

## Social Media: Business Benefits and Security, Governance and Assurance Perspectives

### **Abstract**

Initiated as a consumer-oriented technology, social media is increasingly being leveraged as a powerful, low-cost tool for enterprises to drive business objectives such as enhanced customer interaction, greater brand recognition and more effective employee recruitment. While social media affords enterprises many potential benefits, information risk professionals are concerned about its inherent risks such as data leakage, malware propagation and privacy infringement. Enterprises seeking to integrate social media into their business strategy must adopt a cross-functional, strategic approach that addresses risks, impacts and mitigation steps, along with appropriate governance and assurance measures.

# SOCIAL MEDIA: BUSINESS BENEFITS AND SECURITY, GOVERNANCE AND ASSURANCE PERSPECTIVES

## ISACA®

With more than 86,000 constituents in more than 160 countries, ISACA ([www.isaca.org](http://www.isaca.org)) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and the Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA offers the Business Model for Information Security (BMIS) and the IT Assurance Framework™ (ITAF™). It also developed and maintains the COBIT®, Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfill their IT governance responsibilities and deliver value to the business.

## Disclaimer

ISACA has designed and created *Social Media: Business Benefits and Security, Governance and Assurance Perspectives* (the “Work”), primarily as an educational resource for security, governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security, governance and assurance professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

## Reservation of Rights

© 2010 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

## ISACA

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [info@isaca.org](mailto:info@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

*Social Media: Business Benefits and Security, Governance and Assurance Perspectives*

CRISC is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

# SOCIAL MEDIA: BUSINESS BENEFITS AND SECURITY, GOVERNANCE AND ASSURANCE PERSPECTIVES

## **ISACA wishes to recognize:**

### **Project Development Team**

Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico, Chair  
Ben Bradley, Macon Raine Inc., USA  
Michael Kiefer, BrandProtect, USA

### **Expert Review Team**

Victor Chapella, Sm4rt Security Services, Mexico  
Clyde Hague, CISM, CISSP, First Merchants Corp., USA  
Peter M. Rodgers, CISA, Resources Global Professionals, USA  
Jon Sternberg, CISA, CISM, CISSP, FFSI, FLMI, Northwestern Mutual, USA  
Chris Tignor, CISM, CISSP, Capital One Financial, USA

### **ISACA Board of Directors**

Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, International President  
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA-NV, Belgium, Vice President  
Yonosuke Harada, CISA, CISM, CGEIT, CAIS, InfoCom Research Inc., Japan, Vice President  
Ria Lucas, CISA, CGEIT, Telstra Corp., Australia, Vice President  
Jose Angel Pena Ibarra, CGEIT, Alintec, Mexico, Vice President  
Robert E. Stroud, CGEIT, CA Technologies, USA, Vice President  
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President  
Rolf von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany, Vice President  
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG Ltd., Russia, UK, Past International President  
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President  
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Director  
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director  
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Director  
Jeff Spivey, CPP, PSP, Security Risk Management, USA, ITGI Trustee

### **Guidance and Practices Committee**

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Chair  
Phil James Lageschulte, CGEIT, CPA, KPMG LLP, USA  
Mark A. Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA  
Adel H. Melek, CISA, CISM, CGEIT, Deloitte & Touche, Canada  
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA, Capco IT Service India Pvt Ltd., India  
Anthony P. Noble, CISA, Viacom, USA  
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico  
Eddy Justin Schuermans, CISA, CGEIT, ESRAS bvba, Belgium  
Frank Van Der Zwaag, CISA, CISSP, Westpac, New Zealand

## Impacts of Social Media

Gone are the days of recommendations to keep social media usage out of the enterprise. Businesses today find that social media use is no longer the exception, but rather the rule. Business units such as research and development, marketing, human resources, sales, and customer service are realizing the potential for utilizing social media tools to stimulate innovation, create brand recognition, hire and retain employees, generate revenue, and improve customer satisfaction. Social media use is no longer just an option for enterprises that want to lead in today's business environment.

---

**Of the *Fortune* Global 100 companies, 65 percent have active Twitter accounts, 54 percent have Facebook fan pages, 50 percent have YouTube video channels and 33 percent have corporate blogs.**

---

Use of social media has even begun to impact brand recognition and enterprise revenue. A 2009 study by ENGAGEMENTdb found that the most valuable brands in the world are experiencing a direct correlation between top financial performance and deep social media engagement. Findings of the study show that enterprises that aggressively embrace social media as part of their strategy are more financially successful.<sup>1</sup>

It is encouraging that enterprises have seen not just a return on investment (ROI), but also revenue increases from the use of social media. But enterprises must be cautious since there have also been negative impacts such as liability for libel, privacy violations and damage to brand recognition.

