Protecting Corporate Assets and the Brand in a Digitized, Global Environment

Technology and globalization are reshaping the business landscape—enabling companies to extend their reach, real-time connectivity, and brand visibility in markets around the world. Yet, this digitized, global environment also makes it more challenging than ever to protect corporate assets and maintain the integrity of the organization and its reputation—"the brand."

Indeed, with supply chains, networked technologies, and strategic growth opportunities tightening the interconnection of businesses and markets—and cyber attacks growing more sophisticated and persistent every day—companies are increasingly vulnerable to fraud, misconduct, and compliance risk. Coupled with increased government regulation and stepped-up enforcement, this new compliance and data-intensive world poses a host of business challenges with implications for corporate strategy, operations, compliance, and security.

"Corporate reputations have always been fragile, but they've never been so vulnerable," noted one director attending KPMG's Fall Audit Committee Roundtable Series – *The Business Integrity Challenge: Protecting Corporate Assets and the Brand in a Digitized, Global Environment*. "When our risk management discussions focus specifically on reputation risk, the conversation takes on a dramatically different tone. What are the biggest risks to the brand? How are they being managed? And do we, as a board, need to change what we're doing in light of all the new risks and changes taking place out there?"

Engaging 1,500 directors and governance professionals in 27 cities, the dialogue and survey findings from KPMG's roundtable series shed light on critical governance challenges posed by digitization, globalization, increased government regulation, and stepped-up enforcement, including how these four "game changers" are impacting the board's oversight practices. Does the audit committee—so often the default "risk committee"—have the time and expertise to oversee major risks beyond its core responsibilities?

Four game changers are reshaping the business and risk environment and heightening reputation risk.
For many businesses and boards today, the convergence of digitization, globalization, increased government regulation, and stepped-up enforcement has brought reputation risk to the forefront. Maintaining the integrity of the organization and its brand—including protecting corporate assets and ensuring the right ethical/compliance culture—is a growing challenge.

Aside from financial reporting risks, most directors and senior management surveyed at the roundtables cited "cyber breaches—including theft of customer data, intellectual property, and nonpublic information"—as the top risk to their company's reputation, followed by "regulatory compliance" and "failure of the company's ethics and controls (tone at the top, culture, and excessive risk taking)." One in four said they aren't satisfied that the board understands the status of the company's efforts to manage these top reputational risks.

© 2013 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. NDPPS 139815

Top Risks to the Brand

Aside from financial reporting risks, what are the most critical risks to your company's reputation? (Select three)

Cyber breaches
74%

Regulatory compliance risks (other than FCPA and other anti-bribery laws)
69%

Failure of ethics/control environment (tone at top, excessive risk taking)
55%

Supply chain risks
40%

FCPA and anti-bribery compliance
26%

Board oversight failure
25%

Managing Reputational Risks

How satisfied are you that the board understands the status of management's efforts to manage the company's top reputational risks?

Satisfied
76%

Not satisfied
24%

Cyber Security Reports

How frequently does your board or audit committee receive reports from management regarding cyber security, including the status of management's efforts to protect the company's critical digital assets?

At least quarterly
20%

Twice a year
17%

Annually
33%

Infrequently or not at all
30%

Cyber security is a top concern as companies and boards struggle to keep pace with the risks and challenges posed by digitization. Cyber terrorism, protection of IP, data privacy and security, and brand reputation in the social media world are growing concerns as value continues to migrate online, digital data becomes more pervasive, and malevolent actors—including state-sponsored hackers—become more sophisticated.[1]

As highlighted in the roundtable discussions, corporations are expected to be more open than ever before, and employees expect access to corporate networks through the same mobile devices they use in their personal lives. In social media communities—Twitter, Facebook, LinkedIn, etc.—the company "no longer controls its brand." Supply chains are increasingly interconnected, and a company's defense against attacks often hinges on the security policies of its partners and customers.

Cyber security was cited by most roundtable attendees as their company's top reputational risk; yet, directors expressed concern about cyber-risk updates provided by management: While nearly 40 percent of attendees said their board or audit committee receives management reports on cyber security at least quarterly or twice a year, nearly one-third said such reporting happens "infrequently or not at all."

While many companies have dramatically strengthened their cyber security capabilities in the last several years, surveys indicate that many boards and senior management teams have not yet undertaken key governance activities to help manage cyber risk—such as identifying the company's most critical information assets, conducting enterprise-wide vulnerability assessments, addressing cyber security at the most senior levels, and clarifying the role of the board and its committees in overseeing cyber risk.[2] As a number of roundtable attendees noted, "cyber security insurance" is becoming more common to cover the potentially significant costs related to cyber-breaches.

Globalization is a double-edged sword, extending the company's reach and elevating its exposure. Strategic growth opportunities, complex supply chains, emerging technologies, social media, and other forces continue to tighten the

[1] McKinsey Quarterly, June 2011

[2] Carnegie Mellon University CyLab Report – *Governance of Enterprise Security, 2012*

© 2013 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. NDPPS 139815

interconnection of business and markets worldwide. This globalized environment poses a host of risks across the enterprise—strategic (market entry, local competition, and exposure to political and economic instability); operational (finding and deploying talent, and managing the extended organization); cultural (translating the company's commitment to ethics/compliance into the local business culture); and compliance (including FCPA and other anti-bribery laws).

Of those roundtable participants whose companies have international operations, most pointed to the "complexity of managing the extended organization" and "legal/regulatory compliance (including FCPA and other anti-bribery laws)" as their top international concerns. "How are you vetting your business partners?" asked one roundtable attendee. "What about your suppliers' suppliers? You really need to look at the entire extended organization." Government relations and the handling of procurement issues were also highlighted as key international issues requiring the board's attention.

