Towards a Risk-Based Security Requirements Engineering Framework

Nicolas Mayer, André Rifaut, Eric Dubois

Centre de Recherche Public Henri Tudor
Centre d'Innovation par les Technologies de l'Information (CITI)
29 Av. John F. Kennedy, L-1855 Luxembourg, Kirchberg
{nicolas.mayer, andre.rifaut, eric.dubois}@tudor.lu

Abstract. Information Systems (IS), particularly e-business systems, are required to be more secure in order to resist to the increasing number of attacks. Security is no longer just a desirable quality of IT systems, but is required for compliance to international regulations. The Requirements Engineering (RE) community has started to make successful contributions in the domain of security engineering. This concerns the integration of RE techniques at the early stages of security engineering, as well as the iterative management of security requirements, due to the intertwining between requirements and software architecture design. This paper proposes to complement these results by adapting and integrating another key activity of security, namely risk analysis. The aim of this paper is to show, that using and adapting an appropriate set of existing tools and techniques of risk analysis methods, improves the effectiveness of an iterative security engineering method starting at the earliest stage of IS development.

1 Introduction

IS development is typically top-down, at the opposite of most popular and traditional security methods, that are most often applied in a bottom-up fashion [5], starting from the analysis of the architectural design once it has been produced. As a consequence, there is a gap between security requirements and business security needs. This often results in a mismatch between the security components and the business. It is thus generally accepted that early stages of IS development must be concerned with security aspects.

RE community has started to be aware of this problem in the last years and a lot of security requirements engineering approaches has been developed. For example, in the framework i*, the analysis of security requirements is based on the concept of strategic social actors [19]. This framework allows the modelling of a wide range of concepts from business aspects to architectural aspects. Other efforts like those regarding the use of Problem Frames [10] have shown the inevitable intertwining existing between the elicitation of requirements and the elaboration of the system architecture.

The aim is now to best fit the security components of the IS with the strategic objectives of the business; in other words, to improve the business alignment of the IS. For example, in the case of a business service like an Intranet, is it better to secure it with a

password or with a certificate associated with a PKI[1]? The PKI is more secure, but the analysis should consider the value of the asset: what are the impacts on the business if a non-authorised user is using the service? This technique of linking the risk impacts with the business value is well identified in a security component called risk analysis.

Risk analysis is considered as central in all proposed professional methodologies. Moreover, more and more regulation bodies, like the Basel II agreement [1] for financial institutions published in 2004 (imposed on most banks of the world), support the improvement of risk management systems. Those systems should include the creation of a corporate culture about risk management; in particular, they advocate that risk analysis should be done at all stages of IS development.

Our proposal is therefore to improve techniques proposed in the RE literature, by the integration of a risk management component, supporting an iterative security engineering process, starting at the earliest stages of IS development process. Although the techniques used are well-known, their integration into a rigorous framework supported by tools is original. The engineering activities are driven by key indicators based on a risk analysis, ranging from the business context down to the architecture.

Section 2 introduces the basis of the iterative security engineering process supporting the alignment with the business. It introduces also the case study, which is a fragment of a medical application that will be presented within the framework i*. Section 3 explains the security engineering process driven by the risk and business analysis. Section 4 details the key risk and business indicators being at the core of our method. Then Section 5 illustrates the method through its application on the case study. Finally Section 6 summarizes the work and concludes with future works.

2 Iterative security engineering aligned with business

The development of secure IS results from a process involving many concepts and knowledge domains, such as business constraints and architectural constraints. However, in this section, it is shown that an iterative process, starting at the earliest stages of RE activities is very effective. Our proposal is illustrated with the fragment of a case study in the medical domain.

2.1 Case study

The aim of the example is the design of a new IS for Health Insurance. The IS shall be able to store and manage requests for reimbursement. Due to lack of space, only security aspects of the database will be addressed, the database being the most sensitive IS component. It contains patient personal information (e.g. phone number and email address) in addition to the patients' medical treatment information. The IS shall protect the privacy of patients and their associated medical records. The confidentiality of data shall be guaranteed. Moreover, the database shall be available for allowing the access of patient medical information in case of urgent need. These security goals are analysed in the next sections.

