Focus on information protection intensifies as market forces and regulatory disclosure requirements increase

Market forces such as those around the increasing use of social media,[1] the cloud,[2] the need to leverage and protect massive amounts of data proliferating daily, and the reputational risks that ensue from breaches have already moved cybersecurity higher on the corporate agenda.

Lately, dialogue in Congress and the most recent disclosure guidance issued by the Securities and Exchange Commission (SEC)[3] have underscored the importance of establishing and monitoring a robust information protection culture and strategy. Senate Commerce Chairman John D. Rockefeller IV who has long been a proponent of enhanced cybersecurity regulation commended the recent SEC guidance saying, "It will allow the market to evaluate companies in part based on their ability to keep their networks secure."[4]

This creates a delicate balance between disclosing so much information that competitive advantages may be lost and disclosing too little. Companies disclosing too little could fail to meet shareholder and regulator expectations, but worse, may find details of sensitive topics becoming part of the social media discourse before they can be reported to the board or SEC.

Considerations for companies and their boards:

- Does your organization have policies surrounding all the ways in which data is shared such as via different types of social media or cloud initiatives?
- Do the aforementioned policies consider third-party sourcing and other business partners subject to the policies?
- Has your organization reevaluated roles, reporting, responsibilities, and the need for subject matter experts in areas of dynamic change such as technology and new media as well as evolving information protection regulation?
- Are key compliance and monitoring programs as well as compliance reporting lines well aligned with evolving business plans in the rapidly changing environment?
- Do those accountable for IT risks such as the CIO, technology, or marketing groups provide regular, effective communication in business terms to the board across a common framework and reporting metrics?
- Do Enterprise Risk Management (ERM) plans incorporate IT risks and opportunities into strategic business decisions such as competitive analysis, new product launches through new media, or multinational growth (considering different privacy rules/cybersecurity risks, intellectual property rules by country)?

[1] "Social Media: Time for a Governance Framework," Mary Pat McCarthy and Sanjaya Krishna, *NACD Directorship*, September 2011.

[2] "Don't Forget the 'Offensive' Side of IT Risk," Mary Pat McCarthy and Steve Hill, *NACD Directorship*, June/July 2011.

[3] *Defining Issues: SEC Staff Issues Cybersecurity Disclosure Guidance*, KPMG LLP, November 2011, No. 11-58.

[4] "SEC Asks Companies to Disclose Cyberattacks," Jim Finkle and Sarah N. Lynch/ Reuters, October 14, 2011.

But the SEC guidance is not the end of the regulatory or legislative dialogue. Cybersecurity, and other data matters, continue to be a hot topic on the congressional agenda and are also reflected in a recent Executive Order on government-wide actions designed to reduce the risk of a future breach.[5] Other recent government initiatives illustrate an escalating interest in social media and other Internet tracking and data exposure.[6] For example, legislators seem intent on creating a "privacy bill of rights" and the Commerce department has developed both an Internet privacy paper and a task force which cites cloud computing as one of its areas of focus.

Board members rank the IT function as one of the top two functions most in need of organizational change over the next 12 months.

42% of board members indicated that over the next 12 months the IT function should modify either their skills, enabling technology, reporting or responsibilities as a result of the stresses of the complex legislative and regulatory environment.

The Impact of Legislative Changes on Business, Public Policy Business Initiatives KPMG LLP survey of board members, December 2011

IT strategies now have to account for new data needs, new media, as well as the impact of legislation on data needs and data use. Even the most sophisticated companies are recalibrating their IT governance model to create a more holistic view rather than use a more traditional siloed approach.

On the legislative front, the Dodd-Frank Act is creating new data needs stemming from the registration of additional investment advisers[7] and as the new Consumer Protection Bureau[8] establishes its data needs, sectors other than financial services that provide consumer financing may also be impacted. Additionally, one of the most discussed data drivers will likely be the health insurance and information exchanges required by healthcare legislation.[9]

Exchanges will store and transmit more private information to different business partners than ever before while dealing with enhanced HIPAA[10] enforcement. Even before the advent of these exchanges, large pools of data have been accumulated by employers who are monitoring employee wellness and other healthcare data. This practice generates similar information protection considerations especially when shared via new media.

[5] Both the House and the Senate are presently debating a bevy of related issues—including cybersecurity broadly, "do not track" proposals, and data breaches. In addition, the Obama administration issued an Executive Order October 7, 2011 governing sensitive information on computer networks following the work of a committee charged with a review of "policies and practices surrounding the handling of classified information, and to recommend government-wide actions to reduce the risk of a future breach" in the executive branch.

[6] The Commercial Privacy Bill of Rights is a topical example of a bill to help curb Internet tracking. One example of such tracking is portrayed in the *WSJ* article indicating that Facebook's many apps were found to be transmitting information about the users to advertising and Internet tracking companies. *WSJ Online October 18, 2010.*

[7] Under Dodd-Frank, most alternative investment managers will be required to register with the SEC by March 30, 2012, which will entail (among other things) enhanced disclosure requirements for filings made on Form ADV Part 24. "Dodd-Frank Act Will Transform the Investment Management Industry in the Coming Years," John Schneider, *Harvard Business Law Review Online*, July 2011.

[8] *Dodd-Frank: Beyond Financial Services*, KPMG LLP, September 2011.

