54

LEGAL RISK ANALYSIS WITH RESPECT TO IPR IN A COLLABORATIVE ENGINEERING VIRTUAL ORGANIZATION

Tobias Mahler
Norwegian Research Center for Computers and Law (NRCCL), University of Oslo, tobias.mahler@jus.uio.no
Fredrik Vraalsen
SINTEF Information and Communication Technology, Fredrik.Vraalsen@sintef.no
NORWAY

Establishing and operating a virtual organization implies a number of challenges from many different perspectives, including socio-economic, organizational, legal and computational issues. This paper focuses on the legal aspects with a particular view on legal risks with respect to intellectual property rights. A risk analysis with respect to legal issues can either be based on abstract legal reasoning or it can focus on the business reality and the specific characterizations of the virtual organization. This paper follows the latter approach; it presents selected findings of a legal risk analysis of a business scenario in the collaborative engineering field. The legal risk analysis was performed in collaboration between lawyers and other professionals in order to highlight how different legal and non-legal aspects relate to each other. Graphical models of risks and treatments were utilized in order to reduce communicational barriers between experts in this multidisciplinary setting.

1. INTRODUCTION

A virtual organization (VO) can be understood as a temporary or permanent coalition of geographically dispersed individuals, groups, organizational units or entire organizations that pool resources, capabilities and information to achieve common objectives (Dimitrakos et al 2004).

From a legal point of view, it is advisable to base the establishment and operation of a VO on a clear contractual basis, which outlines rights and duties of the VO participants. An example of such a contract is outlined e.g. in (ALIVE 2002a). The ALIVE template provides a good starting point for negotiating contracts for VOs where the partners will collaborate on a medium-term to long-term basis, similar to a joint venture.

There is no general European legal framework for the establishment and operation of virtual organizations, thus legal issues in relation to VOs are still a topic for research. A recently published *strategic roadmap for advanced virtual organizations* points out that the analysis of legal risks arising in operating VOs and the development of legal strategies to overcome them is an important research task in order to support collaborate networked organizations (Camarinha-Matos et al.

2004, p. 296). One area where VO participants face a number of legal risks is the protection of intellectual property rights (IPR), which is the focus of this paper.

Others have addressed risk management for projects (e.g. Baccarini & Archer 1999, Raz & Michael 1999), focusing on general risks for the project as such. Compared to these approaches, this paper focuses not on general risks but only on risks that can be related to legal issues; in this sense it is more specific. The legal risk analysis presented in this paper utilized some of the UML-based graphical models for risk analysis developed by the CORAS IST project to facilitate documentation and communication of risk analysis results (den Braber et. al. 2005). The goal of the analysis was twofold; 1) to identify legal risks and treatments related to IPR in the selected VO scenario, with the aim to create a set of reusable results for use in future analyses, e.g. in the form of templates and checklists, and 2) to evaluate the suitability of risk analysis, in particular the CORAS model-based risk analysis (MBRA) methods and graphical language, with respect to supporting the analysis of legal issues in relation to contract formation in VOs.

The remainder of this paper is structured as follows: Section 2 describes how legal risk analysis can be performed utilizing graphical models; section 3 introduces the collaborative engineering scenario which is the basis for the analysis; section 4 outlines the role of IPR issues in VO-related contracts; section 5 presents selected results of the legal risk analysis performed on the basis of the scenario. Finally, section 6 draws the main conclusions.

2. LEGAL RISK ANALYSIS

The establishment of a VO often occurs under the pressure of time in order to avoid losing the business opportunity which is the primary driver for the collaboration. On the other hand, the parties need to define a contract that sets out the internal functioning of the VO; the contract is a key mechanism for the VO management.

In such cases it is advisory to base the contract on an existing template. However, such contractual templates can not be used "off the shelf"; they need to be adapted to the needs of the specific VO. This implies an adjustment of the contractual rules, taking into account the specific aim of the collaboration, how the partners want to organize the internal management of the VO, whether the VO structure is more static or more dynamic, and what kinds of specific risks have to be taken into account.

Legal risk analysis (LRA) can be applied to the process of adjusting a contract template to the specific risks of the VO. The VO needs to avoid two situations: First, the contract should not overlook relevant risks that should have been addressed in the contract. Second, the contract should avoid addressing issues that are of little business relevance and where the related contractual terms would themselves present a barrier for a successful collaboration, e.g. by providing very bureaucratic rules for cooperation.