[1] Public Key Infrastructure

2.2 IS security alignment with stable business assets

There is a general agreement amongst scientists and practitioners to recognize the importance of IT alignment with business. So our proposed method relies on the integration of requirements, security and architectural engineering activities. Moreover, as it can be seen in Figure 1, risks are at the core of the alignment between business and IT systems. One difficulty to overcome is the rapid changes of business requirements, even

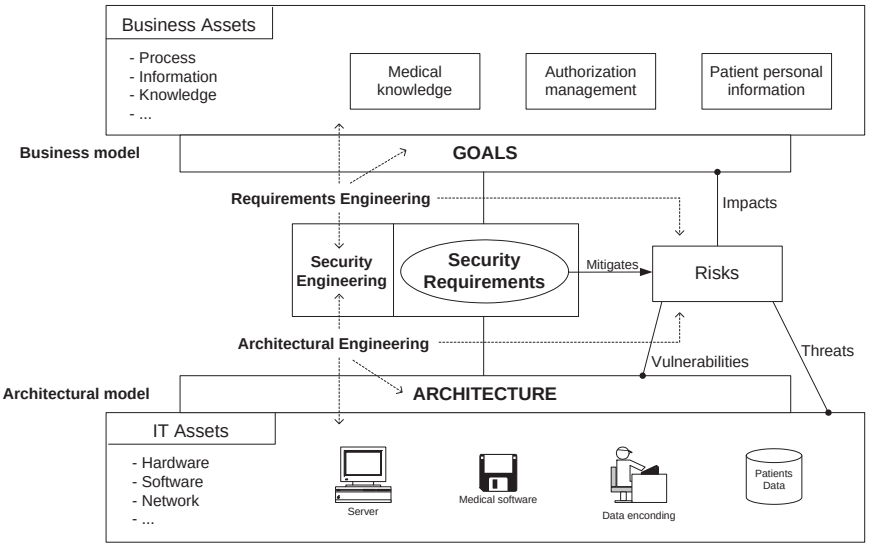

Fig. 1. Engineering domains of design

during the IS development. However, keeping the focus on business assets, which seem more stable, is an opportunity for IT system development, in order to be better aligned with business.

Assets are anything that has economic value to the organization and that is central in the realization of its business objectives. Securing them is essential. Figure 1 shows different kinds of business assets. For example, in our case study, information business assets are patient personal information, a process business asset is a medical authorization management, and knowledge business assets is the medical domain knowledge. *Requirements Engineering* is recognized to make the link between these business assets and the other system engineering domains, such as *Architectural Engineering* (AE).

Lots of contributions has already been done in the RE community for modelling the business and its assets [26] [13]. Business Process Modelling, Enterprise Modelling [27] and Use Cases [31] are well-known proposed techniques. The framework i* aims at a more detailed analysis of organisational environments, in particular the analysis of goals and dependencies between actors and sub-systems, which are important to lay down the strategy of IS development [21] [22]. The KAOS approach [29] has specialized the goal analysis technique to critical system engineering (e.g. safety-critical

systems), which is more adapted for securing critical business assets. We base our approach on these techniques and improve them with security risk management.

2.3 An iterative IS security engineering interacting with requirements and architectural engineering

At the operational level of most organisations, business assets management heavily rely on IT systems and IT resources. Most of the processes are mostly implemented in electronic systems, and the organization sensitive information are stored in databases and transmitted on computer networks. For example, the medical system exchanges the patient data and medical data on IT networks. When a detailed traceability is performed during IS development, it is easy to link business assets to those IT processes and resources, which are called *IT assets*, and are concerning every assets linked to the IS and its environment. They are of different kinds: a data server (hardware), an application server (software), the physician encoding data (human), etc. The IT assets are usually best modelled through *Architectural modelling* techniques.

A detailed presentation of architectural modelling cannot be included in this paper. However, the efficiency of the proposed method is improved when architectural modelling is generated semi-automatically. Existing works are done in this direction. For instance, the Model Driven Architecture (MDA) aims at easily generating platform dependent architectures from platform independent architectural descriptions made in UML [24]. This alleviates the work needed for the iterations between security engineering and *Architectural Engineering* (AE).

An important rationale in computer science is the separation of concerns. However, for *Security Engineering* it is important to address the wide range of information modelled by RE and AE. Indeed, when modifying any model element produced by the RE activity or the AE activity, this may cause major modifications in the models of security engineering. For instance, detailing some security requirements can introduce new business assets, which may cause other security requirements to be modified.

