56 MANAGEMENT OF IT-RISKS IN THE CONTEXT OF INTER-ORGANISATIONAL KNOWLEDGE MANAGEMENT

Thiemo Scherle, Stefan Bleck, Peter Laing, Tomaso Forzi
Research Institute for Operations Management (FIR) at Aachen University
E-Business Engineering Department
{ Thiemo.Scherle, Stefan.Bleck, Peter.Laing, Tomaso.Forzi}@fir.rwth-aachen.de
GERMANY

In order to improve their competitive position, small and medium sized enterprises increasingly concentrate on their core competencies and hence take part in co-operations. If the main purpose of the co-operation is the information of explicit knowledge in terms of documents, the most effective way of communicating is sharing information electronically. But it is known from experience that the electronic inter-organizational knowledge exchange only works if personal, organizational and technical requirements are fulfilled. For instance, all co-operation partners have to be sure that their knowledge is not "forwarded" to an unauthorized third person. Considering the example of an existing co-operation of components suppliers it is shown how the realization of an IT security concept enables the controlled exchanged of document-based knowledge.

1. STATE OF THE ART OF INTER-ORGANISATIONAL KNOWLEDGE MANAGEMENT

Medium-sized enterprises generate a huge amount of innovations and numerous new products (Evers, 1998). Tough international competition leads to short product live cycles and innovative production technologies. As a result, production processes become increasingly knowledge-intensive. Small and medium-sized enterprises can improve their competitiveness in this environment by concentrating on the core competencies and creating value in co-operation with complementary partners (Killich, Luczak, 2003). As a consequence of such close co-operations, powerful knowledge networks come into existence. A prerequisite for the smooth operation of such networks are powerful organizational concepts for knowledge management. Therefore, the importance of inter-organizational knowledge management constantly increases.

In order to transmit information among the partners efficiently, usually information and communication technologies are used which are based on internet technology. Thus, the exchange of documents and information such as norms,

laboratory results, material properties, certification procedures and contact data is supported effectively (Klein, 1994).

The demands on organizational and especially technical design of such inter-organizational knowledge networks are high in respect to planning, building and operating such systems. The well-known methods of intra-organisation knowledge management can only be applied in this context if the partners of the network trust each other. Only static entrepreneurial networks can achieve such a state of trust due to their long-term co-operation. Therefore, only static networks can build up a technical platform for knowledge management based on these methodologies.

Nevertheless, even in such environments there is a considerable risk that single partners withdraw knowledge from the network and distribute it uncontrollably. This is the more true if some companies co-operate on some markets, but compete at other markets at the same time. The knowledge source therefore has a strong interest in controlling precisely which partner of the network has access to what knowledge. These aspects apply even more to dynamic corporate networks that are frequently joined and left by partners. This represents a remarkable obstacle for companies to share their knowledge. As a result of this, important information is only hesitantly made available to the network and the desired synergy effects occur only to a very limited extent.

The requirements of the knowledge source are therefore especially in being able to control access, authorization of use and distribution, protection against espionage as well as manipulation of erroneous delivery of documents and evidence about how certain knowledge donated to the network has been used or distributed. The following paper will show, how these requirements can be met by the application of the Aachen IT-Security Concept. It explicitly takes the risks within inter-organizational networks into consideration.

2. IT RISK MANAGEMENT IN CORPORATE NETWORKS

2.1 Network risks

During the recent years many inter-organizational co-operation have failed due to various reasons, e.g. overambitious goals or lack of project management. However, the expected results where not achieved. (Crowley, 2001; Drage, 2001; Karsten, 1998; Nichols, Thomson, Yates, 2001; Rajagopalan, Subramani, 2002). One important and quite common cause for problems in inter-organizational value creation lies in the insufficient consideration of so-called network risks, which occur in entrepreneurial co-operation. Considerable network risks arise, for instance, from an opportunistic behaviour of certain partners or from the unprotected exchange of information.

