Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings

Proceedings

Corporate Risks in Social Networks – Towards a Risk Management Framework

Richard Braun
Department of Business and Economics Chair for Information Systems, esp. Systems Engineering, Technische Universität Dresden, Dresden, Saxony, Germany., richard.braun@tu-dresden.de

Werner Esswein
Department of Business and Economics Chair for Information Systems, esp. Systems Engineering, Technische Universität Dresden, Dresden, Saxony, Germany., werner.esswein@tu-dresden.de

Recommended Citation

Braun, Richard and Esswein, Werner, "Corporate Risks in Social Networks – Towards a Risk Management Framework" (2012). *AMCIS 2012 Proceedings*. 9.
http://aisel.aisnet.org/amcis2012/proceedings/VirtualCommunities/9

Corporate Risks in Social Networks – Towards a Risk Management Framework

Richard Braun
Technische Universität Dresden
richard.braun@tu-dresden.de

Werner Esswein
Technische Universität Dresden
werner.esswein@tu-dresden.de

ABSTRACT

Social networks like Facebook or LinkedIn can be used by companies in various fields like marketing, distribution, product development or support for gaining business value. However, in contrast to these opportunities there are also corporate risks regarding the usage of social networks, for example resulting brand damages, industrial espionage or inefficiency. So far, only little understanding of corporate risks in social networks exists. Just a few single risks are discussed in literature. Thus, an extensive literature analysis was conducted for the creation of a systematic risk catalog. For a better understanding of the domain, a reference data model was developed consisting of data objects that could be exploited by attackers in social networks. Finally, a first approach towards a risk management framework is proclaimed in order to be used by companies in social networks. It integrates the identified risks, dedicated process steps and specific IT artifacts.

Keywords

Social Networks, Risk, Framework, Threat, Social Media, Business, Data Leakage, Identity Theft.

INTRODUCTION AND MOTIVATION

Online social networks (in the following referred to as “social networks”) like Facebook, LinkedIn or Twitter gained much more importance in the last years. 50% of the 800 millions of Facebook users log into their personal account every single day and about 7% of the daily internet traffic is caused by Facebook (Wang, Xu and Grosslags, 2011). Additionally, a lot of companies increasingly operate in social networks: They have (brand specific) profiles, initiate marketing campaigns or help their customers online (Sinclaire and Vogus, 2011). Boyd and Ellison (2007) define social networks as web-based services where users can create (semi-) public profile pages and can establish and maintain contacts to other users. According to Richter et al. (2009) such web pages are also identified as social networks if their primary effort is not only directed towards enabling and supporting social networking but also to providing and exchanging content or media. Examples for these special types of social networks are Youtube (characterized by presenting content) and Twitter (allowing micro blogging) (Richter, Riemer, vom Brocke and Große-Böckmann, 2009). The growing relevance for companies of existing social networks is already mentioned in the literature (Barnes, 2011; Braun and Esswein, 2012; Richter, Riemer and vom Brocke, 2011; Segrave, Carson and Merhout, 2011). Companies are able to profit from the social network phenomenon in five business areas: Marketing, distribution, human resources, research and development as well as support (after sales service). Braun and Esswein (2012) systematized these benefits and developed a framework that is depicted in figure 1.

So far, the topic of risks has been primarily discussed from a private user’s point of view. Relevant issues in this context are privacy and data security (Hasib, 2009). Culnan et al. (2011) emphasize the strategical relevance of corporate risk management in social networks from an institutional perspective (Culnan, McHugh, Zubillaga, 2011). Fournier and Avery (2011) notice that mitigation of risks in social networks is an essential topic on the management level (e.g., for managing reputational risks). For the most part, the literature discusses singular problems (e.g., loosing control during stakeholder communication; Pekka, 2010) or gives insight into collections of empirical examples (Langheinrich and Karjoth, 2010). Furthermore, Hardy and Williams (2010) show that existing frameworks like ISO 27001/27002 are inadequate to depict risks of web 2.0. Such frameworks are unable to deal with threats arising from social networks. In general, a great lack exists concerning a comprehensive and thorough understanding of the problem. To the best of our knowledge there is neither a domain-specific risk management framework nor a risk management system to solve this problem. Decision makers on the ground as well as researchers have only little understanding of specific risks and have no reference for managing, monitoring and mitigating those. Of course, it is nearly impossible to develop and establish effective counteractions since the specific risks remain unclear.

Because of research gaps in theory and practice the first question of the paper is formulated as follows: *What are corporate risks in social networks and how can they be systematized?* The second research question is: *What is an adequate corporate process for the mitigation of these risks?*

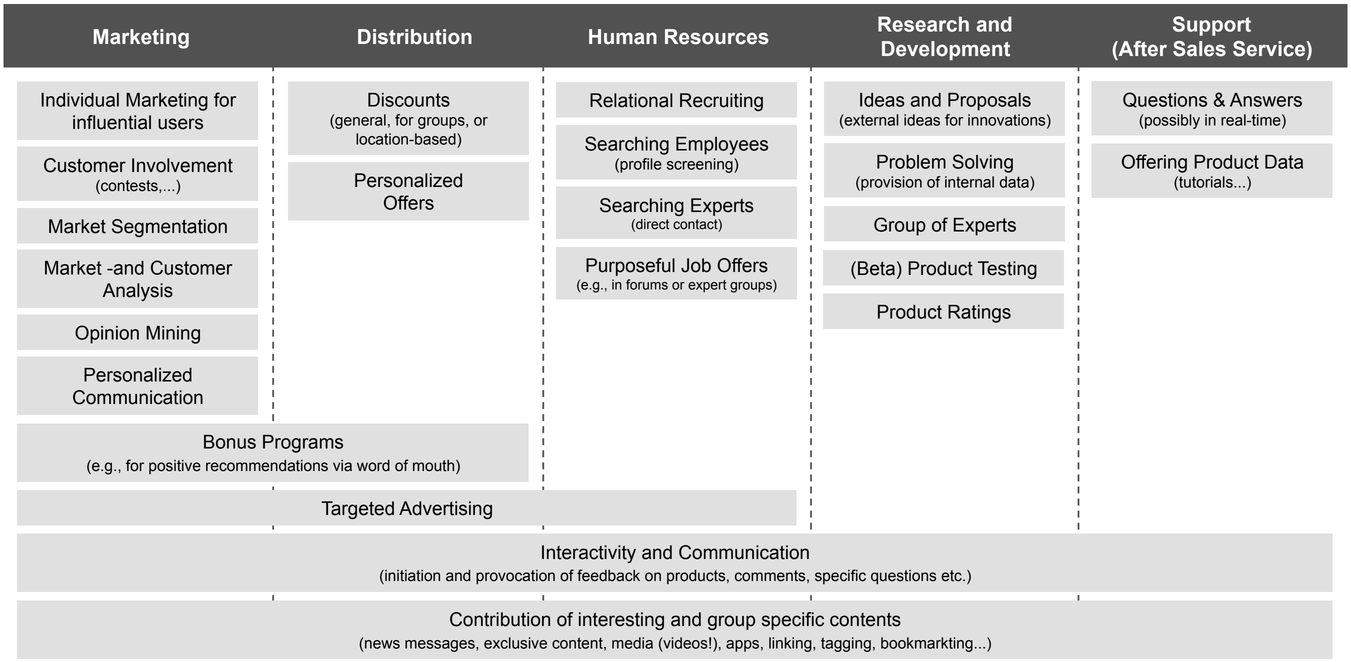
Marketing
Distribution
Human Resources
Research and Development
Support (After Sales Service)
Individual Marketing for influential users
Customer Involvement (contests,...)
Market Segmentation
Market -and Customer Analysis
Opinion Mining
Personalized Communication
Discounts (general, for groups, or location-based)
Personalized Offers
Relational Recruiting
Searching Employees (profile screening)
Searching Experts (direct contact)
Purposeful Job Offers (e.g., in forums or expert groups)
Ideas and Proposals (external ideas for innovations)
Problem Solving (provision of internal data)
Group of Experts
(Beta) Product Testing
Product Ratings
Questions & Answers (possibly in real-time)
Offering Product Data (tutorials...)
Bonus Programs (e.g., for positive recommendations via word of mouth)
Targeted Advertising
Interactivity and Communication (initiation and provocation of feedback on products, comments, specific questions etc.)
Contribution of interesting and group specific contents (news messages, exclusive content, media (videos!), apps, linking, tagging, bookmarkting...)