For the purpose of this paper, we define LRA as a risk analysis that focuses on the one hand on risks that stem from the legal domain (e.g. loss of a legal right) and on the other hand on non-legal risks that can be treated with legal means. The advantage of this rather broad understanding is that it provides an integrated

approach, where legal risks also can be treated by non-legal means and non-legal risks may be addressed with typically legal approaches, e.g. a contractual rule.

2.1 Model-based Risk Analysis

Risk analysis requires a clear understanding of the system to be analysed. Normally, this understanding can be obtained only through the involvement of different stakeholders, e.g. legal experts, security experts, system developers and users. In fact, most methods for risk identification make use of structured brainstorming sessions of one kind or another, e.g. Hazard and Operability (HazOp) analysis (Redmill et. al. 1999), involving 5-7 stakeholders and domain experts with different backgrounds. The effectiveness of such sessions depends on the extent to which the participants are able to communicate with and understand each other. The CORAS language for threat modelling (den Braber et. al. 2005) has been designed to mitigate this problem within the security domain. Recent work has focused on application of the CORAS language and methodology to the analysis of legal issues (Vraalsen et. al. 2005).

The CORAS language covers notions like asset, threat, risk and treatment, and supports communication among participants with different backgrounds through the definition of easy-to-understand icons (symbols) associated with the modelling elements of the language. The CORAS language is an extension of the UML 2.0 (OMG 2004a) specification language, the de facto standard modelling language for information systems. It is defined as a UML profile (Lund et. al. 2003), and has recently become part of an OMG standard (OMG 2004b).

3. COLLABORATIVE ENGINEERING SCENARIO

This section presents the scenario which is being used in the remainder of the paper. It is a simplified version of a collaborative engineering scenario from the aerospace industry which is being used in the TrustCoM IST project (www.eu-trustcom.com) as part of a test bed. It is being analyzed from different perspectives, including computational aspects, socio-economic aspects and legal aspects. A similar version of this scenario is described in (Wesner et al., 2004), who focus more on computational aspects.

The scenario addresses a collaborative engineering project typical of the aerospace industry, where a lead contractor collaborates with a large number of subcontractors and peer organizations on the development of an airplane or similar product over a 15 year time period, followed by a 20-40 year deployment period. The TrustCoM collaborative engineering scenario consists of three VOs:

- An airliner VO, (Air VO) consisting of the carrier, support and maintenance teams;
- A Collaborative Engineering VO, (CE VO) which has the technical expertise to specify, design and integrate systems into complex products, and which may also manufacture the solution for the customer. This VO's business goal is to win a contract with the Air VO regarding the upgrade of a particular aircraft type with a new feature. One of the partners of the CE

VO, the Systems Integrator (SI), is specialized in the integration of different aircraft systems.

- A number of engineering analysis consultancies that form a VO to support design activities within engineering companies. The Analysis VO (AVO) supports general analysis work across engineering and scientific sectors.

The themes covered by TrustCoM in this scenario include:

- Design and analysis data security; protection of intellectual property;
- Enforcement of Trust and Security policies through the interpretation of contracts and by reacting to notable business 'events';
- Contract negotiation between clients and service providers to support collaborative agreements and service level agreements.

Whilst the main focus of this paper is the protection of IPR in a contractual context, we also attempt to relate the legal issues to the trust and security issues addressed by other parts of the TrustCoM project.

4. INTELLECTUAL PROPERTY RIGHTS IN VO CONTRACTS

A number of different contracts will govern the internal and external relations in the scenario. These will include at least the following types of contracts: (1) VO-internal consortium agreements, which establish consortia of organizations with respective VO goals. All CE VO members will be parties to a consortium agreement. (2) Contracts about the provision of a service or the purchase of a good, without establishing a consortium. This type of contract will be in place between the CE VO (possibly represented by a lead contractor) and the two other VOs, AVO and Air VO. Both types of contracts should also cover IPR issues.

Intellectual and industrial property (IP) rights consist of a variety of rights, including copyright, database protection, patent protection, trademark and design protection and the protection of confidential information (i.e. know-how and trade secrets). The legal framework for these rights shows some variations, taking into account the nature of the protected intellectual property. The law is regulated in slightly different ways in the various member states of the European Union, despite a harmonization of selected IPR issues in European law.

