ISSUE 131

BOARD PERSPECTIVES: Risk Oversight

OPERATIONAL RESILIENCE GETS A MAKEOVER IN THE "NEW NORMAL"

Churchill said he strived "to foretell what is going to happen tomorrow, next week, next month, and next year — and to have the ability afterwards to explain why it didn't happen." His acknowledgment of the futility in predicting the future is especially apropos today as markets transition to the eventual "new normal."

The business model is akin to a finely tuned machine requiring the coordination of multiple components to deliver value to customers according to a company's brand promise. Business models vary by industry. For example:

- A manufacturer's model combines a robust supply chain, an accessible labor pool, cutting-edge innovative processes, efficient facilities and equipment, and access to power, water and other necessary resources to produce quality products at competitive prices.
- A bank's business model might emphasize critical third-party providers, differentiating skills and competencies, and proprietary systems to enable superior customer experiences.
- An e-commerce retailer's model leverages supplier partnerships, efficient channels, world-class logistics and distinctive branding to offer a compelling value proposition to consumers.

Unless an organization has an effective response plan, the absence or ineffective functioning of any of these components compromises the business model's viability. A loss of one or more components can take away the advantages of the model's underlying cost structure, the ability to produce or deliver products, and the capacity to provide essential services and/or accessibility to customers. Herein lies the crux of operational risk, or the risk that one or more scenarios impair the business model's effectiveness in fulfilling customer expectations and realizing acceptable returns.

protiviti®
Face the Future with Confidence

The COVID-19 pandemic has proven to be an object lesson on how severe this risk can be. Many were unprepared for an event that literally shut down major segments of the economy and even whole industries dependent on the gathering and concentration of people. Widespread failures of supply chains and third-party providers[1] and almost complete cessation of demand for products and services in some industries are unforgettable experiences that many might have regarded as implausible before the onset of the crisis.

The pandemic experience has served as a reminder that, in today's interconnected global marketplace, most companies are boundaryless due to their tight coupling with upstream suppliers and providers and downstream channels to reach ultimate end users. The concept of an extreme but plausible event becomes more pervasive when these dependencies extend, for example, as far upstream as third- and fourth-tier suppliers. Furthermore, the determination of "plausibility" when assessing extreme events continues to evolve as their frequency, severity, velocity and persistence increase.

But COVID-19 is just one example of a resilience event that stops the show. There are others, such as a cyberattack or catastrophic event. The velocity of such events varies. Whereas companies could see pandemic risk on the horizon charging toward them like a gray rhino, cyberattacks can occur suddenly and without warning.

As scenarios previously considered "implausible" were jolted into the "plausible" category — in effect, shifting probabilities assigned to tail-risk events closer to the mean — the question arises: What is the board's role in overseeing operational resilience post-pandemic? Below we offer several considerations for directors:

Learnings from the COVID-19 experience should drive advancements. There has been much emphasis on continuous learning during the COVID-19 experience to understand what went well and what did not go well. The pandemic's severity offers powerful lessons for companies to consider and apply to facilitate an effective response plan should another pandemic or equally severe catastrophic scenario occur. Boards should encourage this review and request a summary of actions that management plans to take because of it.

Concentration risk warrants close attention. While the term "concentration risk" is most often used in financial services to refer to exposures within a bank's asset portfolio arising from concentration to a single counterparty, sector or country, it also applies to other industries.

Geographic concentrations of critical assets, significant operational exposure to a geographically specific event (including sovereignty risk and regional conflicts), the concentration of information assets with outsourced functions, reliance on sole suppliers of critical raw materials and components, dependence on major customers for business, and other factors specific to a company's business model can create concentration risk.

For example, what if major customers were to fail, major customer contracts were not renewed, or major customers were to consolidate? Directors should be aware of these risks and, when they exist, ask management whether the specific concentration risk has been weighed against the cost and ability to recover within an appropriate time frame from an extreme but plausible event.