Intra-organizational units are subject to control by the top management. The immanent risks of knowledge exchange are therefore rather limited. On the other hand the behaviour of network partners or even completely external companies cannot be controlled and it can only be anticipated to a limited extent. Therefore it is necessary to include network risks into the project planning in co-operations (Lück, 2000; Merkle, 1999; Voß, 2002). Deficits of single partners directly influence the success of the project (Strack, 2001).

Corporate IT infrastructure must therefore not only ensure reliable operation within the companies' borders, but also need to enable the secure exchange of information and documents with external partners. However, the exchange of information along a supply chain or with entrepreneurial networks bears immanent risks. For instance, the participants need to guaranty that information transmissions cannot be intercepted or manipulated by third parties. Moreover, each document containing non-public information has to be linked with data about its owner, be it either a company or an individual. For such purpose powerful cryptographic algorithms are available.

The co-operation in knowledge intensive entrepreneurial networks can be considerably improved and the risks of a complete failure can be diminished by the development and implementation of a powerful IT risk management (Kleitsch, 2000; Vaughan, 1997). Different forms of co-operations, like virtual organizations, value nets, networks with or without broker, horizontal or vertical networks etc., bear different types of risks. Different network structures and typologies have therefore to be considered along with their respective context (Davidow, Malone, 1993).

2.2 Tasks and approaches of risks management

The main tasks of risk management are the systematic and complete risk analysis and assessment, risk response development and risk response control (Brühweiler, 1980; Gleißner, 2002). During the risk analysis the most significant risk, which an enterprise is confronted with, are identified. Afterwards, these risks are analyzed, both regarding cause effect and damage (Brühweiler, 2001; Erdenberger, 2001; Kleitsch, 2000). Risk analysis and assessment are of special interest because only identified risks can successfully be managed. A substantial challenge lies therefore in the early recognition of risks, even currently low, might develop into a considerable thread (KPMG, 1998). Based on a decision profile measures for risk response can be derived. These measures are afterwards assessed in respect to their feasibility and degree of success in the phase of risk controlling (Gleißner, 2002; Mann, 1989; Neubürger, 1989; Strack, 2001). In the beginning of a risk management process the management needs to formulate a risks strategy. This strategy afterwards has to be assessed regularly in terms of feasibility.

2.3 Network oriented risk management

The well-known methods and approaches for risk identification and response are insufficient to meet the challenges and the associated opportunities and thread in the context of entrepreneurial networks. Theories like game theory and system theory, for instance, provide methods for the representation and design of co-operations and give hints on how to cope with or avoid opportunistic behaviour of single partners.

Within science and also in practice there are many methods for IT Security and IT Risk Management. But they are not appropriate for application in the context of inter-organizational networks due to various reasons. Technically oriented methods like the Role Based Access Control (RBAC) (Sandhu, Coyne, Feinstein, Youman, 1996, Ferraiolo, Sandhu, Gavrila, Kuhn, Chandramouli, 2001), Security Model for Cooperative Work (Coulouris, Dollimore, 1996) and Task-Based Access Control

(Thomas, Sandhu, 1994) consider the aspect of inter-organizational information exchange explicitly. But these methods mainly concentrate on accessing information. The control of distribution and usage of information are not considered. They also do not take the dimensions organization, and human aspects into account. Methods like the ISO 17799 and the user guide for IT Security base-protection (Grundschutzhandbuch) of the BSI (GSHB, 2003), on the other hand consider organizational und human aspects, but they do not take the inter-organizational networks into account. However, companies require an integrated and broad approach for analysis of and response to IT risks. The Aachen IT Security Concept provides the basis for a systematic, network oriented IT risk management. These risks can be considered as external factors in a classic risk management.

