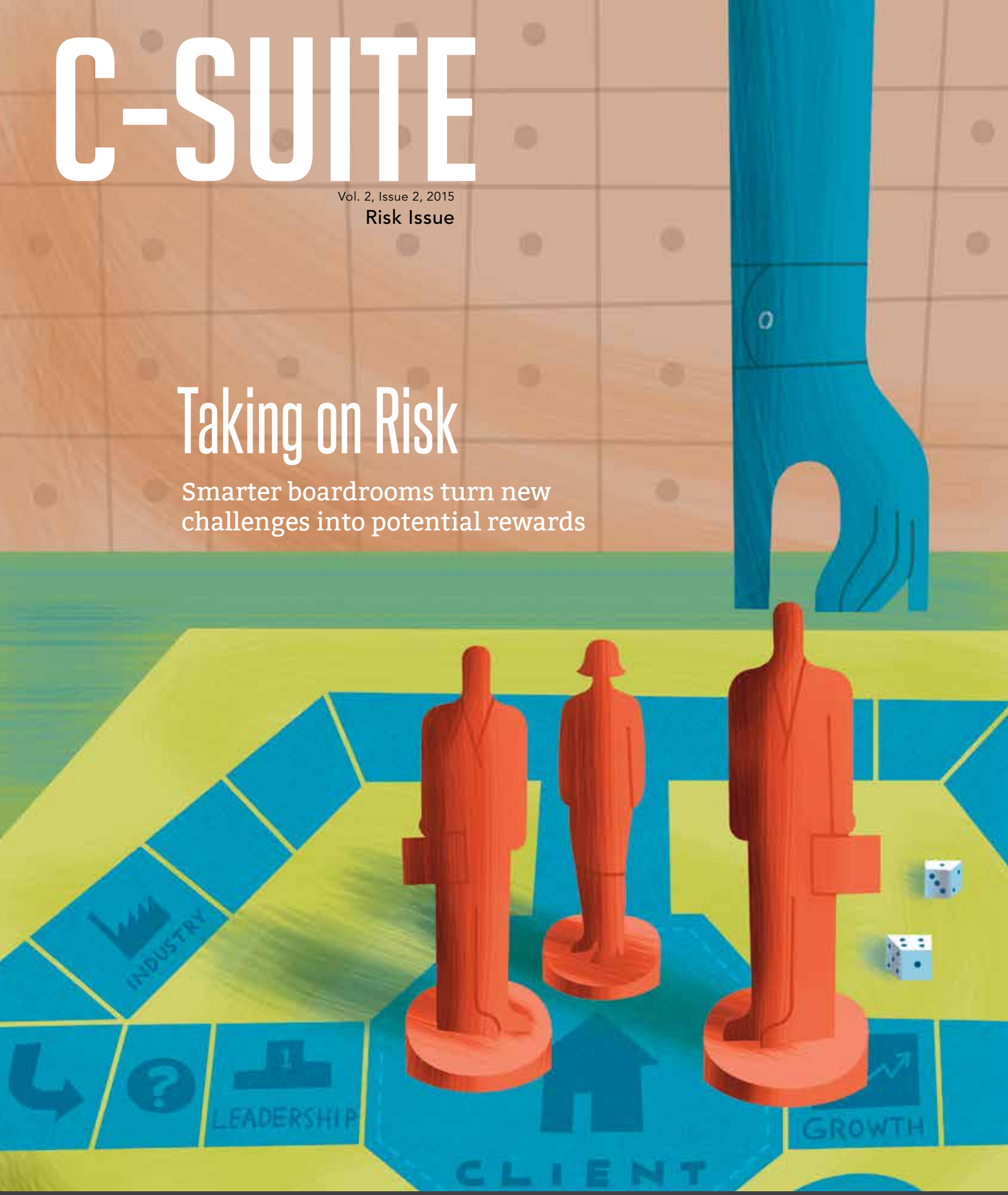
# C-SUITE

Vol. 2, Issue 2, 2015
Risk Issue

# Taking on Risk

## Smarter boardrooms turn new challenges into potential rewards




Considering the universal ballot

Safeguarding against cyber attacks

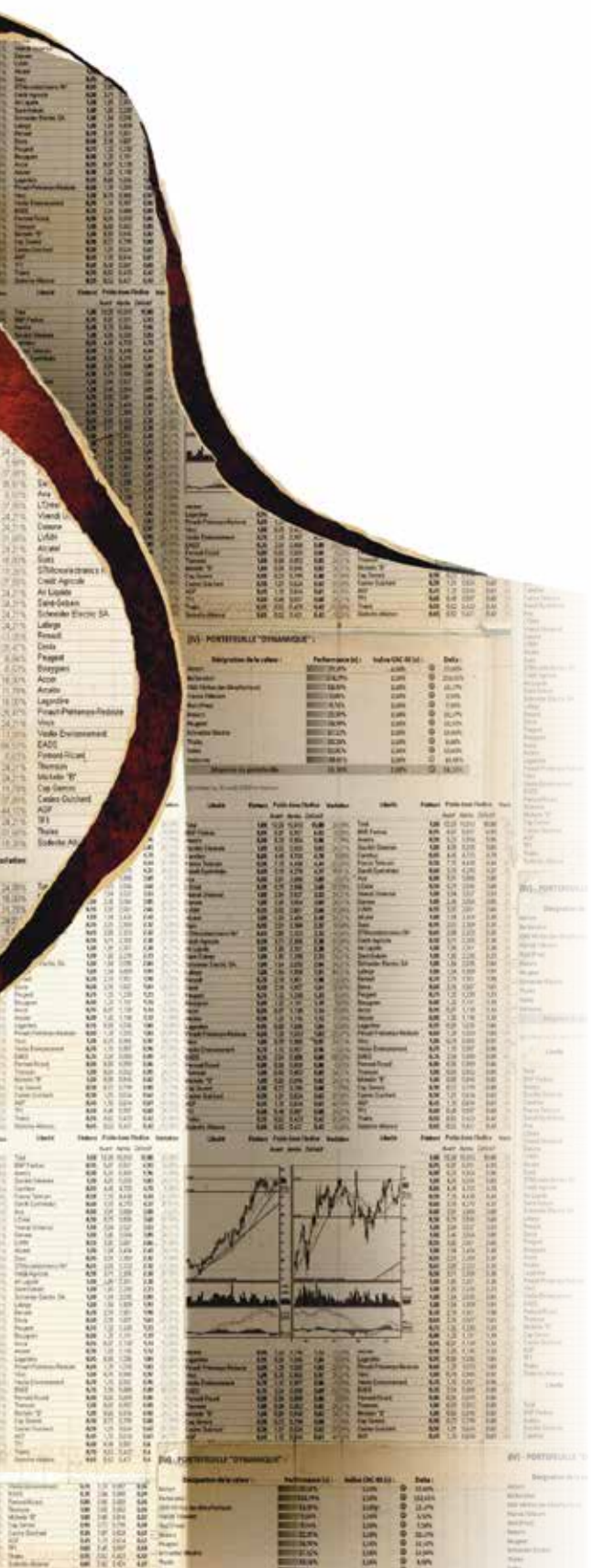
What will be the biggest risk facing boards in 2016?

Overcoming risk on critical projects

Interviews with Sabastian Niles and Suzanne Vautrinot

EQUILAR

# What Will Be the Biggest Risk Facing Boards in 2016?



KELLY WATSON
*Partner and National Service Group Leader*
KPMG LLP'S RISK CONSULTING SERVICES

Kelly Watson is a Partner and the National Service Group Leader of KPMG LLP's Risk Consulting Services, which helps organizations to transform risk and compliance efforts into competitive advantage by applying a risk lens to corporate strategy to improve risk intelligence and decision making, protect financial and reputational assets, and enhance business value. Kelly previously served as Office Managing Partner of KPMG's Short Hills, N.J. office, where she was responsible for leading market development efforts across all functions in New Jersey. She has over 27 years of global auditing and advisory experience serving the pharmaceutical, biotechnology and industrial product industries.

Boards are facing an unprecedented number of new risks, in addition to those already crowding their agenda. The specific risk factors fall into three primary categories—strategic, operational and external risks or "signals of change." Boards have always been very focused on strategic risk as they evaluate threats to corporate strategy. For operational risk, which entails known risks such as compliance, information security and supply chain risk, boards heavily rely on management to prioritize and report those requiring board attention. Given the severity of some operational risks, boards challenge management to ensure that these risks are appropriately managed.