## What Is Considered “Social Media”?

Social media technology involves the creation and dissemination of content through social networks using the Internet. The differences between traditional and social media are defined by the level of interaction and interactivity available to the consumer. For example, a viewer can watch a news broadcast on television with no interactive feedback mechanisms, while social media tools allow consumers to comment, discuss and even distribute the news. Use of social media has created highly effective communication platforms where any user, virtually anywhere in the world, can freely create content and disseminate this information in real time to a global audience ranging in size from a handful to literally millions—in less time than it takes to read this document.

There are many types of social media tools: blogs such as WordPress and TypePad, microblogs such as Twitter and Tumblr, image and video sharing sites such as Flickr and YouTube, social networking sites such as Facebook and MySpace, and professional networking sites such as LinkedIn. The common link among all forms of social media is that the content is supplied and managed by individual users who leverage the tools and platforms provided by social media sites.

## The Business Benefits of Social Media

Social media has become a powerful tool for enterprises across the globe. A 2010 Burson-Marsteller study showed that, “of the *Fortune* Global 100 companies, 65 percent have active Twitter accounts, 54 percent have Facebook fan pages, 50 percent have YouTube video channels and 33 percent have corporate blogs.”<sup>2</sup>

---

**Enterprises that aggressively embrace social media as part of their strategy are more financially successful.**

---

<sup>1</sup> ENGAGEMENTdb, *The World's Most Valuable Brands. Who's Most Engaged? Ranking the Top 100 Global Brands*, [www.engagementdb.com/downloads/ENGAGEMENTdb\\_Report\\_2009.pdf](http://www.engagementdb.com/downloads/ENGAGEMENTdb_Report_2009.pdf)

<sup>2</sup> Burson-Marsteller, *The Global Social Media Check-up Insights: From the Burson-Marsteller Evidence-based Communications Group*, [www.burson-marsteller.com/Innovation\\_and\\_insights/blogs\\_and\\_podcasts/BM\\_Blog/Documents/Burson-Marsteller%202010%20Global%20Social%20Media%20Check-up%20white%20paper.pdf](http://www.burson-marsteller.com/Innovation_and_insights/blogs_and_podcasts/BM_Blog/Documents/Burson-Marsteller%202010%20Global%20Social%20Media%20Check-up%20white%20paper.pdf)

## SOCIAL MEDIA: BUSINESS BENEFITS AND SECURITY, GOVERNANCE AND ASSURANCE PERSPECTIVES

Enterprises are using social media in many functional areas of the business and are enjoying numerous tangible benefits such as increasing brand recognition, sales, search engine optimization (SEO), web traffic, customer satisfaction, and revenue.<sup>3</sup> In addition, rapid feedback and insight from consumers provide a mechanism for executives to assess consumer opinion and use this information to improve products, customer service and perception.

Enterprises have also discovered that they are able to monitor the market, their competition and their customers via social media outlets. This allows engaged enterprises to be on top of any changes that may be needed and to proactively make appropriate adjustments to strategies, products or services.

The ability to search for and communicate with potential employees is another area that has seen great enhancement via sites such as LinkedIn and Plaxo.

Given its ease of use and measurement and its ability to reach large populations almost instantly, social media is becoming a powerful force in the way businesses reach, attract and engage their customers, employees and other stakeholders.

### Risks, Security and Privacy Concerns

Not wishing to be left behind, many enterprises are seeking to leverage social media tools. Since the tools are new to many enterprises and do not require new infrastructure, social media technologies may be introduced to the enterprise by business and marketing teams without IT involvement, a project plan or risk assessment. It is therefore important that the enterprise create a social media strategy and have a plan to address the risks that accompany the technology.

While the use of social media does have inherent risks that could negatively impact enterprise security, it also presents opportunities such as accelerated business growth and improved brand recognition. Therefore, simply choosing to prohibit the use of social media can also incur an opportunity cost based on forgoing these potential business benefits.

