2005

Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management

Stefanie Jahner
Technische Universitat Munchen, jahner@in.tum.de

Helmut Krcmar
Technische Universität München,, krcmar@in.tum.de

Beyond technical aspects of information security: Risk culture as a success factor for IT risk management

Stefanie Jahner
Technische Universität München
Chair for Information Systems
jahner@in.tum.de

Helmut Krcmar
Technische Universität München
Chair for Information Systems
krcmar@in.tum.de

ABSTRACT

Increasing numbers of security incidents such as malware or hacker attacks prompt companies to spend billions of dollars on protecting their information systems. In this context IT risk management (ITRM) has become an important organizational function to control internal and external risks associated with IT. Much effort has been put on mitigating IT risks by means of physical, procedural, and technological solutions. However, the socio-cultural perspective of managing these risks has largely been ignored and thus a "cultural gap" in ITRM can be identified. This paper introduces risk culture as an essential component of an integrated IT risk management and presents a theoretically motivated framework for analyzing the construct risk culture. Based on this framework we conducted a case study that underpins the crucial role of a vital risk culture in an organization. From the empirical findings we derived important factors for establishing risk culture such as (among others) communication campaigns or top-management involvement.

Keywords

Risk Culture, Information Security Culture, IT Risk Management, Information Security, Security Awareness.

MOTIVATION

Along with increasing numbers of security incidents such as malware or hacker attacks, theft of proprietary information, or insider net abuse companies in different industries all over the world continuously spend a multibillion-dollar amount of money in the protection of their information systems and sensitive data. According to a current survey on key business initiatives of business-technology managers for 2005 "updating security procedures, tools, or services" was ranked as their top business priority by 82% of the respondents (Chabrow, 2005).

In this context IT risk management (ITRM) has become an important organizational function to control and handle internal and external risks concerning and resulting from the use of information technology and information management (Krcmar, 2005). Several theoretical approaches found in the literature as well as established standards, handbooks or guidelines deal with managing risks in information management, e.g. CObIT, Code of Practice (BS7799/ISO 17799), Common Criteria (ISO 15408), or the German IT Baseline Protection Manual. With different scopes on processes, methods, or requirements of managing IT risks these approaches are intended to provide broad guidelines rather than a detailed set of recommendations how to mitigate these risks. Also most of them have a strongly or even exclusively technical focus.

However, neither a purely technology-based or procedural, nor a physical approach seems to be sufficient when dealing with risks in information management. Managing risks in IT is often less a problem of absent security arrangements, but more an issue of inappropriate behavior towards sensitive information or little knowledge of IT use among employees. Several authors also show that the highest risk in information management is not to be found in external threats such as virus or hacker attacks, but in internal incidents committed by insiders (Randazzo, et al., 2004; Schlienger and Teufel, 2002).

Also the subject of information systems itself calls for an integrated view on IT risks: Information systems are defined as complex, socio-technical systems that encompass both human and technical components and their interaction (Krcmar, 2005). They are "the means by which people and organizations, utilizing technology, gather, process, store, use and disseminate information" (Ward and Peppard, 2003). These definitions show the one-sidedness of a solely technical-oriented perspective towards IT risks and emphasize the necessity of taking the human component, i.e. the users, developers, and

managers of information technology into account. Users may not be regarded as an enemy towards the use of technology (Adams and Sasse, 1999). Managing IT risks is also a strategic management issue that is often disregarded. Sherer points out that not only IS managers, but the senior management in particular has to be involved (Sherer, 2004).

Summing up the status quo in theory as well as in practice one can identify a cultural gap in IT risk management. We will therefore introduce the concept of risk culture as an essential component of an integrated IT risk management. We present a theoretically motivated framework for analyzing the construct risk culture. Based on this framework we conducted a case study that underpins the crucial role of a vital risk culture in an organization. From the empirical findings we derive important factors for establishing risk culture. Our research process is guided through the following questions: What does risk culture mean and which elements does it have? What is an adequate framework for understanding and analyzing the nature of risk culture? What does risk culture look like in practice and which recommendations can be derived for establishing a risk culture as part of an integrated ITRM?

TERMINOLOGY AND CLASSIFICATION OF IT RISK MANAGEMENT AND RISK CULTURE

IT Risk Management

Originally evolving from the banking and insurance sector general risk management encompasses the process of identifying, analyzing, controlling and monitoring the company-wide exposure to internal and external risks that jeopardize strategic and operational business continuity. This includes aspects of securing and saving sensitive data, managing the threat of loss, and ensuring the quality and reliability of business processes by anticipating possible threats. As the use of information technologies as well as the resource information itself has become an essential part of business, managing risks in information management becomes a strategic success factor for companies. Information management is understood as a part of business management and deals with the optimal allocation, use, and management of the resource *information* with regard to business objectives (Applegate, et al., 2001).

