Participative Design of a Security Risk Reference Model: an Experience in the Healthcare Sector

Lou Schwartz[1], Eric Grandry[1], Jocelyn Aubert[1], Marie-Laure Watrinet[1] and Hervé Cholez[1]

[1] Luxembourg Institute of Science and Technology, 5, avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg

{lou.schwartz, eric.grandry, jocelyn.aubert, marie-laure.watrinet, herve.cholez}@list.lu

Abstract. In this paper, we propose a participative method to design a security risk reference model, composed of a domain model and a security risk model. We relate the application of the method to our attempt for a design of a national reference model of the medical laboratories in Luxembourg, for which we ran five participative workshops with domain experts to gather their knowledge. We validated the designed models with both the participating experts and non-participating experts. The design method and the structure of the participative workshops are described and results obtained are discussed.

Keywords: Participative Sector-specific Modelling, Enterprise Model, IS Security Risk Management, Healthcare Sector, Medical Laboratories

1 Introduction

The healthcare sector is undergoing profound changes that are triggered by diverse and opposite drivers [1]: a demographic shift leading to an increase in chronic diseases and a need for continuity of care, associated with increased patient expectations in terms of healthy living and quality of life; increasing costs of medication and medical devices generated by the pace of technological innovation (smart living, genetics, nano-medical universe) associated with an economic pressure to reduce social security spending. Healthcare providers have to cope with these challenges by leveraging multiple system integration solutions: the development of new collaborations (business process integration, organizations' merger, etc.); the sharing of medical and IT resources (technical integration); the development of electronic health records system (data integration). These integration points require information flowing beyond the classical healthcare organizations boundaries [2] and lead to increased risks in information security.

In order to address these increased information security risks, we propose sector-specific risk analysis approaches relying on a security risk model and a domain model of the sector [3]. This paper describes the approach we have developed to acquire and

S. España J. Ralyté, P. Soffer, J. Zdravkovic and Ó. Pastor (Eds.):
PoEM 2015 Short and Doctoral Consortium Papers, pp. 1-10, 2015.

structure the knowledge of a sector in a participative way. It then gives insights on the experimentation of the method with medical laboratories.

1.1 Cooperative approach to improve enterprise model quality

According to Barijs [4], the quality of both the modelling process and modelling product is linked to collaboration, participation and interaction: completeness and accuracy of the enterprise model, as well as speed and efficiency of the modelling effort are positively impacted by (1) the collaboration of modellers, analysts and domain experts; (2) the participation of domain experts and employees to acquire shared knowledge; and (3) interactions' ease to capture the complexity of the system under observation. The integration of domain experts in the modelling activity can be envisaged from two perspectives [5]: first in the participatory approach to modelling, stakeholders meet in modelling sessions, led by a facilitator, to create models collaboratively; or in consultative participation, where an analyst creates the model and the domain experts are consulted to validate the outcomes.

Our approach is inspired by participatory modelling and has been built incrementally, along a path of experiments. In previous research [6], we experimented on participative knowledge gathering in the telecommunication sector. The interest of the domain experts' involvement was validated, however our approach was not structured enough to be easily repeated and continuously improved. In our healthcare case, we have structured a participative modelling method, inspired by existing approaches, and validated it in the design of a reference model for information security risks.

2 A participative modelling method

The sectorial demand in Luxembourg is important for the creation of national ISSRM models (professionals of the financial sector, telecommunications, e-archiving, and now, health sector). That is why we need to define a structured process to gather the essential information needed for the creation of national reference models, and also to make this method transferable to the market at a later moment. Our objective is to define a reproducible participative design method that satisfies participants in terms of collaboration, information sharing and results, and involving business experts of the addressed sector. Furthermore, the method should sufficiently support the modelling experts by gathering the right information at the right time.

2.1 Method description

The method we have developed combines activities from facilitated group modelling and consultative participation: (1) the domain experts participate in the knowledge acquisition; they however do not directly manipulate the model; (2) a facilitator leads the modelling session with techniques borrowed from the creativity domain; (3) the modelling experts participate in the modelling sessions, but also

formalise the knowledge offline; (4) the domain experts are consulted to ensure that the shared knowledge is reflected in the final model.

