strategy+business
a pwc publication

28 FEBRUARY 2023

Building resilience in a polycrisis world

To stay operational, even in the worst of times, focus on what matters most. It will change your risk culture.

by Bobbie Ramsden-Knowles, James Houston, David Stainback, and Paul Williams

Bobbie Ramsden-Knowles co-leads the PwC Global Centre for Crisis and Resilience. Based in London, she is a partner with PwC UK.

James Houston is a leading practitioner with PwC UK's risk practice specializing in operational resilience. Based in Edinburgh, he is a partner with PwC UK.

David Stainback co-leads the PwC Global Centre for Crisis and Resilience. Based in Atlanta, he is a principal with PwC US.

Paul Williams is a specialist in operational resilience with PwC UK. Formerly, he was responsible for supervision and policy development for nonfinancial risks at the Bank of England.

Stella Nunn, Duncan Scott, Rory Spedding, and Claudia van den Heuvel contributed to this article.

The confluence of crises facing business leaders right now is nothing short of remarkable. Some of the emergencies are manifestations of once-in-a-generation risks: the war in Ukraine, high inflation, and the ripple effects of both the pandemic and the "great resignation." Others, such as significant cyberattacks and extreme weather events, once seemed rare but are now worryingly familiar. It's a moment some are aptly calling a *polycrisis,* and as this stew of interrelated geopolitical, economic, and climate threats heats up, the immediate concern for CEOs and other business leaders should be whether or not they are prepared.

Many are not. At the heart of the problem is the fact that many executives are inadvertently behaving as if nothing's changed. They're blinkered by an outdated risk-management mindset that seeks to master risks by rigidly allocating resources and management attention according to a mix of probability and impact. But that approach falls short as so-called low-likelihood/high-impact events become more unpredictable, more complicated, and, via their widespread knock-on effects, more costly. Think of the far-flung business disruptions that ensued when the *Ever Given,* one of the largest container ships in the world, ran aground in 2021: US$9.6 billion in global trade was held up for each of the six days it was stuck in the Suez Canal.

Moreover, companies often take an inward-looking, siloed approach to managing risk, considering each business unit separately and failing to think hard about how they interact—let alone what customers will see or experience. This

is visually depicted in the elaborate "stoplight" charts that companies use to display the risk levels of various functions, or businesses using red, amber, or green indicators. The resulting rolled-up picture *seems* complete, but these analyses sometimes exclude the connections between the silos. At their very worst, the charts are biased, better at depicting company politics than risk. Human nature (and weak risk cultures) can make it tempting for contributors to nudge a red light to amber, or an amber to green—particularly when reputations and budgets are at stake.

And senior executives often start out on the back foot when risks materialize because they have long instinctively prioritized financial resilience over operational resilience. They may have hedged against currency risk or liquidity issues but not paid enough attention to vulnerabilities embedded in the operating infrastructure that delivers their services and products to their customers—the things that matter most and that they're in business to provide.

Digitization, for example, can change how services are delivered, making them less tolerant of disruption, which is something that leaders can miss. And they may not understand the effects that nondelivery of these services have on customers. In overlooking critical—but otherwise unglamorous—areas, CEOs are placing enormous bets on their ability to deliver that they may not even be aware of. It was a single damaged database file, according to the Federal Aviation Administration, that grounded all planes flying to and from the US in January 2023, disrupting close to 5,000 flights.

The good news is that taking on these ingrained challenges—and the weak risk cultures that often prop them up—is relatively straightforward, provided that CEOs and their leadership teams are committed to revamping how they think about, and approach, risk. The key is to put aside the notion that it's possible to understand or address every threat in a probabilistic way. Leaders need to zero in on the risks that might *plausibly* disrupt the most important aspects of the operations, the ones that are most crucial to customers—and thus, the company. And today, these risks are many. Should any or all of them arise, leaders can discover blind spots, improve resilience, create value, and, in some cases, gain a competitive advantage by developing a deeper cross-functional understanding

of what it takes to deliver key operations, be it a product or a service, from start to finish.

Taking on this challenge demands C-suite and even board attention, because improving operational resilience over the long haul can require a sweeping change in corporate culture—detoxifying failure in order to increase transparency—and a rethinking of incentive structures, and even investment strategies.

Start with what matters most

Seeing and responding to risk differently first requires leaders to clearly pinpoint where plausible risks could materialize and do the most damage to key operations and services. This can be tricky if companies have traditionally approached risk in a siloed way. Company leaders should spend time with one another to work through *what if?* scenarios, with an eye toward highlighting where exactly in the business a problem or failure would be most catastrophic to customers.

For example, at a workshop for a bank's C-suite leaders, the initial count of "most important" services surfaced more than 350. Further conversations winnowed the list to 34. But the real breakthrough came when the bank's leaders flipped the question around from what would hurt the *company* most to what would hurt *customers* most. This helped the leaders see that the biggest customer pain point was the ability to get cash on demand, and that this mattered more to the business than other considerations.