Figure 1: Business opportunities in social networks (Braun & Esswein, 2012)

In order to answer the first question a structured literature analysis was conducted (see second chapter "literature analysis"). The identified risks are classified and concluded in a catalog using a risk modeling language. Thus, it is possible to get an integrated overview over all threats and their main attributes (see third chapter "risk catalog"). Since social networks are data intensive areas it is necessary to point out the most important data objects regarding potential risks. Therefore, a data reference model for the analysis of user profiles in social networks is presented in the first part of the fourth chapter "risk management framework". The second part of the fourth chapter deals with the second research questions and the development of a first approach to risk management based on the ISO 31000:2009 guidelines. Corporate management of risks constitutes the main purpose of that process, which describes how to use and manage the identified risks in the company (see third chapter "risk catalog"). Especially the chapter "risk management framework" is relevant for practitioners since it gives dedicated process steps for the mitigation of risks. The fifth chapter "conclusion and further research" sums up research contributions, limitations and ideas for further research.

The research work is based on the design science paradigm (Hevner and Chatterjee, 2010). Research artifacts were developed as a supporting tool for decision makers. Conceptual and theoretical bases were made for developing a management-supporting tool (being the superior research goal). This IT based management system is supposed to identify, monitor and manage risks arising from social networks.

LITERATURE ANALYSIS

In this work, risk is seen as a subjectively perceived threat to achieving organizational goals (Willcocks and Margetts, 1994) as well as a set of negative effects caused by uncertainty to corporate objectives (Strecker, Heise, and Frank, 2010). Uncertainty is the result of unpredictable events or a lack of information during a decision making process (ISO 31000:2009). For example, harsh unexpected customer criticism represents an unexpected event and insufficient management decisions are caused by missing data or information (see chapter "risk catalog"). Thus, risk management falls in the remit of top level management and requires a top-down-approach (ISO 31000:2009). According to the discipline of information systems risks also arise from technical threats. These threats are defined as „any potential occurrence, either accidental or malicious, that can have undesirable effects on the assets and resources of organizations" (Newman, 2006). Consequently, technical threats are understood as possible damaging events. The realization of these threats stays uncertain (ISO 31000:2009). Corporate risks in social networks can have different causes. First, risks can be inherent in the technology and the characteristics of social networks as itself. Furthermore, characteristics of social media (e.g., user-generated content, sharing, ratings and low access barriers) determine some risks. Second, risks can occur due to responses towards the behavior of the company (e.g., negative feedback to social marketing campaigns) or because of inappropriate behavior of employees in social networks (e.g., unintended revealing of confidential information). Third, risks can occur within the company respectively in managing the company. For example, the assessment of activities and efforts on social media and social networks is still a huge problem and can cause inefficient resource allocation (Fisher, 2009).

The analysis method by vom Brocke et al. (2009) was applied for the systematical analysis of the literature. Within this method the research scope comprises risks for companies in using social networks. Explicitly, the use of social networking technology within companies is not of interest in this paper (e.g., as a intranet tool). In the style of Cooper (1988) the analysis focuses on a specific research goal: the consolidation and systematization of existing literature („integration objective“; Cooper, 1998; vom Brocke, Simons, Niehaves, Riemer, Plattfaut, and Cleven, 2009). The analysis is conceptual, tries to reflect an objective representation of the state of research and integrates the majority of available literature (vom Brocke et al., 2009). Relevant search phrases were identified in the phase „conceptualization of the topic“. Since there was very little general literature on the topic – except from empirical descriptions (e.g., Langheinrich and Karjoth, 2010) – search phrases had to be generalized. Thus, literature that deals with risks of social media and web 2.0 in general was also explored. In the analysis phase „literature search“ databases and journals were sifted through using the defined search phrases (vom Brocke et al., 2009). Terms from the social network domain (social network, social networking site, online social network, Facebook, social media, web 2.0) and the risk context (risk, threat, danger, attack, insult, crime) were combined to 36 search phrases. These phrases were applied to the following databases: EBSCOHost, ACM Digital Library, ScienceDirect and ISI Web of Knowledge. Additionally, AIS Electronic Library and the IEEE Xplore Digial Library were examined. The results were explored by applying forward and backward search. Hence, we investigated 34 articles. Afterwards, every single article was analyzed regarding to the title, the keywords and the abstract. If the article seemed to be appropriate to the research scope, two researchers analyzed the full text of the paper separately. Finally, the following 13 articles were identified as significant literature: Fournier and Avery (2011), Langheinrich and Avery (2011), Hardy and Williams (2010), Hasib (2009), Hoffman et al. (2009), Huber et al. (2011), Irani et al. (2011), Newman (2006), Pekka (2010), Timm and Perez (2010), Rudman (2010), Wang et al. (2011) and Weir, Toolan and Smeed (2011). The synthesized result of the literature analysis is presented in chapter “risk catalog”.