IT risk analysis

Besides the basic criteria of system security, i.e. integrity, confidentiality, authenticity and availability, especially general threads as well as the requirements of all participating enterprises have to be taken into consideration. Therefore, the description of threads and possible attacks are of fundamental importance. The identification of threats can be achieved by the assessment of how far the loss of integrity, confidentiality, authenticity and availability results in any kind of possible damage. During the risks analysis in inter-organisational networked IT infrastructures it should be considered additionally who or which organisations could be a possible attacker and what could be a possible motivation. As a result, possible attacking scenarios become more transparent.

IT risk assessment

When assessing IT risks, a differentiation between damage frequency and damage severity has to be made (Horster, 2000; Laing, Pohlmann, 2003). Based on so-called risk portfolios for the different risk categories single risks can be classified (see figure 2). All risks, which lie in the fourth quadrant (high damage frequency and severity), have to be influenced by suitable measures in such a way that the remaining risk level is diminished to an acceptable degree. If either the damage frequency or severity is high (quadrant II and III), specific considerations have to be done; according to each individual case it has to be decided whether risks prevention or reduction measures need to be implemented or not.

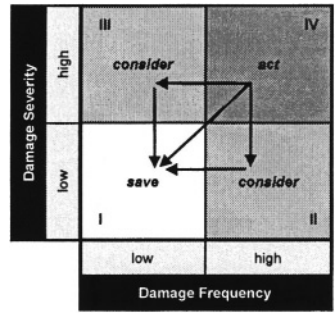

Figure 2 – Qualitative IT risk assessment

IT risk response

The objective of risks response lies in the design and implementation of measures, which reduce all risks considered as critical threats to an acceptable level. All of these measures and the according procedures are part of an IT security concept.

Considering for example the IT risks of an internet intermediary is as to be made sure that (a) general threads and risks, (b) corporate requirements as well as (c) the basic criteria of system security are considered and that, after the definition of a security policy, suitable preventive measures are implemented. All these measures should be based on the security criteria. The Aachen IT Security Concept allows to reduce the frequency and severity of risks to a acceptable level, as required (see figure 3).

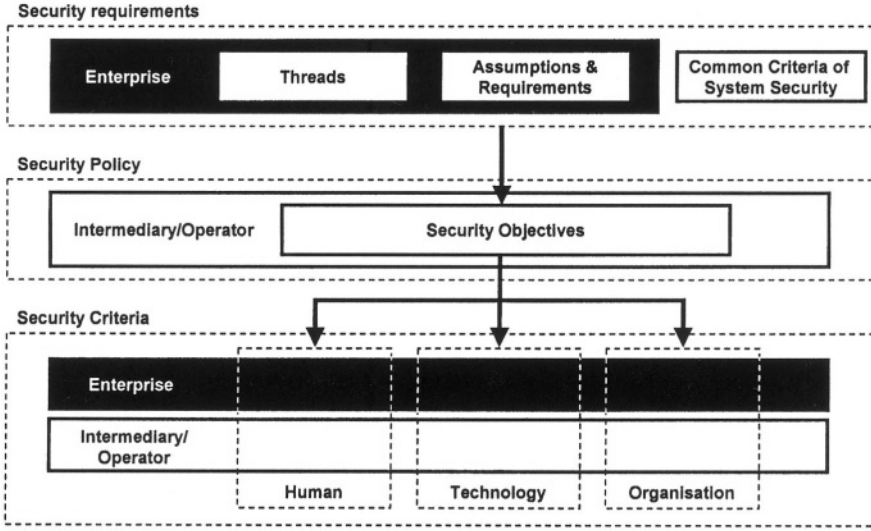

Figure 3 - Aachen IT Security Concept

The purpose of the security policy is to create a common mindset and to deliver guidelines how to cope with the mission critical topic of security for internal organization, technical implementation and external communication. A major

objective of the security policy is the general and shared acceptance of the required level of security. In order to fulfil its purpose to increase the security in all intra and inter-organizational communication, a security policy needs to be easy to understand and implement and to give hints about how to derive related organizational rules, procedures and practices in terms of security. Opposed to a mathematical-scientific definition of security, the formulation of a security policy must therefore be leaner and understandable.