Often the terms information security, IT risk management, and IT security management are used synonymously. Given the definitions above the term IT risk management can be defined along two dimensions: information and risk management (see *Figure 1*). In a narrow sense IT risk management deals with the appropriate assignment of information technologies with regard to security, quality and reliability of the systems. For our purposes we adopt a broad perspective of ITRM. It can thus be defined as "the overall activities, processes, and institutions for identification, analysis, control and monitoring of risks that arise in the context of information management or by using information technology" (Krcmar, 2005). In this classification information security and IT security management are understood as specific components of an overall IT risk management of an organization, covering the traditional objectives of information security that determine if information is protected, i.e. availability, confidentiality, and integrity of systems (Pfleeger, 1997).

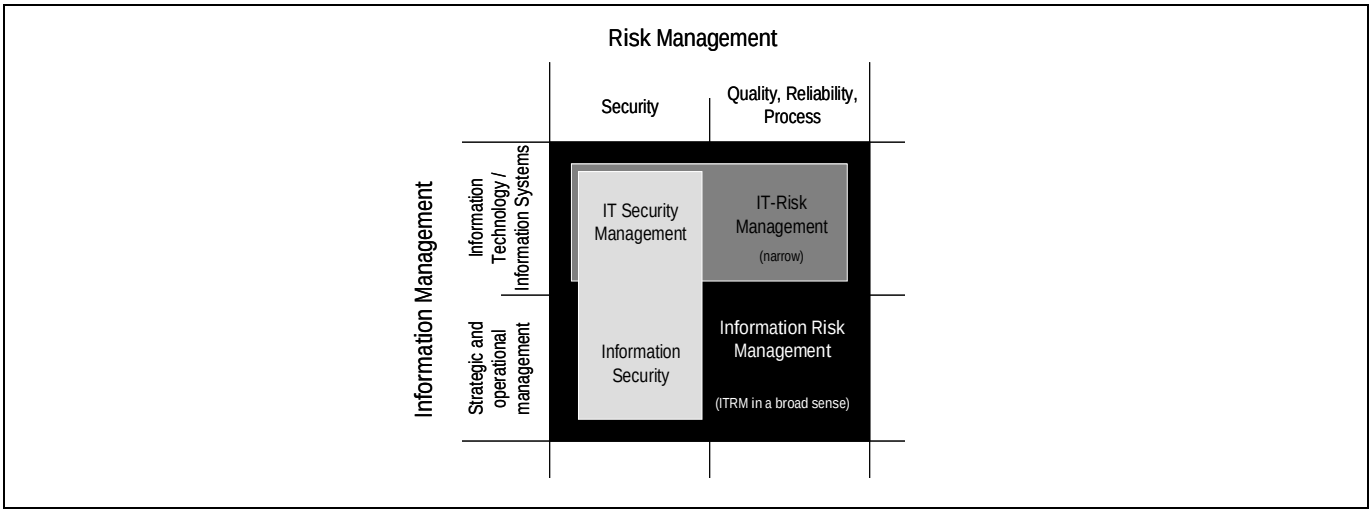

Figure 1: Categorization of IT risk management

IT Risk Culture

As previously pointed out physical, technological or procedural security countermeasures are not sufficient to avoid or mitigate risks in IT and depict only one side of an integrated IT risk management. According to Rossiter (2001) effective risk management needs to address two elements: the soft behavioral side embodied in the organization's risk culture and environment, and the more concrete side embodied in the specific risk management program that guides the enterprise. Adopting a behavioral focus besides the technical one means a paradigm shift in IT risk management. Von Solms calls the focus on socio-cultural aspects the "third wave" in the development of information security management, after focusing on purely technical measures and procedural aspects in the 80s and 90s (von Solms, 2000). But before focusing on the specific risk culture in IT risk management a basic understanding of the term (corporate) culture is necessary.

Corporate culture is often defined very vague, using unspecific, intangible or complex terms, which underpins the assumption that what we commonly understand as culture is difficult to grasp. According to Schein "corporate culture is a pattern of basic assumptions […] which have worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems" (Schein, 1985). Culture in the context of organizations is therefore a complex and dynamic phenomenon that consists of different tangible and intangible elements, changes over time and can be influenced and designed by the management of an organization.

Following the definition of corporate culture above risk culture can be defined as *a shared underlying norm and value framework of the management and members of an organization. Based on this framework risks are assessed, analyzed and controlled. Risk culture manages the awareness and disposition to identify and communicate risks and to act accordingly*. Risk culture does not only belong to IT risk management in regard to content and nature, it is also a specific part of an organization's overall corporate culture. However, risk culture does not necessarily have to be equivalent to corporate culture although consistency of both is to be intended. In analogy to Schein's three layer model (Schein, 1985) IT risk culture is allocated on different levels (see *Figure 2*). On the most visible level of artifacts obvious elements of an organization's risk culture can be found, i.e. visible security measures such as password protection, computer locks, guidelines or signs containing codes of behavior as well as security awareness campaigns. Basis for these elements are espoused values, norms, and knowledge of assessing and handling IT risks designed and established by the management and shaped by the members of the organization. As behavioral codes, rules and attitudes become permanently accepted and incorporated by the members, these elements are established on the very basic underlying level of assumptions and beliefs. The process of diffusion and implementation of an IT risk culture into the consciousness and basic attitudes of the members of an organization takes a long time and cannot be designed or influenced instantly.