A virtual environment enhances resilience. The pandemic has accelerated workplace redesign in most organizations. Companies able to virtualize their processes have been more successful during the pandemic lockdown than those unable or unwilling to do so. Going forward, there is an opportunity to reimagine work processes to ensure the highest form of resilience possible,

[1] For example, a McKinsey survey of senior supply chain executives from across multiple industries and geographies indicated that 73% encountered problems in their supplier base, and 93% of respondents indicated that they plan to increase the level of resilience across their supply chain; see "Resetting Supply Chains for the Next Normal," July 21, 2020: www.mckinsey.com/business-functions/operations/our-insights/resetting-supply-chains-for-the-next-normal?cid=other-eml-alt-mip-mck&hlkid=fcba4c6a9dcc43a98273ecd1b4da4388&hctky=1368724&hdpid=3c3b6fa7-b102-490d-acd3-6380ab54b8e2.

which distributes the workforce, continues remote work arrangements, and supports a hybrid model that combines remote work with work physically performed in an office environment. The objective is twofold — accommodate the "new normal" workplace and contribute to increased operational resilience in facing catastrophic events that restrict workforce mobility.

Technology can be leveraged to increase resilience. As noted above, companies able to operate their business virtually have provided an object lesson on the power of technology to facilitate resilience. Also, while most companies use the cloud, there are still quite a few that do not fully exploit its unique benefits. The cloud offers a scalable ecosystem, where damage to or the loss of operation of any single component of that ecosystem would not have a significant effect on the company's overall operations. Therefore, the cloud can contribute to the efficient deployment of the technologies that enable a virtual environment and improved operational resilience.

The right factors facilitate response readiness assessments. Directors should ensure that management is asking the right questions when assessing exposure to extreme but plausible scenarios. The first is which critical business model functions, services and ecosystem components are most affected by the scenario? With respect to each scenario, what is:

- The velocity or speed to impact — that is, can the loss of key functions, services and ecosystem components occur without warning (e.g., a power outage)?
- The persistence of the impact, the duration of time before the loss of the functions, services and ecosystem components can be addressed, and the "headline effect" regarding the organization's attempts to recover?
- The extent of the company's agility and readiness in responding to the event?
- The magnitude of uncompensated risks the company faces due to the loss of the component (e.g., loss of revenue stemming from downtime of services, permanent loss of customers, or the emergence of health and safety issues)?

The likelihood of occurrence is not a prime consideration in this assessment. The focus is on what management will do when the event occurs.

Operational resilience intersects risk and crisis management. Every director and CEO faces the specter that, no matter what they do, there will always be the possibility of an unforeseen disruptive crisis occurring for which there is no playbook available. But this reality should not stifle efforts to plan and prepare for disruptions. Just as a crisis is a severe manifestation of risk, crisis management is the natural follow-on to risk management.

Rapid response to sudden, unexpected events depends on the enterprise's preparedness and response plans. Building a reliable crisis management capability is a management imperative for scenarios with a high-reputation impact and velocity. A world-class response to a persistent crisis is vital to the company's ultimate recovery and preservation of its brand image. Operational resilience assessments focused on the factors mentioned above can help identify areas where preparedness is more critical.

The board needs to be more focused on resilience. Now that we've experienced the worst pandemic in a century, directors should pay more attention to operational resilience going forward. With disruptive change the norm, it is necessary to be agile and adaptive.

The board should understand and offer input on the operational resilience strategy, including the identification of functions, services and ecosystem partners defined as critical to the execution of the business model. The board should request that it be notified promptly when an event occurs that is likely to require public or regulatory disclosure or that meets specified criteria — for example, "close

calls" such as a nearby hurricane or an attempted cyberattack that could have adversely affected an important business function or service. When reportable events are brought to the board's attention, directors should also understand and advise on management's strategy for improving resilience.