Some proposals are made in RE for dealing with security at the earliest stage of IS design. In the NFR framework [4], security is a class of non-functional requirements . Security aspects can be modelled in UML with proposals to extend the Use Cases models, such as Misuse Cases [7] and Abuse Cases [8]. These aspects are also considered in the CORAS UML profile [28]. Jackson's Problem Frames has also been extended with Abuse Frames [11] [12] to model security aspects. Our work proposes to complement these approaches with a tighter integration of risk analysis during all the incremental stages of the IS architecture elaboration. This may also guarantee a better business/IT alignment.

2.4 The i* modelling framework

As already mentioned, business and architectural modelling are key models for improving the development of security requirements. It is a good way for identifying the enterprise structure, goals, and business assets and to maintain the traceability from the IT assets down to security components of the IT system.

The i* framework was developed for the modelling and analysis of organizational environments and their information systems [21] [22] [23]. The framework is based on the intentionality relations between actors which represent human agents as well as sub-systems. The dependencies between actors can be of four types: Goal, Resource, Task and Softgoal[2] . The case study involves three actors: Health Insurance, Patient and Database. Patient depends on Health Insurance for health reimbursement. On the other side, there is a dependency between Health Insurance and the database for data checking and updating. Finally, there are two softgoals between actors, considered as security goals: Health Insurance depends on the database availability and patient depends on the database for keeping his personal information confidential.

Figure 2 presents the i* model of the initial example.

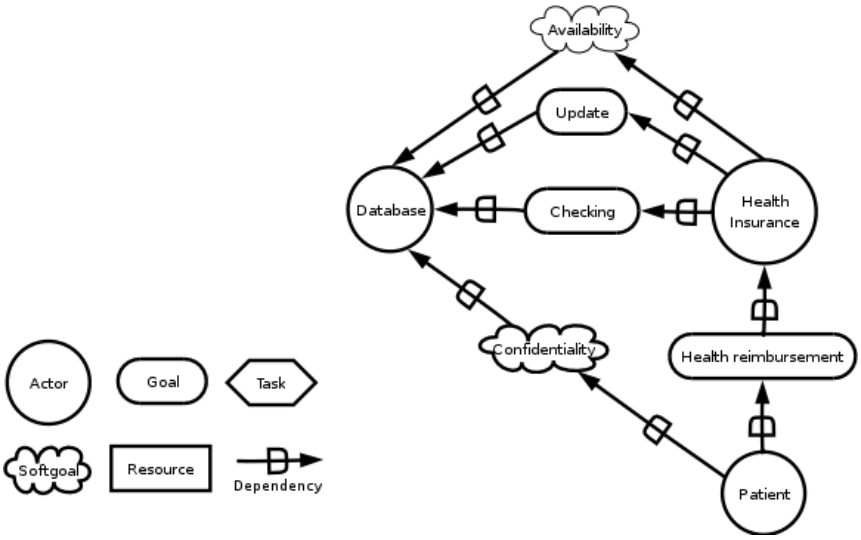

Fig. 2. i* representation of the case study in the initial step

The IT system architecture can also be modelled within the framework i*. *Means-end* links allow to detail the goal achievement into sub-goals. *Decomposition* links provide a hierarchical decomposition of goals into tasks and subtasks. The tasks found at the bottom of the hierarchy define closely requirements on the IS. Although those links are important for our approach, they are not illustrated here. This makes the framework i* being a cornerstone of our method because it best fits our modelling needs: i* provides a set of tools and techniques for analysing and gluing a wide range of models, from business models to architectural models and, as already mentioned, it is suited to model security aspects [20] [19].

[2] Softgoals are goals that do not have a clear-cut criterion for their satisfaction

3 Adapting risk analysis to early security engineering

After having focussed on the analysis of business and IT assets, it is necessary to explain how to secure them against the risks they are exposed to. Only IT risks will be considered, excluding, for example, financial (investment) or organizational risks (like hiring a new CEO). The way security will be implemented must always be continuously aligned with the business. Even if, from the technical side, a PKI guarantees a high security level, customers might not accept that solution, since the value of the business assets is not enough to justify the high development and exploitation costs of a PKI. In order to get the alignment with business, the proposed method puts forward the use of well-known techniques, that can ease the analysis of different alternatives and, therefore, facilitate the selection of the best security choices for the business.

3.1 Security and RE activities

The process of security engineering can be characterised in terms of four main activities. As depicted in Figure 3, the risk analysis is set apart from those four activities, because in our method, it is the driver during the iteration of those four activities.

