UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Wirtschafts- und Verwaltungsinformatik

FB 4
Informatik

Categorising Social Media Business Risks

Verena Hausmann
Susan P. Williams

Nr. 4/2014

Arbeitsberichte aus dem Fachbereich Informatik

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Lämmel

Kontaktdaten der Verfasser

Verena Hausmann, Susan P. Williams
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
E-Mail: vhausmann@uni-koblenz.de, williams@uni-koblenz.de

Categorising Social Media Business Risks

Susan P. Williams & Verena Hausmann

University of Koblenz-Landau

Abstract. The aim of this paper is to identify and understand the risks and issues companies are experiencing from the business use of social media and to develop a framework for describing and categorising those social media risks. The goal is to contribute to the evolving theorisation of social media risk and to provide a foundation for the further development of social media risk management strategies and processes. The study findings identify thirty risk types organised into five categories (technical, human, content, compliance and reputational). A risk-chain is used to illustrate the complex interrelated, multi-stakeholder nature of these risks and directions for future work are identified.

Keywords: social media, risk, governance, classification, categorisation.

1. Introduction

Social business has gained considerable attention in both the academic and practitioner literatures (McAfee, 2006, Raeth, et al, 2010; Eberspächer & Holtel, 2010; Cortada, Lesser & Korsten, 2012). The growing significance of social business is confirmed by the results of a recent survey of 4,803 business executives and managers (Kane et al, 2014). The survey found that in 2014, 73% of respondents believe social business to be important today; this represents a significant jump from 52% of respondents in 2011 (Kane et al, 2014). Many social business initiatives that began as experimental or pilot projects are now becoming more embedded within organisations, leading to calls for more in-depth studies of its impact (Kane et al, 2014). However, there remains a gap between the interests and focus of academic researchers and the imperatives of practice.

In a previous study we examined the extent to which scholarly research addresses the challenges and imperatives of practice (Williams et al. 2013). Our findings revealed that to date, scholarly research has been largely descriptive and exploratory, focused on social software adoption and use, that is, understanding *what* is being used and *why*. Meanwhile, organisations are focused on understanding *how* these systems can be integrated into their existing infrastructures and processes, in ways that are sustainable and supportable. In particular, attention is being given to the governance, risk and compliance (GRC) aspects of social business; organisations are seeking guidance on the identification and management of social business risks and for social business governance (Williams et al. 2013; Thompson, Hertzberg & Sullivan, 2013; ISACA, 2010; Protiviti, 2014).

In this study we respond to this need for greater understanding of social business risks. We focus attention on social media, the external facing, externally hosted applications such as social networks, blogs, wikis and multimedia content sharing applications hosted on open platforms on the Internet (e.g. Facebook, LinkedIn, foursquare, Twitter) (Schubert & Williams, 2010). Recent EU statistics on the use of social media by enterprises reveal that in 2013, 30% of EU enterprises have already integrated some form of social media into their business (Giannakouris & Smihily, 2013). Of these, social

networks were the most popular form of social media with 28% of enterprises using them to connect to customers by enabling them to create profiles, share feedback, express opinions and create online communities around the enterprises' products and services (Giannakouris & Smihily, 2013).

Our aim is to identify and understand the range and scope of risks and issues associated with the use of social media by organisations by identifying the dimensions of social media risk and developing a framework for categorising social media risks. We use the terms risk and issue purposively to (1) encapsulate both events that could occur and events that have already occurred, and (2) draw on an existing, widely recognised risk vocabulary. We use the Office of Government Commerce (OGC) definitions of risk and issue to align our work with the language in use by practitioners (OGC, 2007). In the OGC Management of Risk (MoR) framework risk and issue are defined as follows:

Risk. An uncertain event or set of events, which should it occur, will have an effect on the achievement of objectives (OGC, 2007).

Issue. A relevant event that has happened, was not planned, and requires management action (OGC, 2007).

Our goal is to contribute to the evolving theorisation of social media risk and provide a foundation for the future development of social media risk management strategies and processes. The paper is structured as follows. We begin by providing an overview of the relevant literature to provide a background and context to social media risk and risk categorisation. This provides the basis for our research objectives, which are briefly discussed in the section on research design. We then present the findings of our study and a discussion about the emerging categorisation and the issues and challenges of categorising social media risks. We end the paper with some concluding remarks about the next steps for research in the area of social media risk.

2. Background: Social Media Risk and Risk Categorisation

In this section we provide an overview of the extant literature on social media risk. This is then followed by a review of the literature and current thinking in the area of risk categorisation.

2.1. Social media risk

Social media risks have been addressed in a number of studies, however often the treatment is indirect or focused on one type of risk such as security risk or reputational risk. For example, Oehri and Teufel (2012) examined the topic of social media from a security viewpoint with the aim of determining the elements to be included in social media guidelines. In doing so they focused attention on the human dimensions of social media management and only indirectly address the identification of social media risks such as damage to reputation, loss of control, social engineering and malware attacks. Other work identifies threats and vulnerabilities associated with social media from a governance and assurance perspective with the aim of developing controls and strategies for addressing such threats (ISACA, 2010) or for formalising the process of managing social media risks (Protiviti, 2014). Abdul Molok et al. (2010) examine threats of information leakage through social media and Aula (2010) extends research on reputational risk (*cf.* Eccless et al, 2007) by considering new exposures to reputational damage arising from social media.

A number of authors have also indirectly addressed social media risk through the topic of social media policies (Krüger, Brockmann & Stieglitz, 2013). Social media policies are an organisational response to the management of social media use. Many of the recommendations in social media policies are direct responses to social media risks. However, few of these studies examine the risks (as catalysts for management action by the development of usage policies) in any detail.