The method is composed of a set of performed functions: (a) Domain Knowledge Acquaintance is performed by the Modelling Experts; (b) Co-Modelling Workshop Organisation is performed by the Modelling Facilitator, with the support of the Modelling Experts; (c) Knowledge Acquisition and Sharing are performed by all roles in participative workshops; (d) Sectorial Model Consolidation is performed by the Modelling Experts; (e) Sectorial Model Validation is performed by Domain Experts, with the support of the Modelling Experts.

The process is run iteratively and the reference model is built incrementally: each iteration focuses on a specific aspect of the model (environment of the system, processes and activities, technical architecture and infrastructure, security threats and vulnerabilities, information security risks) and is the object of a specific three hour workshop with all participants.

From an organisation perspective, the modelling experts' team is made up of four persons, two experts in Enterprise Modelling and ArchiMate [7], and two experts in ISSRM. We doubled the roles of modelers to ensure a completeness of the models: two persons capture more information than just one, and negotiation between them is a first step of validation. They all have previous experience in collaborative modelling. The facilitator is an expert in creativity techniques and focus group animation. None of the team members had any particular knowledge of healthcare.

2.2 Validating the method in a medical laboratories' ecosystem

We experimented with our participative modelling method in the context of the medical laboratories. The participative workshops were designed on the basis of the information we wished to collect to build the domain and security risk models. Five participative workshops were necessary.

Two private medical laboratories and one hospital laboratory composed the sectorial committee. One to three representatives of each actor attended the workshops. Different profiles were identified and required in order to smoothly run the workshops: biologists, software engineers and business intelligence experts.

During the Domain Knowledge Acquaintance, the modelling experts gathered some preliminary information on the sector: they identified industry standards and the legal framework relevant for the medical laboratory activities: ISO 15189 [8] and the Luxembourg National Public Health Code [9], as well as ISO 27799 [10] and the Guide to Information Security for the Health Care Sector [11] were analysed. During the Co-Modelling Workshops Organisation, the modelling experts and the facilitator planned the workshops according to the structure of the models that were to be designed. After each participative workshop, the modelling experts consolidated the knowledge (Sectorial Model Consolidation) in specific modelling language (ArchiMate models for the domain model and risk catalogues for the risk model). These models were validated with the domain experts (Sectorial Model Validation), to ensure that they actually reflect the outcomes of the participative modelling effort.

3 Participative workshops

The participative workshops and their associated results are presented below.

3.1 Workshops description

WS0: Objectives and approach. In the first meeting with the sectorial committee, we presented the detailed objectives of the project and the participative approach. We also took benefit of this first session to collect both the suggestions and potential objections. Some participants were particularly worried about exchanging potential confidential information with their competitors. We proposed a Non-Disclosure Agreement, and offered them the possibility to exchange sensitive information offline in private meetings or per email.

WS1: Identify the environment of medical laboratories. The objective of the first participative workshop was to draw a high-level view of the ecosystem: identify the types of medical laboratories; identify and classify the services; and identify the involved actors.

We identified the types of laboratories through a short brainstorming session and compared the outcomes with the literature. We only identified differences in naming.

To identify common delivered services we first proposed an interactive approach, but participants were still reluctant to "physically" participate. We continued with successive brainstorming and open discussions to identify the common delivered services, their categorization and the involved actors. The correlation between types of laboratory and the services was performed through an open discussion. We quickly observed a common approach between medical laboratories.

WS2: Business layer. During this workshop, the objectives were the validation of the first domain model built, and the description of processes and activities.

We presented the ArchiMate model built from WS1 and validated it with the participants.

Following this, the processes identified in the literature and the inputs gathered in the first workshop were presented to participants. For each process, we asked participants to detail the performed activities, as well as the entry and exit conditions (see Table 1-a). Each activity was then specified along the following dimensions: *who* (actors), *what* (objects and information manipulated), *where* (site) and *how* (systems used to perform the activity), see Table 1-b. We interactively built a matrix of the activities: the matrix was displayed on the wall, and we positioned sticky notes to model the multiple aspects of each activity. The colour of the sticky notes was associated with one of the specific dimensions. We prepared sticky notes in advance as an outcome of our Domain Knowledge Acquaintance activity; we were also adding new sticky notes on demand, based on the input of the participants.

Table 1. (a) Matrix displayed to support discussion on process definition. (b) Matrix displayed to support exchanges on the activities definition. Different colours were used for each concept. This is only an illustration of possible results.