Noting the proliferation of anti-bribery laws and initiatives around the world, one director said his board's discussions "aren't limited to FCPA anymore. We operate globally, so we talk about anti-bribery risks in all shapes and jurisdictions." Others emphasized the importance of incorporating compliance into the company's enterprise risk management activities, with clear lines of responsibility. "Who owns it? And is the board providing the right level of oversight?"

The vast majority of those roundtable attendees whose companies operate internationally said they are satisfied that the board "has a good sense of the company's compliance culture—the tone at the top and in the middle."

Increased government regulation and stepped-up enforcement continue to raise the stakes on compliance risk. From FCPA and other anti-bribery laws around the world, to the sheer volume and complexity of new regulations at every level, to industry-specific compliance "hot spots," navigating the global regulatory environment—and helping to ensure the effectiveness of compliance programs—is a formidable challenge. As one director noted, "the goal is to get compliance right, without getting buried by it."

Roundtable discussions highlighted ways that audit committees are getting their arms around the compliance challenge, including understanding the company's significant compliance risks and hot spots, and whether appropriate controls are in place; ensuring robust (global) compliance training programs; understanding how the effectiveness of compliance programs is measured; and ensuring regular reports to the audit committee/board on compliance program assessments and issues.

Monitoring policies impacting a country's economic and investment climate, e.g., policies on revenues, spending, deficits, and debt – and maintaining a watch list of legislative/regulatory developments potentially affecting the company's compliance efforts and business plans were also cited as important practices.

Are audit committee agendas reaching a tipping point? "Our audit committee agenda is exploding," noted one director, echoing a majority of roundtable attendees (55%) who said it is becoming "increasingly difficult or unrealistic" for the audit committee to oversee the range of risks on its plate. Thirteen percent said their audit committee "does not have the time or expertise" to oversee major risks beyond financial reporting.

Most roundtable attendees said their audit committee has oversight responsibility for IT risk, legal/regulatory

International Risks

What risks associated with your company's international operations pose the greatest threat to your company? (select two)

(Respondents with international operations)

Complexity of managing the extended organization
63%

Legal/regulatory compliance, including FCPA and other anti-bribery laws
53%

Finding and deploying talent
36%

Intellectual property protection
31%

Business interruption
9%

Monitoring Global Compliance Culture

How satisfied are you that your board has a good sense of the compliance culture – the tone at the top and in the middle?

(Respondents with international operations)

Satisfied
82%

Not satisfied
18%

© 2013 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. NDPPS 139815

Risks on Audit Committee's Plate

In addition to financial reporting and control risk, and oversight of external and internal auditors, for which categories of risk does your audit committee have primary oversight responsibility? (Select all that apply)

Risk management process
59%

Legal/regulatory compliance (other than FCPA/anti-bribery)
56%

IT risk, including cyber security
56%

FCPA and anti-bribery
39%

Global operations
25%

None of the above
6%

Audit Committee's Time & Expertise

Are you satisfied that your audit committee has the time and expertise to oversee the major risks on its agenda in addition to carrying out the audit committee's core oversight responsibilities?

Yes
32%

Yes – but increasingly difficult/unrealistic
55%

No
13%

Value of Additional Board Committee

Would an additional committee—such as a compliance committee, risk committee, or technology committee—help improve the effectiveness of your board and/or audit committee?

Yes
38%

No
50%

Board has already formed an additional committee
12%

compliance, and/or operational risks, as well as the company's enterprise risk management process. Given the audit committee's workload, roundtable attendees emphasized the importance of concise meeting materials, prioritized agendas, and quality discussion (versus listening to presentations).

Whether audit committees have room on their plates for additional oversight responsibilities will depend on the company's size and complexity, whether it operates outside the U.S., and the scope of the audit committee's current responsibilities. Yet, all boards should be considering whether the current allocation of oversight responsibilities among its committees is appropriate. More broadly, is the board recalibrating its oversight in light of digitization, globalization, and the new legal/regulatory environment? Does the board have the right composition? Have the board's governance and oversight processes changed—and advanced—as the business environment has become more complex? Is there a need for an additional committee such as a risk, technology, or compliance committee?

While 14 percent of roundtable attendees said their board has already formed an additional committee ("technology" and "risk" committees are the most prevalent), others were divided on whether an additional committee would improve the board's effectiveness.

Fall Roundtable Locations

Atlanta
Boston
Charlotte
Chicago
Cleveland
Dallas
Denver
Detroit
Fort Lauderdale
Houston
Kansas City
Los Angeles
Minneapolis
Nashville
New York
Orange County, CA
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland, OR
San Francisco
Seattle
Short Hills, NJ
Silicon Valley
St. Louis
Washington, DC

About KPMG's Audit Committee Roundtable Series

Launched in 1999, the Audit Committee Roundtable Series is hosted by KPMG's Audit Committee Institute (ACI) in approximately 30 cities every spring (May/June) and fall (November/December). Highly interactive and panel-driven, the roundtable sessions bring together audit committee members, directors, senior executives, and leaders in governance to discuss challenges, emerging trends, and leading practices affecting the oversight of financial reporting and related risks. For more information about the Roundtable Series and resources and events offered by ACI, visit auditcommitteeinstitute.com, or contact ACI at 1-877-KPMG-ACI or auditcommittee@kpmg.com.

© 2013 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. NDPPS 139815