ISSUE 125

BOARD PERSPECTIVES:
Risk Oversight

OPERATIONAL RESILIENCY AND THE ROLE OF THE BOARD

Every organisation, in the face of adverse, disruptive change in its operating systems, must be prepared to continue the delivery of its critical business services. The board has a vital role to play in overseeing this preparedness.

To gain fresh perspectives on board oversight of operational resiliency, Protiviti met with a group of active directors during a roundtable at a December 2019 National Association of Corporate Directors (NACD) event to discuss their experiences. Below are some takeaways.

Every company is a technology company. Most companies rely heavily on a business model powered by digital technologies. That alone makes operational resiliency — an organisation's ability to withstand adverse, disruptive change in its operating environment and continue delivering critical business services and economic functions — a vitally important skill. Operational resiliency is achieved through processes that help the business detect, prevent, respond to, and recover and learn from catastrophic operational and technological failures, such as a major cyberattack, power outage or pandemic.

The resilience concept continues to evolve as firms expand their programs and capabilities to (1) address a broad range of threats that could cause business failures, systemic risk, and economic impacts sparking the interests of regulators, policymakers and other external stakeholders, and (2) improve business, cyber, third-party and technology resilience.

To illustrate, operational disruptions to the products and services that financial services organisations provide have the potential to harm consumers and market participants, threaten the viability of the organisations themselves, and create instability in financial markets. As a result, the topic of operational resilience has pervasive implications and, in some industries, can muster regulatory attention.

protiviti®
Face the Future with Confidence

The NotPetya cyberattack is a great example of the pervasiveness of operational resilience events, as it hit companies in multiple industries, making it clear that cyber warfare imperils every company's infrastructure.[1] And the conversation is broader than cyber. For example, major power outages can happen anywhere, as a result of human error, terrorist acts, utility systems failures, or climate-related catastrophic events — and, most important, can affect every business.

Where does operational resiliency begin? The directors agreed that operational resilience starts with a "front-to-back" evaluation of the business services and functions that are critical to the execution of the business and have a significant economic impact. When considering "impact," it is important to look beyond the four walls of the organisation to consider external stakeholders (e.g., customers, third parties, regulators and investors, as well as the environment). Examples of criteria for determining criticality include the percentage of overall revenue that a service supports, the service's estimated daily impact on the customer experience, the number of market participants providing or using the service, the length of time the business can operate without it, and the extent of regulatory interest should a major resilience event affect the service.

Once the most important services and functions are determined, the organisation can then assess its exposure to adverse, disruptive events and how to prevent and detect them as well as respond and recover from them. The organisation can then build operational resiliency through a program that enhances its ability to learn from catastrophic operational and technological failures.

During the roundtable, the directors agreed that a "front-to-back" view extended beyond the four walls of the company's internal operations. It is important to understand whether an adverse event for a particular service will impact external stakeholders because most organisations today are boundaryless.

What will we do if it happens? For each critical service and function, management should also assess their impact tolerance. For example, up to what point would an organisation be tolerant of an event that stresses operational resiliency before it is necessary to trigger a recovery and resolution plan? What is the customer base's tolerance for accepting the event occurring and continuing to do business with the organisation? What are the expectations of other external stakeholders, and how would they respond to a major incident affecting the organisation?

When evaluating the organisation's resiliency in addressing an extreme but plausible catastrophic event resulting in the loss of a critical service or function, management should consider the event's velocity or speed to impact; the persistence of the impact; the sufficiency of the company's response plan if the event occurs; and the extent of uncompensated risks, if any, that the company faces as a result of the event (e.g., significant environmental, health and safety exposures). While the likelihood of occurrence can sometimes be a consideration, it is not as significant a factor in evaluating exposure to catastrophic events as the enterprise's response readiness. The question is not "Will it happen?"; it's "What will we do if it does happen?"

How should the board be involved? The question around the board's proper role in this scenario surfaced many times at the NACD roundtable. Overall, the group agreed that the board should be notified promptly of an event that is likely to require disclosure to investors, regulators or both. Additionally, the board should be aware of the company's response to the event, but should not drive the action. The board also should be engaged with (1) understanding and supporting the strategy for operational resiliency, including management's delineation of those services identified as the most critical, (2) selecting the tolerances used to gauge and measure impact, (3) providing governance and oversight of management's execution of the operational resiliency strategy, and (4) working with the CEO to address mission-critical issues.