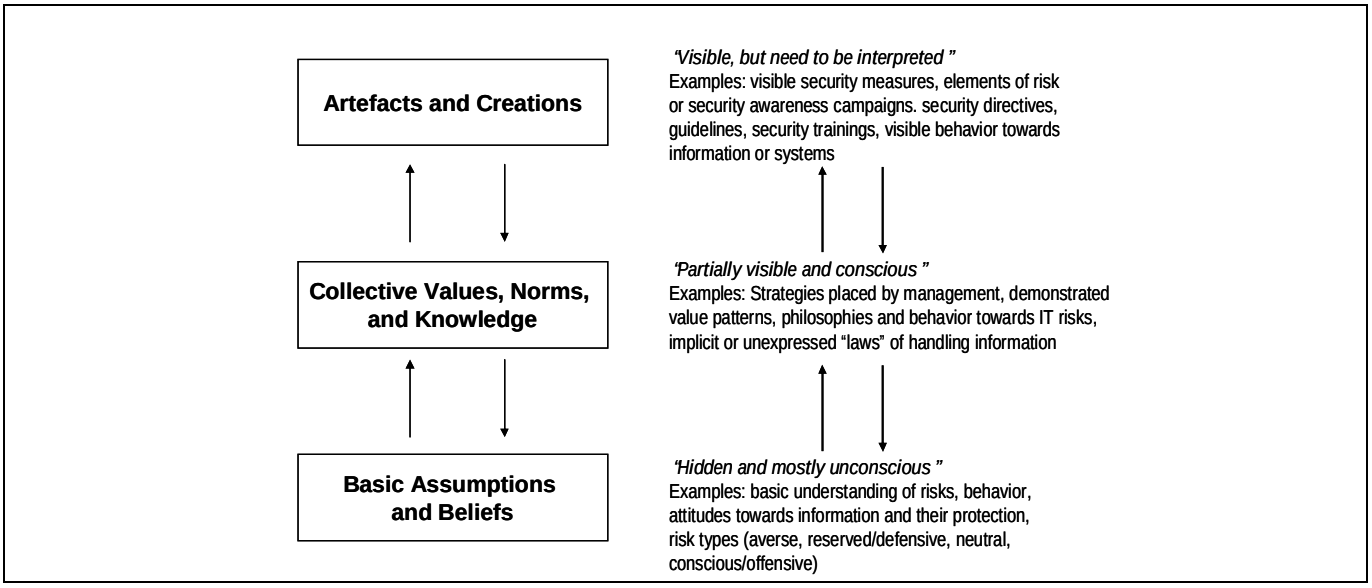

Figure 2: Layers of IT risk culture and their interactions (adapted from (Schein, 1985))

Figure 2 also outlines exemplary elements and attributes on different layers that constitute an effective risk culture. For a systematic understanding these elements can be classified into four major categories that are derived from the definition of IT risk culture. The categories are orientated along the question "*WHO* initiates *WHAT* and *HOW* to *WHOM*?", showing that the

establishment of risk culture is to be seen as a process with different sources, initiators and recipients, all playing a major role in the implementation of risk culture in a company.

1. (Top) Management and strategy
2. IT infrastructure and processes
3. Organization and artifacts
4. Individuals

While traditional IT risk management focuses on securing processes and IT infrastructure IT risk culture additionally takes the senior management, the organizational structure, artifacts and organizational members into consideration and thus underpins the multi-level character of an integrated IT risk management. It is important to note that these categories are interdependent. *Figure 3* illustrates the elements of an integrated IT risk management and also indicates on which levels (corresponding with *Figure 2*) these elements can be allocated.

