NACD Directorship
January – February 2016 Issue

Andrea Bonime-Blanc is CEO of GEC Risk Advisory. She is an advisor on global strategic governance, integrity, and compliance matters to boards, executives, investors, and advisors.

Effective Risk Governance

The top five strategic risks: reputation, cybersecurity, leadership and culture, compliance, and resilience.

To write about emerging risk in a vacuum—without a specific industry, sector, location, or focus in mind—might be considered a fool's errand. That said, it is possible to single out several ongoing and emerging strategic risks that most boards should consider as they exercise oversight. The top strategic risks for 2016 can be boiled down to five, though there are other serious strategic risks, such as geopolitical risk, that should be on a board's radar screen as well. There is another emerging risk, however, that is perhaps the most fundamental of all: the risk that an entity lacks strategic risk governance.

Reputation

Called by *The Economist* the "risk of risks" in 2007, reputation risk is now broadly recognized globally as a strategic risk by boards and executives. The reason? It affects stakeholders' expectations and behaviors. Reputation risk is an amplifier risk that layers on or attaches to other risks—especially environmental, social, and governance (ESG) risks—adding negative or positive implications to the materiality, duration, or expansion of the other risks for the affected organization, person, product, or service.

The ongoing scandals at Volkswagen, FIFA, Petrobras, and Takata present vivid examples of how reputation risk, when layered upon another risk gone wrong that an organization ignored or actively perpetrated (e.g., consumer fraud, corruption, product defects), can amplify, accelerate, and worsen the damage to the company and its stakeholders. The opposite is also true: companies that understand their risks and have the right mitigation strategies and programs in place can avoid major crises, build resilience, and even create competitive advantage.

Cybersecurity

In an October 2015 study, risk management firm Marsh found that reputation risk associated with cyber risk is the number one strategic concern of boards and executives globally. Cybersecurity continues to evolve into one of the true mega-risks of our time. It is a multifaceted, constantly morphing threat that can present an existential risk to any company or entity.

Cyber risk isn't primarily about technology. It is first and foremost about governance requiring proactive involvement by the board in companies and organizations of all sizes. In 2015, many cases of cyber-risk management gone wrong were disclosed, and we will likely see more this year, including breaches at small- and medium-size businesses as well as other entities and sectors not previously targeted.

One important takeaway from a 2015 Conference Board research report on emerging practices in cyber-risk governance is the recommendation of a triangular approach that includes close and coordinated board oversight, CEO/C-suite strategy, and implementation by frontline business and operations executives in charge of cybersecurity.

Leadership and Culture

Two of the biggest risks—which no enterprise or strategic risk management program takes into account because of their inherently complicated, personal, and potentially embarrassing nature—are those of leadership and culture. Leaders set the tone. When they set the wrong tone through negative, overly aggressive, unethical, or illegal behaviors, they can create distress that hurts stakeholders and possibly even dooms their organizations. Leadership risk can also create a more pervasive high-risk culture, which may foment risky behaviors by the rest of management and deeper into the organization. Think of Enron, WorldCom, and Lehman Bros. as extreme examples of leadership and culture risk gone terribly wrong.

The unfolding cases of Volkswagen, FIFA, and Petrobras underscore this issue, as does the recent conviction of Massey Energy's former CEO, who presided over a dangerous culture of treating health and safety violations as the cost of doing business, leading eventually to the deaths of 29 coal miners.

What can boards do to mitigate this risk? The buck stops with the board in terms of reviewing candidates for the chief executive role and the ongoing performance of the CEO. It is no longer enough to measure a CEO's performance by financial results alone. Boards should use more holistic metrics, providing not only financial but also non-financial and cultural measures to understand the full effect of the CEO's and management's performance. And they need to keep a close eye on the tone and culture set by the CEO and top management.

Compliance

Compliance with laws and regulations continues to be a grow-

ing bucket of risk. The expansion of not only national but international coordinated law-enforcement investigations and prosecutions—regarding corruption, money laundering, fraud, tax evasion, and human-rights abuses, among others—should underscore that in this age of big-data analytics, surveillance, and transparency, law enforcement, too, is having its day in the sun.

How do boards deal with this issue? There is a growing body of good and best practices adopted in many industrialized and emerging nations of what an effective organizational ethics and compliance program looks like.

Boards must ask management what is being done in the company, demand proof of such a program, and maintain a proactive stance, which includes receiving periodic reports from the chief ethics and compliance officer. Companies with these programs have a much better opportunity to reduce the impact of the risks and scandals that might come, to lower the fines and costs of such risks, and even to gain a competitive advantage relative to their peers.

Ineffective risk governance occurs when the board is not fully equipped to gauge and oversee enterprise and strategic risk management.

Resilience

Resilience traditionally refers to the trifecta of protective programs of business continuity, crisis management, and disaster recovery. Resilience risk occurs when an organization does not have one or more of these three pillars of resilience, thereby exposing itself to greater loss of life, injury, or damage to persons, assets, and reputation.

What should boards do? In addition to understanding and encouraging the creation of an effective enterprise and strategic risk management program, they should demand to see and test the company's crisis management, business continuity, and disaster recovery plans. Today, some of the more advanced and proactive boards have agreed to be part of tabletop crisis management (especially relating to cyber risk) for this very reason.

A Fundamental Emerging Risk

What is ineffective risk governance? It occurs when a board is not fully equipped to gauge and oversee enterprise and strategic risk management. In today's increasingly complex, high-risk world, this is disturbing for many companies. Considering that most boards are still made up almost exclusively of financial and operational (former) senior executives and rarely include someone with deep and broad experience with governance, risk, and compliance, this is a troubling but reparable flaw.

Effective strategic risk governance, on the other hand, occurs when the board is properly equipped to oversee risk, including the following.

Board Makeup:

- There are one or more board members that have a rich, diverse, or highly sought-after background or experience in governance, risk, and compliance relevant to the company.
- The board may have more than an audit committee to oversee non-financial risk management and has considered or created a separate risk (and/or compliance) committee.

Risk Oversight:

- There is a clear understanding of the company's enterprise and strategic risk management profile.
- The right questions are being asked of management and of the heads of risk, compliance, and other key functions.
- The type of information and reporting that reaches the board from risk management is robust, periodic, useful, and focused primarily on the company's strategic risk.

Role of the CEO/C-suite:

- The C-suite is fully and periodically informed on enterprise and strategic risk issues.
- The frontline risk management leadership and team are effective, interconnected, and properly resourced to deal with the risks of the enterprise.
- Both are interconnected with the board in a synchronized way in terms of risk reporting.

Role of the board in building resilience:

- The board understands and requires the existence of business continuity, crisis management, and disaster recovery programs at the company.
- The board participates from time to time in crisis management exercises.

Like last year, 2016 will present a host of challenges to companies, some of which are difficult to predict. But if the proper and balanced risk governance approach is created—wherein the board, the C-suite, and the risk management team have a coordinated and integrated approach to enterprise and strategic risk—the blows will be lessened, and the opportunities for resilience and growth potentially greater.

—Andrea Bonime-Blanc