CG NEWS UPDATE

IS YOUR BOARD FUTURE-READY?

June 5, 2019 By Jim DeLoach

Most organizations face an uncertain future that will be shaped by a mix of exciting market opportunities and emerging threats. With unrelenting, continuous, and disruptive change the norm, board members must ask themselves a fundamental question: "Are we future-ready?"

The term "future-ready" captures an action orientation with a focus on an important question: Does the board's composition, focus, and agenda position it to best serve the company? Is the board ready to represent its stakeholders and achieve sustainable, long-term growth and profitability? Below are eight suggestions for preparing to be a future-ready board.

1. Engage in big picture, out-of-the-box, bold, and disruptive strategic thinking.

Enough agenda time and focus should be allocated to engage in future-oriented thinking. Future-ready boards consider how to integrate disruption considerations into setting strategy; challenging strategic assumptions; exploring "what if" questions; reviewing scenario analysis results; considering mergers and acquisitions and partnering opportunities; and reimagining the company's position within the value chain. The future-ready board is resourceful in integrating outside perspectives into the dialogue with management to stimulate fresh points of view about market developments and trends and their strategic implications—particularly when there are shifts in strategic context. The prepared board is committed to continuous education and networking both in and outside the industry while striving to learn as fast as the world is changing.

1. 2. When warranted, challenge the CEO and management team to take a long-term focus in a constructive manner.

The focus of a future-ready company is on balancing the entrepreneurial drive to create enterprise value with the appropriate prudence to protect enterprise value. The right mindset is to achieve this balance consistent with the board- and CEO-approved risk appetite,such that neither the emphasis on creating value nor on protecting it is too disproportionately strong relative to the other. To support this balance, the future-ready board should consist of a diverse group of independent directors that is prepared to challenge key

CG NEWS UPDATE

assumptions underlying the strategy and business model, evaluate management and company performance, exercise appropriate due diligence, and ask the tough questions when necessary—all with the objective of supporting the CEO in delivering long-term shareholder value.

3. Ensure management focuses on appropriate sustainability objectives while delivering acceptable financial results.

The future-ready board is mindful of the developing interest in the impact of environmental, social, and governance (ESG) issues on long-term value creation, and ensures that management keeps ESG in focus when formulating strategy and policy. There are evolving business cases around ESG performance and reporting, voluntary initiatives and disclosures by competitors, and the specter of possible regulation, legislation, and proxy battles in specific ESG areas such as climate change. All fuel the future-ready board's focus on integrating sustainability considerations into the strategy-setting process.

3. 4. Foster diversity in skills, experience, and perspectives in the boardroom, C-suite, and management ranks.

Starting at the top, emphasis on diversity in director selection and in the C-suite facilitates desired diversity outcomes within the executive ranks and throughout the organization. Gender diversity and pay equity are important priorities in many industries. The future-ready board understands that a diverse organization is likely to be better positioned to attract and retain top talent, expand into new markets, gain and sustain competitive advantage, and maintain a talented executive bench that facilitates succession plans

4. Think and act digitally

The future-ready board has access to the expertise and experience needed to understand how digital disruption can affect the organization's business model, value proposition, and industry. For example, it has an eye on the demographic, social, and technological trends affecting the workplace and ensures that management has processes in place to evaluate their implications to the company's labor model and make adjustments as necessary. It encourages management to align the velocity of key decision-making processes to the speed of change. It also encourages management to be immersed in digital business concepts, building digital ecosystems and leveraging digital hyperscaling platforms to facilitate

CG NEWS UPDATE

rapid growth. It ensures that management digitizes new and enhanced products and services to strengthen customer engagement and deploys digital technologies to improve operational performance and information for decision-making.

6. Focus on innovation performance.

The future-ready board allocates time for discussing the company's innovation strategy and culture. It insists on supporting this dialogue with appropriate, innovation-specific metrics. The scorecard should tell the full story of how the innovation and growth strategy is performing relative to competitors, customer feedback, return on investment targets, and the effectiveness of the company's innovation culture.

7. Foster effective communications with shareholders.

The future-ready board places a premium on communicating with shareholders in proxy reports, at annual meetings, and through other venues in accordance with the securities laws on relevant topics (e.g., CEO evaluation and succession, executive compensation, the board's nomination and selection process, strategic direction, and emerging issues).