There is also an important and growing literature providing guidance about managing social media risks in specific industries, for example in the finance industry risks relating to information disclosure (FINRA, 2010; 2011) and consumer compliance risk (FFIEC, 2013); and on the risks arising for various professional groups (e.g. lawyers and the judiciary (Lackey & Minta, 2012) and healthcare providers (Terry, 2010; 2011). In these situations the risks are not only business risks, but professional risks that may have a significant and lasting impact on an individual's professional standing (Lackey & Minta, 2012). From this examination of the existing literature it becomes clear that a limitation of current work is that it is fragmented across multiple domains, and that social media risks are often only indirectly addressed. With the exception of the literature on professional risks (Lackey & Minta, 2012; Terry, 2010) the extant literature provides lists of potential risks with little analysis or explanation of those risks and their consequences. Nor does the work go further and examine those risks in order to provide theoretical and practical guidance about how to think about and approach managing them.

2.2. Risk Categorisation

The first stage in any risk management process is risk analysis; an activity that combines risk identification, categorisation and assessment (OGC, 2007). The effectiveness of risk assessment (and ultimately risk management) depends on the completeness of the initial process of cataloguing and classifying risks (OGC, 2007; Morgan et al, 2000).

Categorisation and the intellectual organisation of information about 'things' are as old as humanity itself and the selection of appropriate or meaningful categories is challenging (Bowker & Star, 2000; Svenonius, 2001). The process of risk categorisation is therefore not unproblematic (Morgan et al, 2000; Fischhoff, & Morgan, 2009); decisions must be made about what categories get represented in a classification and what is left out. Categorisation can be approached in different ways. Morgan et al. (drawing on Komatsu, 1992; Medin & Ortony, 1989; and Cvetkovich & Earl, 1985) provide a review and synthesis of different risk categorisation approaches. They identify two broad approaches, *similarity-based* and *explanation-based*. With similarity-based, or essentialist (Cvetkovich & Earle, 1985) classification, an item is added to a category based on shared common properties. *Explanation-based*, or constructivist (Cvetkovich & Earle, 1985) classification (the approach adopted in this study) is based upon human decisions constrained by knowledge of the world and subjective relational categories. Thus, risk classification schemes can vary greatly depending upon the approach and knowledge used in their construction. Further, categorisations (especially those founded on explanation-based approaches) are not fixed but evolve as humans gain deeper and more nuanced understandings of the risks involved.

2.3 Investigating the categorisation of social media risks

The first step in managing risk is the identification of risk categories. However, as discussed above the current literature on social media risks remains fragmented and, to date, there is no comprehensive categorisation of social media risks available. With the exception of a few key studies, for example (ISACA, 2010), risks are treated superficially or secondarily and little explanation is provided about why or how such risks exist. For example, numerous studies cite privacy as a social media risk. Privacy is not itself a risk, however an incident that causes a breach of privacy may be a risk. Therefore a more detailed explanation of the risk itself is required to provide a clearer understanding of what it is about a specific incident that constitutes a risk. It is the goal of this study to begin the process of categorising social media risks and providing greater detail about the nature of those risks through reference to specific cases where that risk became an issue for a business. This work is part of a wider programme of research into the risks and benefits of social business, the aim is to identify risk categories for social media risks and examine the issues involved in the process of their categorisation. The findings will assist us in improving risk categorisation in the future and help us to better plan for the governance management of social media risks.

The following sections outline our research approach and the steps involved in deriving a preliminary categorisation of social media risks.

3. Research approach and research design

The aim of this research is to identify and understand the range and scope of the risks associated with the use of social media by organisations. The research objectives are to:

RO1: identify and explain risks of social media usage by organisations.

RO2: develop a preliminary categorisation of the identified risks

RO3: describe the aspects of social media risk identification and their implications for risk management

The study adopts an iterative, interpretative and qualitative research approach drawing data from the research literature, reported incidents and cases of social media risks/issues. The study is organised into four phases (**Fig. 1**).

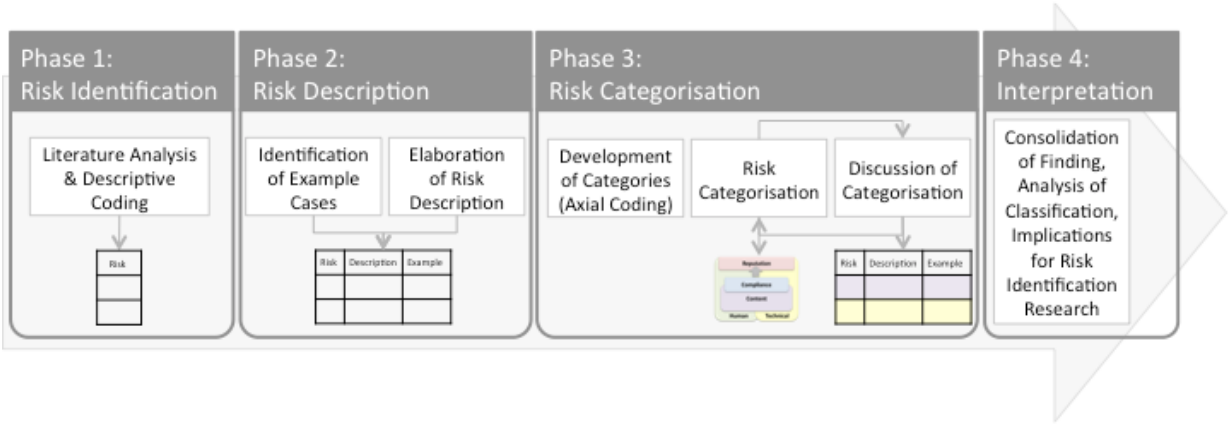

Fig. 1. Research Design

Phases 1 and 2 provide the foundation for addressing RO1, to identify and explain the risks and issues of social media in organisations.

Phase 1: Risk Identification. In the first phase of the study an in-depth analysis of the recent academic and practitioner literatures on social media and risk was conducted with the aim of identifying the catalogue of risks and issues organisations are facing through their use of social media. The literature search was purposefully broad to capture work from multiple disciplinary and professional areas and was based on combinations of the core search terms: social business; social media; E2.0; risk; risk management; risk classification. The primary databases used to identify relevant academic literature were EBSCOhost, ProQuest Central, Web of Science Core Collection, Springerlink and ACM Digital Library. The search was extended to the practitioner literature to identify professional reports, surveys and white papers on the topic of social media risk. Overall more than 200 articles were identified and retrieved, after filtering for relevance the corpus used in the analysis comprised 61 articles. These articles were then analysed using a process of descriptive coding to generate a catalogue of social media risks.