- **Context analysis and assets identification**
  This activity is not specific to security engineering, but also exists for systems development, aiming at the improvement of the IT alignment with business. As explained in section 2, the business assets and the IT assets are modelled. IT assets are often modelled in terms of architectural components. The business goals are also modelled, using goal-oriented method. Some examples of assets and business goals were presented in section 2.
- **Security goal determination**
  For each asset, it is necessary to identify the goals needed to secure it. Those goals are similar to business goals, but specialised to security aspects. They are called security goals and are usually expressed in terms of confidentiality, integrity and availability. More recent types of security goals are also commonly used, such as accountability or authenticity. For example, a security goal is the confidentiality of the information (business level) stored in a database (IT level).
- **Security requirements elicitation**
  The security requirements are the refinements of the security goals. However, requirements should be free of all technological biases. Risk analysis is the preferred tool used to determine this refinement. It helps to choose the security level (high,...,low) best suited for protecting an asset. Refinements in i* are modelled with means-end links. Common security requirements are access control policy (for a confidentiality goal) or non-repudiation of operations (for the integrity goal of an automated process) [14].
- **Countermeasures selection**
  Once the security requirements are selected, countermeasures (or safeguards) should be chosen in order to satisfy them. Countermeasures refer to security solutions suited to security requirements. When countermeasures are selected, a possible residual risk is evaluated. In order to keep countermeasures aligned with business,

their cost should also be evaluated. More importantly, countermeasures can result in the introduction of new additional assets, goals or requirements, which all have costs that must be evaluated against the initial business purpose. Security countermeasures are for example a firewall, an encryption module or a physical security of a building.

3.2 Risk analysis

Before explaining the specificities of our iterative risk analysis, let us explain the concepts of risk and risk analysis, and discuss about the limits of the current risk analysis methods.

Risk is defined as the combination of the probability of occurrence of harm and the severity of that harm [30]. IT risks are generally further decomposed into three components:

```
Risk = Threat * Vulnerability * Impact
```

In other words, risk is characterized by the opportunity of exploiting one or multiple vulnerabilities, from one or many entities, by a threatening element using an attack method, causing an impact on business assets. This definition is used in this paper. *Risk analysis* is the activity of analyzing threat, vulnerability and impact on each component of the system. Its purpose is to give an accurate ratio between the probability of attack (internal or external, accidental or intentional) and the cost of a failure, and to measure the residual risk after applying countermeasures.

Most of the traditional risk analysis methods are often used very late in the IT system development life cycle. Usually, security engineering activities, including risk analysis, occur when the system is already in operation. We can cite some methods used in the industry, like OCTAVE [17] in the USA, EBIOS [15] and MEHARI [16] in France or CRAMM in the UK.

The method proposed in this paper advocates that security engineering should begin at early stages of IT system development, including the use of risk analysis. This position is in accordance with recent research results like the CORAS UML profile [28]. In [25], the proposed framework for security RE includes the risk elements. The proposal in [2] is to extend the modelling framework i* with risk analysis components. The concepts presented in this section are notably modelled with this extension. Toval et al. are also developing a risk analysis method specific to the early stage of system development [9]. However, their work focuses more on the reuse of security requirements.

The method presented here is also in accordance to recent works showing that RE methods give best results when used in an iterative approach of IT system development. Moffet already urged to use an iterative process for IS design [6], or Laney et al. recommend ”to move backwards and forwards between architectural and requirements perspectives” [10]. The work presented in this paper pushes forward those works in the security engineering domain, by constraining this iterative process to be consistently focussed on the risk and costs analysis. Risk identification will be assisted by knowledge bases extracted from risk methods presented before. This is detailed in the next section.

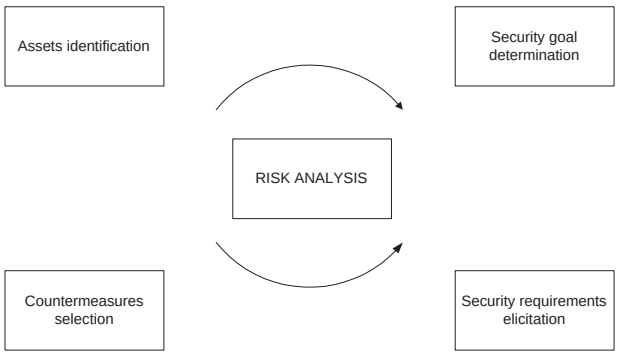

Fig. 3. The risk analysis process in the context of security and RE activities

4 Security driven by key risk and business indicators

As explained in the preceding sections of this paper, risk analysis is the main tool used to guide the security engineering activity into the broad scope of models, describing high level business goals as well as IT architectures. Using risk analysis in this context is very promising, but quite unusual. Hence, it is important to adapt risk analysis to this context, which is the aim of this section.

