The Russia-Ukraine war: Boardroom considerations

March 10, 2022

As the Russia-Ukraine war unfolds—and recognizing that the implications for companies will vary by sector and geographic reach—a number of issues will be front and center for boards to weigh and business leaders to monitor, including:

The well-being of employees and those affected by the war. The war's impact on lives—including upwards of 2 million Ukrainian refugees[1]—has rippled worldwide, compounding the anxiety and toll that two years of pandemic-related hardship has taken on workers. Understand how the company is supporting employees in Ukraine, Europe, and around the world. For companies with a significant employee base in Russia, deciding whether to cease operations in light of reputational risk and pressure will no doubt be difficult.

The company's public position. Expectations for companies/CEOs to make public statements condemning the Russian government's invasion (as many companies have done) and activist demands for divestitures in Russia and/or assistance to Ukrainian refugees reinforces the importance of having a clear internal process for determining and articulating the company's public positions—on this and other major crises—with consistency. Also monitor for potential reputational issues posed by disinformation via major social media platforms and understand how the company is viewed by its stakeholders and the broader public in the context of the war and evolving narrative. Proactively communicate with key investors about the rationale for, and implications of, the company's position(s).

Cybersecurity. As recommended by the Cybersecurity and Infrastructure Security Agency (CISA), all organizations should be "shields up"—adopting a heightened posture when it comes to cybersecurity and protecting their most critical assets.[2] The increased risk of cyber threats—whether retaliation for sanctions or in response to a company's public support for Ukraine, increased hacking and ransomware activity, or the impact of malware "released into the wild"—should be prompting fresh tabletop exercises, a review of business continuity plans, and assessment of third-party/vendor vulnerabilities. Consider the adequacy of the company's cyber-related talent and resources in the event of a major breach, disruption, or failure of critical infrastructure, as well as the company's connectivity and coordination with law enforcement. Monitor regulatory and/or legislative developments impacting cybersecurity incident reporting and disclosures.[3]

Risk-related disclosures. Risks posed by the Russia-Ukraine war may need to be addressed in the company's risk-factor disclosures—e.g., if the business depends on imports/exports to or from Russia; if Russia, Ukraine, or affected countries have a material customer base; or if the company's key third-party vendors are affected by the war.

---

[1] Joanna Sugden, "Two Million People Have Fled Ukraine, Says U.N.," Wall Street Journal, March 8, 2022.

[2] www.cisa.gov/shields-up

[3] KPMG Regulatory Alert, Cybersecurity: SEC Proposals for Public Company Reporting, Disclosures, March 10, 2022.

Macroeconomic, trade, and supply chain issues. The impact of the war on the global economy will continue to be multidimensional and interrelated—from increased energy and food costs to supply chain disruptions; slowed economic growth for Europe, the U.S., China, and globally; and continued stock market volatility amid heightened risk aversion among market participants. Firms with foreign clients could see slower global demand for goods and services if the war persists for an extended period. Concerns about inflation have already prompted interest rate hikes by central banks—with implications for capital allocation decisions—although future interest rate hikes may be more measured than previously thought given concerns of slowing growth. Scenario analysis and planning for persistent inflationary pressure in the near term, particularly from rising commodity and input costs, should be a top-of-mind consideration for many firms. Trade restrictions and compliance with sanctions and export controls—including understanding counterparty and third-party risks, along with associated controls like Restricted Party Screening—should be front and center.

Geopolitical volatility and the company's risk profile. Reassess the company's global risk profile in the context of shifting geopolitical dynamics—within Europe and around the world. These and other geopolitical uncertainties highlight the critical importance of robust scenario planning, including spending time envisioning the future and challenging the company's strategic and risk-related assumptions and making scenario planning an ongoing, iterative process. More fundamentally, has the speed and impact of the war surfaced any critical gaps in the company's risk management process or crisis readiness—or the board's risk oversight—that need to be addressed?

Implications for U.S. policy priorities. Monitor the direction of U.S. policies that could impact the company and/or its operations—including any shifts in defense, ESG, sanctions, energy, cybersecurity, and cryptocurrency policies and spending, among others.

Board oversight. As many companies learned firsthand during the COVID pandemic, the depth and frequency of reports to the board on how the company is responding to a crisis should strike a balance between keeping the board sufficiently informed without unduly burdening or distracting management. The Russia-Ukraine war and its wider geopolitical implications also reinforce the importance of having geopolitical expertise in the boardroom, whether on the board, in management, or from a third party.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC—which includes the KPMG Audit Committee Institute and close collaboration with other leading director organizations—promotes continuous education and improvement of public and private company governance. BLC engages with directors and business leaders on the critical issues driving board agendas—from strategy, risk, talent, and ESG, to data governance, audit quality, proxy trends, and more. Learn more at kpmg.com/us/blc.

Contact us

kpmg.com/us/blc
T: 1-800-808-5764
E: us-kpmgmktblc@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia