protiviti®
Face the Future with Confidence

Operational Resiliency and the Role of the Board: Insights From Active Directors

Below is the full summary, including key takeaways, of a discussion among a group of active directors facilitated by Protiviti during a recent National Association of Corporate Directors (NACD) event. An abbreviated summary of this roundtable is provided in Issue 125 of *Board Perspectives: Risk Oversight* (available at www.protiviti.com/US-en/insights/bpro125) and on NACD/BoardTalk (see blog at https://blog.nacdonline.org/authors/42).

Every organization, 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.

Large-scale technology outages and cybersecurity attacks in recent years have both exposed systemic vulnerabilities and intensified stakeholder attention, creating top-of-mind concerns for board members as well as executives, regulators and policymakers. To gain fresh perspectives on the board's oversight of operational resiliency, Protiviti met with a group of active directors during a dinner roundtable at a December 2019 NACD event to discuss their experiences. Below are some of the important points covered during that discussion, including key takeaways.

Every Company Is a Technology Company

Operational resiliency is an organization's ability to withstand adverse, disruptive change in its operating environment and continue the delivery of critical business services and economic functions essential to the execution of its business model. Not a new concept, but one that is receiving increased scrutiny, operational resiliency is achieved through processes that help the business detect, prevent, respond to, and recover and learn from operational and technological failures that impact the delivery of critical business functions or underlying services ("catastrophic operational and technological failures"). 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.

Operational resiliency is broader than business continuity, extending across all industries to encompass cyber and other extreme but plausible threats that have the potential to cause harm to consumers, threaten the viability of firms and create instability in the marketplace. For example, operational disruptions to the products and services that financial services organizations provide have the potential to harm consumers and market participants, threaten the viability of the organizations themselves, and create instability in financial markets. As a result, the topic of operational resiliency has pervasive implications and, in some industries, can muster regulatory attention.

An example: The NotPetya cyberattack hit shipping giant A.P. Moller-Maersk particularly hard, causing outages of its computer systems throughout the world. Maersk saw every business unit — including container shipping (the company handles one out of seven containers shipped globally), port and tug boat operations, oil and gas production, drilling services, and oil tankers — affected by the destructive malware attack.[1] Merck, the giant pharmaceutical company, was also hit, costing the company US$1.3 billion to repair its computer networks.[2] So was Federal Express, generating a loss of US$300 million.[3] This destructive malware disaster delivers the specter of an unmistakable reality: Cyber warfare imperils every company's infrastructure.

Indeed, our global risk survey[4] identifying the top risks for 2020, based on input from board members, CEOs and other C-level executives, reports that cyber risk — the risk that organizations may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage the brand — is the sixth-rated risk on a global basis. Two-thirds of the 1,063 survey respondents rated this risk as a "significant impact" risk concern. From an industry grouping standpoint, cyber was included in the top five list of risks for manufacturing and distribution as well as energy and utilities.

The conversation is broader than cyber, though. For example, a global summary of major power outages, defined as widescale, unplanned power outages affecting at least 1,000 people *and* lasting at least one hour, resulting in at least 1,000,000 person-hours of disruption, shows that these outages can happen anywhere, even in developed countries.[5] A multitude of factors — human error, terrorist acts, utility systems failures, or climate-related catastrophic events — can cause these outages. Most important, they can affect every business.

> **Key takeaway:** Every company is a technology company that relies heavily on a business model powered by digital technologies. No company is immune to the risk of failure or compromise of these technologies. Many executives and directors realize their organizations may be vulnerable to a cyberattack or the occurrence of unpredictable catastrophic events.

---

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

[2] "Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?" by Riley Griffin for Bloomberg, *The Philadelphia Inquirer*, December 3, 2019: www.inquirer.com/wires/bloomberg/merck-cyberattack-20191203.html.

[3] "NotPetya Cyber Attack on TNT Express Cost FedEx $300M," by Danny Palmer, ZDNet, September 20, 2017: www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/.

[4] *Executive Perspectives on Top Risks for 2020: Key Issues Being Discussed in the Boardroom and C-Suite,* Protiviti and NC State University's ERM Initiative, December 2019: www.protiviti.com/US-en/2020-top-risks.

[5] "List of Major Power Outages," Wikipedia: https://en.wikipedia.org/wiki/List_of_major_power_outages.

Where Does Operational Resiliency Begin?