RISK CATALOG

In this chapter results of the literature analysis are presented by introducing all risks. 16 risks were identified in total. Six of them were classified as main risks (accentuated through a gray-shaded background in figure 2). The other ten are understood as “drivers” or primary contributors for the main ones. To gain an overview, all risks and their interdependencies were systematized in a model that is depicted in figure 2. The risk modeling method by Strecker et al. (2010) was utilized. Some concepts of their RiskML (risk modeling language) were slightly customized. Only the object type “risk” and the covered property “visibility” were used. “Visibility” provides information about the recognizability and controllability of a risk. This implies how difficult it is to discover (and manage) a risk. The property can have the following values: Invisible, low, medium or high. The property “isReversible” describes whether the damage of a risk can potentially be recovered (Stecker, Heise and Frank, 2010), which implies how suitable a company can react when a risk occurs. If the value of the property is set to “false”, the resulted damage cannot be corrected. As mentioned in chapter “literature analysis”, literature on risks in social networks is very rare. Subsequently, detailed information about other properties of risks (e.g., measures or measure impacts; Strecker, Heise and Frank, 2010) is missing. Hence, only those properties of RiskML are used which are suitable for the general topic. Nevertheless, the RiskML meta model (Stecker, Heise and Frank, 2010; p. 602) was extended by adding one property. The property “isInternal” expresses whether a risk is internal (saying that the significant reason is within the company) or external.

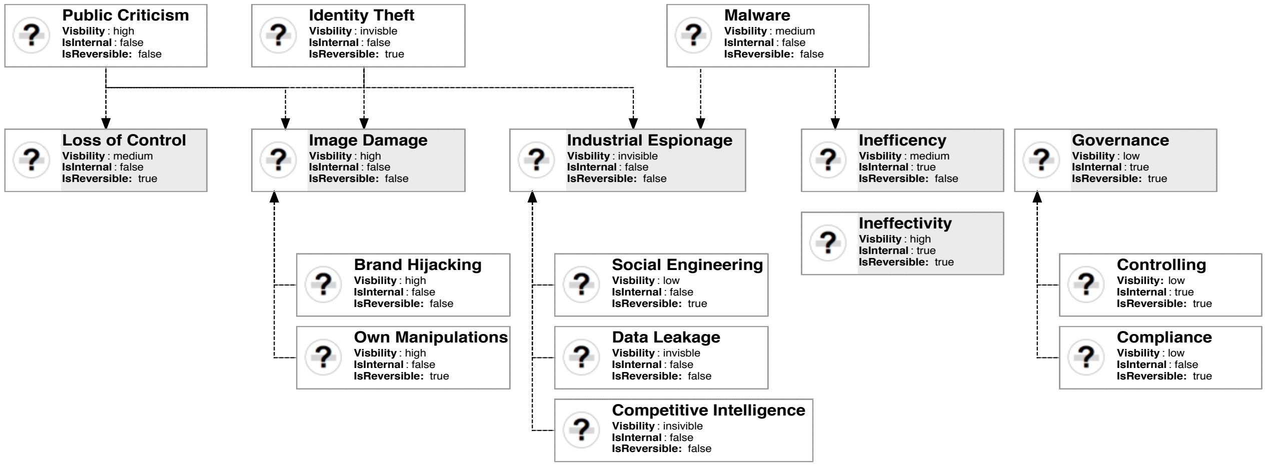

Figure 2: Identified corporate risks in social networks (RiskML model)

All risks and all relationships between them will be described in detail in the following paragraphs. In addition to the results of the literature analysis first basic approaches will be given that could assist in identifying corporate risks in social networks.

Loss of Control

The extremely high interconnection in social networks and the inexpensive dissemination of data between users lead to very high prevalence rates of messages (Pekka, 2010). The transparency of messages is facilitated by public comments as well as by linking and copying (Fournier and Avery, 2011). These mechanisms can be seen as a potential benefit in the field of (viral) marketing (Ermecke, Mayrhofer and Wagner, 2009). Beyond this, for companies it is very tricky to react adequately to critical or even incorrect messages (Kaplan and Haenlein, 2010; Langheinrich and Karjoth, 2010). Since social networks are not controllable by nature, diverse connections between members of different stakeholder groups (employees, partners, customers, competitors or former employees) are possible. These connections can cause some collision of interests or even data leakage. Moreover, communications about companies are very hard to control regarding content, scope and frequency (Mangold and Faulds, 2009). Possible “waves of critics” are very problematic for companies as shown in Langheinrich and Karjoth (2010). For companies it is possible to reclaim lost control by applying a high feedback frequency and a comprehensive monitoring of all online conversations. Thus, the risk is “reversible” (see figure 2). One indicator for this risk can be the percentage of negative conversations about the company in multiple channels (e.g., company profile on Facebook, tweets, diverse brand profiles).

Identity Theft

The term “identity theft” can be defined as the mischievous takeover of a user’s online identity (Timm and Perez, 2010). Either the password of the account is hacked or a new user account is created if the victim has no account in a specific social network yet (Hasib, 2009; Timm and Perez, 2010). Thereby attackers profit from weak passwords or easy password questions (Hasib, 2009). Furthermore, social networks typically do not request real authentication during the registration process. With the help of an occupied user identity an attacker can acquire access to personal data of the victim and is able to spy contacts of the victim since they trust him. If the victim is connected to colleagues it is very easy to gain confidential information (e.g., organizational structures, hierarchies or customer information) by analyzing private groups or simply asking colleagues via private messages. On the other side, an attacker can execute phishing attacks or publish content under the name of the victim (as an employee of a company) (Langheinrich and Karjoth, 2010; Weir, Toolan and Smeed, 2011). If the victim is a leading employee this could be very crucial since they have a huge (hierarchical) impact. Further, identity theft is dangerous for the communication between stakeholders in business social networks like LinkedIn. Another important aspect is the (semi-) public accessibility of demographic data in profiles (e.g., birthday or current residence) that can be misused for authentication in IT systems (e.g., helpdesks; see Lanheinrich and Karjoth, 2010). This is important with respect to the section “industrial espionage”.

