Webinar with the author - Thursday, July 21, 2022
See end of report for details

July 19, 2022

RISK AND RESILIENCE AS A COMPETITIVE ADVANTAGE
Where Boards Can Invest To Prevent Business Disruptions

By Atul Vashistha

Volatility is a grim reality in business today, and the last two-and-a-half years have demonstrated just how impactful risk events across the globe can be to local supply chains. While supply chains worldwide were still experiencing prolonged pandemic-related production shutdowns and port closures, the Russia-Ukraine conflict compounded those impacts with a new source of disruptions. Today, an enterprise's survival requires the ability to anticipate, effectively respond to, and learn from a crisis rapidly – otherwise known as resilience – and requires agility to pivot to avoid disruptions and maintain continuity. With today's unprecedented and complex to predict future supply chain disruptions and other material risks, it's clear why achieving resilience is top of mind for most organizations.

Organizations continuously work toward achieving greater resilience, and when they do, they gain a competitive advantage that stems from an increased ability to embrace change at all levels. Organizations develop products and services that better fit conditions brought about by long-term environmental changes. The quest to build resilience benefits both sides of the ledger – on the one hand, resilient companies can better withstand the buffering that comes when unexpected threats emerge quickly. On the other, firms that are more resilient over time develop a suite of offerings that better fit the direction of change.

Over the last 24 months, headlines have forced organizations to reexamine how they confront risks. Today more than ever, avoiding disruption requires proactive vigilance and, where needed, agile intervention. Unfortunately, most enterprises rely on legacy risk management practices that fail to support the nimble decision-making and fast actions needed to avoid disruptions. Instead, agility requires an always-current view of supply chain health and early warning when the supply chain risk landscape changes.

What is Organizational Resilience?

British Standard 65000:2014 defines organizational resilience as "the ability of an organization to anticipate, prepare for, respond and adapt to everything from minor everyday events to acute shocks and chronic or incremental change. Resilience is a goal, not a fixed activity or state, and is enhanced by integrating and coordinating the various operational disciplines that the organization might already be applying."

ISO defines organizational resilience as: "the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper."

Ref: BS 65000:2014, Guidance on Organizational Resilience, 2014.
ISO 22316, Security and resilience - Organizational resilience - Principles and attributes; 2017.

Leading enterprises are updating their approach to risk management. A more holistic approach enables them to advance resilience across the organization. Instead of focusing on surviving the latest crisis, enterprises can learn from and anticipate disruptions and turn enhanced resilience into their competitive advantage.

RISK MANAGEMENT AND THE ROLE OF THE BOARD

With rising business disruptions, boards are increasingly held accountable for an ever-expanding risk landscape. The traditional board focus on financial risks and requirements first expanded to include cybersecurity vulnerabilities and now incorporates a host of reputational and ESG risks. Beyond shareholder's interests and regulator's requirements, boards must also consider the impact of corporate actions on a wide range of stakeholders from current and future employees and customers to partners and even individuals in the communities in which their firms operate.

Unfortunately, many enterprises are ill-prepared. According to an EY Global Board Risk Survey, only 21% of boards said their organization was prepared to respond to an adverse risk event from a planning, communications, recovery, and resilience standpoint. In its recently released "2022 The State of Risk Oversight" report, The AICPA and North Carolina State University found that only 33% of respondents had a complete Enterprise Risk Management (ERM) process. [1]

THE INADEQUACIES OF CURRENT RISK PRACTICES

Why do current practices fail to support the agile decision-making and quick actions required to avoid disruptions and achieve resilience?

To begin with, most procurement and risk management programs offer a limited view of risk that is typically overly focused on financial and cyber risks. Today's disruptions originate from a much more comprehensive range of risks. The most obvious example is the pandemic, which was initially viewed as a location-based epidemic. That risk, however, quickly morphed to impact operations on a worldwide basis. Organizations with narrow risk apertures fail to look beyond financial and cyber risks and are missing a view into a large portion of their third-party and supply chain risk landscape. Limited risk perspectives constitute a significant barrier to resilience – organizations can't take action to mitigate a risk they never saw coming.

Also, current due diligence and ongoing risk practices rely on periodic, point-in-time assessments where data may become stale quickly. In the early days of the pandemic, many enterprises could not ascertain their third parties' health and risk status. Why? Because they were forced to rely on months or even years-old assessments. This stale data was unreliable as it failed to provide a current view during such a volatile time. An excellent example of these issues includes the bankruptcy filings of firms like Golds Gym, Frontier Communications, Diamond Offshore Drilling, and J Crew, whom all stated the lack of demand at the onset of the pandemic as their demise. At the same time, none of these point-in-time assessments gave any insights as ports and cities closed and opened and closed again as infections spread.

