protiviti®
Face the Future with Confidence

Resilience Practices Can Help Firms Mitigate Supply Chain and Third-Party Provider Risks

Customers are major drivers of change in the marketplace. In times of stress, how well companies manage customer experience and expectation can determine whether they succeed. At the height of the COVID-19 pandemic, amid demand spikes and panic buying of household items like groceries and cleaning products, companies that successfully addressed customers' demands (e.g., restocked alternative products quickly and adopted contactless payments and same-day delivery services) were rewarded with increased loyalty and profits, whereas many that failed to meet changing expectations lost significant market share.

Today, customers' expectations of quality and timeliness of service delivery continue to increase, especially in industries where disruptive and/or alternative providers exist. Companies are under pressure to build more resilient enterprises that, in the event of a disruption, can rapidly recover business services to minimize customer impact. This means having a strong focus on the broader customer delivery ecosystem, including the derivative risks associated with all suppliers. It means not only working to mitigate identified supply chain bottlenecks but also paying particular attention to concentration risks arising from third parties and other outsourcing relationships, arrangements that are increasingly difficult to understand because they often involve multiple locations, businesses and layers of subcontractors.

The post-pandemic supply chain landscape requires companies to incorporate operational resilience concepts and practices, which, at their core, prioritize identifying important business services and setting tolerance levels for risk, and, perhaps most significant, are driven by the overarching goal of minimizing customer harm in all cases.

Aligning expectations means managing resilience

In the current business landscape, there is a very clear expectation (from all customers) and even a requirement in certain jurisdictions (from some regulators) for firms to maintain control and responsibility over their relationships with third-party suppliers. While most firms

recognize this responsibility, increased digitization, globalization, and the need for specialized skills and services via outsourcing have made supply chain and service delivery shocks more complex and difficult to manage. As recent incidents have shown, supply shocks are occurring more frequently, can originate from half the world away, cripple commerce across multiple industries, and disrupt the operations of businesses of all types and sizes, with dire financial, brand and reputational implications.

Earlier this month, for example, when the world's largest meat processing company was hit by a ransomware attack, knocking plants in the United States and globally offline, the supply crunch pushed beef prices up and affected orders at grocery stores, restaurants and other local sources of meat across the country. It exposed a meaty issue: The country's meat supply chain is highly concentrated among a handful of suppliers.

Similarly, when San Francisco-based cloud service provider Fastly experienced an outage on June 8, dozens of major websites, including CNN, Reddit, Pinterest, certain Amazon sites and the U.K. government's main public services portal, also went offline and could not be accessed. The disruption (apparently caused by an internal configuration error) lasted roughly an hour, but the ripple effect exposed the reliance of many of the world's biggest websites on a handful of third-party content-delivery networks.

Whether it be the ransomware attack on Colonial Pipeline in May, which led to panic buying and widespread gas shortages across the U.S. Southeast region, or the shortage of the chemicals used to make foam and other poly-pad supplies, which impacted not only the furniture industry but the automotive industry as well, these various disruptions raise critical questions about resilience:

- What happens the next time there is a significant outage or shock that impacts critical infrastructure for days or even weeks?
- How do organizations in industries dominated by a few critical service providers (like cloud service providers) manage their concentration risks?
- How can companies leverage operational resilience concepts that financial services companies are now adopting with pressure from some regulators to augment supply chain and third-party provider expectations?

A resilient organization is one that can absorb operational disruptions and still maintain continuity of service. The organization should have formal substitutability and transferability plans in place to mitigate supply chain and third-party vendor service disruptions.

A transferability plan would allow a national retail company that depends on truck deliveries to switch all its freight services to a competing provider if the current carrier's trucks are grounded for whatever reason. The ability to supplement all or some of an organization's important third-party provider services quickly and when needed, as well as the cost of doing such, should be a part of the overall resilience program.

Concentration risks

Concentration risk is one of the major areas related to outsourcing and third-party services delivery that can affect an organization's resilience. There are many variations of concentration risk; it can be geographical in nature, driven by third or fourth parties, or reverse-systemic — meaning that a service provider has a handful of key clients whose exit could impact the service provider's viability, or those clients are all in a single sector of the economy.