Steps (a)	Step 1	Step 2	Step 3
Begin End Activities			

Functions	Step 1		Step 2		Step 3		Support functions	
(b)	Activity1	…	Activity i	…	Activity n	…	Activity x	…
Who What Where How								

WS3: Infrastructure layer. The third participative meeting was dedicated to the identification of the generic infrastructure.

First, we started with the usual validation of the consolidated domain model integrating the outcomes of the WS2. Participants proposed minor changes. We then switched to the modelling of the generic infrastructure supporting the business activities. For each activity, the participants detailed the involved supporting assets (hardware, software, network, people, facility and system). As they were quite reactive to the matrix presentation, we continued with a matrix displayed on a wall (see Table 2). Literature review and previous session allowed us to prepare a list of potential items of each category on sticky notes.

Table 2. Matrix displayed to support exchanges on the generic infrastructure definition. Different colours were used for each concept. This is only an illustration of possible results.

Functions		Step 1		Step 2		Step 3		Support	
		Activity1	…	Activity i	…	Activity n	…	Activity x	…
Supporting assets	Devices Software Networks People Facilities Systems								

WS4: Generic infrastructure finalisation and security risk awareness. In this workshop we finalized the generic infrastructure and gave some introductory information security risk training to the participants. This was required to ensure a shared view on the concepts of information security risk, as the participants were not experts in this area.

The proposed scales (risks, threats, vulnerabilities and impacts) were presented and discussed. Only the impact scale required adaptation to the specific context, and we

scoped the adaptation in the WS5. We observed a disengagement of some participants during this phase: the session was a lot less interactive than the others, and we were requesting participants to acquire a large set of new knowledge.

To finish in a participatory manner, a brainstorming allowed listing the generic threats identified by participants in their specific domain. After a check, we observed that the threats listed by participants are quite the same as the generic threats listed in literature.

WS5: Generic security threats and vulnerabilities. The last workshop was dedicated to the identification of threats and vulnerabilities, and the definition of the scales used in our information security risk model.

We asked the participants to state if the threats (identified in WS4) may concern the previous listed activities, and to identify generic vulnerabilities that can be exploited by these threats (see Table 3). We did this exercise by group of activities to avoid a too huge cognitive load. In this step it is important to remember the supporting assets: it helps to identify the vulnerabilities.

Finally, the propositions for risk, threat and vulnerability scales were quickly presented and validated. The impact scale required more attention. For each component of the impact (Availability, Integrity, Confidentiality and Non-repudiation) participants defined the extreme values, then the intermediate values, and finally, reformulated the definition of each value.

Table 3. Matrix displayed to support exchanges on threats and vulnerabilities elicitation.

Functions		Step 1		Step 2		Step 3		Support	
		Activity1	..	Activity i	..	Activity n	..	Activity x	…
Supporting assets	Devices Software Networks People Sites Systems	*Defined previously* *Defined previously*		*Defined previously* *Defined previously*		*Defined previously* *Defined previously*		*Defined previously* *Defined previously*	
Threats	Threat 1 Threat 2 … Threat n	Vulnerability 4		Vulnerability1 Vulnerability 2 Vulnerability 6		Vulnerability 5 Vulnerability 7		Vulnerability 3	

3.2 Model consolidation and continuous improvement

Between each workshop, the modellers worked on the modification of the different models to integrate the inputs of participants. In particular, between WS2 and WS3, the collected data was aligned to the literature findings on standard models in the healthcare sector. Between WS4 and WS5, the non-repudiation criterion was added to

the basic impact scale at the request of domain experts, and the listed threats were compared to the generic threats from literature.

3.3 Results

Domain Model. The Domain Model has been built during the workshop sessions by addressing the multiple views on the system: (operating and support) functions and activities, localisation, roles, information, IT application and infrastructure.

Information System Security Risk Management (ISSRM) Model. The ISSRM model for healthcare has been built based on a generic ISSRM domain model [12] in which sector-specific generic concepts (i.e. assets, threats, vulnerabilities, security requirements, etc.) have been specialized and specified based on the initial review of the literature as well as based on the workshops results.