[9] "Healthcare legislation" references the product of two bills: Patient Protection and Affordable Care Act (PPACA), Pub. L. No. 111-148, March 23, 2010, and Health Care and Education Reconciliation Act of 2010 (HCERA), Public Law No. 111-152, March 29, 2010.

[10] The Healthcare Insurance Portability and Accountability Act (HIPAA) adopts national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. Pub.L. 104-191, 110 Stat. 1936, enacted August 21, 1996.

In addition, social media is becoming a more broadly used method of communication and a key element of business strategy.[11] It involves two-way transparent communications in real time and can therefore rapidly create opportunities and risks in real time. For example, new product launches, customer complaints, and whistleblower "hot spots" can originate in social media sites. Recent whistleblower legislation[12] highlights the need to monitor and understand the impact of new real-time voices on brand and market position. Providing guidance to employees and vendors on how social media should be used, as well as understanding how they are used by customers and other external constituents to talk about the company is critical to establishing a comprehensive governance structure. This is especially true in light of the way evolving legislation and regulation is changing the risk profile.

> "If you can demystify social media, especially at the leadership level, and you can take that through the organizational structure and prepare your organization around that, then you can leverage the benefits that it brings."
>
> *Social Media in the C-Suite: Listening, Learning and Creating a Strategy from the Top Down, Knowledge@Wharton, October 12, 2011.*

> "Strongly governed organizations receive 20 percent higher return on assets." remarks Tina Nunno, VP, Gartner, Inc. discussing good IT governance practices. "CIOs with great governance create competitive advantage by embracing emerging technologies, innovation and, most important, the concept of calculated risk."
>
> *How IT Leaders Can Master IT Governance at Gartner PPM & IT Governance Summit 2011, June 13, 2011*

Despite legislative activities and relevance in the market, many executives are not comfortable with the current state of governance related to IT risks. In fact, cyber risk was cited as the second greatest systemic risk facing companies behind economic and financial risk, according to a recent KPMG Audit Committee Roundtable survey.[13] Only 10 percent of those board members surveyed felt that their company's strategic planning process is very effective in dealing with the pace of innovation and technology change in the business. And less than two- thirds felt they receive enough information from the right sources to adequately oversee IT risk.

Data-driven issues are changing the dialogue in the C-suite and the boardroom. Directors in leading companies are looking for a balanced discussion that looks at new opportunities as well as how to govern the associated risks. There is some concern that the technical tool discussion focused primarily on security risks may not provide the broader discourse needed to develop innovative market ideas or growth potential. Additionally, there is no substitute for a culture of information protection throughout the company supported by sustained training campaigns and modifications to existing communication protocols—including those communications amongst board members themselves.

[11] "Social Media: Time for a Governance Framework," Mary Pat McCarthy and Sanjaya Krishna, *NACD Directorship,* September 2011.

[12] *Defining Issues: SEC Adopts Final Rule for Dodd-Frank Whistleblower Provisions,* KPMG LLP, June 2011.

[13] ACI's Spring 2011 Audit Committee Roundtable Report, KPMG LLP, July 2011.

"The place to start is the governance structure," says Greg Bell, KPMG LLP principal, Information Protection. "Establishing a strategic, long-term view of information protection provides the company not only with protection but also a warning system capable of detecting potential conflicts as they evolve into different business needs and new types of enabling technologies such as social media, technology or cloud initiatives across an evolving business partner ecosystem. It is this warning system that provides the business decision agility and long-term protection."

As governance structures are reevaluated in light of new data needs, data sharing, and legislative concerns, organizations must assess whether they have the correct people, skills, processes, and technology in place to link information assets, data security, and business processes. Establishing a unified vision of an organization's information protection approach amidst the cacophony of new data needs, shifting regulation, and advancing technology is an immediate need—and long-term challenge. However, companies that develop a long-term view of data-driven impacts to their strategic business decision processes may be creating a clear advantage.

Governance over information protection: leading practices for a unified vision

- Use the governance structure to encourage a culture of information protection reinforced by incentives and penalties around compliance
- Establish communication protocols with common frameworks for elevating incident reporting including to risk committees and as necessary, the board
- Establish clear accountability keeping in mind the need to empower those held accountable to respond quickly to incidents
- Establish standardized policies and procedures for all significant information-sharing initiatives supported by strong monitoring programs including approval processes around the launch of new IT enabled programs
- Evaluate roles, responsibilities, and subject matter experts in areas of dynamic change and when or where specific regulations or jurisdictions demand specific skill sets
- Refresh training, change management, and awareness programs on a real-time basis as new data sharing needs arise
- Collaboration between marketing and IT departments is critical to the proper alignment of information protection risks and opportunities
- Incorporate IT needs generated by market forces (new media, cloud, regulation) into strategic decisions analysis focusing on risk as well as innovation (examples might be a new product launch using new media or multinational growth complicated by differing laws on privacy and cybersecurity)
- Reevaluate the impact of IT strategies on the company's ERM profile
- Understand how information acquired through social-mobile initiatives/applications is being collected, shared, stored, and utilized to assess the impact on the company's electronic discovery, records retention, and regulatory compliance obligations
- Utilize monitoring technology to understand whether protected information may be inappropriately making its way into social media

Contact us

Kapila Anand
KPMG LLP
Partner-In-Charge, Public Policy Business Initiatives
T: 312- 665-5094
E: kanand@kpmg.com

Greg Bell
KPMG LLP
Principal, Information Protection
T: 404-222-7197
E: rgregbell@kpmg.com

kpmg.com