Board members seem to feel the most angst over unknown risks. Some of the largest risk factors often are found in external risks, with which most boards are intuitively familiar. However, based on the complexity, inter-relationships and speed at which some signals of change impact the organization, this evaluation often requires additional scrutiny and formalization to ensure management and board alignment. These risks could include disintermediation, geopolitical factors, demographics, changing customer behavior, etc., and can greatly impact the company's strategy, business model and operations, let alone its reputation and/or ultimate survival. Boards are challenging management to evaluate the impactful signals of change and isolate them from the noise through deep and ongoing analysis.

How are these external risks being addressed and monitored given that the exact nature of those risks constantly change? And, is the company culture one that understands and respects these risk such that there is timely identification and escalation of issues? With the intense scrutiny and personal liability that boards face, the "what we don't know and therefore can't have oversight of" are top of mind.

JOSEPH A. HALL
*Partner*
DAVIS POLK

Joseph Hall is a member of Davis Polk's Corporate Department and head of the firm's corporate governance practice. He works on the full range of capital markets transactions, and advises public companies and regulated entities on corporate governance and financial regulatory compliance. He is a frequent speaker on topics of corporate governance and SEC compliance.

Mr. Hall began his career at Davis Polk in 1989. Between 2003 and 2005 he served at the U.S. Securities and Exchange Commission, ultimately as Managing Executive for Policy under Chairman William H. Donaldson. As a member of Chairman Donaldson's senior management team, Mr. Hall assisted in directing the Commission's policy-making and enforcement activities.

We recently had another reminder—as if one were needed—about the threat companies face from data security breaches and other cyber threats, whether targeted at their own networks and products or those of companies they do business with. In August, prosecutors in New York and New Jersey joined the SEC in announcing insider trading charges against hackers inside and outside the United States who broke into computer servers at widely-used wire services, and used the embargoed information to trade ahead of market-moving corporate announcements. The damage caused by the 2014 Sony and 2013 Target data breaches—not to mention more recent revelations about the hacking of personnel records at the U.S. Office of Personnel Management, or the 1.4 million vehicles recalled after exposure of an entertainment system security flaw that may have left the vehicles vulnerable to remote commandeering—underscores both the scale and the pervasiveness of this multifaceted threat.

The spate of alarming news has directors asking what the board's role should be in protecting the company from cyber threats, and many boards have arrived at the conclusion that cybersecurity risk oversight is a fundamental component of the board's oversight of risk management generally. There are good reasons for this view. No matter the industry, a company touched by a cybersecurity breach or flaw can be exposed to heavy liabilities—spanning public relations nightmares, loss of customers, product recalls, shareholder litigation and regulatory investigations. And we have seen enough widely-publicized examples of these consequences in the last five years that corporate boards are on notice of the rapidly metastasizing risk facing their companies.

While large numbers of boards don't appear to be setting up stand-alone committees to handle cybersecurity oversight, boards are thinking about where in the existing committee structure these risks should be addressed—for example, whether the audit committee, which often has initial responsibility for risk oversight, should be tasked with cybersecurity risk oversight as well. Different companies will take different approaches, but most boards will want to understand:

PHILIPPE COURTOT
*CEO*
QUALYS

As CEO of Qualys, Philippe Courtot has worked with thousands of companies to improve their IT security and compliance postures. Philippe received the SC Magazine Editor's Award in 2004 for bringing cloud-based technology to the network security industry and for co-founding the CSO Interchange to provide a forum for sharing information in the security industry. He was also named the 2011 CEO of the Year by SC Magazine Awards Europe. He is a member of the board of directors for StopBadware.org, and in 2012, he launched the Trustworthy Internet Movement, a nonprofit, vendor-neutral organization committed to resolving the problems of Internet security, privacy and reliability.

- Which members of the management team own cybersecurity risk
- What is being done to identify and scope cybersecurity risks; for example, whether management is using the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or another industry-specific framework
- How management ranks the various cyber threats faced by the company
- What financial and employee resources and insurance coverage are available to mitigate cybersecurity risk
- What policies and training have been instituted around cybersecurity risk
- What testing and other programs are employed to assess and mitigate cybersecurity risk
- The details of management's game plans if the company is exposed to a cybersecurity event

PATRICK HAGGERTY
*Partner*
PAY GOVERNANCE

Pay Governance®
Advisory Services to Compensation Committees

Patrick Haggerty is a Partner in the New York office of Pay Governance. He has over 18 years of experience working with companies on a wide range of executive compensation issues. Clients for whom Patrick serves as the Board or Management advisor include major U.S. companies in the energy, healthcare, financial services, medical devices and pharmaceutical industries. His experience extends to working with public and private companies as well as assisting companies with transactions such as acquisitions, spin-offs and IPOs.

Among the biggest compensation-related risk factors facing corporate boards in 2016 will be establishing short- and long-term incentive goals that are selected and calibrated to motivate behavior while driving corporate results and company total shareholder return (TSR). This issue will be more transparent in 2016 due to the SEC's proposed pay for performance (P4P) disclosure rules.

At a high level, the proposed P4P disclosure rules require that registrants include:

- A standardized table in proxy statements that includes a new calculation of compensation actually paid (CAP), compensation from the current summary compensation table, and TSR for the company and a peer group.
- A narrative description and/or graph to describe relationship between CAP and company TSR, and also between company and peer TSR.

Unfortunately, as proposed, the P4P disclosure rules measure executive equity awards at vesting, where any alignment or misalignment with end-of-year TSR is inherently coincidental, or even false. This mismatch may provide a hazy or even coincidental understanding of pay for performance linkage at best. We expect that many companies will not show alignment of pay and performance in the P4P disclosure table.

Since executive compensation disclosure is subject to close scrutiny by media, proxy advisory firms, investors and regulators, it will be critical that the narrative and/or graphic explanation clarify pay for performance alignment.

Cybersecurity continues to be an imminent risk for large companies. Hackers have become more sophisticated in terms of gaining remote access through networks, luring people to give them credentials or even targeting individuals. Furthermore, the needs of the business to communicate more and more electronically have enhanced, and the attack surface has exponentially increased.

The truth is that large corporations have much bigger challenges than smaller companies because they've already invested in larger infrastructure. Small businesses—and even medium-sized businesses—can easily outsource to a security provider. Meanwhile, many large companies don't have a good idea of how many web locations they have, how many servers, how many portals. They have to do the cartography of their enterprise, put in firewalls and they need a lot of security products to cover everything. Actors just need to compromise one thing to enter into the network, and companies have to defend every door.

Even two years ago, the board was not very involved in cybersecurity measures. There was no real technical understanding coming out of the era that the cloud was "dangerous." But when they saw $100 million security breaches, lawsuits and brand issues, the board got concerned.

It's going to take some time for large companies to migrate to the cloud, and they need a security network that is compatible. But the main thing for the board is to be aware of it, and take it very seriously to ensure that the company can describe what the strategy is to secure the enterprise. The other thing is that you cannot look at cybersecurity independently of IT. They are absolutely together, and at some point the CIO should be responsible for security and provide metrics to roadmap what the company is doing to measure improvement.

RAJEEV KUMAR
*Senior Managing Director*
GEORGESON

Georgeson

Rajeev Kumar is a senior managing director of research at Georgeson. His extensive knowledge of and research on complex corporate governance issues are quintessential components of Georgeson's service offering. Rajeev specializes in advising clients on issues of executive compensation, proxy contests, M&A transactions and complicated shareholder proposals, among other proxy matters. Using his in-depth knowledge of corporate governance issues and the policies of proxy advisory firms and institutional investors, he advises Georgeson clients on their investor engagement strategies and shareholder outreach efforts.

In his more than 20 years of experience, Rajeev has held various positions in the areas of corporate governance, mergers and acquisitions, corporate development and strategic business planning and analysis at Pegasus Communications, Teligent and Sprint, among others.

In 2016, we will see a continuation of challenges, with activist threats, cybersecurity, proxy access and regulatory developments representing some of the major issues. While the main risk factor a board might face in 2016 will be unique based on a company's situation, if speaking generally, then the biggest governance risk would be the failure to recognize and address the deficits in its board composition. As companies evolve and new challenges in the changing landscape emerge, the boards may get stale. Board changes resulting from replacement of a departing director are not enough. The boards must proactively examine their composition to eliminate any potential vulnerabilities, fill any skill gaps and enhance the expertise and experience required for the many challenges that a board will likely face. Among the likely challenges, long-tenured directors are frequently targeted by activist shareholders. There is an increased focus and demand for greater board diversity. Companies with board composition-related concerns are more likely to be targeted with the proxy access proposal. Shareholders have increased expectations from the boards and are looking for greater direct engagement to understand how the directors think, interact and the skills they bring to the table.

The boards need to view the issue of board composition not just with the perspective of risk but also one of opportunity. By establishing a regular process of board refreshment, the boards would be better able to manage risks and allow themselves greater opportunity to focus on the more important task of creating shareholder value.