Social media policy in South Africa

G Mushwana
Department of Auditing
University of Pretoria

H Bezuidenhout
Department of Auditing
University of Pretoria

ABSTRACT

Social media use is a growing trend worldwide. It is viewed as a revolution in electronic communications and an effective business marketing tool. Despite the business benefits, social media is viewed as a risk within organisations. This study examines the perceptions of CAEs (Chief Audit Executives) on the state of development and implementation of social media policies in companies in South Africa.

The study reveals that even though social media is perceived to be a risk, most of the organisations surveyed have not implemented a social media policy. This might be because social media policies are not perceived to be effective, or because social media is classified as a lower priority risk within the organisations. The study reveals that social media is not part of the internal audit universe in most organisations, supporting two perceptions: that it might be viewed as a lesser risk; and that the organisations and internal audit functions have not yet fully understood the nature and potential negative impact social media usage can have on business.

Key words

Social networks; social media policy; internal audit; risk management; workplace

1 INTRODUCTION AND BACKGROUND

Social media is the collective term for those usually internet-based networks of users who interact, share information and communicate with multiple similarly connected users in real time (Cavico, Mujtaba, Muffler & Samuel 2013:26). Social media allow users to construct private or public profiles within a restricted system, identify a list of users with whom they can connect and whose lists of connections they are also enabled to navigate (Boyd & Ellison 2007:211). Social media can also make use of mobile technology systems to access the internet and/or the mobile networks' own interactive sites and applications, in order to achieve interactive dialogue between users (Cilliers 2013:571).

Social media platforms are no longer viewed as merely social platforms: they have become key elements of business strategy (McCarthy & Krishna 2011:88). Social media use has become prevalent around the world with increasing numbers of people accessing the internet to interact on social networking sites (Kim 2012:1). Businesses globally are using social media platforms to cultivate collaboration in the workplace. In addition, this technology is increasingly being used to reach and engage with customers in order to improve customer experience, and to enhance brand image (Kumar, Verma & Pabboju 2013:120). In addition, social media have been proven to uncover intellectual capital amongst employees; to enhance employee motivation and satisfaction; to aid product development and knowledge management, and to facilitate recruitment and skills retention (Kaupins & Park 2010:84). As a vote of confidence in social media's usefulness in the workplace, employers have been encouraging employees to use social media services in order to synergistically reap their full business benefits (Khan, Moore & Weal 2011:1).

Despite the business benefits, in the business environment exposure to social media is also considered to be a business risk (Shullich 2011:3). Using social media, employees can easily publish negative material to millions of people around the world, thereby causing harm to the employer's economic interest, and undermining the assets of brand image and reputation (Cavico *et al* 2013). According to Merrill, Latham, Santalesa and Navetta (2011:7) social media have also created opportunities for abuse, and sometimes bring out the worst in employees who react negatively to challenging situations, often without giving cogent thought to the consequences of their actions. Consequences arise from having contravened the terms and conditions of service of the social network. In addition, increasingly severe consequences arise from copyright infringement, and from having breached privacy, confidentiality and disclosure constraints in employment contracts, to those that arise from publication of defamatory statements, and from indulging in activities which constitute criminal acts; these criminal acts include harassment, identity theft, incitement and the publication of offensive material (Henderson 2011:3).

The reputation of an organisation has long been recognised as an asset, and if this asset is impacted negatively the results can damage the company (Shullich 2011:10). Employees are an important part of corporate reputation management; their views and actions can make or break the business. If their actions do not live up to the published values of the business and the expectations created about the business, the overall reputation of the business can be damaged (Gotsi & Wilson 2001). Employees who disparage fellow employees, management, suppliers and customers, and/or even the company itself, whether intentionally or not, can damage a company's reputation (Merrill *et al* 2011:5). The problem is exacerbated by the fact that the rise of social media use has blurred the lines between work and private time, making it difficult to manage and control access and uploads to these sites (Baker, Buoni, Fee & Vitale 2011:6).

According to the study social networking and reputational risk in the workplace Deloitte LLP 2009 ethics & workplace survey results (2009:4), 74% of employees surveyed stated that it was easy to damage a company's reputation on social media. Employers must therefore accept the changing realities of the workplace environment posed by social media and its associated technologies; they must face it and take action (Thompson & Bluvshtein 2008:284). In the effort to minimize their exposure to liability arising from their employees' abuse of social media sites, employers are advised to adopt a clear, written and detailed social media policy (Recalde 2010:2). This will go a long way to help the employer avoid costly legal problems and other associated risks arising from situations that are otherwise beyond the employer's immediate control (LaPlaca & Winkeller 2010:15). The recommendation is based on the assumption that the use of social media in the workplace has a potential to increase risk (Baker *et al* 2011).

The effectiveness of the policy is dependent on how well it is implemented and the extent to which it is enforced (LaPlaca & Winkeller 2010:16). The policy should be coupled with training and monitoring. Training programs are essential to educate employees on the economic impact of excessive use of social media in the workplace (Herlle & Astray-Caneda 2012:71). All of this provides a useful defence to an employer facing a social media-based civil lawsuit, because it demonstrates the employer's conscious intent and desire to prevent it from happening (Lieber 2011:99). Adopting and enforcing policy on social media is the best available action to minimise liability as a result of social media use by employees (LaPlaca & Winkeller 2010:15).