An overreliance on a single critical third-party service provider by multiple firms can create operational failures if the service provider experiences a significant outage or simply decides to exit a critical line of business. A company may also have high levels of concentration within third-party service provider arrangements, reducing its ability to exert influence and control over those third parties. Additionally, because many third-party service suppliers operate in multiple jurisdictions with varying and inconsistent regulatory standards, resilience requirements may be inadequate in certain locations.

Technological changes have been one of the biggest drivers of concentration risk and, by extension, operational disruptions. At the same time, technology has advanced organizations' ability to withstand adverse events by, among other things, enabling the decoupling from a desktop, decreasing certain types of concentration risks, and enhancing the storage and availability of data. The net effect of both the risk to organizations and their ability to recover cannot be overlooked.

Still, companies undergoing technology transformation have to consider several issues. For example, in the cloud computing space, some consumer groups and regulators worry about the limited number of providers supporting critical financial services such as real-time money settlement applications, trade settlement processes and ATM transactions. While the major cloud service providers have invested heavily in their infrastructure to increase security, availability and redundancy, the fact that they have significant dependencies raises concerns that their potential failure could threaten not just individual institutions but also the stability of financial markets and economies.

Similar fears have been raised about content data networks. The most recent outage had a wide damage radius and was described in a report in The *Financial Times* as "an object lesson in internet fallibility." But the incident also revealed an important element: Many customers were able to mitigate the impact of the outage by shifting workloads to alternate providers, proving the important concept of substitutability.

Clearly, companies need to spend more time and effort understanding their concentration risk to develop effective mitigation strategies. In their October 2020 interagency paper, *Sound Practices to Strengthen Operational Resilience*, U.S. federal agencies recommended that firms identify risk transmission channels, concentrations and vulnerabilities by analyzing interconnections and interdependencies within and across their critical operations and core business lines, considering third-party risks, and use the information obtained from these analyses to inform their tolerance for disruption.

Given the current complex supply chain landscape, companies should collaborate with critical vendors and third parties on setting and managing impact tolerance (or tolerance for disruption). The collaborative engagement would encourage prompt reporting of vulnerabilities and effective communications of operational disruptions. It would also give companies additional visibility into the workings of fourth and fifth parties — the tangled web of dependencies in which a vendors' vendor may be operating without much oversight.

What Companies Should Do Now

The scale and frequency of recent disruptive events have exposed the fragility of supply chains. These incidents call for broad implementation of operational resilience practices and detailed and continuous monitoring of suppliers — third, fourth and fifth parties that deliver important business services or processes — as well as concentration risks.

Organizations should consider these practical actions:

- Identify important processes and streamline end-to-end documentation, including inputs, internal and external processes and outputs.
- Identify critical suppliers. This process should include assessment of the organization's aggregate supply chain and concentration risk across all its locations (domestic and international), businesses and service provider relationships.
- Leverage available technology solutions, such as security ratings tools, to enhance supplier oversight.
- Build in redundancy for key value-driving activities to minimize possible disruptions.
- Focus on supporting infrastructure and data to help identify key points of failure across profit-generating activities.
- Assess how a disruption within a third party will impact an organization's ability to operate within its tolerance thresholds.
- Design scenarios against which to test and monitor third, fourth and fifth parties' resilience and effects on impact tolerance.
- Establish a governance regime to monitor supply chain and third-party risk controls.

To learn more about the board and C-suite leaders' role in overseeing operational resilience and key considerations for implementing across the enterprise, read this recent white paper, Operational Resilience: Considerations for Boards, the C-Suite and Enterprisewide Implementation.

Also, visit our Operational Resilience web site to access additional insights and our industry-leading operational resilience framework.

Contacts

Brian Kostek
Managing Director,
Risk & Compliance
+1.928.614.2316
brian.kostek@protiviti.com

Doug Wilbert
Managing Director,
Risk & Compliance
+1.917.697.1572
douglas.wilbert@protiviti.com