The second kind of identity manipulation in social networks is known as fake profiles (Hasib, 2009; Weit et al., 2011). Fake profiles are primarily used to produce artificial interest in a specific topic (e.g., a new product) and to produce electronic word of mouth effects (Ermecke, Mayrhofer and Wagner, 2009). Fake profiles can also be used to defame other users (e.g., competitors) via negative postings or ratings. Although social networking providers permit the creation of fake profiles it is very easy and cheap to create one. If the "identity theft" risk has occurred it is possible to revoke some of the actions of the attacker. For example, it is possible to send an information message to all contacts and to check all sent messages. Hence, we assess this risk as "reversible". But, of course, lost data is irreversibly lost (see section "data leakage"). A possible indicator for the identification of identity theft can be a sudden change of a user's behavior (e.g., unusual content, increasing activities or messages).

Image Damage

Image damages or reputational damages are named as key risks in the literature (Fournier, and Avery, 2011; Hardy and Williams, 2010; Langheinrich and Karjoth, 2010; Rudman, 2010), since reputation is "the currency of Web 2.0" (Fournier and Avery, 2011). The image or the reputation of a company can be damaged either by actions of users or by actions of the company itself (see subsequent sections). Actions of users can be understood as comments or assessments. Thereby, attackers could manipulate a recommendation system as shown exemplarily by Hoffman et al. (2009) and Lang, Spear and Wu (2011) and they can also use fake accounts to expedite critical discussions or to disseminate damaging contents. Users utilize the interconnectivity of social networks (see section "loss of control") as well as their low transaction costs (Langheinrich and Karjoth, 2010). Companies can also cause harm to themselves if they do not act authentically or if they are not accepted within the social network (Fournier and Avery, 2011). If that risk becomes real it is very expensive and difficult to correct the image damage. Hence, the risk property "isReversible" was set to "false" (see Figure 2).

Public Criticism and "Anti" Campaigns

According to Langheinrich and Karjoth (2010) public criticism is the main reason for image damages. It is possible to distinguish between founded and baseless (or even wrong) criticism. Critical statements of (perhaps hypercritical) customers (users) are very dangerous for companies since these statements can influence other users (Fournier and Avery, 2011). Baseless critic is often based on deliberately placed misinformation or assertions (Langheinrich and Karjoth, 2010) that could seem to be concerted "anti" campaigns from competitors (e.g., via different fake profiles). Counter statements against these assertions require considerable efforts for companies (Fournier and Avery, 2011). Aside from customers and competitors, other stakeholders like NGOs can also use social networks for harsh criticism of businesses. Except these active and obvious attacking modes there is also the risk of defamation via reputation systems or recommendation systems (Hoffman et al., 2009; Lang et al., 2010). Although a proof of manipulation is theoretically possible (Lang et al., 2011) it is very difficult to implement under acceptable efforts. In general, companies can reply well to that risk if they try to implement appropriate counteractions like public excuses or coupons (as shown exemplarily in Fournier and Avery, 2011). Hence, the reversibility of this risk was set to "true". One possible indicator for that risk is negative ratings in recommendation systems or an accumulation of negative comments in profiles or in micro blogs.

Brand Hijacking

Another brand risk is the "alienation" of corporate campaigns in social networks by stakeholders (especially customers and competitors). User groups use activities of companies in social networks as a bandwagon for the realization of own objectives. Langheinrich and Karjoth (2010) and Fournier and Avery (2011) show several possible scenarios for that, e.g., the propagation of criticism on profiles or shifting a co-creation contest to a parody (Fournier and Avery, 2011). Another scenario deals with the loss of customers to a competitor: If a customer complains about a defective product feature via the public profile of a company and a competitor reads that public message, he can try to poach the disappointed customer by offering a working product. Since profiles of social networks are mostly public, it is quite easy to monitor competitor's online data streams manually or automatically (e.g., by using monitoring software like Radian6). Once a brand's profile or a specific campaign is "hijacked" it is very hard to regain. So, that risk is not reversible.

Own Manipulations

It seems to be attractive (as well as illegal) for some companies to use the abovementioned risks as chances to gain business profit. This piquant topic is not discussed in literature so far, although there are even first applications for simulating crowds by the orchestration of dozens of fake users. In 2010 the German company Telekom made headlines when it became known that a PR agency created fake blogs for the company. Companies have to expect dramatic image damages if such manipulations become public. Since that risk is an internal risk (responsibility and control are on management level) it is also reversible. Companies can just stop or curb such manipulations.

Industrial Espionage

While employees and stakeholders increasingly connect with each other in social networks, more and more business data can be exchanged as well (e.g., current states of projects, new customers, opinions about the company). Thus, the risk of losing confidential data or even intellectual property increases (Hasib, 2009). An analysis of organizational structures or procedures is possible if attackers gain entrance to online company groups by applying social engineering or identity theft attacks (Deloitte, 2009). Leading employees, IT admins, key users und customer support employees are critically at risk for these attacks (Deloitte, 2009). The IT security firm Cyperoam presented a study for analyzing companies on the basis of accessible information in social networks. They observed several profiles of employees in different social networks and agglomerated them to highly informative "master" profiles. These profiles were analyzed with the help of a content analysis to gain insights on the organization and current topics of the company (Hill, 2011). It should be noted, that it is widely possible to automate the process of data aggregation by using APIs (e.g., OpenSocial, Facebook Graph or Twitter API) of social networks. Generally, that risk is dependent on what business data employees share in social networks and how they configure their privacy settings (Wang et al., 2011). A second basic problem is the fact that approximately 40% of all users accept friend requests without any verification (Sophos, 2009).

(Reverse) Social Engineering

Social networks are particularly well suited for social engineering attacks (Deloitte, 2009; Irani et al., 2011; Langheinrich and Karjoth, 2010; Rudman, 2010). In addition to classical social engineering, reverse social engineering is a serious problem (Irani et al., 2011). The victim connects with the attacker by itself for different reasons and has therefore a greater confidence in the attacking user (Irani et al., 2011). A prerequisite for this is some kind of appeal (in the sense of usefulness) of the attacker (e.g., interests, expertise, status). Therefore the attacker has to construct a pretext for attracting the interest of the victims (Irani et al., 2011). For example, the attacker can enter appropriate (demographic) data in his profile, built up a pseudo network of contacts (fake profiles) or deliver any kind of relevant content. This information is then processed by recommendation engines, visitor tracking or demographic-based engines in social networks. The engines give users (victims) recommendations about similar users (e.g., based on the profile). Possibly, the user sends a contact request to the attacker (Irani et al., 2011). As shown by Irani et al. (2011), these (recommendation) mechanisms as well as APIs of social networks can be exploited for such a scenario. Basically that risk is reversible since victims can cancel the relationship to the attacker after the recognition of the attack.