4 Validation

The main objective of the proposed method is to improve the way the information is collected from domain experts, i.e. the modelling process. The product of the process (the model) has also been validated: (1) A first internal check was done by modelling experts with regard to the national regulation and ISO standards. Then, each part of the produced models was validated by domain experts during specific steps of the participative workshops. (2) After the WS5 we validated the ISSRM model with external ISSRM experts. (3) As we identified several minimal differences between hospital and private medical laboratories, we plan to meet medical laboratory representatives from other hospitals and present the model to check the differences. If other differences appear, we will discuss the necessity to split the domain model into two specific sub-domain models. (4) The domain model will be presented to the specific instance regulating the healthcare sector for validation. (5) Finally, the use of the generic ISSRM model during risk analyses that will be done by laboratories in the future will enable to verify the completeness of the model.

4.1 Satisfaction of participants

In previous works, we had validated the value of a participative approach in the design of sector-specific ISSRM model. In order to improve the approach, we structured the activities in a method and experimented it in the medical laboratories' sector. We distributed a questionnaire to business experts at the end of the participative phase, to measure how they perceived the participatory aspect of the method, with a pair Likert scale from 1 (Not satisfied at all) to 4 (Very satisfied). We asked them how they perceived the consideration of their comments (M=4 SD=0.52), the diversity of exchanged points of views (M=4, SD=0.52), the possibility to express themselves (M=4, SD=0) and the listening and exchange between participants

(M=3.5, SD=0.55), see Fig. 1. With regard to these results, we checked the interactivity of the participative sessions. Furthermore, we achieved our goal of designing reference models: the modelling experts gathered the necessary information to build and check them with participants. We also identified room for further improvements; some of them will be implemented before running our next experiment, while others require additional research and development.

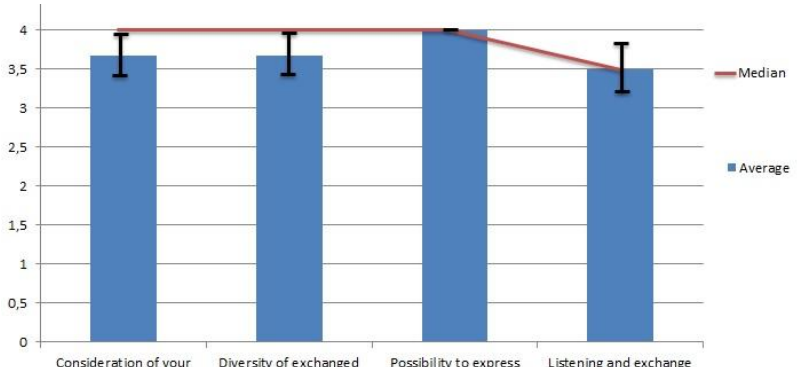

Fig. 1 Satisfaction of business experts on the participative aspect of the method

4.2 Advantages in modelling

The proposed method brings valuable improvements compared to our previous experience in the telecommunication sector, not only in terms of the experts' participation, but also in terms of produced artefacts. We actually structured the domain model in a (semi)formal modelling language: the collaboratively designed domain model represents the agreed common knowledge of the domain experts, and is a very useful input to drive the design of the associated ISSRM reference model.

The involvement of multiple medical laboratories' representatives in participative workshops enables to reduce the time needed to acquire knowledge from all of them. It also easily leads to consensus during the discussion itself, therefore also reduces time in negotiation: the composition of the domain experts' committee allowed us reviewing three visions and reaching consensus. This enabled to complete the information of each other directly and to negotiate on finding the more generic point of view when different possibilities were enumerated.

The quality of information provided by the participants permits us to quickly reach a high level of quality in the produced models, for both the domain and the information security risks sides. The model quality is checked by the fact that all experts in the domain understand it, and that it is useful for its purpose: the models are actually currently being exploited to support information security risk analysis.

Although we have given them the opportunity to adopt private sessions to protect confidential information, none of the involved laboratories have asked to share information offline, without their competitors. We can assume that the active participation of each laboratory created enough trust in the process, and also that we managed to adopt the right level of details in the design of the model.

The co-modelling workshops organisation activity also helped to share the same language between the modelling experts themselves and the modelling facilitator. This step facilitated the consolidation of the different models.

It may be noted that laboratories' representatives participated well and were involved throughout the workshops. That is a key factor of success for this method of participative modelling.