Currently international laws do not directly address social media usage, according to Kaupins and Park (2010:83). While in South Africa there is also no legislation dealing specifically and explicitly with social media. The laws applicable to social media are obtained in a variety of other statutes and the common law: key statutes include the Constitution of the Republic of South Africa Amendment Act, No. 108 of 1996; Labour Relations Act, No. 66 of 1995; the Code of Good Practice in the Labour Relations Act, No. 68 of 2008, Electronic Communications and Transactions Act, No. 25 of 2002, Regulation of Interception of Communications and Provision of Communication-related Information Act, No. 70 of 2002 and the Trade Marks Act, No. 194 of 1993. In terms of employment law, as discussed *infra*, a number of South Africa court cases held that the dismissal of employees based on their posting of derogatory comments on social media sites were lawful. In South Africa there is evidence of an increase in dismissals of employees who have engaged in defamation of their employers online (Cilliers 2013:575). In addition, there is evidence of an emerging trend to hold companies liable for the actions of their employees on social networking sites (Infolaw 2013). In terms of marketing and advertising, the same laws that apply to traditional media also apply to social media (Deloitte 2013). All of this highlights the reality of the risk social media usage poses.

The increase in the use of social media and technology by employees has resulted in an increase in cases of misuse and ultimately in litigation (Thompson & Bluvshtein 2008:298). In order to balance the benefits and risks associated with employees making use of social media, employers have an obligation to put in place policies and processes that protect their assets and reputations against any form of damage as result of the actions of employees. The prevention of such damage and abuse requires employers to put in place measures that are effective in mitigating social media related risks. This includes the implementation and practical application of a social media policy, training employees on its scope and impact, and enforcing the policy.

Prior research relating to social media in the workplace has focused on its negative impact, specifically the legal, security and ethical implications of social media use for both employers and employees (Baker *et al* 2011; Kim 2012; Kumar & Verma & Pabboju 2013; Cilliers 2013; LaPlaca & Winkeller 2010), as well as on the role of social media policy in the mitigation of social media related risks, and the structure and content of such policies (LaPlaca & Winkeller 2010; Cavico *et al* 2013). Although much has been written about social media policy elsewhere in the world, significantly less has been written about it in South Africa.

The next sections of this article outline the research objective, and provide an overview of internal audit's role in efforts to prevent social media risk. Thereafter, section 4 discusses some examples of social media incidents and cases in South Africa, and this is followed by the results from the research survey component of this study (section 5), discussions of these results (section 6) and the presentation of a final conclusion (section 7).

2 OBJECTIVE OF THE STUDY

This research study was undertaken to establish the current perceptions held by Chief Audit Executives

(CAEs) registered with the Institute of Internal Auditors South Africa (IIA SA) on the implementation of social media policy in South African business entities. The aim of the study was to determine if organisations in South Africa have social media policies, (and if they do, are they fully operational), and if they are perceived to be effective from a CAE's perspective. Specifically, the study sought to answer the following questions:

- What is the perceived level of social media policy implementation in South Africa?
- What is the perceived level of adoption of a social media policy within organisations, and what is the degree to which the policy is implemented?
- What is the perceived risk posed by social media usage in the organisation, from the CAE's and from the organisation's perspectives?
- What is the perceived effectiveness of a social media policy as a means to minimise the risks associated with social media exposure, from a CAE's and from the organisation's perspectives?

3 SOCIAL MEDIA AND THE ROLE OF INTERNAL AUDIT TO PREVENT SOCIAL MEDIA RISK

Social networking sites allow users to create relationships with fellow users based on a distinctive identity they present online. The terms 'social media' and 'social networking' are often used synonymously, even though there is a slight difference in meaning; the former term refers to the way communication is transmitted and the latter refers to functional tools used for information sharing (Cavico *et al* 2013:26). In this paper the two terms will used synonymously and interchangeably.

The use of social media has revolutionised the way people connect and share information (Ployhart, 2014:1). It has become a popular avenue for people to communicate with family, friends and colleagues as it is accessible from anywhere around the world (Kumar, Verma & Pabboju 2013:1). Users can communicate and collaborate with family, friends, acquaintances, professionals, colleagues and others in various ways, making use of audio (via telephonic-type links), written words (via instant messaging), and by posting pictures or videos on their personal pages or communal web spaces, amongst others..

Before the advent of social networking, maintaining a professional network was labour intensive (Bennett, Owers, Pitt & Tucker 2010:140). Traditional social networking used to take place in physical places where people who shared common interests would meet; social interactions would typically occur in pubs, clubs, and parties, and professional or hobby/recreational interactions would be facilitated by seminars, lectures and "chambers of commerce-type briefings". This has been simplified by the introduction of social media, which have created meeting places in the cyberspace that are independent of time and spatial constraints (Kim 2012:12).

According to Boyd and Ellison (2007:214), the first recognizable social media platform was launched in 1997 and was called SixDegrees.com. From 2003 onwards it was followed (and probably eclipsed) by popular social media platforms such as LinkedIn, MySpace, Facebook, and YouTube. In 2012, the top five social media platforms were Facebook, YouTube, Wikipedia, BlogSpot and Twitter, with the numbers of unique visitors estimated as 950 million, 880 million, 410 million, 340 million and 170 million respectively (Cilliers 2013:571). The use of social media technologies is proliferating at an incredible pace worldwide, with millions using the technologies daily (Treem & Leonardi 2012:143). In July 2011 it was estimated that at least one half of the total universe of Facebook users visited the site daily, and that by 2010, some 65 million "tweets" were being sent every day (Cavico *et al* 2013:27).

