Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 121 (2017) 266–273

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2017, 8-10 November 2017, Barcelona, Spain

Categorizing the Business Risks of Social Media

Susan P. Williams*, Verena Hausman

Institute for Information Systems Research, Faculty of Informatics,University of Koblenz-Landau

Abstract

This paper examines the risks arising from the business use of social media and develops a framework for describing and categorizing social media business risks. Using descriptive and axial coding methods an analysis of the academic and professional literatures on social media identified thirty risk types that were grouped into five risk categories. The coding and analysis process revealed further dimensions and issues for social media risk management, including the need to consider the evolutionary nature of risk classification, the existence of risk chains and interdependencies between risks. These are discussed in the context of future work on risk assessment and risk governance.

Peer-review under responsibility of the scientific committee of the CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies.

Keywords: social media; business risk; risk classification; risk chain; categorization; reputational; compliance.

* Corresponding author. Tel.: +49 261 287-2552; fax: +49 261 287 100 2552.
E-mail address: williams@uni-koblenz.de

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies.
10.1016/j.procs.2017.11.037

1. Introduction

In this study we respond to the call for greater understanding of the business risks of social media[1,2,3,4]. Recent EU statistics reveal that in 2016, 45 % of EU-28 enterprises made use of social media; representing a growth of 15% between 2013 and 2016 [5]. Social networks were the most popular form of social media with 42% of EU-28 enterprises using them[5] to connect to customers; enabling them to create profiles, share feedback, express opinions and create online communities around the enterprises' products and services. Our aim in this study is to identify and understand the range and scope of risks associated with the business use of social media by identifying risk types and categories and developing a framework for classifying these risks. Our goal is to contribute to the evolving theorization of social media risk and provide a foundation for the future development of social media risk management strategies and processes.

2. Social Media Risk and Risk Categorization

Social media risks have been addressed in a number of studies, however a limitation of these studies is that the focus is often indirect or gives attention to only one type of risk. For example, Oehri and Teufel (2012)[6] 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 other 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[3] or for formalizing the process of managing social media risks[4]. Abdul Molok et al. (2010)[7] examine threats of information leakage through social media and Aula (2010)[8] extends research on reputational risk[9] by considering new exposures to reputational damage arising from social media. Other work has indirectly addressed social media risks through the topic of social media policies[10]. Social media policies are an organizational response to the management of social media use and many of the recommendations in social media policies are direct responses to social media risks. However, few of these studies examine these risks 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 the risks relating to information disclosure[11,12] and consumer compliance risk[13]. Attention has also been given to the risks arising for various professional groups such as lawyers and the judiciary[14] and healthcare providers[15,16]. From this examination of the existing literature it becomes clear that a significant limitation of current work is that it is fragmented across multiple domains with no comprehensive view of the social media business risk landscape.

2.1. Risk Categorization

The first stage in any risk management process is risk analysis; an activity that combines i) risk identification, ii) categorization and iii) assessment[17]. The effectiveness of risk assessment (and ultimately risk management) depends on the completeness of the initial processes of risk identification and risk categorization[17,18] and it is this activity that forms the main focus of this paper. Categorization and the intellectual organization of information about 'things' are as old as humanity itself and the selection of appropriate or meaningful categories is a challenging activity[19,20]. The process of risk categorization can be problematic[18,21]; decisions must be made about which categories are represented and which are left out of a classification. Categorization can be approached in different ways. Morgan et al. (2000)[18] building on earlier work[22,23,24] provide a review and synthesis of different risk categorization approaches. They identify two broad approaches, *similarity-based* and *explanation-based*. With similarity-based, or essentialist[24] classification, an item is added to a category based on shared common properties. Explanation-based, or constructivist[24] 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, categorizations (especially those founded on explanation-based approaches) are not fixed but evolve as humans gain deeper and more nuanced understandings of the risks involved.