As with any new initiative, enterprises should take care to consider risks vs. benefits when deciding on a social media strategy. There are several scenarios that should be considered when evaluating the impact of social media on the enterprise. Initially, the enterprise should consider the risks of using social media as a business tool to communicate with customers or constituents. Enterprises must also consider the risks of employee access to social media sites while on the corporate network. Finally, enterprises should consider that employees also use social media tools from their corporate-issued mobile devices. Although mobile devices may be an organizational asset, they are often not subject to the same controls and monitoring as the enterprise's computers. Vulnerabilities such as insecure applications may exist on an employee's personal social media page; those vulnerabilities may cause unacceptable exposure on a corporate network. Additionally, malicious outsiders could use employee social media pages to launch targeted attacks by gathering information to execute sophisticated social engineering campaigns.

A final, although perhaps more controversial, consideration is employee personal use of social media from home and personal computing devices. With the exception of the threats of infection of organizational computing assets with viruses and malware, all of the risks that exist for personal use of social media sites in the workplace also exist when employees access social media sites from home or other areas not controlled by the enterprise or its policies. Close collaboration with organizational human resources and legal departments is critical when considering an approach to this situation.

---

<sup>3</sup> ENGAGEMENTdb, *Op. cit.*

## Strategies for Addressing Social Media Risks

Since enterprise use of social media tools usually requires no additional technology to implement, an enterprise social media presence does not always begin with a project plan and risk assessment. To effectively control social media usage by both the enterprise and employees, a documented strategy (and associated policies and procedures) should be developed with the involvement of all relevant stakeholders, including business leadership, risk management professionals, and human resource and legal representation. This holistic approach to integrating emerging technologies into the enterprise helps to ensure that risks are being considered in the context of broader business goals and objectives.

---

**A documented strategy (and associated policies and standards) should be developed with the involvement of all relevant stakeholders.**

---

While the use of social media presents an additional entry point for technology risks such as malware and viruses, these risks are elevated primarily because more employees may be using social media sites without understanding the threats that exist. Therefore, any strategy to address the risks of social media usage should first focus on user behavior through the development of policies and supporting training and awareness programs that cover:

- Personal use in the workplace:
  - Whether it is allowed
  - The nondisclosure/posting of business-related content
  - The discussion of workplace-related topics
  - Inappropriate sites, content or conversations
- Personal use outside the workplace:
  - The nondisclosure/posting of business-related content
  - Standard disclaimers if identifying the employer
  - The dangers of posting too much personal information
- Business use:
  - Whether it is allowed
  - The process to gain approval for use
  - The scope of topics or information permitted to flow through this channel
  - Disallowed activities (installation of applications, playing games, etc.)
  - The escalation process for customer issues

Training should be conducted on a regular basis and should focus on the benefits and opportunities as well as on the dangers related to use of social media. Emphasis should be placed on the specific dangers and methods of social engineering, common exploits, and the threats to privacy that social media present. Training should also ensure full understanding of the rules governing acceptable use and behavior while on social media sites.

Technical controls that exist for other e-commerce opportunities will benefit the enterprise when embracing a social media strategy. Technology can assist in policy enforcement as well as in blocking, preventing or identifying potential incidents. This strategic component should utilize a combination of web content filtering, which can block all access or allow limited access, and in some cases provide protection against malware downloads and end-user system antimalware, antivirus and operating system security to counter such attacks. As with most security technology strategies, a layered approach is optimal.

**Figures 1 and 2** provide risk mitigation techniques for both the risks of a corporate social media presence and the risks of employee personal use of social media.