Data Leakage

Data leakage in social networks is a consequence of inconsiderate publishing and sharing of business data as well as (reverse) social engineering (Langheinrich and Karjoth, 2010). Furthermore the use of malicious apps can lead to data leakage if the user has only poor privacy settings (Wang et al., 2011). Wang et al. (2011) using an empirical study show the possibility of getting a lot of profile data from users and their contacts if they do not configure their privacy settings well enough. A set of vulnerable data types in social networks is presented in figure 3 in chapter "risk management framework". The main reasons for that risk are inadequate privacy settings (basically, many users do not have any understanding of this problem) as well as unclear access options during the installation process of (Facebook) apps (Hasib, 2009, Wang et al., 2011). Another threat is so-called spear phishing (Newman, 2006) that have a high success rate in social networks (Hasib, 2009). Of course, data leakage is irreversible since it is not possible to recover lost data. Further, that risk is nearly invisible and so it is very difficult to detect. Possible indicators for data leakage could be unsecure privacy settings in user profiles or even the amount of installed apps per account.

Competitive Intelligence

The exploitation of business data in social networks by competitors is another risk for companies (Hill, 2011; Langheinrich and Karjoth, 2010; Weir et al., 2010). Interesting targets are customer relationship management, internal organization and the current business situation (e.g., revenue and new projects). As mentioned in Langheinrich and Karjoth (2010) it is possible to infer a new customer of a competitor by combining and analyzing his data in business and location based social networks like Foursquare. Reasons for that risk are multifarious shared data in different social networks (see figure 3). De facto, this risk is – similar to data leakage – nearly impossible to analyze, since there are no obvious indicators. The risk is irreversible. An appropriate protection is the limitation of data that is shared in social networks.

Malware

As shown in section "data leakage" the installation of third-party apps in employees' user profiles is a serious security problem regarding to the possible contamination with malicious software. According to Timm and Perez (2010) approximately 60% of all malware attacks are realized with the help of such apps. Besides, so-called like-jacking (Langheinrich and Karjoth, 2010; Timm and Perez, 2010) or redirecting to malware websites by applying tiny URLs (e.g., bit.ly that hides the real URL) are possible attacking techniques. Also, the dissemination of spam messages via social networks is a serious problem (Huber et al., 2011). Malware damages are irreversible if the damage occurs.

Inefficiency

The risk inefficiency contains several internal threats to companies regarding social networks. While employees use social networks at work they are distracted from their regular business and become unproductive (Langheinrich and Karjoth, 2010). Additionally, the business IT network is charged and could cause performance problems (Rudman, 2010). Some companies respond to that problem by blocking entire social networks or single functionalities (Langheinrich and Karjoth, 2010). Usually, the detection and treatment of IT problems caused by malware (see section before) can tie up resources. The prompt reaction to (hypercritical) customers as well as unrealistic expectations of customers regarding to the replying rate of companies lead to high efforts in customer care (Fournier and Avery, 2011). When companies use social media data for their own purposes (e.g., competitive intelligence), they have the problem of the unclear verification of data since the “reality” in the web can be distorted by fake accounts or false information (Pekka, 2010). The mentioned risk “inefficiency” is internal, since it relates to internal processes and structures. Therefore it is also reversible since companies can use experiences to counteract the threats. Possible indicators are: Requests to social networks from the company network, efforts for troubleshooting or for the support and care of users in social networks.

Ineffectivity

Ineffectivity describes the level of realization of a corporate objective with a specific action. In social networks companies offer various content and media to get in contact with users. If these actions do not fit the demand of the users, they become ineffective since they do not reach the intended objectives (vgl. Fournier and Avery, 2011). The challenge consists in the selection of the right actions and campaigns as well as the adequate effort of corporate resources (e.g., implementation costs for developing an app or editorial costs for generating content in social networks). This risk is internal, since internal processes and decisions primarily cause it. Because of this it is also reversible. Possible indicators are (statistical) key figures like downloads, the number of fans or more complex key figures (Fisher, 2009; Murdough, 2009). Internal accounting provides information on the costs.

Governance

Next to the abovementioned risks there are also explicit internal risks. One issue is the right effort of personnel resources for the work in social networks (Fournier and Avery, 2011). Another problem is the communication and collaboration between different departments when it is necessary to develop analysis tools or apps (e.g., Social Media Center and IT department; Symantec, 2011). Another challenge is the guarantee of process flexibility to react on dynamic and arbitrary customer behavior in social networks (Fournier and Avery, 2011). It is also necessary to integrate these processes to corporate process landscape. On a technical level it is important to integrate and consolidate data from several sources (e.g., different social networks) and to integrate them with business data. In the area of customer relationship management Faase et al. (2011) deliver a first approach with their Social CRM. In general, companies have to answer the question whether social networks are useful for the company at all. Basically, the management decision on how to act in social networks is critical. Since this risk is internal it is also reversible. Possible indicators are communication problems, process and integration problems as well as ambiguity about useful key figures and their implications.

Compliance

So far, compliance of internal and external legal provisions in social network engagement is thematized poorly in the literature (Hardy and Williams, 2010; Langheinrich and Karjoth, 2010). However, there is no question that this is an important issue: In regulated industries companies are forced to archive all communication with customers (e.g., dialogues on pin walls); nearly 20% of all data are subject to special rules (Hardy and Williams, 2010). Next to the functional specification what data have to be archived there are currently huge problems in realizing this requirements from an IT point of view (Symantec, 2011). All in all, this risk is internal and reversible.

Controlling

The ability to assess company activities in social networks is both an important and unsolved problem of social media in general (Murdough, 2009). A stereotyped application of classical key figures is hardly possible (Fisher, 2009). Thus, companies have to develop individual key figure systems. Basically, they face the problem of a wrong usage of resources (employees, licenses for software etc.) or a misinterpretation of results. To observe all relevant events in social networks it is necessary to use monitoring software like enterprise listening platforms (Fisher, 2009; Fournier and Avery, 2011). However, companies face the problem of the selection and operation of these systems (Symantec, 2011). Sometimes, complex systems like Radian6 can lead to functional overload. The risk of controlling is internal and thus reversible. Possible indicators are the missing ability to make economic statements and assessments regarding to corporate actions in social networks.

RISK MANAGEMENT FRAMEWORK

In this chapter we present our approach for managing corporate risks in social networks. In the first part we present a data reference model that depicts all data objects users deal with in social networks. The second part contains a procedure model, based on the ISO 31000 standard (ISO 31000:2009).