There are different views as to how granular the board's focus on operational matters should be. But there should be general agreement as to the organization's targeted recovery time for an important business service or process that guides the assessment of resilience plans. Directors should also gain confidence in the company's operational resilience team and with their line of sight into the team's activities.

Operational resilience is a strategic imperative. Directors should inquire about the scope of resilience planning at the companies they serve to ensure that it encompasses an end-to-end extended enterprise view of the value chain that looks upstream to suppliers and third-party providers, and downstream to channels and customer relationships. These business ecosystem partnerial relationships are just as crucial to the business model's execution as the organization's internal processes, personnel and systems. Evaluation of operational threats, therefore, should be directed toward understanding the company's resilience in addressing any of these key links in the chain and whether the time frame to recover is acceptable in sustaining the operation of the business model.

This comprehensive view is important. According to Gartner, business continuity management and organizational resilience programs are not keeping up with digital transformation initiatives and emerging, more complex threats.[2] These programs should be a business-as-usual activity inextricably tied to the achievement of corporate objectives, customer fulfillment commitments, and expressed or implied brand promises. A comprehensive view of all key components of the business model is needed to create that linkage.

The operative question is: What would happen to the organization's ability to execute its business model if any of the model's underlying components are taken away through an unexpected catastrophic event or altered in such a significant way as to place the company at a strategic disadvantage? Said another way, at every stage of the value creation process, what would be the implications of a shortage, disruption or quality problem in an input or output? In such scenarios, how long would the company be able to operate? This pervasive question applies to such inputs as the available labor force and talent pool, the availability of power at a reasonable price, and the availability of lines of credit and working capital. This kind of thinking is needed in a disruptive world.

In considering these boardroom discussions, directors should be kept up to date on business continuity regulatory requirements and standards specific to the sector(s) in which the company operates, as well as the efficacy of management's processes for complying with them. These regulations and standards often provide guidance on required or suggested areas of focus and approaches. The most comprehensive guidelines and standards are geared toward financial services. Using these more rigorous guidelines, it is not uncommon for other industries to apply the strategies and controls that are most relevant, as they offer a best practices model.

[2] "2020 Strategic Road Map for Business Continuity Management," Gartner, February 21, 2020, available at www.gartner.com/doc/reprints?id=1-1YL4N1MD&ct=200311&st=sb.

Questions for Boards

Following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Does the board have sufficient transparency into management's definition of the business functions, services and ecosystem partners critical to the execution of the business model?
- Do directors understand management's process for determining the impact tolerances on important functions, services and ecosystem partners (i.e., how long can the company operate without them)? Does management consider extreme but plausible events that could result in an impact on the business that exceeds established tolerances?
- Is the board informed promptly of events that have occurred that either require disclosure or meet its specified criteria for timely notification?
- How prepared is the organization for operational resilience? Has management implemented reliable processes, systems, metrics and response plans to ensure organizational preparedness? Is the organization conducting periodic tabletop exercises that effectively test its ability to recover against extreme but plausible scenarios? How does the board know?

How Protiviti Can Help

We partner with organizations to develop overall operational resilience internal audit plans, incorporate operational resilience into existing audits, and provide assurance over the operational resilience program. We work with and report to executive leaders and the board, as directed, to address such questions and issues as:

- Have we formally defined the important functions and services vital to the execution of the business model?
- Are impact tolerances established and tested?
- Are "front-to-back" mappings of components of the important functions and services understood and maintained?
- Is there a structure in place to govern resilience across the enterprise properly?
- Are extreme but plausible scenarios tested regularly?

We help organizations demonstrate and improve resilience through a robust testing program, building upon existing business continuity management activities, IT disaster recovery and cybersecurity incident response.

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000 and 35% of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti partners with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on https://blog.nacdonline.org/authors/42/. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* are consolidated into a printed booklet that is co-branded with NACD. Protiviti also posts these articles at protiviti.com.

protiviti®