## SOCIAL MEDIA: BUSINESS BENEFITS AND SECURITY, GOVERNANCE AND ASSURANCE PERSPECTIVES

**Figure 1—Risks of a Corporate Social Media Presence**

Threats and Vulnerabilities	Risks	Risk Mitigation Techniques
Introduction of viruses and malware to the organizational network	<ul style="list-style-type: none"> <li>• Data leakage/theft</li> <li>• “Owned” systems (zombies)</li> <li>• System downtime</li> <li>• Resources required to clean systems</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure that antivirus and antimalware controls are installed on all systems and updated daily.</li> <li>• Consider use of content filtering technology to restrict or limit access to social media sites.</li> <li>• Ensure that appropriate controls are also installed on mobile devices such as smartphones.</li> <li>• Establish or update policies and standards.</li> <li>• Develop and conduct awareness training and campaigns to inform employees of the risks involved with using social media sites.</li> </ul>
Exposure to customers and the enterprise through a fraudulent or hijacked corporate presence	<ul style="list-style-type: none"> <li>• Customer backlash/adverse legal actions</li> <li>• Exposure of customer information</li> <li>• Reputational damage</li> <li>• Targeted phishing attacks on customers or employees</li> </ul>	<ul style="list-style-type: none"> <li>• Engage a brand protection firm that can scan the Internet and search out misuse of the enterprise brand.</li> <li>• Give periodic informational updates to customers to maintain awareness of potential fraud and to establish clear guidelines regarding what information should be posted as part of the enterprise social media presence.</li> </ul>
Unclear or undefined content rights to information posted to social media sites	<ul style="list-style-type: none"> <li>• Enterprise’s loss of control/legal rights of information posted to the social media sites</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure that legal and communications teams carefully review user agreements for social media sites that are being considered.</li> <li>• Establish clear policies that dictate to employees and customers what information should be posted as part of the enterprise social media presence.</li> <li>• If feasible and appropriate, ensure that there is a capability to capture and log all communications.</li> </ul>
A move to a digital business model may increase customer service expectations.	<ul style="list-style-type: none"> <li>• Customer dissatisfaction with the responsiveness received in this arena, leading to potential reputational damage for the enterprise and customer retention issues</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure that staffing is adequate to handle the amount of traffic that could be created from a social media presence.</li> <li>• Create notices that provide clear windows for customer response.</li> </ul>
Mismanagement of electronic communications that may be impacted by retention regulations or e-discovery	<ul style="list-style-type: none"> <li>• Regulatory sanctions and fines</li> <li>• Adverse legal actions</li> </ul>	<ul style="list-style-type: none"> <li>• Establish appropriate policies, processes and technologies to ensure that communications via social media that may be impacted by litigation or regulations are tracked and archived appropriately.</li> <li>• Note that, depending on the social media site, maintaining an archive may not be a recommended approach.</li> </ul>

# SOCIAL MEDIA: BUSINESS BENEFITS AND SECURITY, GOVERNANCE AND ASSURANCE PERSPECTIVES

**Figure 2—Risks of Employee Personal Use of Social Media**

Threats and Vulnerabilities	Risks	Risk Mitigation Techniques
Use of personal accounts to communicate work-related information	<ul style="list-style-type: none"> <li>• Privacy violations</li> <li>• Reputational damage</li> <li>• Loss of competitive advantage</li> </ul>	<ul style="list-style-type: none"> <li>• Work with the human resources (HR) department to establish new policies or ensure that existing policies address employee posting of work-related information.</li> <li>• Work with the HR department to develop awareness training and campaigns that reinforce these policies.</li> </ul>
Employee posting of pictures or information that link them to the enterprise	<ul style="list-style-type: none"> <li>• Brand damage</li> <li>• Reputational damage</li> </ul>	<ul style="list-style-type: none"> <li>• Work with the HR department to develop a policy that specifies how employees may use enterprise-related images, assets, and intellectual property (IP) in their online presence.</li> </ul>
Excessive employee use of social media in the workplace	<ul style="list-style-type: none"> <li>• Network utilization issues</li> <li>• Productivity loss</li> <li>• Increased risk of exposure to viruses and malware due to longer duration of sessions</li> </ul>	<ul style="list-style-type: none"> <li>• Manage accessibility to social media sites through content filtering or by limiting network throughput to social media sites.</li> </ul>
Employee access to social media via enterprise-supplied mobile devices (smartphones, personal digital assistants [PDAs])	<ul style="list-style-type: none"> <li>• Infection of mobile devices</li> <li>• Data theft from mobile devices</li> <li>• Circumvention of enterprise controls</li> <li>• Data leakage</li> </ul>	<ul style="list-style-type: none"> <li>• If possible, route enterprise smartphones through corporate network filtering technology to restrict or limit access to social media sites.</li> <li>• Ensure that appropriate controls are also installed and continuously updated on mobile devices such as smartphones.</li> <li>• Establish or update policies and standards regarding the use of smartphones to access social media.</li> <li>• Develop and conduct awareness training and campaigns to inform employees of the risks involved with using social media sites.</li> </ul>

## Governance and Change Considerations

The introduction of social media use by an enterprise can produce significant shifts in both culture and process—particularly in the areas of communication, marketing, customer service and business development. The dynamic network of communication streams that are facilitated by social media can significantly alter the way an enterprise launches marketing campaigns, collects customer satisfaction data and provides customer support. Business processes in each of these areas may need to be altered to facilitate these changes.

The use of social media also introduces a new communication channel that must be monitored and managed. Depending on the nature of the use, and on the number and type of social media sites utilized, staffing and training requirements may be significant and should be taken into consideration during strategy development.