Often, the budget constraints imposed on the earliest stages of IS development are very tight. This leads to shortening security risk analysis, and adding more security controls than necessary (or less controls where budgets are limited...). Moreover, this results often into unforeseen security weaknesses.

Our proposed method aims at reconciling all these conflicting aspects like: budget constraints, the broad scope of models, separation of concern, and security in the earliest stages of IS development. Firstly, our method uses indicators for focusing at any moment of the iterative security engineering activity on the most critical parts of the IS. The indicators are not only based on risks, but also on their mitigation costs. In other words, we need to face the same trade-off as in other NFRs reconciliation (like performance versus memory space constraints). So, the ranking of indicators is not a simple ranking of risks. Keeping the scope of the security engineering process on just the topmost important indicators, helps to optimize budget resources allocated for the analysis, without weakening the completeness of the risk analysis. Secondly, taking advantage of traceability links, the scope of each iteration is well defined at the right level of abstraction. So, only details meaningful to the scope and abstraction level of each iteration will be added. Lastly, and most importantly, the indicator ranking criteria evolves with the level of details added at each iteration. For instance, depending on the specificities of the IS development project, the following indicators ranking criteria scheme could be as follows:

- At the beginning, only a coarse value of business assets can be taken independently of the probability of risks.
- Next, the probability of main attacks can be considered when some threats and vulnerabilities have been identified.

– Then, the main costs of selected countermeasures can be taken into account.
– After, the details of the costs depending on the IS load are evaluated.
– Lastly, rare events are introduced in the analysis. This is mainly the scheme adopted in the case study presented in the last section.

The main steps of the method are described in the following table:

1	Initially, the main parts of the business context (including the most important business assets) and high-level goals are described, a list is built with the indicators of the business assets, and it is ordered with the most critical business assets at the top.
2	Iterate using the following steps while the residual risk is too high:
	2.1 when appropriate (see the example below), adapt the ranking criteria in relation to the level of details contained in the model
	2.2 reorder of the list of indicators using the risk values, cost values and the ranking criteria ; then select the topmost one
	2.3 using i* models, the scope of the selected indicator is detected by starting at the indicator's model element (e.g. asset, threat, vulnerability, impact) and following the existing traceability links (dependency links, task decomposition links, means-end links) up to the business context and business assets or down to the IT assets and architecture
	2.4 add functional and security aspects by focusing the four engineering activities (Section 3) within the scope defined in item 2.3 ; for instance, starting at the top of the detected scope, add functional goals and requirements, security goals, security requirements, and countermeasures
	2.5 update the threats and/or vulnerabilities and/or impacts analysis, taking into account the modifications made in the preceding item

The extension of these steps to the selection of two or more topmost indicators at each iteration is straightforward.

5 Case Study: the Medical IS

In this section a more detailed iterative security analysis, guided by the key risk and business indicators, will be illustrated on the medical IS case study. As a starting point, we consider Figure 1 including the business context analysis, the modelling of the main business and IT assets, and high-level goals. On this initial situation we explain a number of iterations.

First iteration

A coarse risk analysis is started on the basis of the business context model. At that level, only a partial analysis of the risk components is done. For instance, only impact may be considered.

Next, the indicators are measured and ordered. At this stage, it is difficult to give a precise quantitative measure for comparing the risk indicators, so qualitative comparisons are made. Most often the focus will be given to the most critical business assets, not considering yet a qualitative statement about the risks. However, if possible a very rough qualitative measurement of risk components can also be done.

In the case study, the patient data and its associated medical data are considered as the most critical business assets. Risks are not taken into account at this iteration.

Focusing on the patient data and its relationship with medical data, a privacy goal is associated with them. However medical data (without its associated relationship with patient data) is not constrained by this privacy goal. An availability goal is also necessary to guarantee the business continuity.

This is summarised in the following table. The selected model element originates from the business level and the indicator uses a qualitative ranking criteria which is the criticality of the assets.

Abstraction level	Business assets
Ranking criteria	Qualitative criteria: business criticality
Focus	Patient data and its associated medical data

The risk analysis of the privacy goal uncovers an attack of the system targeting the access to the IT patient data assets. The architect advises the use of the firewall and the IDS. (The other goals are not considered here, in order to keep this example small). However, classical security requirements analysis (e.g. ISO 17799 [18]) imposes operational constraints, such as, in this specific case, a qualified security officer for the role of IDS manager. At the IT level, the officer is added to the assets.

