DHG | views

June 2015

Social Media and Its Impact on ERM

DHG Risk Advisory

ERM is a methodology for managing risk. It includes identifying a risk appetite, assessing risk, integrating risk management in daily decisions, and monitoring risks.

With its immense growth, size and impact, social media has been a double-edged sword to many organizations. Most businesses understand how social media platforms can help them enhance sales, marketing and customer service, remain relevant among competitors, improve recruiting, enable professional networking, strengthen the brand and boost communication with stakeholders. It has evolved into one of the pillars of business strategies for some organizations as it provides companies with additional data and consumer insight.

On the other hand, some companies have been hesitant to engage with social media due to fear of reputational risk, regulatory and legal concerns, loss of intellectual property and for many, the pure unknown. Moreover, companies forfeit the ability to own the conversation, as it is shared among users. Although, they might be able to influence the direction in which those conversations may go. The growth of social media will continue impacting enterprise risk management frameworks and create new challenges for internal and external stakeholders.

Key Stakeholders

+ Investors
+ Analysts
+ News Media
+ Customers
+ Community
+ Business Partners
+ Current Employees
+ Prospective Employees
+ Policymakers and Influencers

Risks and What Could Go Wrong:

Possible risks companies must consider when building social media into their ERM:

- **Reputational.** The social media response to negative events and news can open companies up to a lack of trust by consumers, lost sales, questions about legitimacy, no longer being seen as an employer of choice and being placed at a competitive disadvantage.
  - Bad news and press
  - Negative comments
  - Incorrect or inaccurate information about the company is posted
  - Company not responding real time to an issue
- **Regulatory, legal and compliance.** Every social media activity is discoverable and implications arise more easily and faster through the rapid sharing of social media content.
  - Inaccurate information
  - Proprietary information being improperly released
  - Plagiarism
  - Offensive content
  - Copyright laws
  - Defamation
  - Discrimination
  - Insider trading
  - Data being sold to advertisers
- **Information security.** Viruses, hackers and malware attacks can take advantage of vulnerabilities in companies' social media environment and lead to privacy breaches.
  - Weak passwords
  - Unsecure computers, servers and wireless networks
  - Location sharing
  - Selecting shortened URLs that direct the user to a malicious website
  - Little to no security software
- **Employment protocol.** This relates to both personal and professional use of social media. Employees can put the company at risk for privacy violations, reputational damage, competitive advantage and reduction in productivity.
  - Communication of work-related data
  - Personal social media accounts on work devices
  - Changes in hiring
  - Reduction in productivity
  - Mergers and acquisitions
  - Layoffs

Ways To Improve Your Governance

Control Environment:

- Develop a strong social media policy. A robust policy is visible to employees and articulates the company's stance on activity at the workplace, sharing company owned content, privacy cognizance, and what behaviors are acceptable.
- Reassess or build proper controls. Work with business segments and functional groups to identify, assess and monitor new risks.
- Ensure strong processes and procedures. With the reach and sharing capacity that social media holds, secure methods of actively deciphering and disseminating content must be established.

Training and Ownership:

- Get employees involved early and frequently. Training and educating employees on risk awareness and what is acceptable activity is the key to ensuring policies are understood and followed. Training must not stop at entry level or new employees. Senior leaders and executives should be briefed on new developments and best practices for the broadening engagement and setting an example.
- Allocate clear roles and responsibilities for internal departments affected by social media and maintain documentation. Social media does not reside in one department. Initiatives are jointly owned in compliance, legal, risk, marketing, IT, communications, public relations and human resources. Organizing a team or committee that paves the foundation for social media monitoring and strategy is critical.

Monitoring and Integration:

- Install dashboards and monitoring software for real-time analytics. These measurements provide senior management with quantifiable reporting metrics around source of traffic and shares. Monitoring conversations encompasses employee, shareholder, and external organizational activity.
- Build social media into Enterprise Risk Management programs. Social media has many touch points with a company's ERM strategy. Review the alignment with strategic objectives periodically. Anticipate regulatory changes on the horizon and build them into your strategy.
- Develop crisis communication plans and integrate strategy into business continuity processes. When an event exceeds the company's risk appetite, proper escalation procedures can mitigate risky outcomes.

DHG Risk Advisory Services
riskadvisory@dhgllp.com