Information Governance, Privacy, and Security Considerations for Social Media

Increasingly, a corporate presence on social media channels is no longer a trendy marketing tool, but instead a necessary component of doing business. According to a recent study conducted by KPMG, more than 70 percent of organizations worldwide are using at least one form of social media to enhance their presence on the Web. Additionally, today’s workforce is spending a significant amount of time on social media sites at work, at home, and on mobile devices. In fact, 86 percent of respondents to a KPMG survey of consumers responded that they use social media every day, with three quarters of respondents stating that they access social media from their personal computers. This is fueling massive growth in the amount of information being shared through nontraditional means, including collaboration sites, social and business networking sites, blogs, instant messages, and other social media channels. As companies and individuals continue to use social media technologies in growing numbers and in different ways, the risk of data loss and companies’ exposure to legal liability also increases. Significant areas of risk include:

- Impact to the network, resulting from increased use of bandwidth by individual users who access social media Web sites while at work
- Potential loss of data, including intellectual property and personally identifiable information by employees who are participating in social media channels using corporate accounts or as individual users
- Increased risk of malware exposure on the network and other forms of Web-based attacks
- Increased risk of legal liability if organizations or their employees use social media inappropriately

Organizations can take a proactive approach to addressing these risks by developing a well-reasoned social media privacy and security strategy as a component of the organization’s overall social media governance framework. By including data protection and privacy requirements, the organization can meet its defined objectives for social media, including improved customer relations, brand enhancement, and stronger business development activities. A clear social media privacy and security strategy will also enable individual users to enjoy the benefits associated with being active members of online communities without exposing their employers to risk resulting from behavior that is not compliant with the organizations’ privacy and security policies.

A comprehensive social media privacy and security strategy can help companies navigate the challenges of protecting corporate information assets in customer and workforce environments in which social media is used. KPMG’s Information Protection practice is well versed in security and data privacy challenges of social media usage and can help you to develop, implement, and maintain a risk-aware social media privacy and security strategy.

External Statistics

As social media usage by individuals continues to grow, organizations are also expanding the ways in which they use social media, as indicated by a study conducted by KPMG. As social media usage continues to trend up, individuals are also increasing the frequency with which they use social media channels on a daily basis, hence, the need for organizations to develop social media programs that will meet a growing demand by consumers and employees for a social media presence and accessibility.

---

1 “Going social: how businesses are making the most of social media,” KPMG 2011
2 “The Converged Lifestyle: consumers and convergence 5,” KPMG 2011
How KPMG can help

Organizations can gain a significant competitive advantage by both developing a corporate social media presence and by enabling and governing the use of social media by their employees. However, inherent in the use of these new technologies are a number of challenges related to effective protection and governance of data throughout its life cycle. These challenges include:

- Navigating the evolving landscape of social media regulations
- Managing social media data through its life cycle, including establishing data ownership and governing data handling from initiation, usage, storage, transfer, and archiving, to destruction
- Ensuring that sensitive corporate data is not intentionally or inadvertently exposed
- Providing executives and technical managers with the tools to effectively monitor and take action around potential issues.

To begin to address these challenges, companies must assess their current capabilities and potential exposure in the event of an information breach, and work to establish and implement (or update existing) data governance and monitoring capabilities as part of an overall social media governance framework.

KPMG’s multidisciplinary team recognizes that organizations want to protect and maintain the integrity of information while leveraging its strength as an asset to provide measurable benefits. Organizations need to have the flexibility to achieve the benefits of an effective social media program, while ultimately protecting their data and reputation. Our professionals understand the threats and marketplace trends that organizations are facing and are prepared to bring their knowledge and experience to bear for your organization.

KPMG’s Information Protection practice is dedicated to helping organizations cut through the complexity of technology utilization—and to providing approaches to challenges brought about by the adoption of new technologies, such as social media. Our professionals have a clear focus on sustaining the delicate balance between supporting the increased use of social media and its associated benefits, while helping companies protect valuable corporate information assets. Through the development and implementation of an effective social media security strategy and the ongoing monitoring of social media usage, we help organizations attain a state of social media readiness.