Phase 2: Risk Description. Phase 2 elaborates on and deepens the findings from Phase 1. Our goal here was to identify examples or instances of each of the risks identified through the descriptive coding activity in Phase 1. A limitation of existing research on the topic of social media risks is the lack of risk descriptions and explanations about why a specific event/activity is perceived as a risk.

Thus, the second phase, serves to better understand the risks, to describe and explain them in more depth and to provide evidence of their existence in a real-world setting.

Phase 3: Risk Categorisation. The findings of Phases 1 and 2 provide the input for Phase 3, which addresses RO2: the development of a preliminary risk categorisation. Preliminary categories were identified through a process of axial coding, to identify core groupings/types of risk. Axial coding identifies key categories or groupings of codes and is consistent with the explanation-based/constructivist approach to categorisation discussed above (Morgan et al, 2000). Phase 3 was again an iterative process of analysis, review and refinement of categories. Both the process of categorisation and the findings also led to a number of significant insights for addressing RO3, these are addressed in Phase 4.

Phase 4: Interpretation. In phase four we consolidated our findings and reviewed the implications for social media risk categorisation and risk management more broadly. In particular we focussed on the complex, interlinked and multidimensional nature of social media risks.

4. Findings: Social Media Risk Categorisation

In this section we present the findings of the cataloguing and classification activities from Phases 1, 2 and 3.

4.1. Cataloguing and Describing Social Media Information Risks

The analysis in Phase 1 took the form of descriptive coding (Saldaña, 2009) to create a code catalogue with each code representing a distinctive social media risk.

The coding process was open and all candidate codes were identified and catalogued. Two researchers then reviewed the codes to identify and remove duplicate codes and to harmonise the labelling. 30 distinctive codes (risks) were identified through the descriptive coding process (Table 1)

Table 1: Social Media Risks: Code Catalogue

Abusing authority	Hacking	Loss of reputation
Accessibility	Identity theft	Loss of trust
Astroturfing	Inappropriate/ incorrect content	Malware
Auditability	Information loss	Out of date information
Blurring boundaries	Information overload	Psychological harm
Copyright violations	Language	Reliance on external software (Availability, Ownership, Continuity)
Criticism	Lock out of target group	Responsibility
Disclosure of confidential information	Loss of content control	Spam
Ethical risks	Loss of information quality	Unproductive use of employee's time
Exposure of personal information/ Loss of privacy	Loss of intellectual property	Violation of laws

In Phase 2 a further cycle of analysis identified and added risk descriptions for each of the risks identified in Phase 1. The descriptions are shown in Column 2 of Tables 3-7. We also identified, wherever possible, instances of each risk in practice to provide further evidence of its existence and relevance. For illustrative purposes we have included a subset of these risk instances in Table 2.

Table 2: Cases of Social Media Risks (examples as illustration)

Risk	Example
Hacking SM	CNN's main Facebook account was hacked and statements were posted stating that CNN's reports are all lies (CNN 2014). Burger Kings' Twitter account was hacked and the name changed to McDonald's (Dawson et al, 2009).
Criticism	McDonald's started a PR campaign on Twitter asking to share experience with the hashtag #mcdstories. Users started to post horror stories about the company leading McDonald's to take down the campaign. (Pingler.com, 2013). JP Morgan started a Q&A session on Twitter. It was quickly closed as it was used as a place for commenting by disgruntled customers. (Rawlings, 2013)
Inappropriate language	StubHub posted a twitter message saying "Thank f*** it's Friday! Can't wait to get out of this stubsucking hell hole" (Pingler.com, 2013; StubHub, 2012) Ryanair CEO O'Leary posted a comment saying that a customer is "stupid" (CNBC, 2012).
Astroturfing	The Stillwater Media Group and 18 other companies were detected positively commenting on their own news pretending they were normal customers (Schneiderman, 2013).
Loss of content control	Two employees from Domino's Pizza posted videos showing how they prepared pizza with unsanitary acts. The distribution of the videos could not be stopped (Robinson, 2013).
Blurring boundaries	At Microsoft the person responsible for the official Twitter account accidentally posted something from the Microsoft account that he wanted to post privately (Ritz, 2012).
Violate laws	In the USA 19 companies had to pay penalties between $2500 and nearly $100.000 because they violated the New York Executive Law §63 (12) and the New York General Business Law §349 and 350 by trying to support their own brand with deceptive messages.
Copyright violations	The Content Factory wrote a blog post for a client and used a picture they did not have the rights on. The client was fined $8.000 for copyright violation (DePhillips 2013).

4.2. Developing a preliminary categorisation of social media risk

The main objective of this work is the categorisation of social media risks. As discussed previously a detailed categorisation of social media risks is not yet available. When discussing social media risks a number of authors have begun to group the risks they are describing. For example, Thompson et al. (2013) differentiate between the four categories (1) reputation, (2) disclosure of information, (3) identity theft and (4) legal and compliance violations. Hardy and Williams (2010) outline business and

information risks in six different areas namely: (1) continuity, (2) compliance, (3) auditability, (4) reputational, (5) intellectual property and (6) content risk. These categorisations focus on the consequences of the risk. Ladley (2010) describes business, regulatory and cultural risks, focusing on the locus of the risk. However, for all of these categorisations the categories are not elaborated and there is no comprehensive overview of which risks belong to each category.

Oehri and Teufel (2012) discuss two different categories of risk. The first class of risks emerge from technical aspects; several authors have used this category. Their second risk category is the human dimension, which, they argue should be addressed by rules of conduct. This categorisation focuses on the trigger or cause of the risks. Most risks can be categorised as originating from either a technical or a human cause.

Through our process of axial coding and with the categories already in use by other researchers in mind, we identified five broad risk categories (*human, technical, content, compliance and reputational*) as shown in **Fig. 2**. Tables 3 to 7 also present these five categories and provide examples and descriptions of the risks arising in each category.