Data Reference Model for Social Networks

The UML class diagram in figure 3 depicts typical data structures and data objects that can be created and managed by users (e.g., employees) in social networks. The model was constructed on the base of a general social networks reference model (Braun and Esswein, 2011) and the results from literature analysis (see chapter "risk catalog"). All data objects can – theoretically – monitored, analyzed and utilized by competitors or attackers; e.g., for espionage or for the preparation of attacks (social engineering). The class "Analysis Object" reflects this fact. For the accessibility of a data object the single privacy setting is essential and every data object can be configured individually. An object can be accessible for every user (public), only accessible for (specific) contacts (private) or it is not accessible for any user (invisible). The class "Analysis Entropy" describes the information content of a data object from an external perspective. For example, the status message "Yeah, we've the new customer: ABC Inc.!" contains a high information content. The class "Analysis Probability" describes the likelihood of an exploitation of a data object and their level of observation. The class "Monitoring Tool" should contain all IT tools for monitoring and analyzing data objects in social networks. All these classes belong to the package "External Analysis" that stands for the external view to all objects. The rest of the classes are self-explanatory. Hence, only a few classes should be explained in detail, like the classes "media file" and "current location data": If users upload images to their profile, also meta information like EXIF data can sent to the webserver. The combination of these data – as well as information from location-based services – with data from other social networks can lead to the current or recent positions of a user (Hill, 2011). Usually, users act in several social networks. The class "expression" describes explicit statements (e.g., comments) of a user that could contain company-internal information. That fact is presented by the attribute "insiderInformation" of the class "Topic". The entire class model is designed as a reference model. It should encourage the understanding of structures in social networks as well as instantiated and customized for company specific purposes. Therefore, reference modeling techniques can be used (Fettke and Loos, 2007).

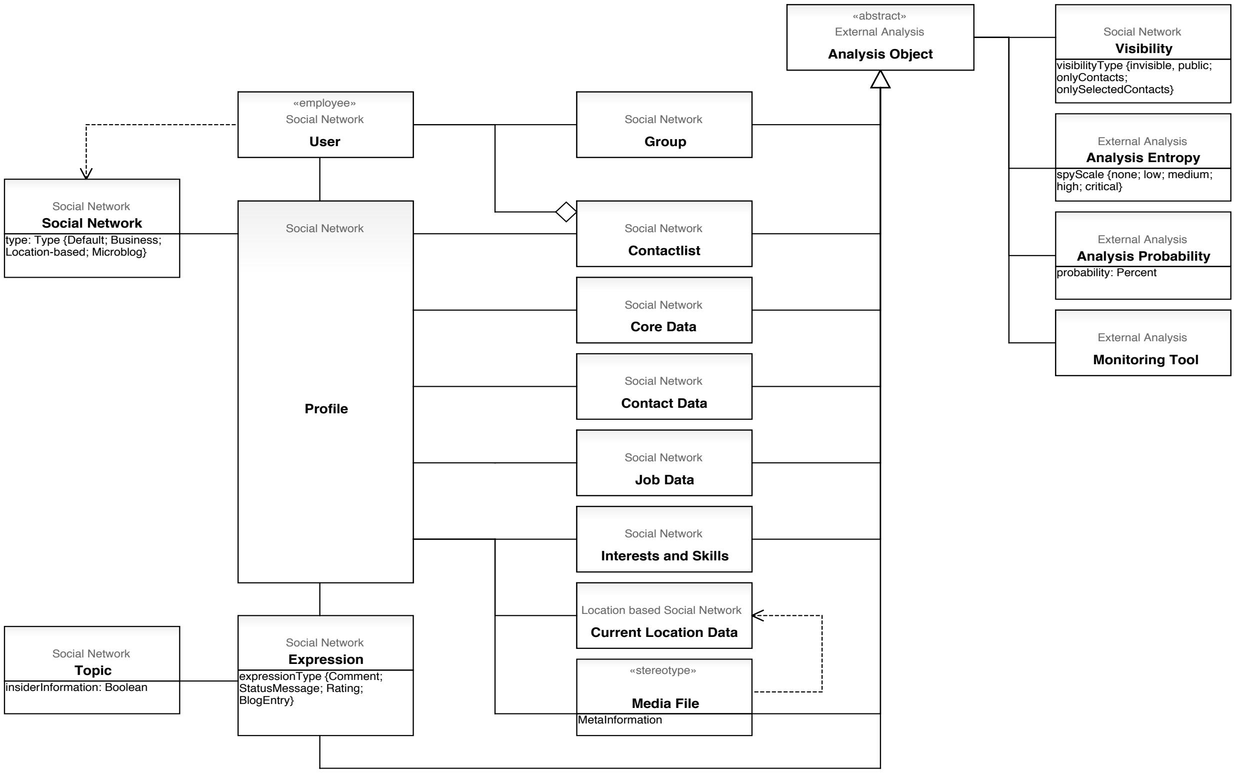

Figure 3: Data reference model for the analysis of user profiles in social network

Framework

To the best of our knowledge, there are no holistic risk management approaches for social networks up to now in literature. Only single risks are discussed separately and some operative counteractions are proposed: For the mitigation of social engineering Newman (2006) proposes the limitation of public accessible information, the sensitization of employees and the implementation of specific technical defensive measures (Newman, 2006). Timm and Perez (2010) emphasize the relevance of high secure passwords. Fournier and Avery (2011) show that offensive reactions to public critic in social networks can mitigate the risk of image damage. Therefore, companies can use direct and public apologies or redemption offers. Sometimes it is also useful to propagate counter statements (Fournier and Avery, 2011). Rudman (2006) proposes a central governance of all social network related activities and emphasizes the necessity of monitoring toolsets (Rudman, 2006). In the area of controlling Bernoff and Li (2009), Fisher (2009) and Murdough (2009) developed first key figures for the assessment. Also in practice there are several ideas: Companies use social media policies, employee trainings and data management to keep confidential information in-house (Symentec, 2011).

In the following section, we present a risk management framework for social networks. According to the ISO 31000 risk management standard we used six main process steps and customized them domain specifically. Furthermore, we used several artifacts and data elements for describing the input and output of each step. The entire framework is for the usage on a management level as explicitly required in ISO 31000. With respect to the limited space of this paper, we do not mention specific IT tools.