For a VO, the protection of copyrights is closely related to the question of legal personality. In principle, only an entity with legal personality can hold legal rights. Therefore, if the VO has legal personality, it can hold most intellectual property rights. VOs that lack legal personality must refer to their members as holders of all legal rights. A general analysis of IPR issues in a VO context was carried out by the ALIVE project (ALIVE 2002b).

Relevant IPR issues that are likely to be encountered in the formation and operation of a VO can, for the sake of simplicity, be split into two principal categories: Internal issues arise among the various members of a VO, whereas external issues arise between the VO and/or its members, on the one hand, and parties outside the VO on the other hand. We should also make a distinction

between pre-existing IP, which is brought into the VO by the partners, and the IP developed during the co-operative process.

5. SELECTED RESULTS OF THE LEGAL RISK ANALYIS

This section presents selected results of the legal risk analysis, which was performed according to the CORAS risk analysis process. The initial step of this process consists of describing the context of the analysis, i.e. the target of analysis and relevant stakeholders and assets. The target for the risk analysis was the scenario presented in section 3, with a focus on the analysis of IPR, as detailed in section 4, in particular know-how and trade secrets (confidential information). The analysis was performed from the viewpoint of the airplane Systems Integrator (SI) partner of the CE VO.

The risk identification was performed during a number of HazOp brainstorming sessions involving participants with backgrounds in law, engineering, economics, computer science and philosophy. Risks were assigned consequence and frequency values and prioritised, and treatments were then identified for the major risks through another brainstorming session. Some examples of identified risks and treatments are presented below.

5.1 *Example of Identified Risks*

The identified risks relate to different IPR issues, including the protection of confidential information (i.e. know-how and trade secrets), the ownership of IP and liability for IPR infringements by other VO partners. It would be outside the scope of this paper to present all identified risks. We will therefore concentrate on risks related to the loss of confidential information, which was identified as a major risk category. The internal collaboration in the CE VO and its cooperation with the AVO and the Air VO, respectively, may imply that confidential information is shared or otherwise disclosed to VO partners or to external parties. This involves a risk that such confidential information is disclosed to third parties or used by VO members for purposes that are not related to the VO.

Figure 1 shows a CORAS UML diagram describing some ways in which confidential information can be disclosed and potential consequences this disclosure may have. In the CORAS language for risk analysis a threat is described using a *threat agent*, e.g. a disloyal employee or a computer virus, typically represented in the diagram by a stick figure. The threat agent initiates a *threat scenario*, which is a sequence of events or activities leading to an *unwanted incident*, i.e. an event resulting in a reduction in the value of the target *asset*. Furthermore, an unwanted incident may initiate or lead to other unwanted incidents, forming chains of events. For example, an unfaithful employee working for one of the CE VO partners may have access to confidential information which he/she could disclose to a third party. This disclosure could lead to the information reaching the public domain and thereby losing its legal protection and value as a trade secret. A similar but opposite scenario is that an employee of our stakeholder (SI) is unfaithful and discloses the client's confidential information. This again could lead to the CE VO or the SI being

sued for breach of the non-disclosure agreement with the Air VO. The latter unwanted incident may not only have consequences for the SI's revenue, it may also lead to further consequences, like negative publicity.

