis method or determining the performance of a method (e.g. time required running the method), the issue of not having the 'correct' answer from the participant might not impact the study. However, if one is interested in determining a specific vulnerability of a system, then the issue of deviation might have a considerable impact on the result of the study.

The participant should have enough information to play the role correctly. For this, the personas and the scenario developed should be such that it is easy for the participants to engage or mimic it. Extensive research is needed to make sure that the assigned persona are good/ valid representations of the stakeholders rather than depicting the point of view of the person writing the persona (as pointed out by [9]). Thus, construct-

ing the right persona(s) is a challenge for the practitioner.

Even though it is made clear to the participants that they are playing a role, it is likely that they feel their choices represent their personal opinion. Thus, it is important to communicate clearly about the process to the participants at the beginning and also during the implementation phase. Getting inspiration from processes used to train actors may be beneficial. However, there is always a limit to how well this will be grasped by the participants. We are also considering professional or student actors as players in CSRP.

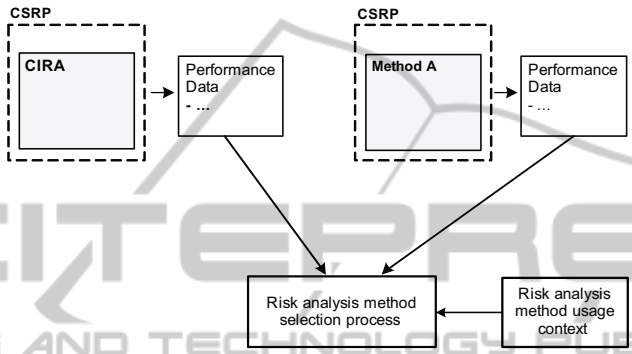

Fig. 4. CSRP as part of a risk analysis method selection process.

Future Work. More work is needed to reduce the above identified limitations. We think CSRP can be used with other approaches such as ISO/IEC 27005:2008 [12], Risk IT [10]. However, this needs to be explored further. Furthermore, one possible utilization of CSRP can be to assess the performance of other risk analysis methods e.g. Method A as shown in Fig. 4. Then, the collected performance data of CIRA and Method A can be compared allowing the most appropriate risk analysis method for a given project to be selected.

7 Conclusions

This paper provides an important contribution to information security management. It explains how CSRP can be used as a research and training platform for gaining new knowledge about risk analysis methods while resolving the inherent problem of risk analysis findings' sensitivity and confidentiality. We expect that CSRP will facilitate an increase in the body of published knowledge on the performance of risk analysis methods. It seems reasonable to expect that this platform will result in improved risk analysis methods.

Acknowledgements

The work reported in this paper is part of the PETweb II project sponsored by The Research Council of Norway under grant 193030/S10.

References

1. C. Alberts and A. Dorofee. Managing information security risks, The OCTAVE approach. Addison Wesley, 2002. ISBN 0-321-11886-3.
2. AS/NZS 4360. Risk management. AS/NZS, 2004.
3. A. Atzeni, C. Cameroni, S. Faily, J. Lyle, and I. Flechais. Here's Johnny: a Methodology for Developing Attacker Personas. ARES, pages 722–727, 2011.
4. A. Chulef, S. Read, and D. Walsh. A Hierarchical Taxonomy of Human Goals. Motivation and Emotion, 25(3):191–232(42), September 2001.
5. A. Cooper. The Inmates Are Running the Asylum. Macmillan Publishing Co., Inc., Indianapolis, IN, USA, 1999.
6. ETSI TS 102 165-1 V4.2.3 (2011-03). Method and proforma for Threat, Risk, Vulnerability Analysis. ESTI, 2011.
7. B. Flyvbjerg. Five Misunderstandings About Case-Study Research. Qualitative Inquiry, 12(2):219–245, 2006.
8. J. Greenberg and D. E. Eskew. The role of role playing in organizational research. Journal of Management, 19(2):221–241, 1993.
9. R. Gudjonsdottir. Personas and Scenarios in Use. PhD thesis, KTH, Human - Computer Interaction, MDI, 2010. QC20100629.
10. ISACA. The Risk IT Framework, 2009.
11. ISO 31000. Risk Management – Principles and Guidelines. ISO, 2009.
12. ISO/IEC 27005. Information technology -Security techniques -Information security risk management, 1st edition, 2008.
13. A. Kotulic and J. Clark. Why there aren't more information security research studies. Information & Management, 41(5):597–607, 2004.
14. M. S. Lund, B. Solhaug, and K. Stølen. Model-Driven Risk Analysis: The CORAS Approach. Springer, Heidelberg, 2011.
15. L. Nielsen. From user to character: an investigation into user-descriptions in scenarios. In Proceedings of the 4th conference on Designing interactive systems: processes, practices, methods, and techniques, DIS '02, pages 99–104, New York, NY, USA, 2002. ACM.
16. NIST. NIST SP 800-39, Managing Information Security Risk - Organization, Mission, and Information System View, 2011.
17. NIST and U.S. Department of Commerce. NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012.
18. J. Pruitt and J. Grudin. Personas: practice and theory. DUX 2003, ACM Press, 2003.
19. L. Rajbhandari and E. Snekkenes. Intended Actions: Risk Is Conflicting Incentives. In D. Gollmann and F. Freiling, editors, Information Security, volume 7483 of Lecture Notes in Computer Science, pages 370–386. Springer Berlin / Heidelberg, 2012.
20. L. Rajbhandari and E. Snekkenes. Using the Conflicting Incentives Risk Analysis Method. In L. Janczewski, H. Wolf, and S. Shenoi, editors, 28th IFIP TC-11 International Information Security and Privacy Conference SEC. Springer, 2013. (accepted for publication).
21. G. Stoneburner, A. Goguen, and A. Feringa. NIST SP 800-30, Risk Management Guide for Information Technology. NIST, July 2002.
22. K. M. Yardley-Matwiejczuk. Role play: theory and practice. Sage Publications Limited, 1997.
23. R. K. Yin. Case Study Research: Design and Methods, volume 5 of Applied Social Research Method Series. Sage, 4th edition, 2009.