Category	Action / characteristic element	Level of IT risk culture
Top Management and Strategy	**Communicate norms & objectives** • Top-down alignment of strategy • Establish norms, policies, and guidelines	**Mostly Layer 2: Collective Values, Norms and Knowledge** Layer 1: Artifacts and Creations
	Demonstrate ethics and values • Share and show ethical values and practices • "Tone at the top"	**Mostly Layer 2: Collective Values, Norms and Knowledge** Layer 3: Basic Assumptions and Beliefs Layer 1: Artifacts and Creations
IT infrastructure and processes	**Identify, assess and measure risk** • Risk assessment practices • Risk tools and processes • IT security infrastructure	**Layer 1: Artifacts and Creations**
	Establish processes, control, monitoring • Process reliability and efficiency • Control effectiveness and efficiency • System access and security • Monitoring risks	**Layer 1: Artifacts and Creations**
Organization and Artifacts	**Develop documents & policies** • Develop guideline, policies, risk & security documents • Resources	**Layer 1: Artifacts and Creations**
	Organizational Structure • Establish "person in charge" for risk and security matters: "security officer" • Develop authorization and rights concepts for access	**Mostly Layer 1: Artifacts and Creations** Layer 2: Collective Values, Norms and Knowledge
Individuals	**Promote awareness and competence** • Competence and critical attitude • Training of employees • Communication across processes	**Mostly Layer 2: Collective Values, Norms and Knowledge** Layer 3: Basic Assumptions and Beliefs
	Assign responsibility, motivation and rewards • Assign ownership, demonstrate accountability • Motivate and reward risk conform behavior by incentives • Performance indicators	**Mostly Layer 2: Collective Values, Norms and Knowledge** Layer 3: Basic Assumptions and Beliefs Layer 1: Artifacts and Creations

Figure 3: Constitutive elements of an integrated IT risk management

CONCEPT OF ANALYZING RISK CULTURE: IT RISK CULTURE CUBE

Recalling the definition of risk culture above the core of risk culture can be summarized in three dimensions: Risk culture manages the awareness and disposition (1) to identify risks and acknowledge them as threats, (2) communicate these risks forthright and target-oriented throughout the organization, and (3) act accordingly to mitigate and control the identified threats.

These three core dimensions derived from the definition of risk culture constitute a framework for risk culture (*Figure 4*). This framework is to be understood as a portfolio that can help management with analyzing and allocating the status and

stage of development of risk culture in an organization. However, as with many portfolio instruments no clear measures for the framework can be provided yet.

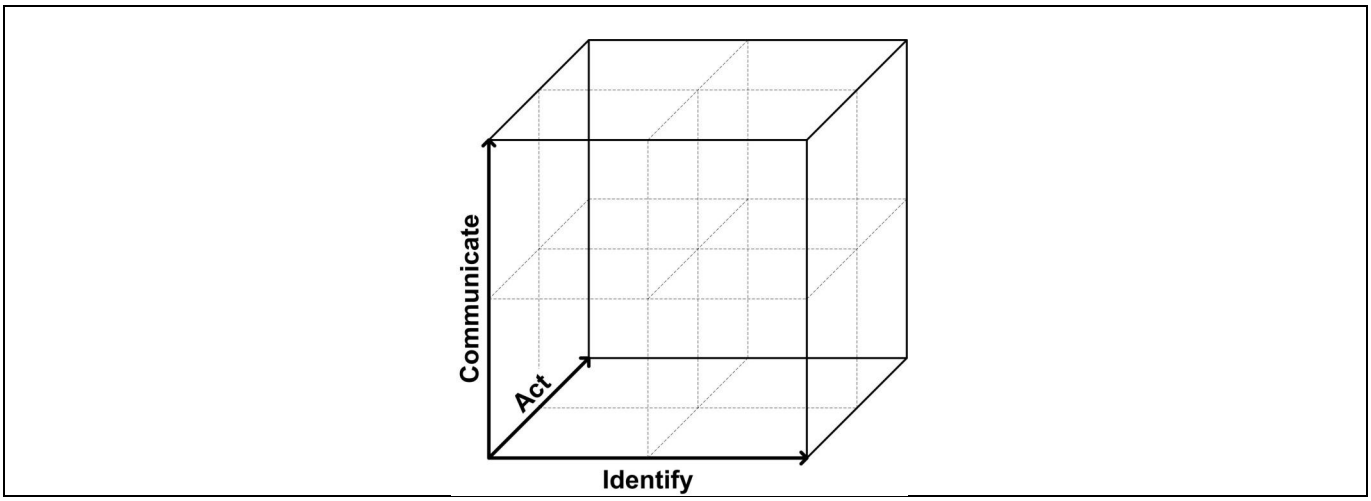

Figure 4: Framework for risk culture: IT risk culture cube

Identify and Acknowledge IT Risks

Before installing any risk management processes, risk monitoring systems or even security awareness campaigns, the acceptance of a general existence of IT risks has to be accomplished. Senior management as well as employees have to recognize and internalize the fact that the organization is exposed to internal and external risks in information management merely by possessing and using information technology. This might sound trivial or dispensable. However, often management negates the existence of risks in the organization and legitimates this assumption with allegedly high technical security standards and "optimal" processes that prevent losses or misuse of IS. In this perception IT risk management is either not existent or not necessary because risks either do not exist or the company's risk management is already optimally designed. Both assumptions are delusive and lead to inefficiencies or biased security measures.