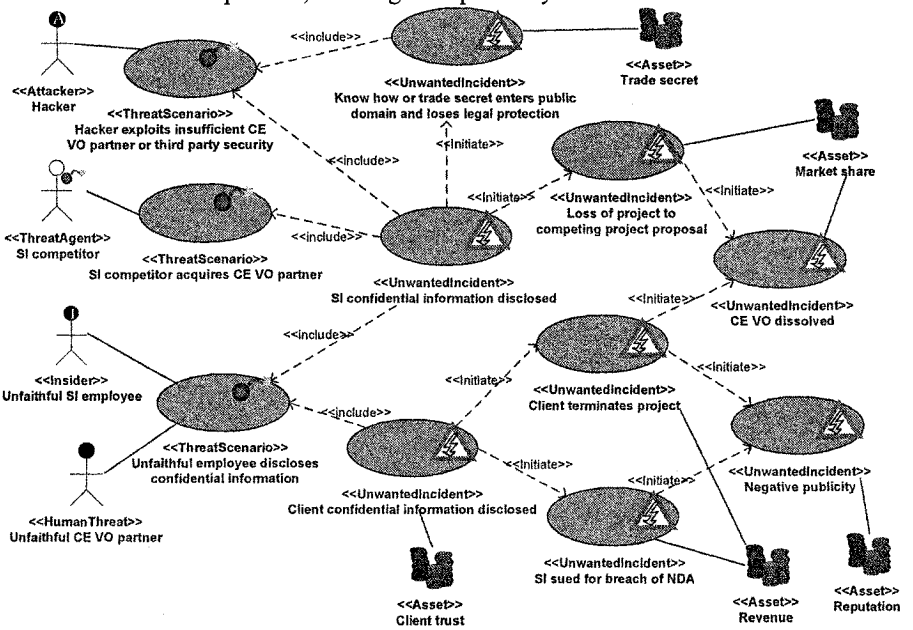

Figure 1 Confidential information loses legal protection

5.2 *Example of Identified Treatments*

For each of the risks, we have explored potential treatments related to three main areas of the TrustCoM project, namely trust, security and contracts. Our aim was to develop an integrated set of treatments, where legal and other measures are integrated. In this context we focused on law as a proactive mechanism, which tries to solve legal issues before they arise; legal reactions *ex post* were not addressed.

Treatments may have different effects on risks, they may e.g. reduce the consequence or frequency of the unwanted incident occurring, or transfer the risk to another party, e.g. through insurance. A selection of treatments to the risks described above is shown in the CORAS treatment diagram in Figure 2. Two of these treatments are clearly within the legal domain: First, a contract clause could avoid the disclosure of confidential information in case of a merger or acquisition, by allowing a re-negotiation of the general VO agreement in this event. Second, specific contractual rules in the VO agreement should address the VO members' liability towards third parties. The remaining treatments involve legal and non-legal elements: Information security mechanisms like limitations to storage time and the deletion of data after an analysis are of key importance. Such mechanisms can be made obligatory via contractual clauses in the agreement between the CE VO and the AVO. If the technology was available, a VO-internal enterprise Digital Rights Management (DRM) system could also reduce the likelihood of confidential

information being disclosed, particularly if some of the contractual obligations could be enforced through technology.