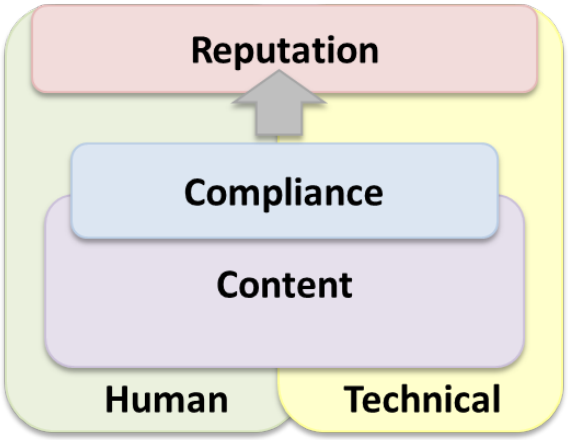

Fig. 2. Preliminary Social Media Risk Categorisation

Human and Technical Risks of Social Media.

Our analysis confirms Oehri and Teifel's (2012) work; human and technical risks provide the basis for discussing almost all social media risks. Some risks are direct consequences of the capabilities of the technology (e.g. hacking, malware, lack of access) (Table 3) or of the behaviour and actions of people (e.g. abuse of authority, blurring of professional and private boundaries, unproductive use of time) (Table 4).

However, the categorisation can be further refined beyond technical and human according to the object of the risk and three additional categories were identified (content, compliance and reputation). Many risks, whilst being human or technical in nature, relate to threats to the social media content itself (content risk), arise from the requirement for compliance with regulations and laws relating to the use and management of social media (compliance) or have an impact on the reputation and standing of the organisation and its employees (reputation).

Table 3: Technical Risks of Social Media

Technical Risks		
Risk	**Description**	**Referenced by**
Hacking	Gaining unauthorized access to social media platforms though e.g. fraud or users giving away/losing their password.	Rudman, 2010, 2011.
Malware	Software to harm computer programs and systems. Examples are viruses, Trojan horses, phishing, screen scraping, keystroke logging, etc. These also occur in social media applications.	Thompson, Hertzberg & Sullivan, 2013; Abdul Molok et al, 2010; Rudman, 2010; Zerfass, et al, 2011.
Spam	Receiving unwanted messages and links through social media and/or using social media accounts to spam.	Joseph, 2012; Nexgate, 2013; Rudman, 2010.
Reliance on external software - Availability - Ownership - Continuity	When using externally hosted software the company cannot easily influence what happens with the software and its content. - The availability of content cannot be guaranteed - It is unclear who owns the content - Backup/access to information might not be provided	Rudman, 2010, 2011; Hardy & Williams, 2010.

Table 4: Human Risks of Social Media

Human Risks		
Risk	**Description**	**Referenced by**
Blurring boundaries	Difficulties clearly separating between professional usage during working hours and private usage in leisure time.	Dutta, 2010; Terry, 2010; Williams & Hardy, 2011.
Psychological harm	Employees might not be comfortable communicating in a public setting and become stressed by negative comments.	Munnukka & Järvi, 2013.
Abusing authority	Through the usage of company social media accounts employees might gain the ability to act with a higher competence/authority than intended.	Rudman, 2011.
Unproductive use of time	Employees might lose time from their core work because of entertainment functions on social media or generally too much use of social media.	Albuquerque & Soares, 2011; Dawson et al, 2009; Dutta, 2010; Rudman, 2010.
Responsibility	In social media it is often unclear who is responsible for sites or comments and therefore who takes care of the company's public representation.	
Ethical risks	These might occur through breach of confidentiality, violating laws, improper behaviour in professional relationships.	Lackey & Minta, 2012.

Content risks of social media.

Social media content itself triggers a wide range of risks (e.g. loss of information, unplanned disclosure of confidential information, out of date or duplicate information) (Table 5). For example, lack of control of the content itself may lead to reposting, copying and loss of intellectual property. The risks with social media are magnified, because once posted, information on social media cannot easily be deleted again and is more rapidly spread to a large number of people (Abdul Molok et al, 2010).

Table 5: Content Risks of Social Media

Content Risks		
Risk	**Description**	**Referenced by**
Information loss	Information can be lost. Reasons are diverse and include loss of intellectual property, disclosure of confidential information, information overload, etc.	Dawson et al, 2009; Krüger, Brockmann & Stieglitz, 2013; Abdul Molok et al, 2010; Oehri & Teufel, 2012; Rudman, 2010.
Information overload	The company might not be able to manage everything if customers write too many messages and comments.	
Loss of intellectual property	Losing information about creations of mind such as employees knowledge, know-how or inventions	Hardy & Williams, 2010; Rudman, 2010.
Disclosure of confidential information	Inadvertently or maliciously publishing content that should be kept secret.	Thompson, Hertzberg & Sullivan, 2013; Oehri & Teufel, 2012; Wilkins, 2012.
Out of date information	Social media is perceived as up-to-date and quickly changing. Customers expect up to date information.	Thompson, Hertzberg & Sullivan, 2013.
Loss of information quality	Messages on social media might be more noisy because statements are often very short, the language used might be inappropriate, etc.	Albuquerque & Soares, 2011; Dutta, 2010.
Loss of content control	It is hard to control content on social media because it can be easily re-used, re-purposed and re-combined and the content rights might be undefined.	Dawson et al, 2009; Williams & Hardy, 2010; ISACA, 2010; Picasso-Vela et al, 2012; Zerfass, et al, 2011.
Inappropriate/ incorrect content	Publishing incorrect information, defamatory statements or offending users though inappropriate language.	Dawson et al, 2009; Joseph, 2012; Nexgate, 2013; Oehri & Teufel, 2012.
Exposure of personal information/ loss of privacy	Personal information originating from or posted into the social profile can lead to unwanted exposure, e.g. job position, date of birth, product preferences or attitudes.	Albuquerque & Soares, 2011; Williams & Hardy, 2010; Thompson, Hertzberg & Sullivan, 2013; Ladley, 2010; Wilkins, 2012.

