Deloitte.

The digital grapevine
Social media and the role of Internal Audit

Preface

Organizations today are embracing new digital technologies to leapfrog or keep pace with growing competition in the marketplace. Powerful platforms — such as mobile, analytics, social media, cloud, and cyber intelligence — can potentially impact every facet of the organization, leading to new opportunities. But these emerging technologies and platforms can also introduce significant disruptive forces into the business. The convergence of these macro forces is reflecting a new basis for competition, changing the environment in which we both live and work, and becoming the core of the "Digital Enterprise." Therefore, it is critical to understand the risks of integration as constantly changing digital technologies become the norm.

This whitepaper is part of our series on the digital Enterprise, which focuses on how organizations can leverage the disruptive forces of digital technologies, mitigate emerging risks, and capitalize on breakthrough thinking. We encourage you to share this whitepaper with colleagues — executives, board members, and key managers at your company. The issues outlined herein can serve as the starting point for the crucial dialogue on helping your company achieve its goals as a Digital Enterprise.

The digital grapevine: Social media and the role of Internal Audit

No longer confined to areas of entertainment and life management, social media and social software have become an integral part of the business landscape. According to a 2012 survey conducted by Burson-Marstellar, a global public relations firm, 87 percent of the *Fortune* 100 is now using social media. Twitter appears to be the channel of choice for this corporate demographic, as the average number of followers per *Fortune* 100 corporate Twitter account nearly tripled within one year — growing from 5,076 in 2011 to 14,709 in 2012.[1] With more and more users linking, liking, friending, and following, the "digital grapevine" is an important medium for communicating with customers, increasing brand awareness, and promoting innovation and collaboration among employees.

While the benefits of social media are alluring, the risks of adoption should not be ignored. Several business executives have expressed concerns that the use of social software and social media — and the potential risks that accompany increased organizational transparency and openness — may erode a company's brand over time. A 2012 Forrsights Security Survey reported that social media was one of the top three concerns for enterprises, with data leakage, social account hijacking, regulatory compliance, and human resources concerns high on the list of challenges.[2]

Here are two instances where social media may have harmed an organization's brand and reputation:

- A major U.S. food chain's Twitter account was hacked, resulting in a flurry of offensive tweets, a rival company's profile picture being swapped for its own, and an announcement that the company had even been sold to this rival. It took half a day for administrators to suspend the account, and a full day for the public relations team to issue an apology on the company's Facebook page.
- A major automobile manufacturer invited the public to create advertisements for a new car. While the campaign was considered an overall success, hundreds of environmentalists created viral videos criticizing the auto company for contributing to global warming.

These examples and other similar incidents are a rallying cry for Internal Audit (IA) to be proactive in understanding the risks and challenges posed by the growing force of social media. Internal auditors have the training and experience to identify and assess risk, and they have a broad view of the organization. This puts IA in an effective position to provide advice on implementing strategies to capitalize on the opportunities presented by the use of social media, while also managing risks appropriately.

[1] "Global Media Check-Up 2012," Burson-Marstellar 2012.

[2] Nick Hayes, "Manage the Risks of Social Media," Q2 2012 Forrsights Security Survey, November 29, 2012, Forrester Research, Inc.

Driving performance with social business

While still in the early stages, social media, social technologies, and associated programs and strategies have the ability to drive business decisions and outcomes across an organization's ecosystem. Hence, the term, "social business." This concept goes beyond the buzz of social media and social technologies and can enable new and more efficient connections, both inside and outside an organization, to drive performance.

According to a 2012 survey conducted by *MIT Sloan Management Review* and Deloitte Consulting LLP, 52 percent of managers across industries believe that social business is important or somewhat important to their business today. Fully 86 percent believe that social business will be important or somewhat important in three years.[3]

Social business is typically viewed as a tool for external-facing activities, and is considered particularly useful for managing customer relationships. Increasingly, its relevance to innovation and competitive differentiation is also being recognized.

In order to take advantage of social business activities while also managing the challenges and risks, organizations should involve IA and other professionals to develop appropriate risk management programs. The following sections in this paper take a closer look at the risk landscape and how IA can assist the organization. As a company adopts social business activities, IA can offer advice on the appropriate strategies that can help the organization manage social media challenges.