2.2. Investigating the categorization of social media risks

The first step in managing risk is risk analysis. However, as discussed above the current literature on social media risks remains fragmented and, to date, there is no comprehensive categorization of social media risks available. With the exception of a few key studies[3], risks are treated superficially 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 categorizing social media risks and to provide greater detail about the nature of those risks through reference to specific cases (instances) where that risk became an issue for a business. This work is part of our wider program of research into the risks and benefits of social business. The findings will assist us in improving risk categorization in the future and help us to better plan for the governance management of social media risks.

3. Research approach and research design

The aim of this research study is to identify and understand the range and scope of the risks associated with the use of social media by organizations. The research objectives are: to identify and explain risks of social media usage by organizations; to develop a preliminary categorization of the identified risks and to describe the fundamental aspects of social media risk and examine 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 organized into four phases.

Phase 1: Risk Identification comprises an in-depth analysis of the academic and practitioner literatures on social media and risk with the aim of identifying the catalogue of risks organizations face when using 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, Web of Science, 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. Over 200 articles were identified and retrieved, after filtering for relevance the corpus used in the analysis comprised 61 articles. These articles were then analyzed using descriptive coding to generate a catalogue of social media risk types.

Phase 2: Risk Description involves the collection of examples or instances of each of the risk types 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, Phase 2 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 Categorization takes the findings of Phases 1 and 2 as input for the development of a preliminary risk categorization. Preliminary risk categories were identified through a process of axial coding, to determine core groupings of risk types. Axial coding identifies key categories or groupings of codes and is consistent with the explanation-based/constructivist approach to categorization discussed above (Morgan et al, 2000)[18]. Phase 3 was again an iterative process of analysis, review and refinement of categories.

Phase 4: Interpretation consolidates our findings and reviews the implications for social media risk categorization and risk management more broadly.

4. Findings: Social Media Risk Categorization

The analysis in Phase 1 took the form of descriptive coding following Saldaña (2009)[25]. A code catalogue with each code representing a distinctive social media risk type was created. 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 harmonize the labelling. Thirty distinctive codes (risk types) were identified through the descriptive coding process and these are listed in Table 2, column 2. Examples of instances of some of the identified risk types are provided for illustrative purposes and shown in Table 1.

Table 1: Examples of instances of social media risks

Risk type	Instance/Example
Hacking	CNN's main Facebook account was hacked and statements were posted stating that CNN's reports are all lies[26. Burger King's Twitter account was hacked and the name changed to McDonald's[27].
Criticism	McDonald's started a PR campaign on Twitter asking customers to share experience with the hashtag #mcdstories. Users started to post horror stories about the company leading McDonald's having to take down the campaign[28]. JP Morgan started a Q&A session on Twitter. It was quickly closed as it was used as a place for commenting and complaining by disgruntled customers[29].
Language	StubHub posted a twitter message "Thank f*** it's Friday! Can't wait to get out of this stubsucking hell hole"[28,30]. Ryanair CEO O'Leary posted a comment saying that a customer is "stupid"[31].
Astroturfing	The Stillwater Media Group and 18 other companies were detected positively commenting on their own news pretending they were normal customers, a practice known as astroturfing[32]
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[33]
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[34].
Violation of 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.[32]
Copyright violations	The Content Factory wrote a blog post for a client and used a picture they did not have the rights to use. The client was fined $8.000 for copyright violation[35].

4.1. Preliminary categorization of social media business risks

The main objective of this work is the categorization of social media business risks. Previous research has sought to group and categorize such risks. For example, Thompson et al. (2013)[2] differentiate between the four categories (1) reputation, (2) disclosure of information, (3) identity theft and (4) legal and compliance violations. Hardy and Williams (2010)[36] 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 categorizations focus on the *consequences of the risk*. Ladley (2010)[37] describes business, regulatory and cultural risks, focusing on the *locus of the risk*. However, a limitation for all of these categorizations is that the categories are not elaborated and there is no comprehensive overview of which risk types belong to each category.

Oehri and Teufel (2012)[6] also identified and discuss different categories of risk. They identify two categories; the first category emerges from technical aspects and the second risk category is the human dimension, which, they argue should be addressed by rules of conduct. Their categorization focuses on the trigger or *cause of the risks* and they argue most risks can be categorized as originating from either a technical or human causes. Through our process of axial coding and with the categories already in use by other researchers in mind, we identified five broad (and overlapping) risk categories (*human, technical, content, compliance* and *reputational*). The five risk categories and examples and descriptions of the risk types in each category are presented in Table 2.

Table 2: Social Media Risk Categories and exemplars of Risk Types

RISK CATEGORY	RISK TYPES (examples)	DESCRIPTION	REFERENCE SOURCE
Technical	Hacking	Gaining unauthorized access to social media platforms though e.g. fraud or users giving away/losing their password.	38,39
	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.	2,7,38,40
	Spam	Receiving unwanted messages and links through social media and/or using social media accounts to spam.	41,42,48
	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 assured/provided	36,38,39
Human	Blurring boundaries	Difficulties in clearly separating between professional usage during working hours and private usage in leisure time.	16,44,45
	Psychological harm	Employees might not be comfortable communicating in a public setting and become stressed by negative comments posted in social media.	46
	Abusing authority	Through the usage of company social media accounts employees might gain the ability to act with a higher competence/authority than intended/authorized	39
	Unproductive use of employee's time	Employees might lose time from their core work because of entertainment functions on social media or generally too much use of social media.	27,38,43,44
	Lock out of target group	Variations in accessibility to different user groups. Includes, privileging access to certain user groups (e.g. digital natives) and reducing ability of other user groups (e.g. persons with disabilities) to participate.	53,54
	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.	42,52
	Ethical risks	These might occur through breach of confidentiality, violating laws, improper behavior in professional relationships.	14
Content	Information loss	Information can be lost. Reasons are diverse and include loss of intellectual property, disclosure of confidential information, information overload, etc.	6,7,10,27,38
	Information overload	The company might not be able to manage the volumes of information generated by many customers writing large numbers of messages and comments.	29,36, 51
	Loss of intellectual property	Loss of information about creations of mind such as know-how or inventions	36,38
	Disclosure of confidential information	Inadvertently or maliciously publishing content that should be kept secret.	2,6,47
	Out of date information	Social media is perceived as up-to-date and quickly changing and customers expect to find up to date information.	2
	Loss of information quality	Messages on social media might be less comprehensible because statements are often very short, the language used might be inappropriate, etc.	43,44
	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.	3,27,36,40,48
	Inappropriate/ incorrect content	Publishing incorrect information, defamatory statements or offending users through inappropriate language.	6,27,41,42
	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.	2,36,37,43,47

Table 2 (continued): Social Media Risk Categories and exemplars of Risk Types

RISK CATEGORY	**RISK TYPES (examples)**	**DESCRIPTION**	**REFERENCE SOURCE**
Compliance	Copyright violations	Sharing content protected by copyright law, where the user does not have use rights	48
	Violation of laws	Failure to comply with various laws/industry regulations e.g. privacy, data protection, legal discovery, records	3,7,36,49
	Identity theft	Taking over the identity of someone else and posing/transacting as that person.	42,48
	Auditability	Inability to verify information and provide a clear audit log of activities	36
	Accessibility	Inability to set/control access rights according to organizational rules	36,50
Reputational	Loss of reputation	People perceiving the company or its products and services less favorably for various reasons, including e.g. criticism or misrepresentation, misleading information.	8
	Criticism	Critical and negative discussion on social media about a company's products, services or the brand in general.	27
	Language	The use of inappropriate language by employees and customers	16
	Astroturfing	Employees of a company posting favorable product reviews posing as a customer.	42
	Loss of trust	Customers/readers losing confidence about the company and/or its products and services because of e.g. incorrect and/or inappropriate information.	41

Human and technical risks of social media. Our analysis confirms Oehri and Teufel's (2012)[6] 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) or of the behavior and actions of people (e.g. abuse of authority, blurring of professional and private boundaries, unproductive use of time).

However, the categorization can be further refined beyond technical risks and human risks according to the object of the risk and three additional risk 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 risk) or have an impact on the reputation and standing of the organization and its employees (reputation risk).

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). This was by far the largest category of risk types identified in the study. 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[7].

Compliance risks of social media. A significant group of risks arise in the area of legal and regulatory compliance. Lack of control of social media due to external hosting or 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.).

Reputational risks of social media. There is a distinct group of social media risks that directly influence the reputation and perception of a company. Examples of reputational risks include: astroturfing (the practice of anonymous promotion/ recommendation), criticism of a company's products and services, the use of inappropriate language etc.

5. Discussion and concluding remarks

In this paper, we take a first step in the direction of deepening our understanding of the business risks of social media. A limitation of existing work is (1) it provides 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 categorization of those risks. We identified a catalogue of thirty risk types organised in five risk categories and have developed systematic documentation about them. Our analysis also identified a number of additional dimensions and issues for social media risk management. These are summarised below and are the focus of our current work.

Evolutionary nature of risk classification. Due to social media's highly interactive, complex and rather uncontrollable nature new risks are arising all the time[42]. Thus, risk categorization is an ongoing process, new risks need to be included in the categorization and over time existing risks may take on greater or less importance. Thus, more detailed risk profiles are required to assess the impact of specific risk types.

Risk chains. Our analysis identified that most risks are interrelated; one risk may be the catalyst for or consequence of another risk. For example, loss of information may result in disclosure of confidential information or the loss of intellectual property. Our analysis revealed many such examples of these risk chains and analysis of risk chains forms the basis of our current research.

Risk appetite. Organizations have differing appetite for social media risks. OGC defines risk appetite as: "An organization's unique attitude towards risk-taking that, in turn, dictates the amount of risk that is considers acceptable"[17]. Our analysis reveals that some organizations have a higher appetite for social media risk than others. For some companies, visibility and exposure, whether favorable 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 our current 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, such risks now also occur through the usage of social media and they need to be explicitly 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 organization's wider enterprise risk management strategy. Our social media risk categorization provides a starting point for the development of a social media risk register, which can be used as a basis for organizations 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.

References

1. 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.
2. 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.
3. ISACA: Social Media: Business Benefits and Security, Governance and Assurance Perspectives. ISACA, 2010.
4. Protiviti: Assessing the Top Priorities for Internal Audit Functions, 2014 Internal Audit Capabilities and Needs Survey, 2014.
5. Eurostat. Digital economy and society statistics – enterprises. http://epp.eurostat.ec.europa.eu/statisticsexplained/ , 2017.
6. Oehri, C., Teufel, S.: Social media security culture. Information Security for South Africa (ISSA), 2012. 1–5, 2012.
7. 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.
8. Aula, P. Social media, reputation risk and ambient publicity management. Strategy Leadership. 38, 6, 43–49, 2010.
9. Eccless RG. et al. Reputation and its risks. Harv. Bus. Rev. 85, 2, 101-114, 2007.