Now that the executives had their focus—the outcome of getting cash—they could begin looking at all the ways customers do so, including ATMs and the workers who service them, brick-and-mortar banks, and the tech and third parties that help with electronic transfer payments and build resilience across all functions, rather than focusing on individual mechanisms.

Prioritization exercises also help leaders tease out false assumptions. Leaders at a UK housing management company had believed that collecting rents via the company's app was the key to business continuity. A deeper discussion of priorities showed that paying its suppliers promptly was far more important. The company could withstand late rental payments resulting from an app

outage much longer than it could live with disrupted key third-party services like heating and repairs, which tenants would find immediately harmful and which could have legal repercussions for the organization.

For a global hotel chain, several rounds of C-suite debate surfaced eight operations the business relied on most. One in particular—payroll—was worrying, because a disruption here seemed likely to cripple all operations and have an immediate, damaging effect on customer service. Why? In part because the combination of the pandemic and the "great resignation" had empowered workers and raised their expectations. Now, cleaners or other frontline employees whose work (or absence) could seriously affect customers were less likely to tolerate any pay delays and thus much more likely to walk off the job with little or no notice.

More eye-opening still for the hotel executives was fully understanding the complexity of all the processes, systems, people, and vendors that underpinned what was needed to keep payroll running across the globe.

Connect dots, reveal blind spots

Determining which operations and other areas of the business are the most vital—and most vital to customers—requires considerable focus and commitment. The next step, mapping out the relevant processes, handoffs, and dependencies, can be equally challenging. Businesses struggle to do this well because it's complex and can involve multiple departments and players. It's not the usual approach in which business continuity is looked at solely within the siloed functions. The way the whole service is delivered, not individual mechanisms, needs to be identified. At that point, the strengthening of the processes involved can be more forensic, because weak areas are identified, and deliver greater resilience. And this sort of planning is time well spent, because it inevitably highlights blind spots and actionable improvement areas.

Though blind spots may lurk anywhere, they often build up where new tech systems have replaced old ones or were patched together on the fly after a merger or acquisition. Poor institutional memory can create unnoticed vulnerabilities, too. For example, an exercise to understand how a manufacturer's key products

are made found that an unassuming, overlooked part of a legacy computer system was at the heart of the production process. The executives recognized that their focus on financial performance had blinded them to the need for more mundane tech upgrades that directly supported operations. Only by getting the team to focus on the entire manufacturing process did the oversight come to light. If the server had failed, 80% of production would have gone down for days.

Blind spots aren't just tech-related. The international payments system at a large bank remained offline for three days because the one employee who had the password necessary to access the back-end system was on a backcountry hiking trip with no internet coverage. The bank's IT department had been unaware of the vulnerability and, in any event, had always assumed it could manage workarounds on the fly. The cost for the bank was a dented reputation and regulatory fines. The episode proved a wake-up call: even though international payments were used by nearly all the bank's customers, no one at the bank had known that the service could fail exactly in this way.

Mistaken assumptions were also an issue at a large financial-services company that discovered flaws in its payments processes—the service that mattered most to customers across all divisions. Company leaders had been confident that manual workarounds would save the day. Each of the company's six divisions had already codified the contingency processes that would be needed should any part of the system fail. Indeed, the company was legally obligated to stress test this function—and had.

But executives were chagrined to learn later (thankfully during a mapping exercise and not a crisis) that the planned workarounds the divisions had prepared didn't account for the need to scale them companywide. And that was the blind spot: had the plans been invoked during an emergency, they only would have been able to handle 12 payments a day across all six divisions. And even that might have been optimistic, given that the plans were created in incompatible formats and used wildly different assumptions of how long it would take to recover operations, ranging from 48 hours to a week.

These realizations led to a larger conversation about what it would take to put in place a system that could absorb the impact of a payments failure—whether

MAKING THE MOST OF A BAD DAY

Visit the online article to see an interactive graphic about how a strong executive team mitigates risk when it responds to a malware issue at a hypothetical EV company.

Source: PwC analysis

it was because of an IT problem or a cyberattack, or simply because the people with authority to sign off on payments were missing in action. Which customers could survive without cash, and for how long? Would it be better to help small businesses, which represented less of the company's revenues but were more vulnerable to payment delays? Or was it better to help larger businesses?

Traditional business continuity planning would focus on recovering business as usual for the whole system, whereas creating resilience flips that assumption to instead ask: how do we recover some degree of operational capacity immediately—and survive a potential catastrophe?

Put it all together

The financial-services company executives were asking the right questions about the right areas of the business. They could have gotten more useful answers by

amplifying the team's human judgment with a tech-enabled boost. Indeed, the best resilience strategies will be underpinned by technology that helps anticipate, simulate, respond to—and learn from—the web of risks and disruptions companies now face. Nevertheless, there is heavy lifting involved in gathering the data and introducing new tech—and no less so in educating leaders on how to respond. These are often investment decisions that require board and C-suite support, as they involve both time commitments and money.