Security criteria and measures can be classified in relation to human, technical or organizational issues. Technical measures need to be accompanied by duties, responsibilities and predefined behaviours according to different scenarios of internal and external attacks. In internet-based environments the aspect of inter-organizational co-operation represents a substantial feature. Therefore, all participating companies need to implement the according measures.

A general problem in risks management is that not all immanent threats are known beforehand. Therefore, the occurrence of damage cannot be determined. Due to this fact it becomes obvious that emergency plans as well as emergency activities have to be designed to limit the impact of possible security violations.

IT Risk controlling

The Balanced Score Card (BSC) is a comprehensive and well-spread instrument to implement and monitor the corporate strategy at all levels of the enterprise and to support it with suitable measures of control and management (Kaplan, Norton, 1996; Niven, 2002). The classical form of BSC considers the four perspectives of "Learning and Development", "Internal Business Processes", "Financial" and "Customers" (Kaplan, Norton, 1996). Since recently the engagement in value creating networks and the design and operation of inter-organisational business processes with partners and supplies becomes increasingly important. Due to this fact the "Customer" perspective needs to be extended and into what we define the "Network" perspective, in order to depict all inter-organisational business activities (customers, suppliers, horizontal and vertical partners); see also figure 4.

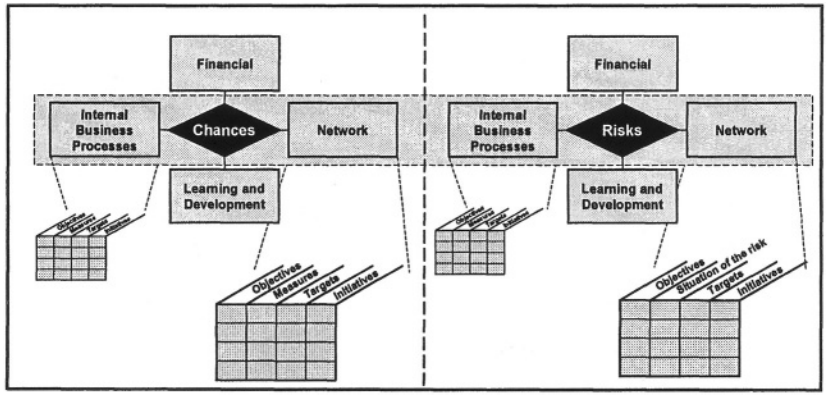

Figure 4 – Relevant Aspects of IT Risk Management

Entrepreneurial decisions need to consider business potentials (i.e. additional revenue) as well as the associated risks. A successful IT (network) risk controlling is characterised by a balanced consideration of risks and chances. Companies, which are engaged within networked business structures, therefore should on the one hand clearly formulate their respective goals and support them by measurable scores and suitable measures to achieve the desired objectives. This enables leverage of the business potentials. On the other hand this balance provides an extensive decision support related to the IT risks immanent to a inter-organizational network. It hence enables the early discovery of dangers (see figure 4).

3 CASE STUDY: INTERMEDIARY KNOWLEDGE MANAGEMENT WITHIN THE AUTOMOTIVE SUPPLIER INDUSTRY

The automotive supplier industry is a sector driven by innovation, which, not least due to the high global competition, is characterised by short product cycles, innovative production procedures and knowledge intensive production processes. Especially small and medium-sized enterprises can only survive in this market if they concentrate on their core competencies and co-operate with complementary partners and form powerful networks. Thus, the importance of inter-organisational knowledge management in the automotive industry ever increases.

This case study considers a co-operation of legally independent, medium sized automotive suppliers from the province of Westfalia, Germany that produce components for national and international companies. The main aspect of co-operation is the distributed development and production of parts and components. In order to achieve a quick and efficient exchange of information, even nowadays information like descriptions of processes and CAD drawings are provided to the network partners as electronic documents via a special internet platform (extranet). The partners can upload documents from the platform, provide complementary documents and update the provided data.