Excessively siloed risk management programs leave organizations without an integrated enterprise-wide view of risk. When risks are viewed in isolation, barriers to information flow result in missed early warning signals. The Kaseya ransomware attack in early 2021 illustrates this point. In the months leading up to the attack, there were early indicators of increased cyber susceptibility in non-cyber-related risk domains. These early indicators included operational risks such as employee attrition and negative employee ratings as well the location risk as software development positions were outsourced to Belarus, considered a high-risk location with known governance and cybersecurity risks. Resilient enterprises remove barriers to information flow and consistently encourage cross-functional collaboration to ensure organization-wide awareness of early warnings and markedly improved preparedness.

Risk management continues to be manual and resource inefficient at most enterprises. As a result, risk teams spend valuable time on surveys, documentation, news, and risk reviews that could be automated, freeing up resources to spend time on the most critical risk mitigation efforts that require human intervention. Today leading enterprises are leveraging these automation capabilities to improve their team's risk management efficiency and effectiveness at preventing disruptions while increasing resiliency.

What Boards should do:

- Verify that management has a complete understanding of third-party and supply chain risk exposures
- Verify that organizational structures enable risk detection and mitigation processes across internal silos and corporate hierarchies
- If not already in place, establish a Risk Committee that reports directly to the Board to ensure adequate oversight on efficiencies and effectiveness of risk and resilience practices
- Include risk and resilience reporting as a mandatory agenda item at each board meeting

---

INVESTMENTS IN MODERN RISK AND RESILIENCE PRACTICES

To ensure sound risk management practices and a resilient enterprise, Boards must fully understand the strategy, practices, and outcomes of the enterprise's risk and resilience programs. They should begin by benchmarking their risk practices and evaluating their risk management structures. Evaluations should consider the need for:

Full-Spectrum Risk Intelligence

Today third-party and supply chain disruptions arise from a broad range of risk events. Your enterprise needs to widen its risk aperture to a full-spectrum view that includes operations, compliance, ESG, Nth party, and location risks.

Continuous Monitoring with Real-time Risk Intelligence and Alerting

Stale assessment data is unable to support proactive risk mitigation strategies. Resilience requires access to a current view of their third party and supply chain risks. Recent advances in automation enable moving beyond periodic risk assessments to continuous monitoring, once a practice highly concentrated in cyber security organizations. Now enterprises can access an always current view of the third party and supply chain health and risk status. Additionally, continuous monitoring provides real-time risk alerting when the risk landscape changes.

Boards should be aware that typical automated negative news services often overwhelm internal risk teams with noise and false positives, forcing them to spend valuable time identifying items that pose material risks to their organization. Alternatively, modern continuous monitoring services leverage machine learning and data science along with automation to accurately identify risks and issue real-time alerts with actionable insights to enable early warning and proactive risk actions. With the right risk management structure in place, this early detection combined with preparedness and collaboration builds efficiency and resilience across the organization.

Automation Across the Risk Management Lifecycle

In recent years, enterprises have increasingly leveraged software to send data collection requests and track risk mitigation actions by human teams. Unfortunately, these risk management software investments are underutilized as they continue to be based on manual periodic assessments and leave large portions of risk management as time-consuming manual processes. Technology today enables automation of many of these manual processes, including risk identification and repetitive risk mitigation actions, leaving risk teams to focus on only the most critical risk mitigation steps that require human intervention. Risk management automation can enable procurement agility, proactive risk mitigation, and accelerated program savings.

Questions a Board should ask management:

- Are our organization's procurement and risk management processes overly focused on cyber and financial issues or do they take a broader risk approach? How can the board be comfortable that all relevant risks are being monitored and that emerging risks are identified before they impact performance?
- Is our organization over-relying on periodic assessments for due diligence and risk management? Which risk domains have continuous monitoring and real-time intelligence?
- Is our organization's risk management process siloed or do we enable an integrated approach?
- Does our organization leverage a negative news reporting service? If so, does excess noise in the solution unnecessarily increase the workload for our team?
- What is the level of automation in our risk management lifecycle? Could increasing automation improve our productivity and effectiveness?

FURTHER INVESTMENTS IN RESILIENCE

Resilience is an increasingly important competitive differentiator. The Board's attention to and investment in resilience can significantly accelerate improvements to enhance this competitive differentiation.

In a recent article on building supply chain resiliency, McKinsey & Company shared how building longer-term resilience can create stability and help stave off future disruptions. Suggestions include creating a "digital twin" of a company's operations to simulate how a product or service will perform before it's implemented and creating "what if" scenarios to test and mitigate weaker parts of the supply chain. Scenarios should be tested in the field, either for testing disaster recovery or business continuity, to help prepare the organization for disruptive events. To build the most realistic scenarios, enterprises require an accurate, real-time Master Vendor List (repository) that captures their vendor population. Creating a complete repository can help identify opportunities to remove redundancies, make more efficient use of disaster recovery vendors, and identify opportunities to consolidate work at fewer vendors while (often) significantly increasing efficiencies. Enterprises can generate these simulations through a risk and resiliency operations center (R^2OC).

The R^2OC functions include acting as a listening post – proactively staying ahead of emerging and cascading risks by continuously monitoring for changes across the enterprise's entire risk landscape, assessing potential risk impact, identifying and assigning risk mitigation actions, executing risk mitigation actions that can be automated, tracking incident resolution, and identifying risk trends.