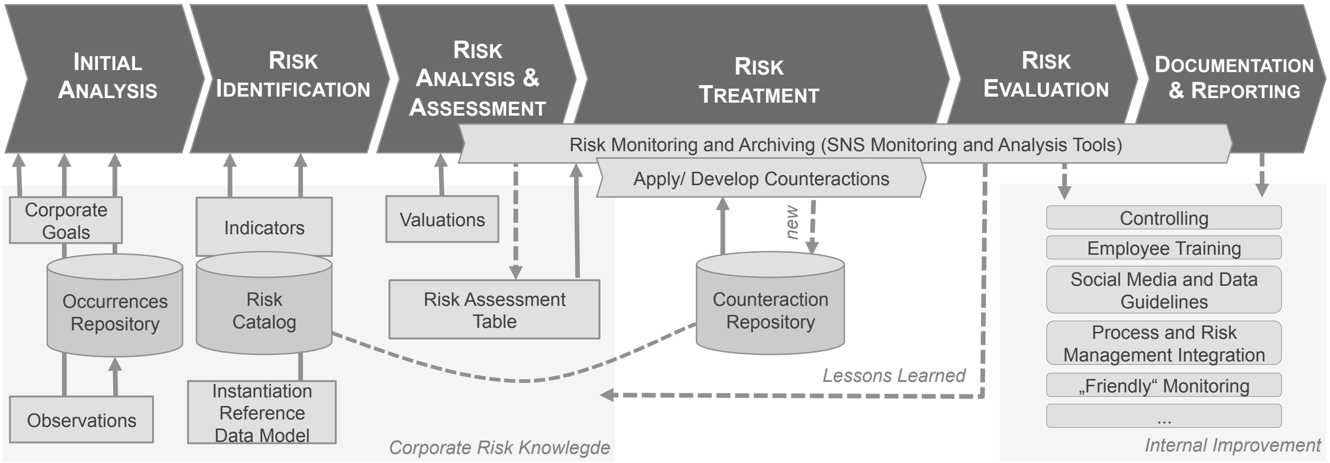

Figure 4: Corporate risk management framework for social networks

The framework is divided into six main steps: Initial analysis, risk identification, risk analysis and assessment, risk treatment, risk evaluation and documentation and reporting. During the initial analysis step the general situation will be analyzed. Therefore, occurred problems, attacks and other relevant events are analyzed. All these information come from the so-called occurrences repository. Entries in this repository come from internal observations as well as from observations of other companies (benchmarking). At the same time it is necessary to consider corporate objectives to identify areas in social networks that are critical to secure. In the next step potential risks are identified based on the risk catalog (see figure 3) that is developed in the previous chapter. For identifying risks it is necessary to describe indicators for them. Also in chapter “risk catalog”, first ideas for indicators were presented.

To get an overview about the threat of exploitation of employee’s user profiles, the social network reference model (see figure 2) should be instantiated by using reference modeling techniques. That helps decision makers to class the risks of the risk catalog to the entire context.

In the next step “risk analysis and assessment”, every single identified risk is assessed regarding its likelihood and the value of damages the occurrence of the risks would cause. Thus, it is possible to create risk rankings. The appraised values for that come from individual assumptions and experiences. The final result of these steps is a risk assessment table. Afterwards, it is necessary to decide whether the analyzed risks are affordable or not. Those risks that cannot be ignored will be treated in the next step “risk treatment”. Thereby, the counteraction repository is used. It gives to every documented risk one or more counteractions and reaction hints. Some of them are presented at the beginning of this chapter. Of course, the noticed actions are not detailed enough and do not deliver counteractions for every risk. Since, it is compulsory to develop and apply company specific counteractions. Basically, this is a fairly long-term iterative process. Inevitable for this is the usage of monitoring and analysis tools that give the chance to built key figures. The results and experiences (e.g., new risks or indicators) of the assessment phase have to be documented as lessons learned in the process phase “risk evaluation”. Also, it is necessary to decide whether the risk could mitigate efficiently or not. Finally, all results have to be documented, reported and communicated. This is an important step to disseminate all results and sensitize all employees. Also internal improvements have to be triggered in this step, for example, regarding to controlling and employee training. Besides, guidelines have to be refined and their compliance has to be proofed. As a measure for that we proclaim the so-called “friendly monitoring” that control publications of employees in social networks and their inherent “potential of exploitation”. Actually, profile pages were audited in that way. Finally, companies have to work on the integration of all process steps and corporate processes as well as the corporate risk management system.

CONCLUSION AND FURTHER RESEARCH

To the best of our knowledge, this paper is the first one dealing explicitly with corporate risks within social networks and it is also the first entire approach regarding to a corporate risk management framework. The main research contribution consists in discovering and systemizing risks affecting social networks from different domains. We could identify several risks, some of their main properties as wells as their interdependencies. Therefore, we worked out a risk catalog based on an extensive literature analysis and can answer to the first research question. Further, we developed a reference data model for social networks to identify critical data objects and their relationships. The reference model can be used and extended in further research to get a better understanding of the entire domain (e.g., object types in social networks and their risk relevance).

Finally, we developed a procedure model to give practitioners (especially managers) a guideline to identify risks and react to them (the second research question). Thereby, the procedure model integrates artifacts from previous chapters like the research catalog (set of all risks) and the instantiated reference model for a specific purpose. In contrast to the hype around the business benefits of social networks, this paper shows some negative issues and should improve the awareness and management of corporate risks in social networks.

Nevertheless, there is some limitation of this research work: The risk catalog has to be extended on the base of further empirical investigations and the framework should be evaluated in case studies (especially in respect of the design science theory; Hevner and Chatterjee, 2010). It is also extremely important to investigate risk indicators and measures for *every* risk. Otherwise it is difficult to operationalize the risks and to control them. Since this is one of the first papers on corporate risks in social networks we are not able to give information on this issue yet. Additionally, there is also no reflection of the occurring costs while applying the framework. Further research should be dedicated to the extension of the risk catalog as well as the development of counteractions and key figures. Also, the conceptualization of corporate actions in social networks should be enhanced to examine the real benefit of social networks to companies.