Compliance risks of social media.

A significant group of risks arise in the area of legal and regulatory compliance (Table 6). The above-mentioned lack of control of social media due to external hosting and restrictive information rights means that organisations risk failing to meet compliance obligations and breaching legal requirements. For example, breaching copyright laws through the reposting of unauthorised content; failing to meet legal discovery requests and records management requirements due to the inability to access information stored on proprietary platforms (e.g. Twitter, Facebook etc.).

Table 6: Compliance Risks of Social Media

Compliance Risks		
Risk	**Description**	**Referenced by**
Copyright violations	Using content that is protected by copyright law and to which the user does not have use rights	Picazo-Vela et al, 2012.
Violation of laws	Failure to comply with various laws/industry regulations e.g. privacy, data protection, legal discovery, records	Götzer et al. 2014; Williams & Hardy, 2010; ISACA, 2010; Abdul Molok et al, 2010.
Identity theft	Taking over the identity of someone else.	Nexgate, 2013; Picazo-Vela et al, 2012.
Auditability	Inability to verify information and provide a clear audit log of activities	Williams & Hardy, 2010.
Accessibility	Inability to set/control access rights according to organisational rules	Ban et al, 2010; Williams & Hardy, 2011.

Table 7: Reputational Risks of Social Media

Reputational Risks		
Risk	**Description**	**Referenced by**
Loss of reputation	People perceiving the company or its products and services less favourably for various reasons, including e.g. criticism or misrepresentation, misleading information.	Aula, 2010.
Criticism	Critical and negative discussion on social media about a company's products, services or the brand in general.	Dawson et al, 2009.
Language	The use of inappropriate language by employees and customers	Terry, 2010.
Astroturfing	Employees of a company posting favourable product reviews posing as a customer.	Nexgate, 2013.
Loss of trust	Customers/reader losing confidence about the company and/or its products and services because of e.g. incorrect and inappropriate information.	Joseph, 2012.

Reputational risks of social media.

Reputational risks are the most visibly discussed risks of using social media in the literature. Many other risks are themselves triggers for reputational risks (see discussion below); however, there is a distinct group of social media risks that directly influence the reputation of a company (Table 7). Examples include: astroturfing (the practice of anonymous promotion/ recommendation), criticism (fairly or unfairly) of a company's products and services, the use of inappropriate language etc.

5. Discussion

Through the process of analysing, cataloguing and categorising social media risks we identified a number of additional dimensions and issues for social media risk management. These are summarised below. We begin with issues arising from the categorisation process itself and conclude with the implications for social media risk management more broadly.

Evolutionary nature of risk classification.

Through our analysis we have been able to provide a preliminary categorisation of social media risks that is more complete than that which has been available to date. However, due to social media's highly interactive, complex and rather uncontrollable nature there are new risks arising from social media all the time [Nexgate, 2013]. Thus, risk categorisation is an on going process, new risks need to be included in the categorisation and existing risks may take on greater or less importance over time.

Risk chains.

Most risks are interrelated; one risk may be the catalyst for or consequence of another risk. Thus *loss of information* for example may result in *disclosure of confidential information* or the *loss of intellectual property*. This study revealed many such examples of these risk chains; **Fig. 3** provides an example of how such a chain of risks occurs and interrelates. The example shows the risk chain started by a hacking attack where external people gain access to the social media account of a company; this triggers a loss of content control and the posting of unauthorised messages. This causes a loss of customer confidence and ultimately manifests in reputational damage, for example through loss of customers, decline in market share etc.

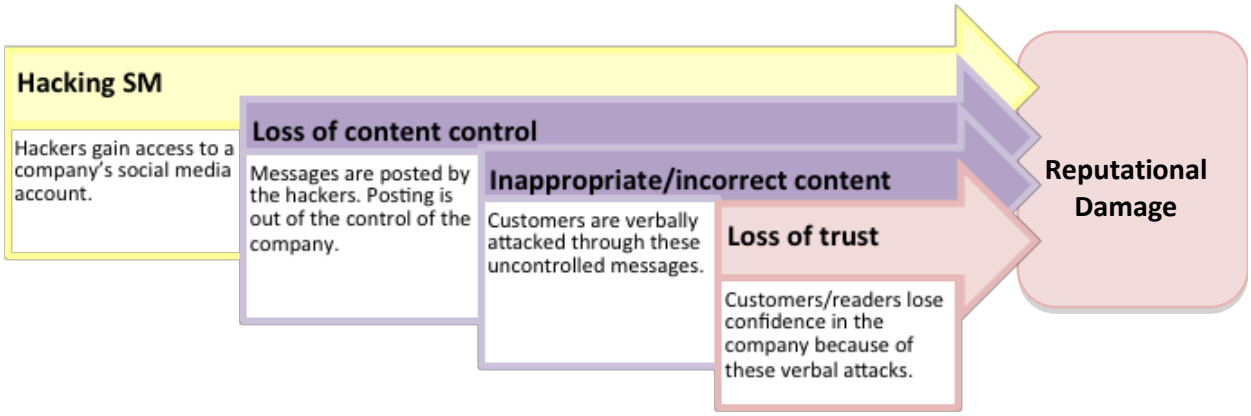

Fig. 3. Risk Chain Example

Risk appetite.

Organisations have differing appetite for social media risks. OGC defines risk appetite as: "An organisation's unique attitude towards risk-taking that, in turn, dictates the amount of risk that is considers acceptable" [OGC 2007]. Our analysis reveals that some organisations have a higher

appetite for social media risk than others. For some companies visibility and exposure, whether favourable or not is acceptable. For example, Michael O'Leary of Ryanair has made a practice of making outrageous comments and handling the negative publicity that arises. Risk appetite is an element of risk assessment and risk ranking and is being addressed in the next stage of our work.

Risk assessment and risk governance processes.

Most of the risks identified above are not unique to social media; however social media bring new versions or places for that risk to manifest itself. Malware for example can originate from browsing normal webpages, e-mails or unsafe external devices, such as promotional USB sticks. However, as such risks now also occur through the usage of social media they need to be addressed when beginning a new social media project and monitored throughout the life of the project. Further, a social media risk assessment should ideally be part of the organisation's wider enterprise risk management strategy. Our social media risk categorisation provides a starting point for the development of a social media risk register, which can be used as a basis for organisations to assess social media risks and to begin to understand the impact they have. Ideally, given the interrelatedness of risks and the existence of risk chains, this social media risk assessment process will be part of, or linked to wider enterprise risk governance.

6. Concluding remarks

In this paper we take a first step in the direction of deepening our understanding of social media risks. A limitation of existing work is (1) it is conducted at a very superficial level, providing lists of potential risks with little analysis or explanation of those risks and (2) the work does not go further and examine those risks in order to provide theoretical and practical guidance about how to think about or deal with them.

Our objectives were to identify the range of social media risks and to provide a more detailed description and categorisation of those risks. This we have achieved, providing a catalogue of thirty risk types organised in five risk categories. Through our analysis we have identified and presented social media risks in a more detailed way. We provide an example of a risk chain to illustrate the complex interrelated, multi-stakeholder nature of those risks. Our study is limited to cataloguing and classifying risks; further work is required to elaborate on this study through industry case studies to examine risk appetite, risk triggers and impact.

References

Abdul Molok, N. et al.: Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats. Australian Information Security Management Conference, Perth Western, Australia. 2010.

Albuquerque, Á., Soares, A.L.: Corporate Social Networking as an Intra-organizational Collaborative Networks Manifestation. In: Camarinha-Matos, L.M. et al. (eds.) Adaptation and Value Creating Collaborative Networks. 11–18 Springer Berlin, 2011.

Aula, P.: Social media, reputation risk and ambient publicity management. Strategy Leadership. 38, 6, 43–49, 2010.

Ban, L.B. et al.: The evolving role of IT managers and CIOs, Findings from the 2010 IBM Global IT Risk Study. IBM 2010.

Bowker, GC. and Star, SL.: Sorting Things Out, Cambridge: The MIT Press. 2000.

CNBC: Ryanair CEO: "Stupid" Passengers Deserve Fees, 07.09.2012, http://www.cnbc.com/id/48942426,

CNN: Some CNN social media accounts hacked - CNN.com, http://edition.cnn.com/2014/01/23/tech/cnn-accounts-hacked/. 2012

Cortada, JW, Lesser, E and Korsten, PJ.: The business of social business: What works and how it's done. Executive Report. IBM Institute for Business Value. 2012.
Cvetkovich, G. and Earle, TC: Classifying Hazardous Events, J.Env.Psych. 5, 5–35, 1985.
Dawson, R. et al.: Implementing Enterprise 2.0. Advanced Human Technologies, San Francisco, 2009.
Deepa, M.: Burger King Twitter Hack and Social Media Security for Teams | Our Social Times - Social Media Agency, Social Media Training, http://oursocialtimes.com/burger-king-twitter-hack-social-media-security-for-teams/, 2013.
DePhillips, K.: $8k in Image Copyright Infringement Penalties: Bloggers, Beware!, http://www.contentfac.com/copyright-infringement-penalties-are-scary/ 2013.
Dutta, S.: Managing Yourself: What's Your Personal Social Media Strategy? Harv. Bus. Rev. 2010.
Eberspächer, J and Holtel, S.: Enterprise 2.0 Berlin: Springer. 2010.
Eccless RG. et al.: Reputation and its risks. Harv. Bus. Rev. 85, 2, 101-114, 2007.
FFIEC: Social Media: Consumer Compliance Risk Management Guidance. 2013.
FINRA: Social Media Web Sites: Guidance on Blogs and Social Networking Web Sites. Regulatory Notice 10-06. 2010.
FINRA: Social Media Websites and the Use of Personal Devices for Business Communications: Regulatory Notice 11-39. 2011.
Fischhoff, B. and Morgan MG.: The Science and Practice of Risk Ranking, Horizons 10, 3, 40-47, 2009.
Giannakouris, K, Smihily, M.: Businesses raise their Internet profile by using social media. Eurostat Statistics in Focus, 28, 2013
Götzer, K. et al.: Dokumenten-Management: Informationen im Unternehmen effizient nutzen. Dpunkt Verlag, 2014.
Hardy, C., Williams, S.: Managing Information Risks and Protecting Information Assets in a Web 2.0 Era. 23rd Bled eConference. pp. 234–247 , Bled, Slovenia, 2010.
ISACA: Social Media: Business Benefits and Security, Governance and Assurance Perspectives. ISACA, 2010.
Joseph, R.: E-Government Meets Social Media: Realities and Risks. IT Prof. 14, 6, 9–15, 2012.
Kane, GC., et al.: Moving Beyond Marketing: Generating Social Business Value Across the Enterprise. MIT Sloan Management Review Report. Reprint Number 56180. 2014.
Komatsu LK.: Recent Views of Conceptual Structure, Psychological Bulletin 112,3, 500–526, 1992.
Krüger, N., Brockmann, T., and Stieglitz, S.: A Framework for Enterprise Social Media Guidelines. Proceedings of the 19th Americas Conference on Information Systems, August 15-17, 2013.
Lackey, M., Minta, J.: Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging. Touro Law Rev. 28, 1, 2012.
Ladley, J.: Making Enterprise Information Management (EIM) Work for Business: A Guide to Understanding Information as an Asset. Elsevier, 2010.
McAfee, AP.: Enterprise 2.0: The Dawn of Emergent Collaboration. MIT Sloan Management Review, 47, 3, 21-28. 2006.
Medin, D. and Ortony, A: Psychological essentialism, in Vosniadou, S. and Ortony A. (eds.) Similarity and Analogical Reasoning, Camb. Univ. Press: New York, 1989.
Morgan, MG.: Categorizing Risks for Risk Ranking, Risk Analysis, 20,1, 49-58, 2000.
Munnukka, J., Järvi, P.: Perceived risks and risk management of social media in an organizational context. Electron. Mark. 1–11, 2013.
Nexgate: Mapping Organizational Roles & Responsibilities for Social Media Risk. 2013.
Oehri, C., Teufel, S.: Social media security culture. Information Security for South Africa (ISSA), 2012. 1–5, 2012.
OGC: Management of risk: guidance for practitioners. Office of Government Commerce; Stationery Office, London 2007.
Picazo-Vela, S. et al.: Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. Gov. Inf. Q. 29, 4, 504–511, 2012.
Pingler.com: Famous Social Media Blunders | General, 30.04.2013, https://pingler.com/blog/famous-social-media-blunders/ 2013.
Protiviti: Assessing the Top Priorities for Internal Audit Functions, 2014 Internal Audit Capabilities and Needs Survey, 2014.
Raeth, P., Urbach, N., Smolnik, S., Butler, BS., König, P.: The Adoption of Web 2.0 in Corporations: A Process Perspective. Proceedings of the Sixteenth Americas Conference on Information Systems, Lima, Peru, August 12-15, 2010.
Rawlings, N.: JPMorgan Cancels Twitter Q&A After an Epic #Fail, http://business.time.com/2013/11/14/jpmorgan-cancels-twitter-qa-after-an-epic-fail/, 2013.