However, this form of information exchange bears considerable risks: once a partner has provided a document he can no longer control nor trace the use of his knowledge. Though the knowledge source can restrict the initial access to a document with a password, he has no control once the document has been downloaded from the platform. Such documents can be duplicated and distributed freely without any further authorisation either as an electronic document or as a printout even beyond the network boundaries.

Such a solution is suitable as long as all participants of the network trust each other. Under such circumstances the well-known methods of intra-organisational knowledge management can be applied in an inter-organisational context. The creation of a co-operative culture and trust (i.e. unrestricted provision of knowledge and confidential handling of sensitive documents) is applicable to inter-organisational contexts only to a very limited extent. On the one hand this is due to the fact that inter-organisational are dynamic, this meaning that partners can join and leave the network frequently. On the other hand most companies, which co-operate on some markets compete on others. In practice this ambivalence leads to hesitation

in providing knowledge to the network. The participating companies fear that competitors might get hold of confidential knowledge within or even out of the network boundaries if single partners behave opportunistic. This would mean a competitive edge, so that knowledge related competitive advantages would be lost. The willingness to provide information to the network is directly dependent on the possibility to precisely control the access and distribution of contents. At the same time the knowledge recipients benefit from such control mechanism, because the knowledge base can be broadened and the authenticity of the documents source can be checked.

Considering inter-organisational knowledge management threads to the IT security come as well form the inside (e.g. sabotage or human errors) as from the outside (e.g. hackers). Analysis have shown that on the one hand the authenticity and integrity of documents as well as the confidentiality of business relations have to be guaranteed on the other hand data cannot be lost. A clear problem is that companies in the automotive sectors demand a high level of security without formulating precise requirements. As a result of this the design of a suitable security concept needs to be based on a thread analysis and the common criteria of IT systems security.

Thus, the following requirements to inter-organisational knowledge management for enterprises in co-opetition can be derived:

- Knowledge sources need to be enabled to control the access to their knowledge
- Knowledge sources need to enabled to control the distribution of their knowledge
- Knowledge receivers need to be enabled to check the authenticity of knowledge sources

3.1 Relevant IT risks and security requirements

The identification of threats can be done by the consideration of potential single incidents and the analysis of which in how far the loss of authenticity, confidentiality, integrity or availability would impose damage. A general problem is that the occurrence of damage can never be surely avoided. Therefore emergency plans and emergency activities have to be elaborated in advance in order to be able to respond to security problems and limited the inflicted damage.

In the companies of the automotive industry especially employees in product development get in contact with confidential data. But also employees from the departments for marketing and procurement need at least read access to documents that contain product and production specifications and thus important competencies of the enterprise.

3.2 Requirements for IT risk management

As already depicted above, a security policy gives hints and directions about how to implement IT security within the organisational structures of the intermediary exchange platform, the external communication as well the technical realisation. A major objective of the security policy is the achievement of the desired level of security and thus the acceptance of the knowledge platform among its users. The

security policy of the platform can be derived form the answers to the following questions, which aim at the operative description of the topic of IT security:

- What needs protection? Protection is required in respect to the integrity and confidentiality of the knowledge provided to the platform as well the functionality of data exchange between companies.
- Who shall protect it? The main responsibility for security issue lies with the operator of the knowledge platform. He has to elaborate a profound security concept and supply the companies, which are involved in the creation of a secure environment and high security standard with the necessary tools and information.
- Against what is protection required? The goods on the platform which are worth protection need to shielded against attacks for side and the inside, human failure as well as force majeure.
- How to protect it? The measures for protection have to be effective on any level (human, technology, organisation). Thus the complete spectrum of thread can be avoided. The loss of data has to be prevented by suitable backup and archiving mechanisms in such a way that possible damaged can be limited.
- What to do in case of emergency? The implementation of a profound and detailed security concept reduces the risks to an acceptable degree. There are, however, unavoidable risks like physical attacks, network failure or fire. Thus it is necessary to complement the preventive measure with emergency activity plans in order to contain the damage inflicted by the emergency situation.