Second iteration

While some critical asset is still left in the list of risks, it is not necessary to modify the ranking criteria. However, when some amount of details are known about the architecture and countermeasures, a rough evaluation of their costs and weaknesses can be made. This is the case of the firewall, the IDS and the security officer[3] identified in the preceding iteration. For instance, the ranking criteria is modified (item 2.1 of the method) to include costs not depending on the load (number of requests,...). At this stage, let us suppose that the security officer asset is ranked topmost due to its high cost, not even considering possible associated risks.

Abstraction level	IT assets
Ranking criteria	Quantitative criteria: business criticality & budget & fixed costs
Focus	Security officer (IDS manager)

Using the traceability links, one can relate this asset also with the IDS, the personal data and the medical data assets (item 2.3 of the method). One way to decrease the cost is to outsource the security officer asset. There are three alternatives in this case:

- outsourcing the security officer only, or
- outsourcing both the security officer and the network, or
- outsourcing the databases (patient and medical data) together with the network and the officer

Any of the 3 alternatives can decrease the ranking of the security officer asset. The last option is selected which seems to have the best ratio cost/security.

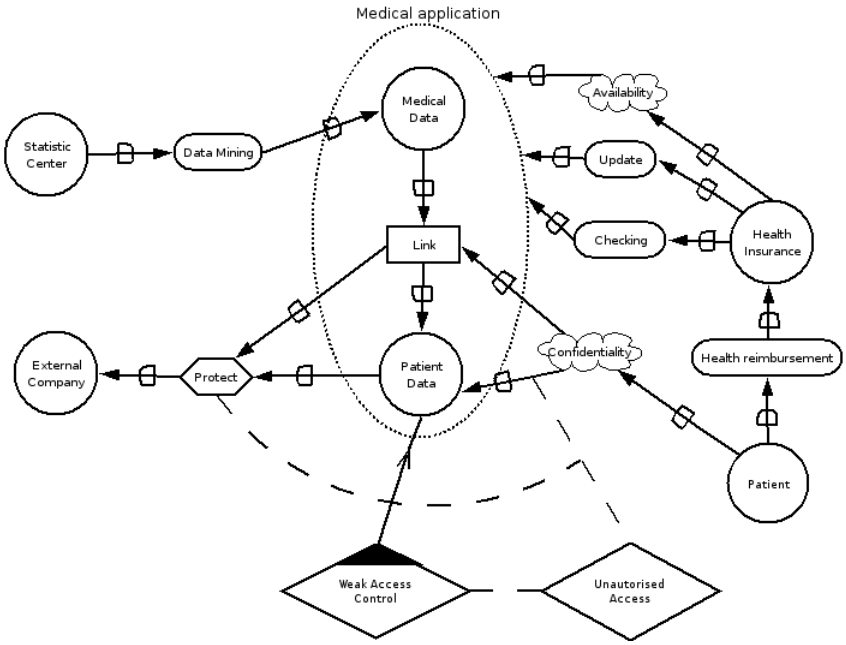

Fig. 4. i* representation of the third step outcome

Third iteration

With the increasing level of details, indicators about goals can be accurately compared on a quantitative basis. For instance, the management costs of the outsourced database increases with the number of requests, in particular the quite large number of access requests needed for data mining the medical data, for example by statistic centers. This increases the outsourcing costs resulting in the ranking of two goals at the top of the list. The first goal is to update both IT related assets (medical and patient) and the second one is to consult medical IT asset. The medical data (i.e. the second goal) can be removed from the outsourcing contractual agreement. This goal will be implemented by the Health Insurance, decreasing the outsourcing costs. To represent this iteration in a graphical, we have proposed some extensions to i* diagrams [2] that depicted in the Figure 4. On this figure, one see a residual risk : the threat (white diamond) targeting the patient data confidentiality (dotted line) can use an access control vulnerability (diamond with a black corner) of the database. We can find this risk in the knowledge base of risk management method [15] [14]. The countermeasure (dotted arc targeting the task node) consists in the patient data outsourcing (including its relationship with medical data).