Communicate IT Risks

Communication is an essential component of a risk culture and is a means for providing and exchanging information and values in an organization. By communication the knowledge of identified risks diffuses in all parts of the organization in a written, oral, or electronic form. This ensures a shared understanding of possible threats and is the basis for a consistent and integrative behavior of all employees. A fallacy in traditional IT risk management is based on the assumption that the ITRM process is optimally designed by identifying, analyzing, and controlling IT risks. However, one has to integrate the "elements" that are concerned with the handling of IT risks – that is the employees. Mueller-Vivil (2000) calls this a communication-driven risk policy that aims at risk awareness, generating trust, explanation of threats, and skilled behavior towards security threats.

Act accordingly to IT Risks

Taking action is the most obvious behavior to handle IT risks since neither the identification nor the communication of risks can be successful if no concrete measures follow in order to mitigate and control these risks. According to the four categories of risk culture elements above measures can be of a technical, organizational, or behavioral nature depending on the target of the action. Technical measures aim at securing the IT infrastructure and comprise the whole range of information security in order to secure the confidentiality, availability, and integrity of sensitive data. Examples can be public key infrastructures, the setup of passwords, or the establishment of a hardware infrastructure such as network firewalls. Organizational measures mainly include the planning of a company-wide ITRM process that specifies tools, responsible process owners, and procedures in the particular stages as well as organizational elements such as documents or authorization structures. Finally behavioral measures concern the identified cultural gap in ITRM and constitute the core of risk culture. Actions in this regard involve security awareness campaigns, trainings, behavior codes, internal PR, or exhibitions.

EMPIRICAL FINDINGS: THE CASE OF ALTA

Methodology

In order to underpin our theoretical considerations we followed an explorative research design and conducted an empirical case study. According to Benbasat et al. (1987) a case study "examines a phenomenon from one or a few entities (people, groups or organizations). The boundaries of the phenomenon are not clearly evident at the outset of the research and no experimental control or manipulation is used." As case studies are often used for complex, innovative, or dynamic fields, especially when no dependent or independent variables can be identified in the beginning of the research process, this method seems to be appropriate to explore the phenomenon risk culture in practice.

Various methods can be used for data collection. As we aim at a broad comprehension of the phenomenon of risk culture the data collection consists of a triangulation of different methods. We conducted three explorative, in-depth, half-standardized expert interviews with internal company experts from the IT risk management department, the head of the steering committee for information protection, and the director of Corporate IT of the IT services branch. Another major source for data collection were documents of the company that were deeply analyzed, e.g. information policies, process manual, internet appearance, intranet sites etc. A last method used for gathering data were observations that could be studied while visiting the company, e.g. about the behavior of the members and artifacts of the organization.

Analysis and Results

Company background

With a revenue of 33,5 billion Euro in 2003 ALTA is a one of the leading chemical companies in the world with its headquarter located in Germany. The company employs approx. 87.000 people in 41 countries. Its product portfolio encompasses chemicals, plastics, performance products, agricultural products & nutrition and oil & gas.

IT Risk Management

IT Risk Management is allocated in the IT security department of ALTA information services as well as in the Corporate Security section. At ALTA IT risks are regarded as a part of an overall information security together with non-IT risks that threaten sensitive information of the company. ALTA established a "Steering Committee Information Protection" as a central coordination function of all issues associated with information security. The main focus of this committee is the establishment of an *ITRM body of rules and regulations* as well as the establishment of a *security awareness campaign for information security.*

For a long time IT risks at ALTA have not been regarded as critical to business compared to general company risks. This was due to the fact that general risks such as environmental incidents accounted for a way larger amount of monetary loss. Main IT risks included the availability of critical applications such as logistics or HR systems, the confidentiality of data and external threats such as virus and hacker attacks. Potential IT risk fields are reported twice a year to a central unit ZZ (controlling and planning) together with other risk types such as financial or organizational risks. Then the IT risk management process is initiated that is very much alike a generic ITRM process with the stages of identifying, analyzing, evaluating and controlling/monitoring IT risks. However, ALTA puts a main focus on the stages of identifying and analyzing IT risks and names four triggers that can initiate the assessment process (*Figure 5*): the ZZ risk reporting, the start of an IT project, an information security audit, or information security incidents. An analysis of the business criticality of the IT systems with the ALTA information risk scorecard determines whether a detailed risk analysis is conducted or not. For IT systems, applications, and IT infrastructure components with low business criticality the baseline security approach is sufficient.