[1] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Andy Greenberg, *Wired*, August 22, 2018, available at www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

There was also much discussion on how granular the board's engagement should be. All of the directors recognised that matters that could damage the company's reputation and erode brand image warranted the board's closest attention and timely oversight.

Individual board members are not required to be technical experts on operational resiliency. But directors should collectively possess adequate knowledge, skills and experience to constructively challenge senior management and evaluate decisions that have significant operational resiliency consequences. Directors at the roundtable agreed that clear accountability and responsibilities should be established for management and that a policy statement can be helpful in this regard. To that end, it can be useful to understand how the company's operational resiliency-testing program is organised, who is responsible for preparing for and responding to various resilience events, and the extent to which line-of-business leaders are engaged for specific business services. Directors should also expect management to provide appropriate information and periodic reporting on the operational resiliency program.

Focus on the big picture, and keep it simple! The point was made during the roundtable that, when defining operational risk, the focus should be on the types of events that may put the organisation out of business. That's the big-picture focus that warrants board engagement. In this respect, reputation and brand erosion risks are important considerations.

A related point: Don't get engulfed in the details on the specific number of events, systems and other considerations. Management should have a clear understanding of what specific services could shut down the business if they were interrupted in a major way. Directors should work with and through the CEO to articulate the desired culture of risk awareness and ethical behaviour for the organisation, both of which influence the firm's commitment to operational resiliency. It is up to management to establish and sustain that culture under the board's oversight.

For a more complete look at this roundtable, read Protiviti's full summary of the event at www.protiviti.com/US-en/insights/operational-resiliency.

Questions for Boards

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

- How prepared is the organisation for operational resiliency? Has management given the topic sufficient attention to ensure organisational preparedness? How does the board know?
- How does the organisation approach operational resiliency, and how engaged are the board and senior executives in establishing the overall operational resiliency objectives and strategy and monitoring the execution of that strategy? Is this topic discussed in the boardroom? If so, how?
- Has the organisation defined its critical business services and the impact tolerances for those services? Has it considered the extreme but plausible events that could result in an impact that exceeds established tolerances? Is this process transparent to the board?
- Has management demonstrated a clear understanding of the organisation's dependencies on third-party vendors and the level of risk they introduce into the delivery of critical business services?

How Protiviti Can Help

We partner with organisations to develop overall operational resiliency internal audit plans, incorporate operational resiliency into existing audits, and provide assurance over the operational resiliency program. In this respect, we work with and report to executive leaders and/or the board or audit committee, as directed, to address issues such as:

- Have we formally defined the critical business services? Are "front-to-back" mappings of components of these business services understood and maintained?
- Are impact tolerances established and tested?
- Is there a structure in place to govern operational resiliency properly across the enterprise?
- Are appropriate "extreme but plausible" scenarios tested regularly?

Through these activities, we help organisations demonstrate and improve operational resiliency through a robust testing program, building on existing activities already performed around business continuity management, IT disaster recovery and cybersecurity incident response.

Audit Committee Self-Assessment Questions

In these dynamic times, it is best practice for boards and their standing committees and individual directors to self-assess their performance periodically and formulate actionable plans to improve board performance based on the results of that process. To that end, audit committees should consider the illustrative questions we have made available at ***www.protiviti.com/US-en/insights/bulletin-assessment-questions-audit-committees****. These comprehensive questions consider the committee's composition, charter, agenda and focus, and may be customized to fit the committee's assessment objectives in light of current challenges the company is facing.*

Is It Time for Your Board to Evaluate Its Risk Oversight Process?

The TBI Protiviti Board Risk Oversight Meter™ provides boards with an opportunity to refresh their risk oversight process to ensure it's focused on the opportunities and risks that truly matter. It offers boards a flexible, cost-effective tool for assessing their risk oversight and mirrors the way many directors conduct self-evaluations. Boards interested in using this evaluation tool should visit the TBI website at ***http://theboardinstitute.com/board-risk-meter/****.*

protiviti®