According to their study entitled South African Social Media Landscape 2014 World Wide Worx (2013) concludes that social media use in South Africa continues to grow, with Facebook leading the trend, growing from 6.8 million users in 2013 to 9.4 million users in 2014. This is followed by Mxit and Twitter currently recording 6 million and 5.5 million users respectively. Also highlighted in the report is the extent to which social media is being used by big corporations for marketing: currently 93% of major brands in South Africa use Facebook.

While social media usage continues to grow locally and internationally because of the power it possesses, the risks inherent in this adoption trend can never be ignored. According to a survey of US executives conducted by Deloitte and Forbes Insights (2013), social media are recognised as posing the fourth-largest risk they will face through 2015. This risk is on the same level as financial risk because it is viewed as an accelerant of other risks. To assess and reduce the risk posed by social media exposure in the organisation, internal audit can play an active role to identify the risk of social media, including making recommendations in order to assist with the mitigation of social media risk. Internal auditors have a broad view of the organisation and they are trained to assess and identify risk; this puts them in a strong position to advise the organisation on the risk of social media (Juergens 2013).

The Institute of Internal Auditors defines internal auditing as:

…"an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes" (IIA 2014; Bailey, Gramling & Ramamoorti 2003:13).

In stating that the internal audit activity should evaluate and contribute to the improvement of risk management, control and governance, the definition recognizes both the assurance and consulting roles performed by internal auditing in risk assessment (Karagiorgos, Drogalas, Michail & Christodoulou 2009:3). Internal auditors have a role to play in assisting management and the audit committee in their risk management and oversight roles (De Zwaan, Stewart & Subramaniam 2011:4). In this case, internal audit should assist the organisation to understand the potential risks related to social media; develop business processes to help mitigate them; monitor compliance with the processes implemented, and assess the effectiveness and efficiency of the implemented controls (Juergens 2013).

According to Deloitte's 2013 social media study, some of the areas where internal audit can play a role to minimise the risk social media exposure poses in the organisation include the following:

- Where failure to manage social media usage can easily spiral out of control and cause risk to the reputation of the organisation, internal audit can assist to identify potential crisis events and to measure the probable impact of these events on the organisation. Internal audit can play a role by testing policies, processes and systems to ensure that the organisation is protected from reputational damage that might arise because of such misuse of social media.

- Internal audit can assist the organisation to conduct a gap assessment or a risk assessment of the current policies and procedures to ensure that they comply with current legislation, and that they are aligned with the organisation's social media landscape.

- Internal audit can provide input when the organisation is defining the data classification methods to prevent loss of information or information leakages through social media.

- Other situations where internal audit could play a role to minimise social media risk include ensuring that proper procedures are followed when outsourcing social media to third party service providers, and by becoming an assessor of social media governance programs.

It is evident that the role of internal audit is a very important component of efforts to ensure that the organisation is protected against risks caused by using social media, and by empowering employees to pursue the social aspects of business. Key audit services that could make an immediate impact in an organisation include a social media risk assessment, a social media governance audit, and a general audit of all social media-related activities. These audit services would ideally be the responsibility of internal audit's IT specialists to perform (Deloitte, 2013).

4 SELECTED EXAMPLES OF SOCIAL MEDIA INCIDENTS IN SOUTH AFRICA

This section discusses pertinent corporate incidents and court cases that highlight the risk posed by the indiscriminate use of social media within organisations. The case law in South Africa pertaining to social media is still developing; recently South Africa has witnessed a number of judgments that are paving the way for the recognition of social media litigation within the judicial system as a discipline in its own right. In addition there have been a number of corporate social media incidents that emphasise the need to formally address the risks posed by social media usage within the organisation.

- In April 2014 First National Bank was involved in a social media incident, when one of its twitter personalities, Rbjacobs, made a joke regarding the whereabouts of "Steve", the FNB radio character. The joke turned bad when, in response to the question: "Where's Steve?" a reply came back saying: "He's somewhere in Afghanistan, putting a bomb under a wheelchair and telling the cripple to run for it!" This insensitive response (ignoring the possibility of malice for now) resulted in the need for extensive damage control by FNB to mitigate the reputational damage done. In addition disciplinary action was taken against the employee (Mybroadband 2014).

- In 2014 telecommunication firm Ericson South Africa fired an employee for posting racist comments on social media (Sowetan 2014). The situation arose after an employee was involved in an accident with a taxi. She took her frustrations to social media to vent. It was found that she had breached the company's business ethics code, resulting in the immediate termination of her contract.

- In 2013 FHM (South African edition) employees were fired for making comments on 'corrective rape' on Facebook (Magcaba 2014). The comments by the two employees were found by the company to be offensive and hurtful, resulting in the dismissal of the employees from the company.

- The South Gauteng High Court in 2013 set a precedent in H v W, when the court granted an interdict preventing a friend from posting about her personal life on social media (SAFLII 2013a). The court found that W's Facebook posts were defamatory and unlawful. This case is important because it adds social media to the list of communication channels that are considered public, thus making their use a de facto placing of views and opinions in the public domain. This ruling adds significantly to the risks posed by the use of social media within an organisation.

- In August 2013 the North Gauteng High Court in Isparta v Richter and another, ordered the author of a post on social media to pay R40 000 in damages for defamation (SAFLII 2013b). In this case the first and second defendants were a married couple. The plaintiff was the ex-wife of the second defendant. The court found that the posts were defamatory of the plaintiff. The court also found that the second defendant was liable because he was tagged in the defamatory posts, and he failed to take any steps to disassociate himself from the posts. When you tag someone on Facebook you are creating a link to their profile. The case is important because it shows that a person who is tagged in a defamatory post (i.e., is directly and specifically associated with a defamatory comment, despite not having personally made that comment), can be found liable for defamation together with the person who made the defamatory post.

- In the case of Sedick and another v Krisray (Polity 2011) that came before the CCMA, the employees, operations manager and bookkeeper of the company were dismissed from work for posting a derogatory statement about the owner and a member of his family on Facebook. The CCMA found that the employees were fairly dismissed.
- In the case of Fredericks v Jo Barkett Fashions (Worklaw 2012), the employee, an administrative assistant, was dismissed for posting derogatory messages on Facebook. It was submitted that the employee had breached the terms of her employment contract, which, despite the absence of a formal company policy on social media usage, the CCMA found to be sufficiently specific to provide grounds to determine that the employee was fairly dismissed.

The incidents and cases listed above illustrate the inherent risk the unmanaged use of social media poses to an organisation. The risk spans a broad spectrum of disciplines: reputational and brand damage on the part of the business, through defamation and hate speech, to vicarious liability and the loss of employment on the part of individuals. Individually and collectively these present a compelling case for organisations in South Africa to adopt preventative and protective measures such as the implementation of a coherent and substantial social media policy.

5 RESEARCH METHODOLOGY

The study was conducted using a web-based survey research tool, SurveyGizmo, to distribute the questionnaire to a database comprising chief audit executives registered with the South African chapter of the Institute of Internal Auditors (IIA SA). The IIA SA newsletter was used to circulate the internet link to the questionnaire, together with a descriptive text of the research. The research instrument took the form of a self-administered, structured questionnaire and covered the following areas:

- organisational information;
- existence of a social media policy in the organisation;
- monitoring and discipline; and
- perceived effectiveness of social media usage policies and procedures.

Fourteen closed ended questions were posed. An effort was made to increase the response rate by minimising the time required to complete the questionnaire to an estimated 5 minutes. These efforts included the use of multiple choice questions, and ensuring that the instructions were clear and the questions were unambiguous and meaningful. The objective of the research was clearly explained in the letter that accompanied the questionnaire and was repeated in the descriptive text which was included in the IIA newsletter (the IIA SA's newsletter is in electronic form and is distributed via email).

The first newsletter containing the link to the questionnaire was sent out on 26 January 2014. Recipients included the 79 CAEs identified in the search of the database of members on the IIA website (IIA SA 2014). The newsletter notified the potential respondents of the research and requested them to complete the questionnaire online. A follow-up reminder was sent on 06 March 2014, and results were received and captured until end of March 2014.

The target was to receive 30 completed responses. A total of 29 completed responses were finally received, a response rate of 35%, which was deemed to be sufficient to justify continuing with the study. When considering the results of the study it should be remembered that the questionnaire was sent to the whole population of CAEs registered with the IIA, which makes detailed statistical analysis redundant.

6 RESULTS AND DISCUSSIONS

The evaluation of the study's responses consisted mainly of frequency and cross tabular analyses. In this section, the main findings of the statistical analyses performed are provided.

6.1 Demographics

The breakdown of respondents according to the size of the organisation which they represent is set out in Table 1. Of the respondents, 41% were from large organisations with in excess of 1500 employees; 24% were from medium sized organisations with between 501 and 1500 employees, and the rest were from organisations with between 101 and 500 employees, and up to 100 employees, the smallest two categories representing "small" organisations. The expectation was that large and medium sized organisations in the private sector would have an internal audit function, as would all public sector organisations. In the private sector, having an internal audit function is a requirement for companies wishing to be listed on some of the stock exchanges, and for banks and other financial institutions with major fiduciary duties. For example adherence to the principles in King III is a listing requirement of the Johannesburg Stock Exchange Limited. In addition, according to SAICA (2009), all organisations should establish an internal audit function which provides assurance regarding the company's governance, risk management and internal controls, as recommended in King III. Public entities and government organisations at both national and provincial levels are required to establish and maintain a system of internal audit according to sections 38(1)(a)(i) and 76(4)(e) of Public Finance Management Act, No. 29 of 1999 (PFMA). In local government and municipal entities, the internal audit function is prescribed in terms of section 165 of the Municipal Finance Management Act, No. 56 of 2003 (MFMA), which also provides for the establishment of the internal audit unit. Provincial and national departments and public entities in South Africa vary greatly in the number of people they employ – from little more than 100 to in excess of 1500, to use the breakdown used in this study.

Table 1: Respondents by size of organisation

Size of organisation	Number of actual responses received	% out of the number of responses received
1 – 100	6	21%
101 – 500	4	14%
501 – 1500 (Medium)	7	24%
1501+ (Large)	12	41%
Total	29	100%

A breakdown of respondents according to organisation type is indicated in Table 2. Slightly more than half are from the private sector and 38% are from the public sector. “Others” draws its respondents from organisations such as non-profit organisations and municipalities.

Table 2: Respondents by organisation type

Organisation type	Number of respondents	% out of the number of responses received
Private Sector	16	55%
Public Entities	5	17%
National Government Department	0	0%
Provincial Government Department	6	21%
Other	2	7%
Total	29	100%

The demographics results are summarised in Table 3 below.

Table 3: Summary demographic results

Organisation type	1 – 100 employees	101 – 500 employees	501 – 1500 employees	1501+ employees	Total
Private Sector	6	1	3	6	16
Public Entities	0	0	1	4	5
National Government Department	0	0	0	0	0
Provincial Government Department	0	3	2	1	6
Other	0	0	1	1	2
Total	6	4	7	12	29

*No response was received from any arm of national government. This, obviously, is a limitation inherent in the study.

6.2 Existence of a social media policy

Implementing a social media policy is regarded as a basic first step to addressing social media related risks within the organisation. The respondents were asked to confirm whether the organisation they represented had a social media policy, or not. It was established during the literature review that social media is a risk, and that it is predicted to become the fourth largest risk, on a par with financial risk, by 2015 (Deloitte & Forbes Insights 2013). In addition, in South Africa companies have already started to experience the negative impact of social media, as illustrated in Section 4 of this study. As a result of this, the expectation was that most organisations would have responded either by putting measures in place such as a social medial policy, or by improving their pre-existing policies, and by making sure the policy was operational. The breakdown of the responses relating to the existence of social media policies is provided in Table 4.

Table 4: Existence of social media policy

Response (Yes/No/Not sure)	Number of respondents	% out of the number of responses received
Yes	10	35%
No	14	48%
Not Sure	5	17%
Total	29	100%

From the survey results it is evident that most organisations do not have a functional social media policy (14). Only 35% indicated that they had implemented a social media policy, and 17% responded “not sure”. A cross tabular analysis was conducted to correlate these results with the size and type of the organisation (see Tables 5 & 6). The cross tabular analysis was important to identify whether there was in fact a correlation between the existence of social media policy and size of the organisation, and secondly, whether there was a correlation between the existence of social media policy and the organisation type. The results were intended to address the perception that large and medium size organisations are more likely to have a social media policy than their smaller sized counterparts. In similar fashion, the second cross tabulation procedure was done to test the perception that private sector organisations were more likely to have a social media policy than were the public sector organisations. It was hypothesised that because private sector organisations have relatively greater capacity than their public sector counterparts, they would be more likely to go the extra mile to protect shareholder and other private interests and reputations.

Table 5: Relationship between the existence of social media policy and organisation size

Response (Yes/No/Not sure)	Total	1 – 100 employees (Small)	101 – 500 employees (Small)	501 – 1500 employees (Medium)	1501+ employees (Large)
Total Responses	29	6	4	7	12
Yes	10	1	0	4	5
No	14	5	1	3	5
Not Sure	5	0	3	0	2

From the results it can be seen that 90% of the organisations with a social media policy are from the large and medium size categories, confirming the perception that the largest organisations are more likely to have a social media policy than their smaller counterparts. The finding takes into consideration that 65% of the total respondents came from medium and large organisation, meaning that 47% of medium and large organisations that responded do have a social media policy.

Table 6 below shows the relationship between the existence of a social media policy and organisation type. The expectation was that the private sector would lead the public sector because the private sector organisations have the capacity and the will to go the extra mile to protect shareholder and other private interests and reputations.

Table 6: The relationship between the existence of a functional social media policy and organisation type

Response (Yes/No/Not sure)	Total	Private Sector	Public Entities	National Government Department	Provincial Government Department	Other
Total Responses	29	16	5	0	6	2
Yes	10	7	3	0	0	0
No	14	7	2	0	3	2
Not Sure	5	2	0	0	3	0

From these results it emerged that 44% (7) of the total private sector respondents have a social media policy. In comparison only 27% (3 out of 11) of the public sector entities (including provincial government departments) have a social media policy. This is despite the publication of social media policy guidelines by the Government Communication and Information System in 2011 (GCIS 2011). The fact that not a single response was received from National Government, which is considered to be the level at which policy is designed and from which it is rolled out, is a further limiting factor when considering the results of this study.

6.3 Determine if social media policy is operational

“Operational” in the sense of this study means that the policy is in existence and has been explained in the organisation (i.e., efforts have been made to ensure all members of staff understand the policy and are committed to its implementation). This analysis was limited to the respondents that have a social media policy (35%) (10), and was undertaken to establish whether the policy was operational or not. The responses are set out in Table 7.

Table 7: Existence of an operational social media policy

Total	Yes	No	Not Sure
10	6	3	1
100%	60.0%	30.0%	10.0%

The fact that 60% of the respondents have an operational social media policy can be an indication that their social media usage policy is not perceived as just another bit of paper, but as a useful measure to manage risk in the organisation. This will be tested further in Section 6.5 when the perceived effectiveness of social media policy is explored according to type of organisation.

6.4 Social media is perceived as risk within the organisation

The risk posed by the use of social media is described in the literature, and is the underlying assumption to this article. In this section the intention was to understand if the organisations surveyed shared the same view that social media usage can be classified as a risk to the organisation. To establish this, the questionnaire was designed to gather the following inputs:

- perception of the organisation regarding social media risk;
- appointment of a risk owner within an organisation, responsible for social media; and
- inclusion of social media in the internal audit universe.