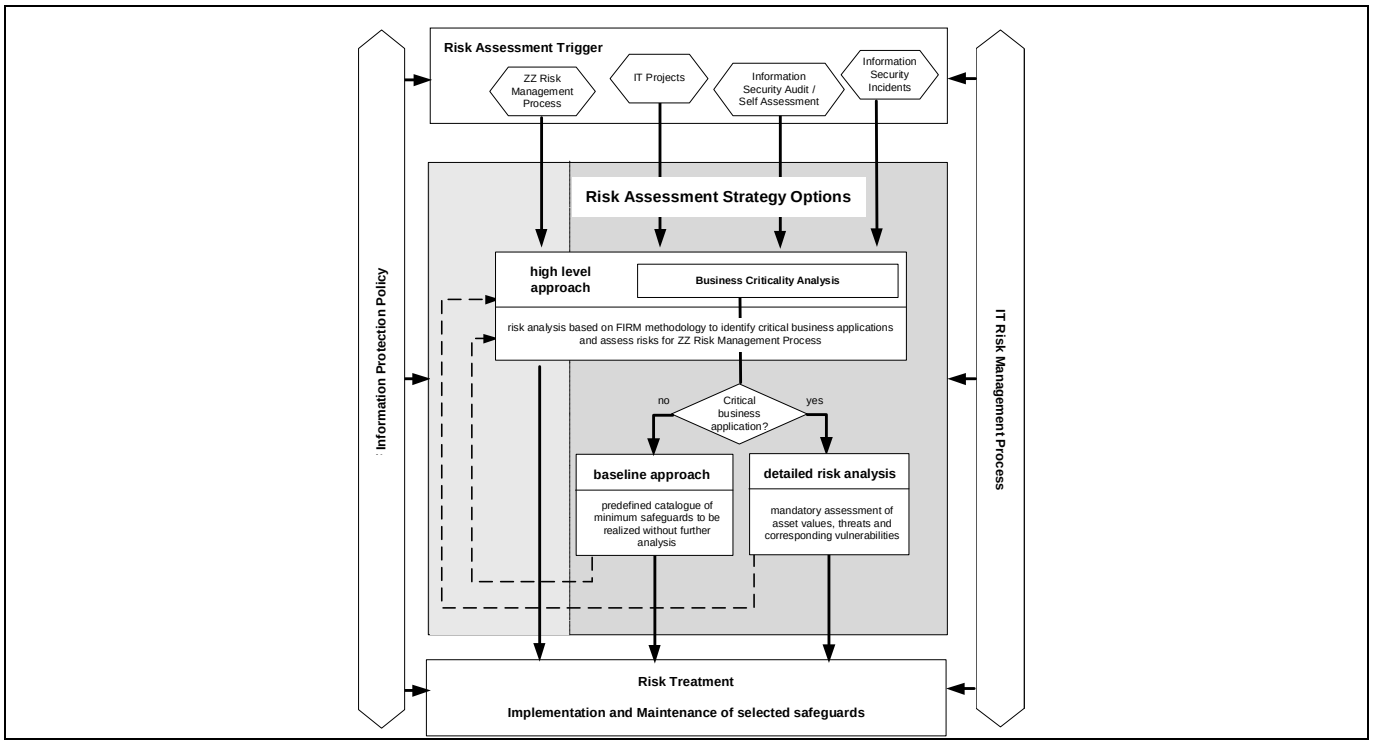

Figure 5: IT Risk Assessment Process and Strategy Options (Lechler, 2004)

IT Risk Culture

ALTA is permanently exposed to many environmental and production risks conditional on the industry it is allocated in. Compared to accidents or breakdowns in the production IT risks account for a relatively small amount of security incidents. However, it is even more astonishing that management holds the issue of risks in information management quite dear. Not only is the Steering Committee Information Protection allocated directly below the management board of directors, but also does ALTA actively initiate and establish information security programs across the company group. The steering committee is the only position that centrally develops and establishes rules and initiatives on information security across the company.

Starting point for establishing an IT risk culture at ALTA was the paradigm shift from a pure IT security (with focus on technical infrastructure aspects) to an overall information security with the focus on information as the company's most valuable resource and most important asset to protect. ALTA identified three design areas for shaping the IT risk culture:

- *Assessing the status quo of security awareness of the employees*: Audits, self-assessment, trainings, statistics
- *Technical security of information*: Security programs, security intranet, classification of documents in order to depict the security stage of data, standardized configuration of all computing machines
- *Establishing security awareness and risk values across the company*: information security campaign & policy, special intranet sites, (web-based) trainings, integration of information security in standard procedures

The core of ALTA's IT risk culture is the *information security campaign*. The fundamental idea of the campaign is based on the fact that the issue of information security is very far away from the daily routines of an employee. Thus the campaign tries to approach the employees successively in terms of both a *local* and a *thematic/topical* approach. In this context local approach means that the matters of the campaign have to be introduced to the employees in a successive physical approximation, while thematic approach focuses on an approximation of the topic from very general statements about information security to specific recommendations for individual situations. Designed for a duration of 3 months the campaign starts with a first stage of catching attention by means of posters in flashy colors (see left image in *Figure 6*). The message of the first stage that lasted about for 4 weeks was: "ALTA is being changed if necessary information is missing." These posters were allocated at common spots such as entry doors or train stations. In a second stage posters and information boards were arranged in frequently used places such as the cafeteria or office doors. The local and thematic density became highest

in the last stage. This phase got more into detail and aimed at catching the awareness of employees directly at their working places. The message of the posters was adapted to the specific working environment. For example an office worker got posters such as depicted in the middle image in *Figure 6*, while a worker in the production area got a message such as depicted in the right image in *Figure 6*. The continuing symbol of all posters, brochures, and flyers was a star in a circle used as a placeholder with a recognition character to demonstrate that "something important is missing."

