Managing Risk in a Social Media-Driven Society

By Tom Andreesen and Cal Slemp, Protiviti

Is social media just a fad? Or is it the biggest shift in the way business is done since the advent of the Internet?

The conclusion is resoundingly clear: social media is here to stay, and it is rapidly altering every aspect of corporate operations from hiring to training, marketing to sales, and yes, auditing and risk management too. The purpose of this article is to discuss the current state of the social media environment, how its use continues to evolve in the workplace and what risks it presents to companies. We will especially look at how the expanded usage of social media requires auditors to begin evaluating social media risks.

Defining Social Media

First, let's clarify what social media is. Social media includes corporate blogs, online video posting sites such as YouTube, social networks like Facebook, microblogging tools such as Twitter, and photo-sharing websites like Flickr. All these differ from other communication methods companies use to reach out to the public and their employees (such as print or TV) in that people use social media to talk back to the company and amongst themselves. Moreover, the participants have the expectation that there will be a dialogue that ensues and a viral distribution of the content.

The Rise of Social Media in the Workplace

Social media tools have been around for less than a decade, yet their penetration among the public and in the workplace is rampant and widespread. Morgan Stanley Research from 2010 showed that Facebook had roughly 470 million unique users; Twitter, 74 million; and MySpace, 120 million. The use of social media has equally expanded in business. In early 2010, 79 percent of the Fortune Global 100 companies were employing at least one social media platform; specifically, 65 percent had active Twitter accounts, 54 percent had Facebook fan pages, 50 percent had YouTube video channels, and 33 percent had corporate blogs.

Benefits of Social Media

Companies are discovering a wide range of benefits to incorporating social media into their communication toolbox. These advantages include:

- enabling companies to communicate with existing clients in new ways, such as through the use of blogs, videos and fan pages.
- helping companies find, attract and reach out to new customers and build new opportunities.
- potentially increasing customer loyalty as a dialogue is created.
- diversifying the channels they can use for marketing and promoting new products or newly developed service lines.
- helping to recruit today's millennial generation of tech-savvy employees who want to work at companies that value social media.
- promoting team-building, collaboration and camaraderie amongst employees.
- potentially increasing productivity, creativity and innovation through greater opportunities to exchange ideas and dialogue.
- helping solidify and strengthen the company's efforts at distinctively branding its products in the public eye.

Case Examples of the Value of Social Media

Here are a few instances of the reputational, PR and sales benefits companies have reaped from using social media in their marketing efforts to reach out to customers:

- Ford Fiesta used social media in its U.S. launch to generate mass reach, build relationships with key targets and achieve reservations-to-conversion sales rates that were 10 times higher than expected. On YouTube, Ford Fiesta generated 6,200,000 views with 132,000 consumers raising their hand for more information. On FlickR, there were 750,000 views; of which 83 percent were new to Ford. On Twitter, there were 40,000,000 impressions, of which 30 percent were car buyers under 25.
- When GM launched "FastLane," one of the first blogs personally written by senior executives, it received the equivalent customer feedback that would have cost the company $180,000/year in traditional focus group research, not to mention the enormous goodwill generated in having the company's executives respond directly to consumers.
- H&R Block used Facebook and Twitter to provide immediate access to a tax professional for Q&A in its "Get It Right" social media campaign. The effort secured 1,500,000 unique visitors and answered 1,000,000 questions for a 15 percent lift in business versus the prior year when the campaign did not exist.
- An e-commerce teen clothing store for girls created a "community" section on the website for users to design their own clothes, publish for reviews, and leverage "wisdom of the crowd." They saw a 21 percent increase in revenue driven by a 10 percent increase in sales and a 10 percent increase in the average purchase per customer.

Assessing the Risks of Social Media

Despite its advantages, it is undeniable that social media introduces new types of risk into companies that executives need to be aware of and auditors need to begin incorporating into their risk assessments. These risks arise at every touch point the company has with social media, both sanctioned and unofficial. There are risks, for example, regarding who has responsibility for and access to the company's official blog(s), Twitter account and Facebook fan page; there are risks in who can post videos to YouTube on behalf of the company and risks in regard to what information can be distributed to the public.

Risks are also embedded in what appear to be innocuous features of many social media tools. For example, an executive's Facebook or LinkedIn profile can potentially leak material of value to competitors who might be able to "mine" their contacts and posts to acquire inside information about the company's plans. Executives who use the TripIt feature of LinkedIn to announce where they will be traveling open themselves up to being followed.