[3] "Social Business: What Are Companies Really Doing?", *MIT Sloan Management Review,* May 30, 2012.

Understanding social media risks

For many companies, the barrier to adopting social business is risk. According to a 2012 survey of 192 U.S. executives conducted by Deloitte & Touche LLP and *Forbes Insights,* social media was identified as the fourth largest risk over the next three years, through 2015, placing it on par with financial risk.[4]

Concerns around social media can be attributed to its ability to act as an accelerant to other risks. For example, as the Deloitte & Touche and *Forbes Insights* survey report noted, "social media may also exacerbate … financial risk associated with financial disclosures in violation of Securities and Exchange Commission (SEC) rules."[5] Other inherent social media risks include information leakage, reputational damage to brand, non-compliance with regulatory requirements, and third-party risks.

In each of these risk categories, IA can play a critical — and proactive — role in understanding the potential risks of engaging in social business. IA can also help develop business processes that will mitigate risks associated with unintended consequences, assume responsibility for monitoring compliance with implemented processes, and assess implemented controls.

Brand and reputation damage

Numerous corporate social media fiascos over the last few years have brought attention to the phenomenon of brand sabotage. They have also demonstrated why brand stewards should be concerned about attacks — whether intentional or unintentional — on their brands.

Information moves faster on the digital grapevine. With a 24-hour news cycle, small social media blunders can turn into public relations catastrophes. This highlights one important factor that sets social media risk apart from many other risks: velocity. According to a 2012 *ISACA Journal* article, "information spreads extremely quickly across social network systems and transitions to conventional news media, in some cases, within a few minutes of some controversial statement or inappropriate remark."[6]

One of the capabilities that an organization should build is a crisis management plan that outlines how to respond via social channels when an incident occurs. The plan should call out the types of crises that the organization could face, content that should be used in the response, tone of the message when responding to incidents, who will be involved in the response, and the appropriate response time frames.

Recommendations for IA:
IA should be involved in identifying crisis events and provide guidance on the impact that each of these events may have on the organization. IA can also play a role in identifying the integration points of social media crisis management with other crisis management plans (e.g., security incident management and businesses continuity crisis management). To support the crisis management plan, organizations should build capabilities and systems that allow them to detect events on social channels that may damage their brands. IA can play a part in testing these solutions once they have been implemented.

Regulatory compliance

Compliance and legal risks arise from the potential for violations of or nonconformance with laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. These risks also emerge when an organization's social media policies and procedures may not have kept pace with regulatory changes. Failure to adequately address these risks can expose an organization to enforcement actions and/or civil lawsuits. Some regulations and guidelines that govern enterprise social media use include:

- Employee rights under Section 7 of the National Labor Relations Act (NLRA) must be considered when creating a social media policy or disciplining an employee for social networking activity.

[4] "Aftershock: Adjusting to the new world of risk management," *Forbes Insights* and Deloitte Development LLC, 2012.

[5] Ibid.

[6] Tommie W. Singleton, "What Every IT Auditor Should Know About Auditing Social Media," *ISACA Journal,* Volume 5, 2012.

- The Federal Financial Institutions Examination Council (FFIEC) mandates that financial institutions have a risk management program commensurate with the breadth of the financial institution's involvement in social media, which allows it to identify, measure, monitor, and control the risks related to this medium.
- The Gramm Leach Bliley Act (GLBA) requires information protection, monitoring for sensitive content, and ensuring that such content is not sent over public channels.
- The Financial Industry Regulatory Authority (FINRA) calls for financial service organizations to retain records and make them accessible; public correspondence requires approval, review, and retention — and this is also extended to communications over social channels.
- The Payment Card Industry Data Security Standard (PCI DSS) requires organizations to prove that cardholder data is not sent over unsecured channels, which include social media sites.

Recommendations for IA:
IA can assist with guidance on the policies that need to be developed so that social media activities comply with current regulations. IA can also perform gap assessments of the organization's current policies and procedures against legal and regulatory requirements (e.g., FINRA, NLRA).