In addition to posters as communication means, also an exhibition on information security, brochures and flyers as well as a telephone hotline where employees could listen to stories on internal security incidents that actually happened in the company were used to support the campaign. The campaign started in the end of 2003 in the German locations. It was planned to carry out the campaign in European division in the middle of 2004 and even a worldwide roll out in 2005.

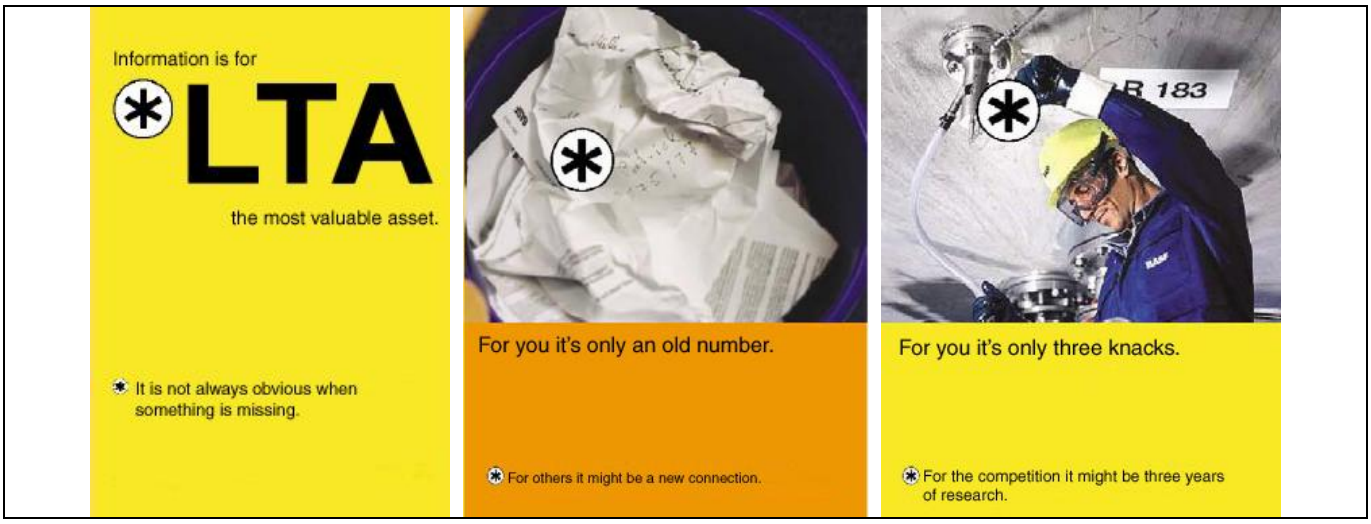

Figure 6: Means of communication and awareness of ALTA's information security campaign (translated from German campaign)

Summary and analysis of the findings

In this case several relevant findings can be highlighted. Allocated in a manufacturing industry with a traditionally low strategic focus on IT or information as a central resource compared to other industries (such as banking/insurance or the IT industry) ALTA performed a radical paradigm shift concerning the role of information: The resource information in general as well as the use of information technology plays a major role for the company although IT is not ALTA's core business. The company realized and acknowledged the potential threat evolving from the existence and use of information technology and thus puts a major focus on the identification of risks in information management. As we pointed out above this attitude cannot be taken for granted since many companies neglect the existence of risks or threats resulting from their IT. At ALTA IT risk management is not only an operational issue, but due to its organizational allocation close to the management board it becomes a strategic function. The handling of IT risks is addressed on several levels: on a technical level in terms of network firewalls, passwords etc., on an organizational level in terms of an established ITRM process, and also on a behavioral level in terms of communication means, i.e. the security awareness campaign, trainings, or security audits.

Table 1 summarizes the findings and also proposes a rough allocation of ALTA within the IT risk culture framework. The allocation within the grid was based on the results and perceptions gathered in the case study. Regarding the dimension of "identify" a well established risk assessment process in the company leads to a high position on that scale. Also the establishment of technical, organizational and behavioral measures results in a high position on the "act" scale. Finally the sustainable implementation of a lasting and integrated communication campaign throughout the whole company accounts for a high development on the "communicate" scale.