When considering new technologies, enterprises should look to established frameworks such as Risk IT and COBIT, which provide clear processes and controls to help form sound social media governance. When creating a social media strategy, some questions to consider are:

- What is the strategic benefit to leveraging this emerging technology?
- Are all appropriate stakeholders involved in social media strategy development?
- What are the risks associated with the technology and do the benefits outweigh the costs?
- What are the new legal issues associated with the use of social media?
- How will customer privacy issues be addressed?

---

When considering new technologies, enterprises should look to established frameworks such as Risk IT and COBIT.

---

- How can positive brand recognition be ensured?
- How will awareness training be communicated to employees and customers?
- How will inquiries and concerns from customers be handled?
- Does the enterprise have the resources to support such an initiative?
- What are the regulatory requirements that accompany the integration of the technology?

## Assurance Considerations

Just as enterprises must develop an appropriate strategy and controls to manage their use of social media, it is the role of assurance professionals within the enterprise to validate and monitor these controls to ensure that they are, and remain, effective and that compliance with these controls is established and measurable. The elements identified in ISACA's Business Model for Information Security (BMIS) present a good foundation for assurance professionals to provide assurance that risks are being managed appropriately:

### 1. Strategy and Governance

- Has a risk assessment been conducted to map the risks to the enterprise presented by the use of social media?
  - The risk assessment should evaluate the planned business processes for leveraging social media and also the specific sites to be used.
  - The risk assessment should be revisited whenever there are substantive changes to the social media resources in use, as well as when new social media resources are considered for adoption.
- Is there an established policy (and supporting standards) that addresses social media use?
  - Policies and standards should be modified or created to define appropriate behavior in relation to the use of social media.
- Do the policies address all aspects of social media use in the workplace—both business and personal?
  - Policies for social media should address four specific areas:
    - Employee personal use of social media in the workplace
    - Employee personal use of social media outside the workplace
    - Employee use of media for business purposes (personally owned devices)
    - Required monitoring and follow-up processes for brand protection

### 2. People

- Has effective training been conducted for all users, and do users (and customers) receive regular awareness communications regarding policies and risks?
  - It is imperative that all users understand what is (and is not) appropriate and how to protect themselves and the enterprise while using social media.
  - Customers who will be accessing an enterprise social media presence will need to understand what is considered an appropriate use of the communication channel and what information they should (and should not) share.

### 3. Processes

- Have business processes that utilize social media been reviewed to ensure that they are aligned with policies and standards of the enterprise?
  - Unless business processes are aligned with social media policies, there cannot be assurance that they will not expose sensitive information or otherwise place the enterprise at risk.
  - Change controls should be in place to ensure that changes or additions to processes that leverage social media are aligned with the policy prior to implementation.

### 4. Technology

- Does IT have a strategy and the supporting capabilities to manage technical risks presented by social media?
  - The vast majority of technical risks presented by social media are also found in the use of malicious e-mail and standard web sites. IT should have controls in place, both network-based and host-based, to mitigate the risks presented by malware.
  - Suitable controls can include download restrictions, browser settings, data leak prevention products, content monitoring and filtering, and antivirus and antimalware applications.
  - Appropriate incident response plans should be in place to address any infection that does get through.

## SOCIAL MEDIA: BUSINESS BENEFITS AND SECURITY, GOVERNANCE AND ASSURANCE PERSPECTIVES

- Do technical controls and processes adequately support social media policies and standards?
  - It should be verified that any required technical controls are present and functioning as expected, or that there are clear plans with timelines and a required budget to reach a specific capability.
- Does the enterprise have an established process to address the risk of unauthorized/fraudulent use of its brand on social media sites or other disparaging postings that could have a negative impact on the enterprise?
  - While scanning for such material can be an onerous task, it is important that the enterprise have a strategy to address this risk. There are vendors that will provide this service, and this is generally the best option for enterprises that deem such monitoring a necessary activity.
  - This risk exists regardless of the enterprise's active use of social media.

### Conclusion

The use of social media is becoming a dominant force that has far-ranging implications for enterprises and individuals alike. While this emerging communication technology offers great opportunities to interact with customers and business partners in new and exciting ways, there are significant risks to those who adopt this technology without a clear strategy that addresses both the benefits and the risks. There are also significant risks and potential opportunity costs for those who think that ignoring this revolution in communication is the appropriate way to avoid the risks it presents. The only viable approach is for each enterprise to engage all relevant stakeholders and to establish a strategy and associated policies that address the pertinent issues.

Click here for additional resources related to social media. [www.isaca.org/socialmedia](http://www.isaca.org/socialmedia).