Unlike past crisis response teams assembled reactively to respond to a single incident, a well-functioning R^2OC is proactive. It's an ongoing entity built into the enterprise risk management structure and staffed with specialized, dedicated resources. An effective R^2OC establishes a continuous capability that enables end-to-end risk management, from risk identification to risk management and mitigation.

What boards should consider when investing in resilience:

- Ensure that an enterprise-wide resilience-building strategy is in place and is adequately documented and resourced
- Ensure that an integrated, enterprise-wide risk scorecard exists and that it is updated and made available to the Risk Committee and the Board
- Allocate resources and instruct management to evaluate the establishment of an R^2OC

Citation:

[1] 2022 The State of Risk Management, AICPA -NC State, June 2022, page 15

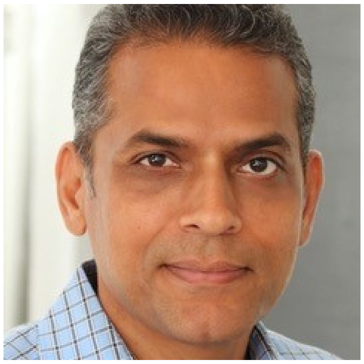
Sources:

EY - Global Board Risk Survey
McKinsey – Supply Chains: To Build Resilience Manage Proactively
Supply Chain Brain - Why Leading Enterprises are Implementing Risk Operations Centers
Security Magazine – The Way Forward with Risk Operations Centers (ROC)
Supply Wisdom – The Need to be Solid as a ROC (Risk Operations Center)
Forbes – The Future of Risk Management is Automated
Harvard Business Review – Five Traits of Resilient Organizations

ABOUT THE AUTHOR

Atul Vashistha
Chairman and CEO, Supply Wisdom

Atul Vashistha is recognized globally as a leading expert on supply chain risk and global business services. He has authored three best-selling books: The Offshore Nation, Globalization Wisdom, and Outsourcing Wisdom.



Atul is the Founder and Chairman of Supply Wisdom. Founded in 2017 as an early warning service for preventing business disruption risk, today, Supply Wisdom® is the market-leading patented supply chain and third-party risk and resilience intelligence solution.

Atul serves on boards on IAOP, Cozera, and Shared Assessments. He also serves as a board member on the US Department of Defense Reserve Forces Policy Board. He has also recently served as Vice-Chair for the US Department of Defense Business Board.

UPCOMING EVENT - This Thursday!

Featuring Atul Vashistha (Author of this Board Risk Report)

Risk Management: Gaining a Strategic Advantage and Instilling a Key Discipline at the Board Level
Thursday, July 21, 2022
10:00am – 11:00am ET via zoom
CLICK HERE TO REGISTER

Join **Women Corporate Directors**, the **Board Risk Committee**, and **Supply Wisdom**, for a panel discussion on best practices and guidance on the different types of risks facing organizations today, the importance of taking a holistic view of cascading and converging risks, incorporating risk management and oversight as a key discipline in your organization at all levels, leveraging your risk program as a strategic advantage, and restructuring how the board addresses these risks.

- **Catherine A. Allen, (MODERATOR),** BRC Founder & Chairman of the Board; WCD Greater New Mexico Chapter Member
- **Ana Dutra**, Director, CME Group, Amyris, First Internet Bancorp, CarParts.com, Elkay Manufacturing Company, Latino Corporate Directors Association; WCD Chicago Chapter Member
- **Shelley Leibowitz**, Director, Morgan Stanley, Elastic N.V., BitSight & Supply Wisdom
- **Laura Oliphant**, Managing General Partner, Serendibite Partners; Director, Aehr Test Systems & BE Semiconductor Industries N.V.; WCD Silicon Valley Chapter Member
- **Atul Vashistha**, Chairman & CEO, Supply Wisdom

__The Board Risk Report__ is the periodic publication of the BRC. __SUBSCRIBE NOW__ to receive complimentary world-class risk management practices delivered directly to your inbox.

WHO WE ARE

The Board Risk Committee (BRC) is the foremost thought leadership peer council for board risk committee members and chief risk officers. The BRC is a nonprofit, non-competitive, trusted place for the exchange of ideas, strategies, and best practices in enterprise risk oversight. We advocate for having risk committees of boards, where appropriate, and for educating board directors about enterprise risk. The BRC aims to foster more effective risk management and board oversight. The BRC is affiliated with The Santa Fe Group (SFG) and Shared Assessments (SA). SFG is a strategic advisory company providing expertise to leading corporations and other critical infrastructure organizations in the area of risk management. SA is the thought leader and provider of tools, education and certifications in the third party risk management space. *The Board Risk Report is the periodic publication of the BRC.*

Contact:
Catherine A. Allen, Founder, Chairman, Board Risk Committee, cathy@santa-fe-group.com
Ellen Dube, Executive Director, Board Risk Committee, ellen@boardriskcommittee.org