Table 8 below show the results of whether social media is perceived as posing a risk to the organisation. Table 9 identifies the owners of the social media risk within the organisation. Table 10 provides a breakdown of whether or not social media has been identified as part of the risk universe within the organisation. The results are important to achieving an understanding of the low number of organisations with operational social media policies.

Table 8: Social media perceived as posing a risk to the organisation

Response (Yes/No/Not Sure)	Number of respondents	% out of the number of responses received
Yes	21	72%
No	6	21%
Not Sure	2	7%
Total	29	100%

From the results it is evident that social media is perceived to pose a risk to the organisation (72%). However, this has not been translated into the adoption of a social media policy by some of the organisations, and the question is: why? Two other questions posed in this section of the questionnaire were intended to establish who within an organisation owns the risk posed by social media, and whether social media forms part of the internal audit risk universe. The responses are contained in Tables 9 and 10.

Table 9: Owner of social media risk within the organisation

Ownership	Number of respondents	% of respondents
Board of Directors	1	4%
Chief Executive Officer	3	10%
Chief Financial Officer	1	4%
Chief Risk Officer	3	10%
Chief Information Officer	9	31%
Legal Adviser	0	0%
Human Resource Executive	2	7%
Chief Security Officer	0	0%
Chief Operations Officer	0	0%
Audit Executive	0	0%
Other	10	34%
Total	29	100%

From the results we have established that the owner of social media risk is most likely to be the Chief Information Officer (31%). This might be because social media usage and access is viewed as a technology issue; the responsibility for auditing social media risk exposure would then in all probability be that of IT internal audit. The “others” account for 34% of the total results and this might be the reason why social media policies are not designed and implemented by most organisations. These “others” might not have included social media risks as part of the risk universe of the organisation. Based on the results it seems that there is a lack of understanding/ analysis within business about how to handle social media risk.

In terms of risk ownership there are a number of grey areas and these are highlighted in the results. The risk owner should be someone responsible for ensuring that the risk is managed and monitored. The difficulty is that social media usage (and abuse) occurs across the entire spectrum of employees and stakeholders: for example human resource (HR) uses social media for talent searches, and marketing uses it to market the business, for brand development and for communication with customers. In addition, social media could be used by employees to collaborate with each other, and to share business-related information, and by management as a communication tool. Thus, the IT department seems to be the better choice to manage and monitor usage and risk, because technology is the underlying common factor to all usage, and IT is the technology gatekeeper in the organisation. However it also seems at times that IT has no control over the process of creating social media accounts, nor is it able to effectively manage how it is utilised in the organisation. Thus, despite its current shortcomings, IT remains the default choice in the organisation due to the technological nature of social media and this is supported by the results.

Table 10: Social media part of the risk universe

Response (Yes/No/Not Sure)	Number of respondents	% of respondents
Yes	7	24%
No	17	59%
Not Sure	5	17%
Total	29	100%

For the majority of the respondents (59%) social media was not part of the internal audit universe. This might be the reason why so few organisations have achieved the effective implementation of a social media policy. This omission might in turn be the result of a lack of clarity regarding ownership of the risk posed by social media (see Table 9). A further possible explanation is that for these South African respondents social media risk is not considered to be of sufficiently high a priority to justify expenditure of resources to develop and implement the policies. If this is the case, this result is at odds with that of Deloitte & Forbes Insights (2013) which found that social media is perceived to pose a serious risk to business entities. A further possible justification for the apparently low risk status of social media in South Africa might be that social media policy is not perceived to be an effective agent of risk reduction. However, that should still not exclude social media from being part of the internal audit universe, unless internal audit has not yet fully grasped the situation regarding social media usage, and its risks. The responses to the question to determine whether social media policy is perceived to be effective are provided in the next section (Table 11).

6.5 Perceived effectiveness of a social media policy to prevent social media related risks

From the result, slightly fewer than half of the CAEs perceived the presence of a social media policy to be effective within an organisation. This might be the fundamental reason for the low number of organisations that have implemented social medial policies. Results in Table 8 show that 72% of the organisations perceive social media to be a risk, while according to results presented in Table 10, 48.3% of the CAEs do not perceive the presence of a social media policy to be an effective mitigation agent for social media related risks. A question was asked whether social media policy is perceived to be an effective measure to address social media related risks within the organisation: the responses are provided in Table 12.

Table 11: CAE perceptions of effectiveness of social media policy to address related risks

Response (Yes/No/Not Sure)	Number of respondents	% out of the number of responses received
Yes	14	48.3%
No	12	41.4%
Not sure	3	10.3%
Total	29	100%

Table 12: Perceived effectiveness of policy on social media to address risks posed to organisation by the organisation

Response (Yes/No/Not Sure)	Number of respondents	% of respondents
Yes	8	27.6%
No	12	41.4%
Not sure	9	31.0%
Total	29	100%

The results in Table 12 support the view that the low number of entities that have social media policies might be so because the presence of a social media policy is not perceived to be an effective tool to address social media related risks. It can also be said that social media exposure is not considered to pose a high priority risk, based on the results in Table 10. This view might be due to the lack of knowledge about social media amongst responding CAEs, and because their internal audit functions have also not yet fully understood the phenomenon to be able to address social media risk.