Allowing employee access to their personal Facebook, Twitter or other social media accounts from the company's internal server opens up numerous security and data privacy risks. People tend to be highly unsuspecting of the risks they can encounter in their ordinary use of social media. The profile of social media users reveals that:[1]

- 64 percent of people on social networks click on links offered by community members or contacts even if they don't know where the link will take them.
- 50 percent-plus let acquaintances or roommates access social networks on their computers.
- 47 percent have been victims of malware infections.
- 26 percent share files within social networks.

- 21 percent accept contact offerings from members they don't recognize.
- 20 percent have experienced identity theft.

There are plenty of examples of breaches of corporate confidentiality and reputation arising from social media usage. For instance, workers at a North Carolina Domino's Pizza posted an unauthorized YouTube video showing them engaging in inappropriate actions that embarrassed the company. Numerous employees have complained about their boss or their jobs on their personal Facebook page. One employee was fired after such an incident, but the latest court ruling as well as the National Labor Relations Board sided with the employee. Others have used Facebook and Twitter social networking sites to tout stocks in what proved to be a classic "pump and dump" fraud. Hospital employees have disseminated information over social media about patients, and doctors have used their cell phones to take photos of patients undergoing surgery and then posted them on social media sites.

One of the distinguishing factors about the risks of social media is that, unlike traditional media, the speed and expanse of the online world can catapult the impact of breaches to a new order of magnitude. In a single instant, an employee can disseminate confidential or private information to thousands of unauthorized recipients within seconds. Mistakes such as forwarding email, the accidental hitting of "Reply All" or the unintentional posting of valuable company information on a social network are irreversible once they are out in cyberspace. Numerous companies have learned the hard way that embarrassing statements or videos about them claim a life of their own. Even if the company manages to have them removed from a website such as YouTube, they are often copied and uploaded to other websites.

The Risks of Social Media

Here is a short-list of the risks that companies open themselves up to when engaging in the widespread use of social media for corporate communications:

- *IP/Sensitive Data Loss* – Information strategic to the company could be inappropriately released (e.g., "My company is working on this cool new project to…").
- *Compliance Violations* – Data that violates regulatory/compliance requirements could be communicated (e.g., "You won't believe who I saw just come into the hospital to have this treatment done…").
- *Reputational Loss* – Slanderous remarks and comments from a disgruntled employee could create damaging perceptions (e.g., "If you work for my company, you will be mistreated and not respected...").
- *Financial Loss* – Remarks about company performance could impact stock price and performance (e.g., "The strategic plan for my company is not going to work, and results are not going to be good…").
- *Safety Loss* – Release of information about what someone is doing or where someone is traveling (e.g., "Our executive team is meeting at Location Z…").
- *Personal Reputation Loss* – Remarks made by an individual or friends of an individual could be viewed by others (e.g., "Let me tell you what happened the other night when I was out for dinner with my boss. He/she drank so much that ….").

These are just a few of the risks. Numerous others may arise due to your specific company's situation and use of social media.

Growing Privacy Risk

Also of growing concern are potential breaches of personal information about employees, customers or other stakeholders of the company. This risk arises from a use of social media that intentionally or accidentally reveals protected personal data; or from hackers who can steal personal identity data through social media websites. Guarding personal data must now be a key concern among companies located nearly anywhere in the world as many governments have implemented strict privacy regulations thatcontinue to evolve with new technologies. Almost every country has some sort of privacy legislation enacted that must be attended to. In the U.S., all 50 states (plus the District of Columbia and Puerto Rico) have privacy laws.

Creating Social Media Policies and Regulations

Until recently, many companies did not focus on the risks of social media in their environment. It was generally perceived that if they simply blocked social media websites (like Facebook) from employees, the potential risk was mitigated. As a result, internal auditors did not typically include social media in their risk assessments and auditing universe.

But with the growing sanctioned corporate use of social media, and employee demands to have access to their personal social media accounts, companies need to become more proactive in analyzing and addressing the risks presented by their social media usage. They must begin establishing clear social media policies and expectations for operational behavior that apply across the board. Auditors must then help assess compliance with the policies and be part of the process to educate employees about the use of social media technologies.