REFERENCES

1. Barnes, N. G. (2010) The 2010 Inc. 500 Update: Most Blog, Friend And Tweet But Some Industries Still Shun Social Media, http://www.umassd.edu/cmr/studiesandresearch/industriesstillshunsocialmedia/ (2011-12-14).
2. Bernoff, J. and Li, C. (2008) Harnessing the Power oft the Oh-So-Social Web, *MIT Sloan Management Review*, Spring, 36-42.
3. Boyd, D. M. and Ellison, N. B. (2007) Social network sites: Definition, history, and scholarship, *Journal of Computer-Mediated Communication*, 13, 1, article 11.
4. Braun, R. and Esswein, W. (2011) Towards a Reference Architecture Model for Virtual Communities, in Kommers, P. and Isaias, P. (eds.) *Proceedings of the IADIS International Conference Web Based Communities and Social Media*, 47-56.
5. Braun, R. and Esswein, W. (2012) Construction of a Management Framework for Social Networking Sites (in German), in Mattfeld, D. C. and Robra-Bisantz, S. (eds.) *Proceedings of Multikonferenz Wirtschaftsinformatik*, 1885-1896.
6. Cooper, H. M. (1988) Organizing knowledge syntheses: A taxonomy of literature reviews, *Knowledge in Society*, 1, 104-126.
7. Culnan, M. J., McHugh, P. J. and Zubillaga, J. I. (2010) How Large U.S. Companies Can Use Twitter and Other Social Media to Gain Business Value, *MIS Quarterly Executive*, 9, 4, 243-259.
8. Deloitte (2009) Cyber Espionage - The harsh reality of advanced security threats, http://www.deloitte.com/view/en_US/us/Services/audit-enterprise-risk-services/Security-Privacy-Services (2012-01-29).
9. Ermecke, R., Mayrhofer, P. and Wagner, S. (2009) Agents of Diffusion - Insight from a Survey of Facebook Users, in *Proceedings of the 42nd Hawaii International Conference on System Sciences*.
10. Faase, R., Helms, R. and Spruit, M. (2011) Web 2.0 in the CRM domain: defining social CRM, *International Journal of Electronic Customer Relationship Management,* 5, 1, 1-22.
11. Fettke, P. and Loos, P. (2006) Reference Modeling for Business Systems Analysis, Hershey, PA.
12. Fisher, T. (2009) ROI in social media: A look at the arguments, *Journal of Database Marketing & Customer Strategy Management,* 16, 189-195.
13. Fournier, S. and Avery, J. (2011) The uninvited brand, *Business Horizons*, 54, 193-207.
14. Hardy, C. A. and Williams, S. P. (2010) Managing Information Risks and Protecting Information Assets in a Web 2.0 Era, in *BLED 2010 Proceedings*, Paper 25.
15. Hasib, A. (2009) Threats of Online Social Networks, *International Journal of Computer Science and Network Security*, 9, 11.
16. Hevner, A. and Chatterjee, S. (2010) Design Research in Information Systems, Springer, New York.
17. Hill, K. (2011) Thy Spy Who Like Me, http://www.forbes.com/sites/kashmirhill/2011/11/02/the-spy-who-liked-me/ (2012-02-12).
18. Hoffman, K., Zage, D. and Nita-Rotrau, C. (2009) A Survey of Attack and Defense Techniques for Reputation Systems, *ACM Computer Surveys*, 42, 1, Article 1.

19. Huber, M., Mulazzani, M., Weippl, E., Kitzler, G. and Goluch, S. (2011) Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam, *IEEE Internet Computing,* 15, 3, 28-34.
20. Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E. and Pu, C. (2011) Reverse Social Engineering Attacks in Online Social Networks, in *Proceedings of DIMVA'2011*, 55-74.
21. ISO 31000 (2009): ISO 31000: Risk management - Principles and guidelines.
22. Kaplan, A. M. and Haenlein, M. (2010) Users of the world, unite! The challenges and opportunities of Social Media, *Business Horizons*, 53, 1, January-February 2010, 59-68.
23. Lang, J., Spear, M. and Wu, S. E. (2010) Social manipulation of online recommender systems, in *Proceedings of the Second international conference on Social informatics (SocInfo'10)*, 125-139.
24. Langheinrich, M. and Karjoth, G. (2010) Social networking and the risk to companies and institutions, *Information Security Technical Report,* 15, 2, 51-56.
25. Mangold, W. G. and Faulds, D. J. (2009) Social Media: The new hybrid element of the promotion mix, *Business Horizons*, 52, 4, 357-365.
26. Murdough, C. (2009) Social Media Measurement: It's Not Impossible, *Journal Of Interactive Advertising,* 10, 1.
27. Newman, R. C. (2006) Cybercrime, identity theft, and fraud: practicing safe internet - network security threats and vulnerabilities, in *Proceedings of the 3rd annual conference on Information security curriculum development*, 68-78.
28. Pekka, A. (2010) Social media, reputation risk and ambient publicity management. *Strategy & Leadership*, 38, 6, 43-49.
29. Rudman, R. (2010) Framework to identify and manage risks in Web 2.0 applications, *Journal of Business Management,* 4, 13, 3251-3265.
30. Richter, D., Riemer, K. and vom Brocke, J. (2011) Internet Social Networking - Research State of the Art and Implications for Enterprise 2.0, *Business & Information Systems Engineering*, 3, 2, 89-101.
31. Richter, D., Riemer, K., vom Brocke, J. and Große-Böckmann, S. (2009) Internet Social Networking - Distinguishing the Phenomenon from its Manifestations, in *Proceedings of the 17th European Conference on Information Systems (ECIS 2009).*
32. Segrave, J., Carson, C. and Merhout, J. W. (2011) Online Social Networks: An Online Brand Community Framework, in *AMCIS 2011 Proceedings - All Submissions, Paper 249*.
33. Sinclaire, J. K. and Vogus, C. E. (2011) Adoption of social networking sites: an exploratory adaptive structuration perspective for global organizations, *Information Technology and Management*, February 2011, 1-22.
34. Sophos (2009) Sophos Australia Facebook ID probe 2009, http://nakedsecurity.sophos.com/2009/12/06/facebook-id-probe-2009/, (2012-01-15).
35. Strecker, S., Heise, D. and Frank, U. (2010) RiskM: A multi-perspective modeling method for IT risk assessment, *Information systems frontiers*, 13, 4, 595-611.
36. Symantec (2011) Symantec Finds Enterprises That Are Not Preserving Social Networking Business Content Risk Increased Litigation Costs and Company Reputation, http://www.symantec.com/about/ news/release/article.jsp?prid=20110721_01 (2012-02-10).
37. Timm, C. and Perez, R. (2010): Seven Deadliest Social Network Attacks, Syngress, Burlington.
38. Wang, N., Xu, H. and Grossklags, J. (2011) Third-party apps on Facebook: privacy and the illusion of control, in *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology, article 4.*
39. Weir, G. R. S., Toolan, F. and Smeed, D. (2011) The threats of social networking: Old wine in new bottles? *Information security technical report*, 16, 38-43.
40. Willcocks, L., Margetts, H. (1994) Risk assessment and information systems. European Journal of Information Systems, 3, 2, 127-138.
41. vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. and Cleven, A. (2009) Reconstructing the giant: on the importance of rigour in documenting the literature search process, in Proceedings of the 17th European Conference on Information *Systems (ECIS 2009).*