[3] Each one, including the security officer, has its vulnerabilities and costs

Abstraction level	Business goals
Ranking criteria	Quantitative criteria: business criticality & budget & fixed costs & variable costs
Focus	1. Update patient and its associated medical data 2. Consult medical data

Fourth iteration

At this iteration, the quantitative risk assessment and countermeasures costs can become so accurate that it is possible to assess the benefits of more than one countermeasure for the same risk. In the case study, one could rely on the contractual confidentiality statements made in the outsourcing contract (which results in confidentiality statements in the hiring contracts made by the external service supplier). However, for decreasing the residual risk, one can enforce the patient data encryption (including its relationship with medical data) even on the outsourced database IT asset. So, a malicious employee of the external company is not able to consult the database and disclose some confidential information about patients.

Abstraction level	Requirements
Ranking criteria	Quantitative criteria: business criticality & budget & fixed costs & variable costs & costs/benefits
Focus	1. Confidentiality when hiring 2. Patient data encryption

Fifth iteration

Lastly, most often the remaining risks are those concerning rare events having disastrous impacts on the business assets, because risks based on those events are difficult to quantitatively assess. At this iteration, the level of details helps to decrease the residual risk. For instance, in our case study, it is possible to share mitigation costs (i.e. backup copies made by a third party company) between catastrophic events risks (e.g. fire) and the outsourced service breakdown risk (e.g disagreement with the outside service supplier company about bills).

Abstraction level	Goals
Ranking criteria	Quantitative criteria: remote events with high impact
Focus	1. Subcontractor risk 2. Business continuity

The case study could easily be extended to a more complex one. In a real case study the number of alternatives grows quickly. Our method analyses alternatives only when entering into the focus. Moreover, only the topmost risks and costs are more deeply analysed, and the comparison method is also adapted to the level of details known at the moment of the risk analysis. When done consistently, and with the help of well-known risk analysis knowledge bases, the completeness of the analysis is reached with an optimal budget for the analysis.

6 Conclusion

Risk management is a crucial activity in the development of secure systems. It is also recognized as central by the RE community and new methodologies are proposed for handling security aspects. Our proposal improves the iterative security engineering activity at the earliest stages of development, by using a set of well-known techniques in an original way. Our focus is put on the integration of risk management in the iterative cycle of IS development. At each step, the iteration's scope is guided by key indicators based on adaptive risk and business analysis.

At the theoretical level, more research will be made about the meta-models that are most suited for each step in order to improve the security requirements elicitation. In addition, we will further investigate the best adaptive schemes for the ranking criteria, depending on the level of details. Experimental real cases study in financial institutions will allow us to validate our results.

However, the use of a tool supporting the management of the models (like i* models) and artefacts needed for each step of the risk analysis is a prerequisite for the effectiveness of the method. We plan to develop such a tool, including traceability and change management, and also a wizard giving advices about the best steps to make at each iteration. A promising research, already in progress, is the integration of security engineering aspects to a specific tool, automatically generating architectures from security requirements [3].

7 Acknowledgments

The work is partially supported by the Research National Fund of Luxembourg (Access-PME project). Part of the research is performed within the context of the LIASIT (Luxembourg International Advanced Studies in Information Technologies) Institute

References

1. Basel Committee on Banking Supervision: *International Convergence of Capital Measurement and Capital Standards. A Revised Framework*, Bank for International Settlements Press & Communications, CH-4002 Basel, Switzerland, June 2004, ISBN web: 92-9197-669-5.
2. P. Gaunard, E. Dubois: *Using Requirements Engineering Techniques for Bridging the Gap Between Risk Analysis and Security Policies*, 18th IFIP International Information Security Conference, Athens, Greece, May 2003.
3. V. Rosener, T. Latour, E. Dubois: *A Model-based Ontology of the Software Interoperability Problem: Preliminary Results*, Enterprise Modelling and Ontologies for Interoperability (EMOI) - INTEROP 2004, CAiSE'04, Riga, Latvia, June 2004.
4. L. Chung: *Dealing with Security Requirements During the Development of Information System*, 5th International Conference on Advanced Information Systems Engineering, CAiSE'93, Paris, France, June 1993.
5. A. I. Antón, J.B. Earp: *Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems*, 1st Workshop on Security and Privacy in E-Commerce, CCS'00, Athens, Greece, November 2000.