Ritz, E.: Microsoft Accidentally Tweets Anti-Ann Coulter Message to Nearly 300,000 Followers, http://www.theblaze.com/stories/2012/09/23/microsoft-accidentally-tweets-anti-ann-coulter-message-to-nearly-300000-followers/. 2012

Robinson, L.: Yikes! 10 examples of social media mistakes, http://www.thesocialmedialife.com/2013/08/26/10_social_media_mistakes/, 2013.

Rudman, R.J.: Using Control Frameworks to Map Risks in Web 2.0 Applications. J. Account. Manag. Inf. Syst. 10, 495–515. 2011.

Rudman, RJ., Incremental risks in Web 2.0 applications. Elect. Libr. 28, 210–230. 2010.

Saldaña, J.: The Coding Manual for Qualitative Researchers. London: SAGE. 2009.

Schneiderman, ET.: A.G. Schneiderman Announces Agreement With 19 Companies To Stop Writing Fake Online Reviews And Pay More Than $350,000 In Fines, 23.09.2013, http://www.ag.ny.gov/press-release/ag-schneiderman-announces-agreement-19-companies-stop-writing-fake-online-reviews-and 2013.

Schubert, P. and Williams, SP.: The Concept of Social Business: Oxymoron or Sign of a Changing Work Culture? 26th Bled eConference, June 2013, Bled, Slovenia. 2013.

StubHub: We've deleted an unauthorized tweet made from this Twitter handle. We apologize to all of our followers for the inappropriate language used. https://twitter.com/StubHub/statuses/254375470844493824, 2012.

Svenonius, E.: The Intellectual Foundation of Information Organization. Cambridge: The MIT Press, 2001.

Terry, NP: Physicians and patients who "friend" or "tweet": Constructing a legal framework for social networking in ahighly regulated domain. Ind. Law Rev. 43, 285-341, 2010.

Terry, NP.: Fear of Facebook: Private Ordering of Social Media Risks Incurred by Healthcare Providers. Neb. Law Rev. 90, 3, 2012.

Thompson, T., Hertzberg, J., and Sullivan, M.: Social media risks and rewards, http://www.grantthornton.com/~/media/content-page-files/advisory/pdfs/2013/ADV-social-media-survey.ashx 2013.

Wilkins, J.: Social Media Governance: The Policy Part 2, 16.04.2012, http://www.aiim.org/community/blogs/expert/social-media-governance-the-policy-part-2 2012.

Williams, S.P. Hausmann, V., Hardy, C. A., Schubert, P. Enterprise 2.0 Research: Meeting the challenges of practice. In: Proceedings of the 26th International Bled eConference, Bled, Slovenia, June 10-13. 2013

Williams, SP, Hardy, CA.: Information Management Issues and Challenges in an Enterprise 2.0 Era: Imperatives for Action. Proceedings Bled eConference. Bled, Slovenia, 56–67, 2011.

Zerfass, A. et al.: Social Media Governance: Regulatory frameworks as drivers of success in online communications. 14th Annual International Public Relations Research Conference. Miami, Florida, USA, 2011.

Bisher erschienen (seit 2011)

Davor erschienene Arbeitsberichte, siehe

http://www.uni-koblenz-landau.de/koblenz/fb4/forschung/publications/Reports

Arbeitsberichte aus dem Fachbereich Informatik

Verena Hausmann, Susan P. Williams, Categorising Social Media Business, Arbeitsberichte aus dem Fachbereich Informatik 4/2014

Christian Meininger, Dorothée Zerwas, Harald von Korflesch, Matthias Bertram, Entwicklung eines ganzheitlichen Modells der Absorptive Capacity, Arbeitsberichte aus dem Fachbereich Informatik 3/2014

Felix Schwagereit, Thomas Gottron, Steffen Staab, Micro Modelling of User Perception and Generation Processes for Macro Level Predictions in Online Communities, Arbeitsberichte aus dem Fachbereich Informatik 2/2014

Johann Schaible, Thomas Gottron, Ansgar Scherp, Extended Description oft he Survey on Common Strategies of Vocabulary Reuse in Linked Open Data Modelling, Arbeitsberichte aus dem Fachbereich Informatik 1/2014

Ulrich Furbach, Claudia Schon, Sementically Guided Evolution of SHI ABoxes, Arbeitsberichte aus dem Fachbereich Informatik 4/2013

Andreas Kasten, Ansgar Scherp, Iterative Signing of RDF(S) Graphs, Named Graphs, and OWL Graphs: Formalization and Application, Arbeitsberichte aus dem Fachbereich Informatik 3/2013

Thomas Gottron, Johann Schaible, Stefan Scheglmann, Ansgar Scherp, LOVER: Support for Modeling Data Using Linked Open Vocabularies, Arbeitsberichte aus dem Fachbereich Informatik 2/2013