3.3 Security Measures for risk response

A stable operation of IT systems can only be achieved if security concepts are implemented on any of the three levels depicted above, i.e. human, technology and organisation. The IT security concept therefore contains criteria and measures on each level.

- *Human issues:* Human actions are characterised apart by the high flexibility, also by the fact of the occurrence of failures. Major damages, for instance by erroneous behaviour, can be avoided by preventing the manipulation or erasure of database records and documents for all users, regardless whether they are members of the platform operator or network participants. The different users represent within their companies different roles with different rights. A security concept has to ensure that users can only carry out actions that they are supposed to do due to the duties of their role. The corporate practice has shown that using conventional methods of information interchange documents where send abroad which where not supposed to leave the company. Such incidents could even easier occur with electronic data exchange. Therefore, according countermeasures are required.
- *Technical issues:* The implementation of a suitable level of security requires technical measures, which include access control, protection against intrusion (e.g. by a firewall), cryptographic procedures and the application of digital signatures (Fumy et al., 1995). Technical security also contains the reliable and permanent archiving of data on non-violatale media. A firewall and regular updating of the operating system and the application software raise the protection of the system additionally. All access to the system is logged, so that it can be reconstructed, which user up- or downloaded documents at a certain time. The

purposeful usage of well-known IT security technology made it possible to achieve the demands of access control and usage control; e.g.: access authorization, usage authorization, encrypted transmission and authentication. Additionally each Document is marked with a robust user-specific electronic watermark, which cannot easily be removed from either the electronic or the paper based version of a document. By this measure it can be reconstructed who downloaded a certain document.

- *Organizational Issues:* The different roles of the persons who are interacting with each other via the knowledge exchange platform have to be considered. The platform operator and the participating companies have to pinpoint which employee can upload, download, read, print and copy documents. Furthermore they have to define which rights are associated with a certain role. To ensure that nobody manipulates or deletes data, it is essential to separate key- and system-administration organizationally.

4 SUMMARY AND PERSPECTIVE

Market development requires that small and medium sized enterprises concentrate on their core competencies and participate in co-operations. Often the main purpose of such networks is the exchange of knowledge. The most effective way to share explicit knowledge in forms of documents is to exchange them electronically via the Internet. But this way of sharing knowledge also implies the danger that single co-operations partners act opportunistically and forward the documents to an unauthorized third inside or outside the network. To reduce these risks certain measures have to be planned and taken. In the context of inter-organizational Networks the methods of intra-organizational IT-Security and Risk Management cannot be applied without changes. The Aachen IT Security Concept integrates and extends existing methods. It explicitly considers the characteristics of intra-organizational networks, as both a intermediary and each enterprise are taken into consideration. The example of an existing co-operation of components suppliers was considered, the Aachen IT Security Concept was applied. Due to the positive experience so far we are going to verify the validity of the method in further areas of application.