Information leakage

Information leakage prevention is an effort by companies to keep sensitive information from leaving the virtual walls of the organization. Because social media allows employees to speak to broad audiences, insufficient controls could lead to the disclosure of sensitive information, such as personal accounts, health information, intellectual property, customer data, personally identifiable information, etc. Information leakage may result in loss of competitive advantage and brand damage. In some cases, there may also be legal consequences.

Recommendations for IA:
IA should provide input into data classification methodology to ensure that appropriate loss prevention controls are applied to data that will be shared in social channels.

Third-party risk

Outsourcing social media activities can expose companies to substantial risks, particularly copyright and trademark infringement. For example, business impersonation (in which social sites or social identities that are similar to your company's name or brand are used for unauthorized business activities) can facilitate abuse of business trademarks and copyrights. In addition, organizations that have relationships with third-party affiliate marketers run the risk of non-compliance with applicable state and federal laws that govern advertising and marketing activities. Any advertising or marketing activities that take place through social media are subject to the same rules and regulations that similar practices would be in traditional media.

In their proposed guidance on the application of consumer protection and compliance laws to activities conducted via social media, the FFIEC recommended that organizations implement due diligence processes for selecting and managing third-party providers.[7]

Recommendations for IA:
IA should ensure that procedures regarding the use of third-party service providers are consistently followed, including due diligence, contract management, and relationship termination. IA should also be involved in the due diligence process in selecting third-party providers, including examining the third party's control environment, security, legal, and compliance history.

[7] "Financial Regulators Propose Guidance on Social Media," Federal Financial Institutions Examination Council, January 22, 2013.

Governance risk

A lack of governance can result in many uncoordinated and inefficient activities, which can also lead to missed opportunities for gaining competitive advantage or sustaining market leadership. The urgency to meet the needs and expectations of departments across the organization, exacerbated by enterprise-grade solutions that are often procured without IT oversight, can result in even greater chaos. Certainly, some bright spots have been found. But even celebrated leaders are facing a wide range of governance risks and challenges, such as:

- Lack of a broad vision for how social media will transform the business, leading many companies to pursue the wrong goals (and metrics) or, worse, not pursue transformative opportunities at all.
- Competing strategies and varying degrees of maturity across functions, which are often the result of companies "jumping into" social media before a governance structure is in place.
- A gap in implementing mature operating models for social media, resulting in duplicate efforts, wasted investment, poorly allocated resources, and limited organizational learning.

Common symptoms of inadequate governance and lack of an appropriate social strategy include improper application of metrics and limited ability to identify, track, and reward success; inconsistent application of leading practices, and with limited accountability; siloed behavior and inconsistency across accounts; and uncertainty on how and where to invest resources and evaluate success beyond volume-based metrics.

Recommendations for IA:

IA should serve as an objective assessor of an organization's social media governance program. Through independent audits and risk assessments, IA can play a critical role in providing insights into the effectiveness of governance structures that have been implemented. IA can also become a catalyst for positive change by providing advice on effective governance structures that are in line with the organization's culture and risk appetite.

Value-adding role for Internal Audit

Leading practices for social media are still in their nascent stages and have evolved, to a large degree, reactively. What's more, many organizations have only fragmented views of their social media infrastructure, which hinders effective risk management. IA's broad view of the organization offers a value-adding opportunity to assist organizations with risks related to brand and reputation, regulatory compliance, information leakage, third-party relationships, governance, and other social business challenges.

With the use of social media on the rise, becoming "anti-social" or disconnecting from the digital grapevine is not an option. Therefore, it is up to IA to be at the forefront of the organization's social business initiative, helping to monitor and manage threats and strike a balance between risks and opportunities.

Contacts

Michael Juergens
Principal
Deloitte & Touche LLP
+1 213 688 5338
michaelj@deloitte.com

Khalid Wasti
Director
Deloitte & Touche LLP
+1 212 436 5156
kwasti@deloitte.com

Steven Odhiambo
Senior Manager
Deloitte & Touche LLP
+1 215 246 2554
sodhiambo@deloitte.com