7 CONCLUSION

- More than half of the respondents were from the private sector, and 38% from the public sector. Of the total respondents 41% represented “large” organisations, and 24% represented “medium” sized organisations.

- Most organisations who participated in the study do not have a social medial policy; only 35% of the total number of respondents have a social media policy. 90% of the organisations with a social media policy are from large and medium size organisation, confirming the expectation that organisations in this category are most likely to have a social media policy, given that they are most likely to have well-established and resourced internal audit functions. 44% of the private sector respondents have a social media policy, while only 27% of the public sector entities have such policies in place. Of the organisations that have social media policies, only 60% have an operational social media policy. For this group social media policy is viewed as substantially more than a “check box compliance” document.

- 72% of the organisations perceive social media to be a risk, but surprisingly, this has not been translated into the implementation of a social media policy. 59% of the respondents indicated that social media exposure was not part of the internal audit universe, and fewer than half of the CAEs perceived social media policy to be an effective risk control mechanism within the organisation. This might be the reason why the implementation of a social media policy is lower than the figure for the presence of such a document in the entity. In addition there is an obvious lack of clarity regarding the ownership of the risk posed to an organisation by social media usage. With regard to the identity of the risk owner, the CAEs’ responses are spread across a significant spectrum of stakeholders; however, the median preference for risk ownership appears to be the Chief Information Officer.

- Social media use is a growing trend amongst employers and employees worldwide. Despite the obvious and acknowledged business benefits, social media is also viewed as a business risk. The impact of a failure to acknowledge the risks associated with social media exposure has already been felt by some South African companies and their employees.

- Social media policy is regarded as the first and most basic step needed to mitigate social media risk within the organisation.

- The study revealed that social media is perceived to be a risk, but the fact that the majority of organisations surveyed have not implemented a social media policy was not expected. This absence of policies guiding social media usage might have arisen because social media policy is perceived to be ineffective in addressing social media risk. The absence of policies might also be because it is classified as a lesser priority risk within the organisation. The study also revealed that social media risk was not part of the internal audit universe in most organisations, supporting the perceptions that it might be viewed as a lesser risk or the internal audit functions have not yet fully understood the nature of the risks posed by uncontrolled social media usage.

- It seems that there is a lack of understanding/ analysis within business about how to handle social media risk; this can be established from grey areas regarding the issue of ownership. The issue of social media ownership can form part of future research coming out of this study.

REFERENCES

Bailey, A.D., Gramling, A.A. & Ramamoorti, S. 2003. *Research opportunities in internal auditing.* Institute of Internal Auditors Research Foundation. Altamonte Springs, Florida.

Baker, D., Buoni, N., Fee, M. & Vitale, C. 2011. *Social Networking and Its Effects on Companies and Their Employees*. Neumann University, Aston.

Bennett, J., Owers, M., Pitt, M. & Tucker, M. 2010. Workplace impact of social networking. *Property Management*, 28(3):138-148.

Boyd, D.M. & Ellison, N.B. 2007. Social Network Sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1):210-230.

Cavico, F.J., Mujtaba, B.G., Muffler, S.C. & Samuel, M. 2013. Social Media and Employment-At-Will: Tort Law and Practical Considerations for Employees, Managers and Organizations. *New Media and Mass Communication*, (11):25-41.

Cilliers, F. 2013. The Role and effect of Social Media in the Workplace. *Northern Kentucky Law Review,* 40(3): 567-592.

De Zwaan, L., Stewart, J. & Subramaniam, N. 2011. Internal audit involvement in enterprise risk management. *Emerald Group Publishing Limited*, 26(7):586-604.

Deloitte. 2013. *The digital grapevine Social media and the role of Internal Audit*. Deloitte. United States.

Deloitte & Forbes Insight. 2013. *Aftershock Adjusting to the new World of Risk Management*. Deloitte United States.

Deloitte. 2009. *Social networking and reputational risk in the workplace Deloitte LLP 2009 Ethics & Workplace Survey results*. Deloitte United States.

Gotsi, M. & Wilson, A.M. 2001. Corporate reputation: seeking a definition. *MCB UP Ltd*, 6(1):24-30.

Government Communication and Information System. 2011. *Social Media Guidelines*. South African, Pretoria.

Henderson, M., De Zwart, M., Lindsay, D. & Phillips, M. 2011. *Will u friend me?: Legal risks and social Networking sites*. Victoria Law Foundation. Victoria, Australia.

Herlle, M. & Astray-Caneda, V. 2012. *The impact of social media in the workplace*. Florida International University. Florida.

IIA SA. 2014. The IIA SA member search database. IIA SA. [Online]. http://www.iiasa.org.za/search/newsearch.asp?bst=audit+executive&cdlGroupID=&txt_country=&txt_statelist=&txt_state=&ERR_LS_20140329_070512_31109=txt_state%7CLocation%7C20%7C0%7C%7C0. (Accessed: 23 April 2014).

IIA. 2014. About internal audit. IIA Global. [Online]. https://global.theiia.org/about/about-internal-auditing/pages/about-internal-auditing.aspx. (Accessed: 04 July 2014).