Criteria	
Industry	Chemical industry
Focus of IT risks	strategic
Initiative/responsibility for establishment of risk culture	Steering Committee Information Protection (directly responsible to management board)
Importance of behavioral aspects of IT risks	High (risk culture actively supported)
Elements of risk culture	
Artefacts and creations	§ Information security policy § Information security campaign (worldwide) § Security trainings/audits
Collective values, norms, knowledge	§ Values of management board established in the information security policy: "information is our most valuable asset" § Risk awareness § Sensitive handling of data § Authorization concept for data/information
Basic assumptions and beliefs	§ Planned: Acceptance of IT risks in daily routines, established awareness for IT risks
Proposed allocation of ALTA in the IT risk culture framework	

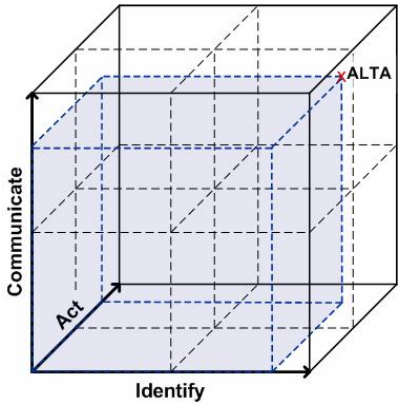

Table 1: Summary of findings in the ALTA case

CONCLUSION AND OUTLOOK FOR FURTHER RESEARCH

In this paper we pointed out the essential role of risk culture for an integrated IT risk management. We thus presented important determining factors for the subject of risk culture and developed a framework for allocating and analyzing the IT risk culture of a company. From the case of ALTA we derive the assumption that the model is an appropriate framework to cover the relevant areas of an integrated IT risk management. However, it must be noted that no *detailed* instructions or recommendations can be derived from this framework. It should rather be regarded as a portfolio instrument to analyze the overall situation of a company's ITRM or risk culture. The framework will also have to be validated empirically with a larger number of cases. In future research we plan to operationalize the dimensions of the risk culture cube as up to now only a rough and obviously no rational allocation of a company within the cube is possible.

In further research also the following questions should be addressed: Is the role of IT risk culture more relevant in certain industries? In other words does a company in the IT industry not need to establish a shared understanding of IT risks due to the fact that IT is its primary business and thus an "industry-related" awareness is already established in the daily routines of the employees? It is also obvious that risk culture is not the only success factor for IT risk management. Others may be the strategic allocation of IT risks or other organizational arrangements.

Finally the problem of operationalizing and measuring a successful risk culture is to be mentioned. In the case of ALTA the step of evaluating the success of the communication means and thus the success of a strong risk culture is still to be done. Until now a broad acceptances as well as positive feedback of the members of the organization seem to show the success of the measures, however there are no quantitative numbers yet. Also values such as "sunk number of security incidents" cannot be attributed to higher security awareness. Measures have to be found to confirm the supposed cause-and-effect-chain.

REFERENCES

1. Adams, A., and Sasse, M. A. (1999) Users are not the enemy, *Communications of the ACM*, 42, 12, 41-46.

2. Applegate, L. M., McFarlan, F. W., and McKenney, J. L. (2001) Corporate Information Systems Management, 5. ed., McGraw-Hill, Boston.

3. Benbasat, I., Goldstein, D. K., and Mead, M. (1987) The Case Research Strategy in Studies of Information Systems, *MIS Quarterly*, 369-386.

4. Chabrow, E. (2005) Outlook 2005: A Strong Foundation, *InformationWeek*, 1, January 3, 2005.

5. Krcmar, H. (2005) Informationsmanagement, 4. ed., Springer, Berlin.

6. Lechler, A. (2004) Risk Analysis Security Guideline ALTA AG, ALTA AG, Ludwigshafen.

7. Müller-Vivil, A. C. (2000) Kommunikationsintendierte Risikopolitik von Unternehmen, Deutscher Universitätsverlag, Gabler, Wiesbaden.

8. Pfleeger, C. P. (1997) Security in computing, 2. ed., Prentice Hall, Englewood Cliffs, N.J.

9. Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. (2004) Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, US Secret Service, CERT Coordination Center Software Engineering Institute Carnegie Mellon University.

10. Rossiter, C. (2001) Risk culture - up close and personal, in http://www.camagazine.com/index.cfm/ci_id/6458/1a_id/1.htm, accessed January 10, 2005.

11. Schein, E. H. (1985) Organizational Culture and Leadership, Jossey-Bass, San Francisco.

12. Schlienger, T., and Teufel, S. (2002) Information Security Culture - The Socio-Cultural Dimension in Information Security Management, *Proceedings of the Security in the information society: vision and perspectives. IFIP TC11 International Conference on Information Security (Sec2002)*, Cairo, Egypt, 191-201.

13. Sherer, S. A. (2004) Managing Risk beyond the Control of IS Managers: The Role of Business Management, *Proceedings of the 37th Hawai'i International Conference on System Sciences (HICSS 37), January 5-8, 2004*, Big Island, Hawai'i.

14. von Solms, B. (2000) Information Security - The Third Wave, *Computers & Security*, 19, 7, 615-620.

15. Ward, J., and Peppard, J. (2003) Strategic Planning for Information Systems, 3. ed., Wiley, Chichester.