Markus Bender, E-Hyper Tableaux with Distinct Objects Identifiers, Arbeitsberichte aus dem Fachbereich Informatik 1/2013

Kurt Lautenbach, Kerstin Susewind, Probability Propagation Nets and Duality, Arbeitsberichte aus dem Fachbereich Informatik 11/2012

Kurt Lautenbach, Kerstin Susewind, Applying Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 10/2012

Kurt Lautenbach, The Quaternality of Simulation: An Event/Non-Event Approach, Arbeitsberichte aus dem Fachbereich Informatik 9/2012

Horst Kutsch, Matthias Bertram, Harald F.O. von Kortzfleisch, Entwicklung eines Dienstleistungsproduktivitätsmodells (DLPMM) am Beispiel von B2b Software-Customizing, Fachbereich Informatik 8/2012

Rüdiger Grimm, Jean-Noël Colin, Virtual Goods + ODRL 2012, Arbeitsberichte aus dem Fachbereich Informatik 7/2012

Ansgar Scherp, Thomas Gottron, Malte Knauf, Stefan Scheglmann, Explicit and Implicit Schema Information on the Linked Open Data Cloud: Joined Forces or Antagonists? Arbeitsberichte aus dem Fachbereich Informatik 6/2012

Harald von Kortzfleisch, Ilias Mokanis, Dorothée Zerwas, Introducing Entrepreneurial Design Thinking, Arbeitsberichte aus dem Fachbereich Informatik 5/2012

Ansgar Scherp, Daniel Eißing, Carsten Saathoff, Integrating Multimedia Metadata Standarts and Metadata Formats with the Multimedia Metadata Ontology: Method and Examples, Arbeitsberichte aus dem Fachbereich Informatik 4/2012

Martin Surrey,Björn Lilge, Ludwig Paulsen, Marco Wolf, Markus Aldenhövel, Mike Reuthel, Roland Diehl, Integration von CRM-Systemen mit Kollaborations-Systemen am Beispiel von DocHouse und Lotus Quickr, Arbeitsberichte aus dem Fachbereich Informatik 3/2012

Martin Surrey, Roland Diehl, DOCHOUSE: Opportunity Management im Partnerkanal (IBM Lotus Quickr), Arbeitsberichte aus dem Fachbereich Informatik 2/2012

Mark Schneider, Ansgar Scherp, Comparing a Grid-based vs. List-based Approach for Faceted Search of Social Media Data on Mobile Devices, Arbeitsberichte aus dem Fachbereich Informatik 1/2012

Petra Schubert, Femi Adisa, Cloud Computing for Standard ERP Systems: Reference Framework and Research Agenda, Arbeitsberichte aus dem Fachbereich Informatik 16/2011

Oleg V. Kryuchin, Alexander A. Arzamastsev, Klaus G. Troitzsch, Natalia A. Zenkova, Simulating social objects with an artificial network using a computer cluster, Arbeitsberichte aus dem Fachbereich Informatik 15/2011

Oleg V. Kryuchin, Alexander A. Arzamastsev, Klaus G. Troitzsch, Simulating medical objects using an artificial network whose structure is based on adaptive resonance theory, Arbeitsberichte aus dem Fachbereich Informatik 14/2011

Oleg V. Kryuchin, Alexander A. Arzamastsev, Klaus G. Troitzsch, Comparing the efficiency of serial and parallel algorithms for training artificial neural networks using computer clusters, Arbeitsberichte aus dem Fachbereich Informatik, 13/2011

Oleg V. Kryuchin, Alexander A. Arzamastsev, Klaus G. Troitzsch, A parallel algorithm for selecting activation functions of an artificial network, Arbeitsberichte aus dem Fachbereich Informatik 12/2011

Katharina Bräunlich, Rüdiger Grimm, Andreas Kasten, Sven Vowé, Nico Jahn, Der neue Personalausweis zur Authentifizierung von Wählern bei Onlinewahlen, Arbeitsberichte aus dem Fachbereich Informatik 11/2011

Daniel Eißing, Ansgar Scherp, Steffen Staab, Formal Integration of Individual Knowledge Work and Organizational Knowledge Work with the Core Ontology *strukt*, Arbeitsberichte aus dem Fachbereich Informatik 10/2011

Bernhard Reinert, Martin Schumann, Stefan Müller, Combined Non-Linear Pose Estimation from Points and Lines, Arbeitsberichte aus dem Fachbereich Informatik 9/2011

Tina Walber, Ansgar Scherp, Steffen Staab, Towards the Understanding of Image Semantics by Gaze-based Tag-to-Region Assignments, Arbeitsberichte aus dem Fachbereich Informatik 8/2011

Alexander Kleinen, Ansgar Scherp, Steffen Staab, Mobile Facets – Faceted Search and Exploration of Open Social Media Data on a Touchscreen Mobile Phone, Arbeitsberichte aus dem Fachbereich Informatik 7/2011

Anna Lantsberg, Klaus G. Troitzsch, Towards A Methodology of Developing Models of E-Service Quality Assessment in Healthcare, Arbeitsberichte aus dem Fachbereich Informatik 6/2011

Ansgar Scherp, Carsten Saathoff, Thomas Franz, Steffen Staab, Designing Core Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 5/2011

Oleg V. Kryuchin, Alexander A. Arzamastsev, Klaus G. Troitzsch, The prediction of currency exchange rates using artificial neural networks, Arbeitsberichte aus dem Fachbereich Informatik 4/2011

Klaus G. Troitzsch, Anna Lantsberg, Requirements for Health Care Related Websites in Russia: Results from an Analysis of American, British and German Examples, Arbeitsberichte aus dem Fachbereich Informatik 3/2011

Klaus G. Troitzsch, Oleg Kryuchin, Alexander Arzamastsev, A universal simulator based on artificial neural networks for computer clusters, Arbeitsberichte aus dem Fachbereich Informatik 2/2011

Klaus G. Troitzsch, Natalia Zenkova, Alexander Arzamastsev, Development of a technology of designing intelligent information systems for the estimation of social objects, Arbeitsberichte aus dem Fachbereich Informatik 1/2011