8. Nurture a flexible, adaptive, resilient, and ethical culture.

Future-ready directors ensure that the incentives and reward systems in place for management are in line with the company's risk appetite, and that the organization is sufficiently adept and agile in navigating change in a complex, changing business environment. They work closely with the CEO to ensure that the company's culture is aligned with the enterprise's strategy and core values, the mood in the middle is aligned with the tone at the top, and any gaps between the current and desired cultures are addressed in a timely manner.

While not exhaustive, the above suggestions represent a good start at improving the board's future readiness. There is, of course, the inevitable "blocking and tackling" around board oversight of such matters as executing strategy, establishing accountability for results, monitoring performance and preserving reputation and brand image. But these oversight activities alone will not deliver future readiness.

Ref.
https://blog.nacdonline.org/posts/is-your-board-future-ready

CG NEWS UPDATE

CYBERSECURITY MUST BE CONSIDERED A TIER-1 BUSINESS RISK

May 30, 2019 By Dustin Owens

"Cybersecurity risks pose grave threats to our investors, our capital markets, and our country."

This statement was issued by the US Securities and Exchange Commission (SEC) in February 2018, as part of its guidance on public company cybersecurity incident disclosure responsibilities. As we look back on this statement today, we see that more companies have embraced cybersecurity as part of their enterprise risk management (ERM) discipline.

And yet, many still have not: Research from Optiv found that only 18 percent of enterprises score "high" in aligning business objectives with security program management. This indicates that cybersecurity often functions outside of corporate business processes, which makes it incredibly difficult—if not impossible—to effectively mitigate cybersecurity-related business risk.

Why is this? Simple: it is hard to think of another enterprise risk that has advanced as quickly as cybersecurity.

Litigation, succession planning, competitive threats, business stability…all of these risks are timeworn and well understood topics. Cybersecurity, on the other hand, is a party crasher—a threat that, even just 10 years ago, did not seem as serious as other traditional business risks to most companies. While there were some major data breaches back then, they never lived up to the negative hype that accompanied them; in those days, businesses suffering breaches saw everything from stock prices to customer traffic and brand sentiment return to normal very quickly. This is not the case today, because the cybersecurity risk landscape is profoundly more complex.

Consider the risk landscape of 10 years ago. Smartphones were still early in their adoption curve, with about 16 percent of mobile phone market share. Cloud computing was in its infancy (Microsoft Azure, for example, was first announced at the end of 2008). Regulations were more scattershot and loosely enforced than today, and ransomware was a fringe cyberthreat (a status that would dramatically change in 2009 when Bitcoin became operational, creating the ideal ransom-fulfillment platform).

CG NEWS UPDATE

From an ERM perspective, cybersecurity was a secondary consideration. Having a data breach in the headlines was an annoyance—and usually the chief information security officer (CISO) or, if there was no CISO, the IT staffer in charge of security, would pay for it with his or her job—but, in general, it was a survivable incident.

Today, however, data breaches and other incidents have far more damage potential than they did 10 years ago due to the increased causticity of attacks (ransomware, nation-state theft of intellectual property, etc.) and the prevalence of novel computing platforms (mobile, cloud) and trends (digital transformation, Internet of Things, etc.) that open companies to new attack vectors. New regulations that have real teeth (GDPR being the ultimate example) are a direct response to these changes. All of the above factors have conspired to make cybersecurity a tier-1 enterprise risk—and for some companies, cybersecurity is the most dangerous source of risk.

Companies that do not realize this are imperiling their competitive position. In fact, if they do not include cybersecurity as a top-tier risk consideration, they stand to make business decisions that may seem sound, but that are potentially disastrous from a cybersecurity perspective.

For example, diversifying supply chains is generally considered a sound business practice. However, if the cybersecurity team is not involved with this process from the beginning, adding supply chain partners also creates brand-new on-ramps for cyberattackers to enter the corporate network. So, while an executive may gain kudos in the boardroom for improving supply chain stability, the company's security organization must play catch-up at a mad pace to secure the enterprise attack surface that was just expanded. Put it all together, and the perceived reduction in risk (a more resilient supply chain) was actually just a transfer of risk (new cybersecurity vulnerabilities).

An increasing number of companies are bringing CISOs into their regular board meetings and treating cybersecurity as a tier-1 business risk. However, there remains a distressing number of companies still living in the world of 10 years past. If those companies hope to be in a position to discuss risk 10 years from now, this needs to change.

Ref.
https://blog.nacdonline.org/posts/cybersecurity-tier-1-risk