Our approach includes the following components:

- **Business, Regulatory, and Legal Requirement Analysis** – Staying current and knowledgeable of evolving social media technologies and knowing the potential legal and regulatory risks they can pose to your company is a critical component of successful social media adoption and use. KPMG’s Information Protection practice can assist your company by helping you to better understand the current legal and regulatory requirements and guidelines regarding social media usage, including FCRA, EEOC, state-specific monitoring laws, FINRA, FRCP ESI Requirements, NLRB/NLRA, as well as pending regulations regarding social media monitoring.

- **Current State Assessment and Gap Analysis** – As a recommended first step, evaluation of social media privacy and security practices and controls, and identification of gaps relative to company policies and/or leading practices can establish a prioritized plan of attack, helping to ensure efficient use of limited resources and budget.

- **Development of a Social Media Privacy and Security Strategy and Roadmap** – While identification of individual gaps and issues can facilitate point remediation activity, a more holistic and thorough approach to protecting sensitive organizational data requires identification of metrics and definition of roles and responsibilities for ongoing management of social media privacy and security. KPMG takes a business-centric, risk-based approach to helping develop programs to promote ongoing and proactive protection of organizational data, including an approach to managing privacy and security concerns associated with social media.

- **Policy and Standard Evaluation and Revision** – Given the changing nature of social media platforms, many organizations are just beginning to anticipate risks and the need to provide additional controls to adequately protect data shared through social media channels. KPMG has extensive experience in helping organizations to customize their policies and standards to ensure effective and efficient governance of social media.
security and privacy policies and standards to support the use of evolving technologies. We can assist in evaluation and development of recommendations for changes to existing security policies based on the impact and evolving risks posed by extensive adoption of social media, including acceptable use, data retention, internal and external privacy policies, rights and responsibilities of the company to monitor postings on social media, incident response plan, and eDiscovery requirements.

• **Training and Awareness Material Customization** – Through our experience in helping large, complex organizations educate their technical and nontechnical employees, KPMG brings a perspective to the development or modification of security awareness training to help educate employees on updated company policies and risks inherent in the use of social media. Our social media training services can be tailored to your needs, whether it is to be included within your organization’s security awareness training, or if you need training targeted to specific employee groups, such as Human Resources, Marketing, or IT.

• **Social Media Data Protection Automation** – Policies and education can serve as a foundation for protection of information shared via social media channels. However, in most instances, they stop short of helping companies fully manage associated risk. KPMG can assist with the selection, implementation, configuration, and ongoing monitoring of tools that automate adherence to corporate social media policies, including notifications and enforcement of business rules regarding sensitive data usage, and monitoring for potential data loss via social media channels.

Through these services, KPMG offers an ability to meet the needs of organizations as they attempt to tackle the risks associated with doing business in a social environment. We take a thorough, business-centric approach to identifying gaps across organizations’ social media landscape by developing improved business strategies, identifying opportunities for supplemental technology solutions and establishment of a thorough social media governance framework. As one of the foremost advisors on risk compliance and information security, KPMG brings an excellent set of credentials to help your organization prepare for the challenges associated with doing business in a social world.

---

**Contact us**

For more information about KPMG’s Social Media and Information Security Services, please contact:

**Greg Bell**
Principal, Global Lead Partner for Information Protection and Business Resilience
404-222-7197
rgregbell@kpmg.com

**Orson Lucas**
Manager, Advisory U.S. Information Governance Center of Enablement Lead
704-371-8159
olucas@kpmg.com

**Justin Weissert**
Manager, Advisory Information Protection and Business Resilience Services
412-232-1598
jweissert@kpmg.com

**H. John Hair**
Director, Advisory U.S. Social Media Governance Lead
312-665-3606
hhair@kpmg.com

**Sanjaya Krishna**
Principal, Digital Risk Consulting
212-954-6451
skrishna@kpmg.com

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International. 24203NSS
Due to auditor independence rules, certain aspects of these services may not be permissible for KPMG audit clients or their affiliates.