Infolaw. 2013. Misuse of social media by employees. *Infolaw.* [Online]. http://www.infolaw.co.uk/newsletter/2013/09/misuse-of-social-media-by-employees/. (Accessed: 11 June 2014).

Juergens, M. 2013. *Social media risks create an expanded role for internal audit*. Deloitte United States.

Karagiorgos, T., Drogalas, G., Michail, P. & Christodoulou, P. 2009. *Internal auditing as an effective tool for efficient risk management*. University of Macedonia. Macedonia.

Kaupins, G. & Park, S. 2010. Legal and ethical implications of corporate social networks. *Employee Responsibilities and Rights Journal*, 23(2):83-99.

Khan, S., Moore, R. & Weal, M. 2011. Social media on the job: an exploration of the potential legal consequences of employees social media activities during the course of employment. WebSci Conference 2011: 1-8.

Kim, H.J. 2012. Online social media networking and assessing its security risks. *International Journal of Security and Its Applications*, 6(3):11-18.

Kumar, D.V., Varma, P.S.S. & Pabboju, S.S. 2013. Security issues in social networking. *International Journal of Scientific and Research Publications (IJSRP)*,13(6):120-124.

LaPlaca, D.R. & Winkeller, N. 2010. Legal implications of the use of social media: minimizing the legal risks for employers and employees. *Journal of Business & Technology Law Proxy*, 5:1-19.

Lieber, L.D. 2011. Social media in the workplace-proactive protections for employers. *Employment relations today*, 38(3):93-101.

FHM. 2013. FHM 'rape comment' employees fired. *Homepage of ENCA*. [Online]. http://www.enca.com/south-africa/fhm-employees-fired. (Accessed: 29 April 2014).

McCarthy, M.P. & Krishna, S. 2011. *Social media: time for a governance framework*. NACD Directorship.

Merrill, T., Latham, K., Santalesa, R. & Navetta, D. 2011. *Social media: the business benefits may be enormous, but can the risks - reputational, legal, operational be mitigated.* ACE Limited. Zurich.

Mybroadband. 2014. FNB Twitter “joke” causes online storm. Mybroadband. [Online]. http://mybroadband.co.za/news/internet/100964-fnb-twitter-joke-goes-very-wrong.html. (Accessed: 29 April 2014).

Polity. 2011. What you say on Facebook can get you fired. *Polity*. [Online]. http://www.polity.org.za/article/what-you-say-on-facebook-can-get-you-fired-2011-11-07. (Accessed: 11 June 2014).

Ployhart, R.E. *Social Media in the Workplace: Issue s and Strategic Questions.* SHRM Foundation. Alexandria, Virginia.

Recalde, M.E. 2010. *The Need For a Social Media Policy*. Sheehan Phinney Bass+ Green PA: Boston.

SAICA. 2009. *Report on Governance Principles for South Africa*. SAICA. South Africa.

Shullich, R. 2011.*Risk Assessment of Social Media*. SANS Institute. Swansea, UK.

South African. 2003. Municipal Finance Management Act, No 56 of 2003. Government Gazette 464(26019). [Online]. http://mfma.treasury.gov.za/MFMA/Legislation/Local%20Government%20-%20Municipal% 20Finance%20Management%20Act/Municipal%20Finance%20Management%20Act%20%28No.%2056%20of%202003%29.pdf. (Accessed: 28 April 2014).

South African.1999. Public Finance Management Act, No1 of 199. Government Gazette 406(19978). [Online]. http://www.treasury.gov.za/legislation/PFMA/act.pdf. (Accessed: 28 April 2014).

Sowetan. 2014. Ericsson employee fired after racist rant on Facebook. Sowetan. [Online]. http://www.sowetanlive.co.za/news/2014/04/09/ericsson-employee-fired-after-racist-rant-on-facebook?filter=all_comments. (Accessed: 29 April 2014).

Thompson, T.M. & Bluvshtein, N.E. 2008. Where technology and the workplace collide - an analysis of the intersection between employment law and workplace technology. *Privacy & Data Security Law Journal*, 3(4): 283-299.

Treem, J.W. & Leonardi, P.M. 2012. Social media use in organizations exploring the affordances of visibility, editability, persistence, and association. *Social Science Research Network*, 36:143-189.

The Southern African Legal Information Institute (SAFLII).*2013a.* H v W (12/10142) [2013] ZAGPJHC 1; 2013 (2) SA 530 (GSJ); 2013 (5) BCLR 554 (GSJ); [2013] 2 All SA 218 (GSJ) (30 January 2013)*. SAFLII.* [Online]. http://www.saflii.org/za/cases/ZAGPJHC/2013/1.html. (Accessed: 11 June 2014).

The Southern African Legal Information Institute (SAFLII).*2013b* Isparta v Richter and Another (22452/12) [2013] ZAGPPHC 243; 2013 (6) SA 529 (GNP) (4 September 2013).*SAFLII* [Online]. http://www.saflii.org/za/cases/ZAGPPHC/2013/243.html. (Accessed: 11 June 2014).

Worklaw. 2012. Fredericks / Jo Barkett Fashions [2012] 1 BALR 28 (CCMA). *Worklaw.* [Online]. http://www.worklaw.co.za/SearchDirectory/CaseLaw/F31-fj.asp. (Accessed: 11 June 2014).

World Wide Worx. 2013. *South African Social Media Landscape 2014*. World Wide Worx. South Africa.