Our view is that the process of mitigating risks begins by clarifying the business purpose for which the company wants to use social media tools. A company would use this context to evaluate whether current policies are adequate in both scope and alignment – with particular focus on existing policies for information security, corporate communications and marketing. In each of these areas, the company should assess how social media pertains to those policies by asking such questions as:

- What policies do we have in place, if any?
- Are those policies efficient and effective?
- How and by whom are those policies monitored?
- How comfortable is management with these policies?
- Do the policies need renewal or update?
- Do we understand the risks involved?
- Do we want to mitigate the risks vs. tolerate them?

These questions and others help lead to creating an official social media policy and also can help in planning what audit and risk assessment procedures and steps need to be implemented.

Suggested Elements of a Social Media Policy

eMarketer reported on a new study from security solutions provider nCircle that found three-fifths of U.S. security and IT professionals say their company has a social media policy and that 40 percent of those policies actually ban all usage of social media while on the job. This is roughly comparable to last year's report where 54 percent of CIOs banned social media in the workplace.[2]

However, in today's world, this may not be as effective as providing guidance for what is deemed appropriate use in the workplace, especially as employees increasingly blur the lines between their professional and personal lives. A meaningful social media policy should establish clear and specific guidelines that the use of social media in an employee's official capacity, whether on company-owned or personal social media accounts, is a form of communication and must therefore follow the rules and procedures for all corporate communications. We suggest that the social media policy address at least the following rules:

- A definition of what is acceptable content and how it must conform to all organizational codes of conduct. One basis for this is the idea that speaking of the firm is the same as speaking on behalf of the firm. For example, the policy might require that any social media communication:
  - contains nothing that conflicts with the interests of the firm, its partners or its clients.
  - includes no negative or inaccurate posts.
  - reinforces that each employee must take responsibility for his/ her actions
- A statement that breaches the policy will incur defined, clear and enforced disciplinary actions.
- A description of how the policy is being made available or transparent to all employees.
- A definition or reinforcement of what data is considered sensitive.
- A timetable and approach for addressing mistakes or misrepresentations.

However, note that the social media policy may not infringe on the employee's federally protected rights to discuss working conditions, wages and other work-related conditions on their own computers during their own personal time. This was the basis of defense in the case cited above of an employee who was fired for posting a comment about her boss on her Facebook page, in which the National Labor Relations Board sided with the employee.

Employee Training

Once a social media policy is defined, it is crucial to train all employees and ascertain their awareness and acceptance. We suggest referencing the policy in the employee handbook and code of conduct and asking employees to sign off on it on a periodic basis. Furthermore, training on the policy should not be a one-time event but an ongoing campaign that stays up to date with the constantly changing technologies and uses of social media. Employees especially need to become aware of protected data privacy regulations in the company's areas of operations to avoid accidental breaches they would not have assumed to be illegal.

Scoping and Executing an Audit

If integrated into the business properly, the process of scoping and executing an audit of social media use is not substantially different than an audit of any other function. We suggest the plan adheres to ten steps as follows:

1. Confirm audit scope and approach in advance. Begin by determining the boundaries of the audit (Exhibit 1) in terms of risks, controls and objectives.