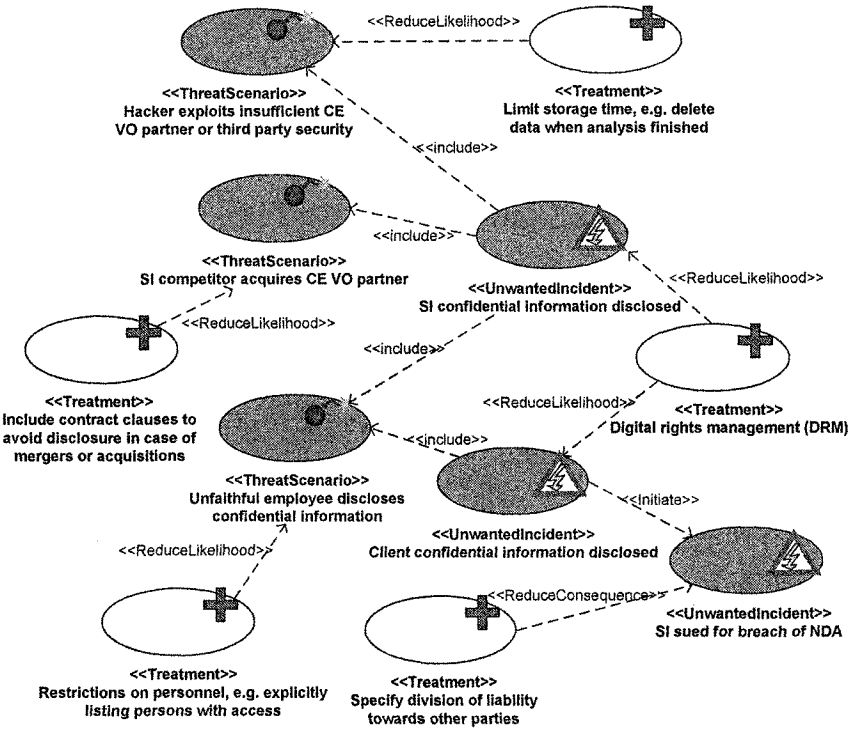

Figure 2 Risk treatments

6. CONCLUDING REMARKS

We have presented results from the analysis of a collaborative engineering VO scenario, where a number of legal risks and treatments were identified. Our risk analysis results indicate how legal risks, such as the loss of protection of confidential information, can be treated by an integrated solution, including contractual elements, trust management and security management. Interestingly, many of the relevant contractual treatments were also included in a general manner in the ALIVE contract template for VOs (ALIVE 2002a). The performed legal risk analysis provided indications about how these rules can be adapted to the specific scenario. Since the graphical representation implies a simplification, a lawyer would have to integrate analysis results into the contractual document in an appropriate way, taking into account the terminology and the system of the contractual template.

The analysis results were generated during a number of brainstorming sessions involving participants with varied backgrounds, including law, computer science, engineering, economics and philosophy. Based on our experiences, the graphical models can indeed facilitate the communication and understanding with respect to legal issues in a multidisciplinary context. Ongoing work is focusing on further adapting the CORAS methodology and graphical language to better suit legal risk

analysis (Vraalsen et. al. 2005), as well as on creating reusable elements in the form of e.g. checklists based on the results of this analysis in order to facilitate future analyses.

7. ACKNOWLEGEMENTS

The results presented here are partly financed by the European Commission under contract IST-2003-01945 through the project TrustCoM and partly financed under the Research Council of Norway through the project ENFORCE.

We would like to acknowledge the work done by David Goldby from BAE Systems, who has defined the collaborative engineering scenario for TrustCoM. We would also like to thank David Goldby, Mass Soldal Lund, Xavier Parent and Claudia Keser for participating in the risk analysis sessions.

8. REFERENCES

ALIVE IST Project (2002a). Report D 17 a, VE Model Contracts, available at http://www.vive-ig.net/projects/alive/docs.html.

ALIVE IST Project (2002b) *Report D 13, ALIVE Project, Intellectual & Industrial Property Rights Legal Issue Subgroup*. http://www.vive-ig.net/projects/alive/docs.html.

Baccarini, D. and Archer, R. *The risk ranking of projects: a methodology*. International Journal of Project Management 19 (2001) 139-145.

Folker den Braber, Mass Soldal Lund, Ketil Stølen, Fredrik Vraalsen. The CORAS methodology: Model based security analysis using UML and UP. Encyclopedia of Information Science and Technology. Information Resources Management Association, USA (2005)

Camarinha-Matos, L., Afsarmanesh, H., Löh, H., Sturm, F., Ollus, M. A strategic roadmap for advanced virtual organizations. In collaborative networked oganizations: a research agenda for emerging business models. Camarinha-Matos, L and Afsarmanesh, ed. New York: Springer 2004.

Dimitrakos T, Goldby D and Kearney P. Towards a trust and contract management framework for dynamic virtual organizations. In E-Adoption and the knowledge economy: eChallenges 2004, IOS press 2004.

Lund, M.S., Hogganvik, I., Seehusen, F., Stølen, K.: UML profile for security assessment. Technical Report STF40 A03066, SINTEF Telecom and informatics (2003).

OMG: UML 2.0 Superstructure Specification. (2004a) OMG Document: ptc/2004-10-02.

OMG: UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms, Draft Adopted Specification (2004b) OMG Document: ptc/2004-06-01.

Raz T and Michael E. Use and benefits of tools for project risk management. International Journal of Project Management 19 (1999) 9-17.

Redmill, F., Chudleigh, M., Catmur, J.: HazOp and software HazOp. Wiley (1999)

Vraalsen, F., Lund, M.S., Mahler, T., Parent, X. and Stølen, K. Specifying Legal Risk Scenarios Using the CORAS Threat Modelling Language – Experiences and the Way Forward. In Proceedings of the 3rd International Conference on Trust Management (iTrust '05). Paris, France, May 2005. Springer LNCS 3477.

Wesner S, Schubert L, Dimitrakos T. *Dynamic Virtual Organizations in Engineering*. Forthcoming, the Proceedings of the Second German-Russian Workshop. Notes on Numerical Fluid Mechanics and Multidisciplinary Design (NNFM). Springer.