5. REFERENCES

1. Brühweiler B. Einführung eines unternehmensweiten Risk-Managements. In io management, 2001, (7/8), S. 54-59.
2. Covington, M, Moyer, M, Ahamad, M. Generalized role-based access control for securing future applications. 23rd National Information Systems Security Conference, Baltimore, MD, October 2001.
3. Coulouris, G, Dollimore, J. A Security Model for Cooperative Work: Technical Report Nr. 674, Department of Computer Science, Queen Mary and Westfield College, August 1994.
4. Crowley S. Identification of failed R&D Projects (working paper). 1999. Download: http.//www.stevencrowley.com/FailedRD.htm.
5. Davidow W, Malone M. Das virtuelle Unternehmen. Campus Verlag. Frankfurt am Main, New York, 1993.
6. Drage R. ITCF Summative Evaluation Project – Partnership and Collaborative Working, July 2001.
7. Erdenberger C. Risikomanagement – Möglichkeiten einer pragmatischen Umsetzung in mittelständischer Unternehmen. In Controller Magazin, (1) 2001, S. 13-16.
8. Evers M. Strategische Führung mittelständischer Unternehmensnetzwerke. München, 1998.
9. Ferraiolo, D, Sandhu, R, Gavrila, S, Kuhn, R, Chandramoulo, R. Proposed NIST standard for role-based access control. ACM Transactions on Information ans System Security, 10 no. 3, 2001.
10. Fumy W, Horster P, Kraaibeek P. Standards und Patente zur IT-Sicherheit. Oldenbourg, 1995.
11. Gleißner W. Ratschläge für ein leistungsfähiges Risikomanagement. Download: http://www.krisenkommunikation.de/akfo53-d.htm.
12. Kaplan RS, Norton DP. The Balanced Scorecard: Translating Strategy into Action. Harvard Business School Press, September 1996.
13. Karsten H. Collaboration and Collaborative Information Technology: What is the nature of the relationship? Proceedings of the Conference Information Systems: Current Issues and Future Changes", Helsinki (SF), December 10th-13th," 1998; 231-254.
14. Horster P. Systemsicherheit. Vieweg Verlag, 2000.
15. Killich S, Luczak H. Unternehmenskooperationen für kleine und mittelständische Unternehmen, Lösungen für die Praxis. Berlin et. al. Springer, 2003.
16. Klein S. Virtuelle Organisation. 1994, Download: www-iwi.unisg.ch/iwi4/cc/genpubs/virtorg.html.
17. Kleitsch D. Risikomanagement. Schäffer-Poeschl Verlag, Stuttgart, 2000.
18. Laing P, Pohlmann N. Digitale Signaturen im elektronischen Materialzeugniswese. In: Proceedings of the DACH Security 2003, Erfurt, 25-26 März 2003.
19. Lück W. Managementrisiken. In: Dörner, Horváth, Kagermann (Hrsg.): Praxis des Risikomanagements. Stuttgart: Schäffer-Poeschl Verlag, 2000.
20. Mann R. Praxis strategisches Controlling. Verlag moderne Industrie, Landsberg, 1989.
21. Neubürger KW. Chancen- und Risikobeurteilung im strategischen Management. Poeschel Verlag, Stuttgart, 1989.
22. Nichols DM, Thomson K, Yeates SA. Usability and open source development. Working Paper of the Dept. of Computer Science, Univ. of Waikato, Hamilton (NZ), 2001.
23. Niven PN. Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results, 1st edition. John Wiley & Sons, 2002.
24. Merkle M. Bewertung von Unternehmensnetzwerken – Eine empirische Bestandsaufnahme mit der Balanced Scorecard, Dissertation der Universität St. Oallen (HSG), Difo-Druck OHG, Bamberg, 1999.
25. Rajagopalan B, Subramani MR. Lessons from New Product Development for Managing Knowledge in Software Engineering, IEEE Software, Special Issue on Knowledge Management in Software Engineering, 2002. Download: http.//www.ids.csom.umn.edu/Faculty/Mani/Homepage/Papers/ Rajagopalan_Subramani_IEEESW.pdf.
26. Strack J. Controlling virtueller Unternehmen, Dissertation der Universität St. Gallen (HSG), Shaker Verlag, Aachen, 2001.

27. Thomas, R, Sandhu, R. Conceptu al Foundations for a Model of Task-based Authorizations' Proc. of the 7th IEEE Computer Security Foundations Workshop, Franconia, NH, June 1994, pages 66-79.
28. Voß W. Ganzheitliche Bewertung von Unternehmensnetzwerken – Konzeption eines Bewertungsmodells, Verlag Peter Lang, Frankfurt a.M. et.al., 2002.
29. Vaughan EJ. Risk Management. John Wiley & Sons, New York, 1997.