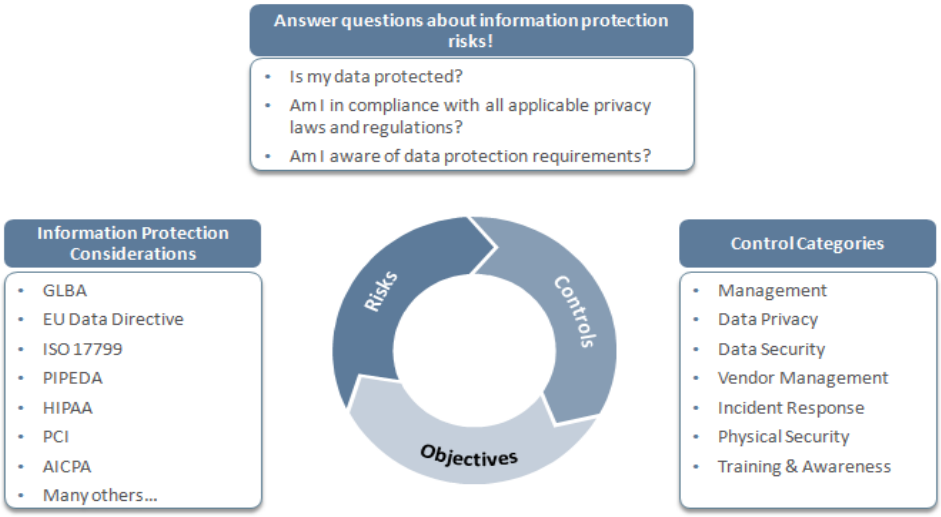

Exhibit 1: Determining Boundaries of Audit

2. Identify what the key risks are (e.g., IP / sensitive data loss, compliance violations, reputational loss as stated in "The Risks of Social Media" box above).
3. Establish a key contact to assist and coordinate audit activities. This person is your "Sherpa" who can expertly guide the internal audit group through the specific areas of risk in each domain of concern.
4. Utilize a standard approach or framework to guide privacy protection practices across all social media usage within the company.
5. Organize a manner in which to display current control activities and map to specific regulatory/legislation requirements.
6. Create and keep current a data classification standard that associates types of data with data privacy practices.
7. Determine vendor, customer and other third-party touch points with respect to privacy requirements.
8. Define policies and procedures governing data privacy, handling, awareness, etc.
9. Determine the best ways to communicate how policies and procedures are enforced throughout the organization.
10. Track what documents are available for review and proof of actions being taken.

These steps exemplify just one approach you can take, so keep in mind they need to be customized to each company's situation. In addition, any plan needs to be updated on a regular basis to account for new uses of existing social media tools as well as new tools that come on the market. For instance, no

one imagined as little as two years ago that companies would be tweeting or maintaining Facebook pages, so a social media policy formulated back then would be out of date today.

Validate Incident Response Processes

The instantaneous nature of social media and the extent to which information is shared presents a formidable challenge for companies as they respond to situations impacting their reputation or operational business components. Companies need to carefully examine how their incident response processes cover social media-related events and ensure they have appropriate oversight. Additionally, given that the risks of regulated privacy breaches increase with the growing use of social media, care must be taken to understand the requirements for the jurisdiction in which the company is operating. In the U.S., for example, 46 states and the District of Columbia currently have specific breach notification requirements (e.g., three states – Florida, Ohio, Wisconsin – require notification letters to be sent within 45 days after discovery of an incident).[3] Breach notification processes need to be in place to meet such regulatory requirements.

Working with IT

More than ever, auditors must coordinate the development of a social media policy and auditing procedure with IT. There is a burden on auditing to be familiar with the technologies and to ask the right questions of IT, but at the same time, IT must be accountable for understanding the need for clear controls and governance of social media tools given the potential risks. Together they share the mutual goal of integrating social media tools into the enterprise in a way that allows maximization of the business benefits that social media offers the organization. Both must be participants in identifying the risks to the company and to offer solutions to mitigating them.

Conclusion

The use of social media reflects an unstoppable paradigm shift in the business world. While many CEOs, CIOs and senior executives continue to reflect on adopting it into their culture, its benefits are far too numerous to deny. Companies that take a narrow view of its value to their business will find themselves losing out to savvy competitors who learn to optimize its many applications in recruiting, building teams, boosting idea exchange and innovation, marketing the company's products, enhancing its brands and attracting loyal customers.

Auditors can make a contribution to the organization by helping management and employees examine the best ways to integrate social media into the company's business processes and procedures in ways that mitigate the risks. Auditing can play a positive role in ensuring the company avoids jumping into the use of social media with the common mistake of "Ready, Fire, Aim."

Instead, they can work with senior leadership, IT and other relevant executives to develop a coordinated plan for evaluating social media usage, including executives and board members. Auditors can play a key role in helping companies define appropriate risk assessment and risk mitigation activities that account for the unique capabilities provided by social media and still provide an environment where employees and the company can obtain defined benefits.

Article Contacts

Tom Andreesen
+1.913.685.6241
thomas.andreesen@protiviti.com

Cal Slemp
+1 203-905-2926
cal.slemp@protiviti.com

References

[1] Source: *http://www.webpronews.com*
[2] "Banning Social Media Doesn't Work, Education Does," by Lisa Barone, Social Media, May 5, 2010.
[3] There are now 46 states with breach disclosure standards, but even the remaining four states (AL, KY, NM, and SD) have some other requirements that could broadly be called privacy laws.

Article from Protiviti KnowledgeLeader – www.knowledgeleader.com.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk and add value. Free 30-day trials available.

Protiviti (www.protiviti.com) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.