Tech-powered dashboards can help executives track in real time the different key dependent operations—and prioritize action (see "Making the best of a bad day," on the previous page). Dashboards also help flag danger signals that require attention, such as missing staff or low cash balances heading into a payment period, and estimate the impact of system failures based on the tolerances set by management. The initial phase of collecting data and building a similar dashboard at the financial-services firm took six months—a significant commitment of resources. Now, if there is a system failure in one part of the payments function, the dashboard will show how many customers are affected and list the actions necessary to recover operations.

For its part, a global manufacturer applied this tech-powered thinking to map out the operations that formed the basis of a main revenue stream. This included the staff involved, the tech systems, and the end-to-end supply chain for parts. To make better sense of the sheer volume of data involved, the company used an AI data-collection program to create a dashboard of all the dependent parts of these operations. Importantly, the dashboard showed two things: places in the world where the company had spare production capacity to absorb shocks, and details on alternative supply routes should the primary ones fail.

And fail they did. When the *Ever Given* bottled up the Suez Canal in 2021 (only the fifth time such a blockage has occurred in the canal's 153-year history), the manufacturer was able to divert ships quickly and adjust its supply chain to maintain uninterrupted deliveries to customers. These results are consistent with separate PwC research that found that companies investing in advanced supply chain capabilities benefit in a host of ways that includes greater resilience to disruption.

The combination of resilience and speed was powerful for the manufacturer, but it wasn't the whole story. Frequently, we find that when companies look at risk with fresh eyes, they find knock-on benefits. The global manufacturer, for example, also used its dashboard capability to cut costs confidently and still ensure operational resilience when it saw that it was duplicating various business processes across different countries. What's more, the company was able to quickly shut down its Russian operations after the country's invasion of Ukraine and swiftly switch manufacturing to other locations that had excess capacity—all while keeping customer disappointment to a minimum.

Promote a strong risk culture

Though the practices we've described can help any organization become more resilient, making the changes *stick* requires attention to company culture and how people work. This includes underlying incentives—formal or tacit. It's true that bringing together a cross-functional team to identify risk blind spots can help tear down silos, but participants aren't going to look terribly hard if they feel they'll be penalized for the problems they might find. That's why there needs to be a true culture of speaking up and identifying potential systemic failures.

Here are a few practical tips for leaders to make sure their companies don't inadvertently improve financial performances at the expense of operational resilience or overlook the role their people play.

Manage up and down and side to side. Boards need to understand why the C-suite has changed the way it views existential risk and buy into the new approach, as it will affect investment decisions and even the compensation of the leadership team. C-suite leaders must ensure they communicate across functions, and, with a mandate from the top, the message also needs to be communicated throughout the business.

Focus on empowerment. When employees have power and choice, they are happier, better at their jobs, more innovative, and more likely to go the extra mile—beneficial traits for any organization seeking to bolster its resilience. Yet 43% of global CEOs in PwC's 26th Annual Global CEO Survey admit that company leaders don't often encourage debate and dissent. This needs to change.

Avoid the blame game. The CEO survey also found that 53% of CEOs said their company's leaders did not often tolerate small-scale failures. This is decidedly unhelpful, as finding blind spots or vulnerabilities in the way we've described requires a close examination of small-scale failures. By embracing transparency and staying blame-free, companies are more likely to spot the weakness before it's too late. Pre-mortem exercises that start with the assumption that a plan can fail can reduce overconfidence and help make finding weaknesses a strength.

Bring all the right people together. For risk to be looked at through a cross-functional lens, key people across the different disciplines—from IT and operations to HR and communications—need to become part of the conversation. Don't make it hierarchical or siloed; instead, let all key people contribute their expertise and voice concerns when necessary. Only by integrating silos can there be true enterprise resilience.

Set resilience KPIs. Being able to absorb shocks depends as much on rapid and decisive response capability as it does on pre-shock risk mitigation and preparation. Work out what is necessary to deliver key services and how long it will take to get them up and running—from end to end, across all the dependencies that are mapped. Set goals for activating backups and workarounds. Understanding the highly interconnected components of operations ensures that rapid responses are accurate, which is critically important when communicating to customers and the media alike.

Invest in preparing people. Effective crisis-management skills are developed through frequent exposure to the characteristics, pressures, and demands faced when disruption occurs. Leaders need to develop the relevant skills, mindsets, and behaviors to respond in times of crisis or disruption. They can do this through tech-based microsimulations or through simple scenario-planning discussions with key stakeholders. It's an approach that builds the muscle memory required for setting strategy, making decisions, and managing stakeholders in an uncertain world.

strategy+business

a pwc publication

- **strategy-business.com**
- **strategybusiness.pwc.com**
- **facebook.com/strategybusiness**
- **linkedin.com/company/strategy-business**
- **twitter.com/stratandbiz**