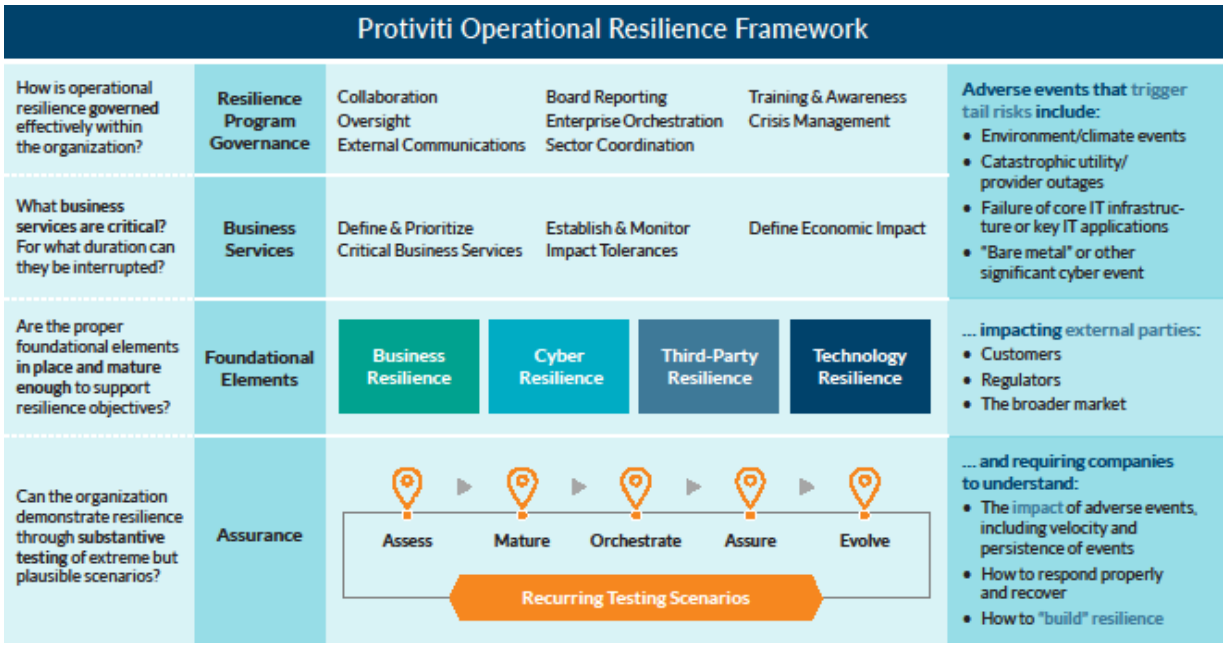
The above exposures suggest the need to establish effective governance functions and implement a "front-to-back" operational resiliency program that enhances the organization's ability to detect, prevent, respond to, and recover and learn from catastrophic operational and technological failures. During the roundtable, the directors agreed that a "front-to-back" view extended beyond the four walls of the company's internal operations to include third-party dependencies. The realities of today's business environment are that most organizations are boundaryless. So, a "four walls" approach to evaluating operational resiliency that focuses solely on internal processes and systems risks misses the big picture. An assessment of operational resiliency should consider upstream suppliers and outsourced services and functions as well as downstream distribution channels (e.g., a third-party host of a customer-facing portal may pose a significant risk if it goes down).

But the context for the operational resiliency program itself begins with how organizations define their critical business services and functions. These services and functions are determined based on criticality as well as their economic impact. Examples of criteria for determining criticality include:

- Volume and value (e.g., the percentage of overall revenue the service or function supports)
- Market share and reputational impact (e.g., the estimated daily impact of the service or function on the customer experience and the number of market participants providing or using it)
- Substitutability (e.g., the length of time the business can operate without the service or function)
- Systemic exposure (e.g., the impact on external stakeholders — customers, third parties and even the environment — and the extent of regulatory interest should a major resilience event affect the service or function)

These criteria are used to identify the services and functions warranting the most attention. They are applied to identify critical services and functions requiring the organization's attention. When considering "impact," it is important to look beyond the organization itself (e.g., the effect on customers, consumers and the environment). A front-to-back emphasis requires consideration of services and functions outsourced to IT and shared services centers as well as services sourced from upstream suppliers. To this point, the directors noted the importance of looking far enough upstream to second- and third-tier suppliers. From a practical standpoint, that may mean examining the operational resiliency of critical sole-source or strategic suppliers.

> **Key takeaway:** Operational resiliency begins with a front-to-back evaluation of the business services and functions that are critical to the execution of the business. Once the most important services and functions are selected, the organization can then assess its exposure to adverse, disruptive events and how to prevent and detect them, as well as respond and recover from them. This is how organizations build operational resiliency.
>
> It may be useful to have an overall operational resiliency framework. An example of such a framework is illustrated below.



What Will We Do If It Happens?

Once critical functions and services are determined, management should assess their impact tolerance. The concept of tolerating service interruption in a systems environment, with its emphasis on systems prioritization, availability, and restart and recovery, is not new. However, an operational resiliency focus takes a broader view. For example, up to what point would an organization 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 organization? What are the expectations of other external stakeholders (e.g., regulators, investors and communities) and how would they respond to a major incident affecting the organization?

To illustrate, what is the impact should any of the following elements of the business suffer a disruptive event: a strategic supplier of essential raw materials or other inputs, availability of reasonably priced power, a key distribution channel, or transportation and logistics for delivering products? Said another way, at every stage of the value-creation process that facilitates a critical service or function, what would be the implications of an operational resiliency event? How long would the company be able to operate, and what is the effect on the end customer?