4.3 Issues in modelling

The quality of the model depends both on the modelling process and on the available knowledge. It was important to have representatives of each kind of laboratory in Luxembourg, i.e. private and public (hospital) laboratories were represented. Although the organization of their activities might differ a lot, they were able to build a common view on both the domain and the risks. This type of approach depends of the skills of participants, their openness and willingness, even though this can be improved by animations techniques. As a matter of fact, some participants prefer certain animations techniques over others; this required certain agility in the use of participative method and particularly of the proposed design method.

Our modelling approach covers the traceability aspect: what is the source of information of which of the model's elements. This is very useful when dealing with the evolution of the sources, such as a legal framework. It is relatively straightforward to implement when we face (semi-)structured information, such as reports, standards, or laws. However when dealing with participative discussion, it brings a new challenge in terms of information traceability.

5 Conclusions and future work

To build a national reference domain and an ISSRM model of the Luxembourg healthcare sector, we began to model the medical laboratories' activities. This step was realised thanks to five participative workshops involving representative domain experts (bio-analysts, IT and business intelligence profiles) from two of the three national private medical laboratories and one hospital laboratory. The participative workshops focused on several aspects of the system: processes, activities, IT infrastructure and information security risks of the laboratories. We observed a large part of commonality in these aspects among the participating laboratories, enabling us to quickly produce a complete generic domain model and an ISSRM model. These models are still under validation for some aspects, but, with regard to first checks, seem relatively complete and coherent.

The proposed participative method to collect, model and validate the information with domain experts was very useful. Based on this observation, the method will be reproduced soon with the Emergencies services and Radiology laboratories in order to incrementally design a reference national healthcare model. This will give us the opportunity to check the replicability of the method.

Some improvements have already been identified, notably to better support the traceability of information used to build the model. The consolidation of the models is also an area for improvement: we currently have to take the outcomes of the participative workshops in the form of flipcharts, pictures, sets of sticky notes, and transform these into elements of a modelling language. We worked on the semantic mapping and shared the same meta-model between any representation, (regardless of whether it is an ArchiMate model or a bunch of sticky notes). We now also envisage working on the infrastructure that will help us to digitalize the gathered information earlier in the process, but without losing the interactivity associated with the manipulation of the real objects, like reported by Ionita [13].

Acknowledgments. The authors thank the participants: *Les Forges du Sud*, *Ketterthill* and *Hôpital Robert Schuman*. The project is funded by FEDER.

6 References

1. UCL European Institute: Future of Healthcare in Europe-Meeting Future Challenges: Key Issues in Context. (2012).
2. KPMG Economist Intelligence Unit: The Future of Global Healthcare Delivery and Management. (2010).
3. Mayer, N., Grandry, E., Feltus, C., Goettelmann, E.: Towards the ENTRI Framework: Security Risk Management enhanced by the use of Enterprise Architectures. In: Advanced Information Systems Engineering Workshops. Springer International Publishing (2015).
4. Barjis, J.: Collaborative, participative and interactive enterprise modeling. In: Enterprise information systems. pp. 651–662. Springer (2009).
5. Stirna, J., Persson, A., Sandkuhl, K.: Participative enterprise modeling: experiences and recommendations. In: Advanced Information Systems Engineering. pp. 546–560. Springer (2007).
6. Mayer, N., Aubert, J., Cholez, H., Grandry, E.: Sector-based improvement of the information security risk management process in the context of telecommunications regulation. In: Systems, Software and Services Process Improvement. pp. 13–24. Springer (2013).
7. The Open Group: ArchiMate 2.0 Specification. Van Haren Publishing, The Netherlands (2012).
8. ISO 15189:2012: Medical laboratories -- Requirements for quality and competence. International Organization for Standardization, Geneva (2012).
9. Journal Officiel du Grand-Duché de Luxembourg: Loi du 16 juillet 1984 relative aux laboratoires d'analyses médicales.
10. ISO 27799:2008: Health informatics -- Information security management in health using ISO/IEC 27002. International Organization for Standardization, Geneva (2008).
11. eHealth Ontario: Guide to Information Security for the Health Care Sector. (2010).
12. Mayer, N.: Model-based management of information system security risk, (2009).
13. Ionita, D., Wieringa, R., Bullee, J.-W., Vasenev, A.: Investigating the usability and utility of tangible modelling of socio-technical architectures. (2015).