10. 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.
11. FINRA. Social Media Web Sites: Guidance on Blogs and Social Networking Web Sites. Regulatory Notice 10-06. 2010.
12. FINRA. Social Media Websites and the Use of Personal Devices for Business Communications: Regulatory Notice 11-39. 2011.
13. FFIEC. Social Media: Consumer Compliance Risk Management Guidance. 2013.
14. Lackey, M., Minta, J. Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging. Touro Law Rev. 28, 1, 2012.
15. Terry, NP. Physicians and patients who "friend" or "tweet. Ind. Law Rev. 43, 285-341, 2010.
16. Terry, NP. Fear of Facebook: Private Ordering of Social Media Risks Incurred by Healthcare Providers. Neb. Law Rev. 90, 3, 2012.
17. OGC. Management of risk: guidance for practitioners. Office of Government Commerce; Stationery Office, London 2007.
18. Morgan, MG. Categorizing Risks for Risk Ranking, Risk Analysis, 20,1, 49-58, 2000.
19. Bowker, GC. and Star, SL.: Sorting Things Out, Cambridge: The MIT Press. 2000.
20. Svenonius, E. The Intellectual Foundation of Information Organization. Cambridge: The MIT Press, 2001.
21. Fischhoff, B. and Morgan MG. The Science and Practice of Risk Ranking, Horizons 10, 3, 40-47, 2009.
22. Komatsu LK. Recent Views of Conceptual Structure, Psychological Bulletin 112,3, 500–526, 1992.
23. Medin, D., Ortony, A. Psychological essentialism, in Vosniadou, S. and Ortony A. (eds.) Similarity and Analogical Reasoning, Camb. Univ. Press: New York, 1989.
24. Cvetkovich, G., Earle, TC. Classifying Hazardous Events, J.Env.Psych. 5, 5–35, 1985.
25. Saldaña, J. The Coding Manual for Qualitative Researchers. London: SAGE. 2009.
26. CNN. Some CNN social media accounts hacked - CNN.com, http://edition.cnn.com/2014/01/23/tech/cnn-accounts-hacked/ 2012.
27. Dawson, R. et al.: Implementing Enterprise 2.0. Advanced Human Technologies, San Francisco, 2009.
28. Pingler.com: Famous Social Media Blunders | General, 30.04.2013, https://pingler.com/blog/famous-social-media-blunders/ 2013.
29. 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.
30. 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.
31. CNBC. Ryanair CEO: "Stupid" Passengers Deserve Fees, 07.09.2012, http://www.cnbc.com/id/48942426, 2012.
32. 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.
33. Robinson, L. 10 examples of social media mistakes, http://www.thesocialmedialife.com/2013/08/26/10_social_media_mistakes/, 2013.
34. 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
35. DePhillips, K. $8k in Image Copyright Infringement Penalties: Bloggers, Beware! http://www.contentfac.com/copyright-infringement-penalties-are-scary/ 2013.
36. Hardy, C., Williams, S. Managing Information Risks and Protecting Information Assets in a Web 2.0 Era. 23rd Bled eConference. 234–247, Bled, Slovenia, 2010.
37. Ladley, J. Making Enterprise Information Management (EIM) Work for Business. Elsevier, Burlington MA, 2010.
38. Rudman, RJ. Incremental risks in Web 2.0 applications. Elect. Libr. 28, 210–230. 2010.
39. Rudman, RJ. Using Control Frameworks to Map Risks in Web 2.0 Applications. J. Account. Manag. Inf. Syst. 10, 495–515. 2011.
40. 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.
41. Joseph, R. E-Government Meets Social Media: Realities and Risks. IT Prof. 14, 6, 9–15, 2012.
42. Nexgate. Mapping Organizational Roles & Responsibilities for Social Media Risk. 2013.
43. 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.
44. Dutta, S. Managing Yourself: What's Your Personal Social Media Strategy? Harv. Bus. Rev. 2010.
45. 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.
46. Munnukka, J., Järvi, P. Perceived risks and risk management of social media in an organizational context. Electron. Mark. 1–11, 2013.
47. Wilkins, J.: Social Media Governance: The Policy Part 2, http://www.aiim.org/community/blogs/expert/social-media-governance-the-policy-part-2 2012.
48. 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.
49. Götzer, K. et al. Dokumenten-Management: Informationen im Unternehmen effizient nutzen. Dpunkt Verlag, 2014.
50. Ban, L.B. et al. The evolving role of IT managers and CIOs, Findings from the 2010 IBM Global IT Risk Study. IBM 2010.
51. Hutter, K.et al. The impact of user interactions in social media on brand awareness and purchase intention: the case of MINI on Facebook. Journal of Product & Brand Management, 342–351, 2013.
52. CGOC. Information Governance Benchmark Report in Global 1000 Companies. 2010.
53. Aichner, T., Perkmann, U. Social media: opportunities and risks for regional market research, Int. J. of Market Res., 55(55), 609-10, 2013.
54. Bertot, JC, Jaeger, PT., Hansen, D. The impact of polices on government social media usage: Issues, challenges, and recommendations, Gov. Inf. Q., 29(1), 30-40, 2012.