When evaluating the organization's resiliency in addressing an extreme but plausible catastrophic event resulting in the loss of a critical service or function, management should consider the following:

- The event's velocity or speed to impact, including whether the loss of the critical service or function can occur without warning (i.e., does it smolder over time or is it sudden?)
- The persistence of the impact (i.e., the duration of time before the loss of the service or function can be recovered and restored as well as the related "headline effect" on reputation and the brand)
- The sufficiency of the company's response plan if the event resulting in the loss of the service or function occurs
- 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)

Management should consider these issues periodically when evaluating operational resiliency. 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 to those events. The question is not "Will it happen?"; it's "What will we do if it does happen?"

> **Key takeaway:** These are the stakes. The key question is "What would happen to the organization's ability to execute its business model if any critical business service or function were taken away or altered in a significant way through either an operational failure or an unexpected catastrophic loss?" Sooner or later, every company, no matter how proud its brand and reputation, faces a crisis. Will its response demonstrate world-class reaction or a state of unpreparedness that is out of step with its brand promise?

How Should the Board Be Involved?

The roundtable indicated a significant level of interest in understanding what response playbooks should look like for cyber and other operational resiliency incidents. There was also much discussion about when and how the board should be involved. Overall, the group agreed that the board should be notified promptly when there is 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 question around the board's proper role in situations involving resiliency surfaced many times at the NACD roundtable. There was general agreement that the board should be engaged with (1) understanding and supporting the strategy for operational resiliency, including management's delineation of those services identified as most critical, (2) selecting the tolerances used to gauge and measure impact, (3) exercising governance and oversight with respect to management's execution of the operational resiliency strategy, and (4) working with the CEO to address mission-critical issues. There was also much discussion on how granular the board's engagement should be. All of the directors recognized that matters that could damage the company's reputation and erode brand image warranted the board's closest attention and timely oversight.

To illustrate, should the board specifically approve management's identification of the important business services for the organization and the impact tolerances that have been set for each of these services? This is emerging as a requirement in financial services, necessitating that boards regularly review assessments of the firm's important business services, impact tolerances, and scenario analyses evaluating its ability to remain within the selected impact tolerances for the identified services. But in most industries, getting to that level of granularity is strictly at the board's discretion.

Individual board members are not required to be technical experts on operational resilience. However, directors should collectively possess adequate knowledge, skills and experience to constructively challenge senior management and evaluate decisions that could have significant consequences to operational resilience. They should also expect management to provide appropriate information and periodic reporting on the operational resiliency program.

> **Key takeaway:** In discussing the board's role, the roundtable focused on how to delineate the responsibilities of management and the board. 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 operational resiliency program is organized, 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.

Management also should be able to demonstrate that they have a clear, front-to-back mapping perspective regarding the possible vulnerabilities affecting those services.

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 those types of events that may put the organization 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 business services have the potential to shut down the company's business if they were interrupted in a major way. It's a red flag for directors if they don't. In short, management should understand and be able to clearly articulate the so-called "crown jewels" that warrant the lion's share of protective, response and recovery cyber measures.

Key takeaway: One way that boards can stay out of the weeds is for directors to work with and through the CEO to articulate the desired culture of risk awareness and ethical behavior for the organization, which influences the firm's commitment to operational resiliency. It is up to management to establish and sustain that culture under the board's oversight.

Emerging and Disruptive Technologies Are Altering the Landscape

Toward the end of our discussion, a significant amount of time was devoted to emerging and disruptive technologies — specifically, artificial intelligence (AI)-enabled technologies and machine learning. Broad-ranging questions were raised, particularly with respect to the effect on workplace dynamics:

- What is the board's role in determining the strategy to implement these technologies?
- What is the company's role in managing displacement and the upskilling and reskilling of human resources?
- What are the organizational constraints that could limit the technology, and present a threat if competitors can manage the opportunities and challenges these technologies present more effectively and timely?
- Most important, how quickly will these concerns be realized?

While the advent of disruptive technologies may appear, on the surface, to be off-topic, imaginative thinking is needed to identify and assess those "tail risk" scenarios that could significantly impact operational resiliency. For example, is serious consideration needed to explore how disruption may occur and what the unintended consequences may be from an operational resiliency standpoint?

Key takeaway: The gist of this roundtable conversation is that imaginative thinking about what the future holds and how it impacts the company will be an important skill to access in the boardroom. That's particularly true for 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 organization for operational resiliency? Has management given the topic sufficient attention to ensure organizational preparedness? How does the board know?
- How does the organization 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 organization defined its critical business services, as well as 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 organization'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 organizations 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 organizations demonstrate and improve their operational resiliency through a robust testing program, building upon existing activities already performed around business continuity management, IT disaster recovery and cybersecurity incident response.