6. J. D. Moffet: *Requirements and Policies*, Position paper for Policy Workshop 1999, Bristol, U.K., November 1999.
7. I. Alexander: *Misuse Cases Help to Elicit Non- Functional Requirements*, Position paper for Policy Workshop 1999, Bristol, U.K., November 1999.
8. J. McDermott, C. Fox: *Using Abuse Case Models for Security Requirements Analysis*, 15th Annual Computer Security Applications Conference, Phoenix, Arizona, December 1999.
9. A. Toval, J. Nicolás, B. Moros, F. García: *Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach*, Requirements Engineering Journal vol. 6, n. 4, pp. 205-219, 2001.
10. R. Laney, L. Barroca, M. Jackson, B. Nuseibeh: *Composing Requirements Using Problem Frames*, RE'04, Kyoto, Japan, 2004.
11. L. Lin, B. Nuseibeh, D. Ince, M. Jackson: *Using Abuse Frames to Bound the Scope of Security Problems*, RE'04, Kyoto, Japan, 2004.
12. L. Lin, B. Nuseibeh, D. C. Ince, M. Jackson, J. D. Moffett: *Analysing Security Threats and Vulnerabilities Using Abuse Frames*, Technical Report No : 2003/10, October 2003.
13. A. van Lamsweerde: *Goal-Oriented Requirements Engineering: A Guided Tour*, RE'01, Toronto, Canada, August 2001.
14. *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004. http://www.commoncriteriaportal.org
15. *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*, Direction Centrale de la Sécurité des Systèmes d'Information (France), February 2004. http://www.ssi.gouv.fr/
16. *Méthode Harmonisée d'Analyse de Risques (MEHARI)*, CLUSIF, Version 3, Octobre 2004. http://www.clusif.asso.fr/
17. *Octave Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)*,Carnegie Mellon - Software Engineering Institute, June 1999. http://www.cert.org/octave/
18. *ISO/IEC. Information Technology - Code of Practice for Information Security Management, ISO/IEC 17799, 2000*.
19. L. Liu, E. Yu, J. Mylopoulos: *Security and Privacy Requirements Analysis within a Social Setting*, Proc. of the 11th IEEE International Requirements Engineering Conference (RE'03), pp. 151-161, 2003.
20. H. Mouratidis, P. Giorgini, G. Manson: *An Ontology for Modelling Security: The Tropos Approach*, Proc. of the KES 2003 Invited Session Ontology and Multi-Agent Systems Design (OMASD'03), University of Oxford, United Kingdom, September 2003.
21. E. Yu: *Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering*, Proc. of the IEEE Int. Symp. Requirements Engineering, Annapolis, Maryland, pp. 226-235, January 1997.
22. E. Yu, L. Liu: *Modelling Trust for System Design Using the i* Strategic Actors Framework*, In R. Falcone, M. P. Singh,and Y.-H. Tan, eds, Trust in Cyber-societies, Integrating the Human and Artificial Perspectives, Springer-Verlag Heidelberg, pp. 175-194, 2001.
23. E. Yu: *Modelling Strategic Relationships for Process Reengineering*, Ph.D. thesis, Dept. of Computer Science, University of Toronto, 1995.
24. OMG: *Model Driven Architecture. A technical Perspective*, OMG Document ab/2001-01-01, 2001. http://www.omg.org
25. J. D. Moffett, B.A. Nuseibeh: *A Framework for Security Requirements Engineering*, Report YCS 368, Department of Computer Science, University of York, 2003.
26. B. Nuseibeh, S. Easterbrook: *Requirements Engineering: A Roadmap*, Proc. of International Conference on Software Engineering (ICSE-2000), Limerick, Ireland, 2000.
27. R. Jochem: *Common Representation through UEML - Requirements and Approach*, Proc. of the International Conference on Enterprise Integration Modeling Technology (ICEIMT'02), pp. 371-379, Valencia, Spain, 2002.

28. R. Fredriksen, M. Kristiansen, B. A. Gran, K. Stølen, T. A. Opperud, T. Dimitrakos: *The CORAS framework for a model-based risk management process*, Proc. of the 21st International Conference on Computer Safety, Reliability and Security (Safecomp 2002), LNCS 2434, pp. 94-105, Springer, 2002.
29. A. Dardenne, A. van Lamsweerde, S. Fickas: *Goal-Directed Requirements Acquisition*, Science of Computer Programming Vol. 20, North Holland, pp. 3-50, 1993.
30. ISO: *Risk management - Vocabulary - Guidelines for use in standards*, ISO Guide 73, International Standards Organization, Geneva, Switzerland, 2002.
31. A. Cockburn: *Writing Effective Use Cases*, Addison-Wesley, 2001.