Deloitte.

21st century resilience
Getting it and keeping it

Contact us

Michael Kearney
Managing Partner, Strategic Risk | Deloitte Advisory
Deloitte & Touche LLP
+1 415 783 4461
mkearney@deloitte.com

Damian Walch
Director | Deloitte Advisory
Deloitte & Touche LLP
+1 312 486 4123
dwalch@deloitte.com

In the summer of 2015, nearly simultaneous "computer glitches" at three prominent enterprises caused many to wonder if there was a connection, and if perhaps some orchestrated attack was underway. Even a government agency took an interest.

But a thorough search for the root causes revealed that each incident was entirely separate and distinct, originating in internally flawed systems. Even though there was no "grand design," each failure cost the respective companies millions of dollars. They also served as startling examples of the vulnerability of major systems and of just how common such disruptions have become.

In recent history, garden-variety human error and a malfunctioning relay were blamed for a partial power outage and a "rare electronics failure" at two national sporting events. Again, there was nothing sinister; just proof that when things can go wrong, they will go wrong.

Faced with challenges from natural disasters and human infrastructure calamities, today's organizations need to be able to respond. Whether it's a mere technical glitch, human failure, or a full-scale catastrophe, there will still be an impact on day-to-day operations and, ultimately, on business reputations.

A risk-based world

The world in which we live is changing, and the threats we face in the 21st century seem to be growing both in volume and complexity. Each day, we grow more connected in terms of technology, economics, and infrastructure than we have ever been in the past. While natural disasters often grab headlines, human-caused events can also have widespread consequences. These can be innocent mistakes or deliberate attacks by hackers or terrorists. Yet because these disruptions are so deeply linked with the very nature of the businesses we conduct and how we pursue them, it's increasingly important to view risks as more intrinsic and ubiquitous than exceptional. They are no longer once-in-a-lifetime concerns.

In other words, risks are a part of the spectrum of operational factors that organizations should build around. To encompass those factors means focusing not just on "recovery" but also on agility and ever-greater resilience, so as to reduce the impact of events and speed up response. In short, organizations should consider the risk of their

business decisions, integrating and strengthening their traditional crisis management capabilities under a new rubric that prepares them to be ready for anything.

Evolving perspectives

Traditional standards and fundamentals of business continuity management (BCM) were largely defined between 1995 and the early 2000s. Unlike earlier times when production, distribution, and end customers were more loosely coupled (to cite an example from manufacturing), the pace of business had greatly increased by the 1990s. Shipments moved at a greater speed. Organizations developed lean practices that improved efficiency but also eliminated cushions, such as large on-site inventories. Increasing globalization in many industries, particularly within financial services and the systems that sector employed, required 100 percent uptime in operations and the ability to facilitate huge transactions. And improving communications meant that customers could, and often did, change preferred providers whenever they believed it could be to their advantage.

Those developments not only tightened the links between a problem in one part of the value chain and impacts elsewhere, but they also heightened the business consequences. At that point, organizations began to recognize their critical dependencies: sole-source suppliers, centralized data centers, and other key facilities that were "too important to fail," because anything but the most rapid recovery could doom the rest of the business.

On that basis, companies built up disaster recovery capabilities and adopted practices that would help them ride out some well-defined "storms." It was a necessary and correct response. But that came before social media, mobile technology, cloud computing, and ubiquitous analytics; developments that further increased the speed of operations and, in many cases, led to new and poorly understood dependencies. In the face of this change, the business continuity management (BCM) discipline itself remained largely stagnant and non-innovative, propped up by habit and, frequently, by industry regulations and standards. What it provided was still important, but it wasn't enough.

Today, *instant* is the word, and 24/7/365 availability is the norm. Additionally, in the years since BCM became a defined activity, financial markets have become truly global and supply chains have continued to evolve, with less "slack" and more points in the chain that can cause critical problems when there is a failure.

The picture that emerges is one of multiplying risks that, in turn, further magnify other risks as they interact to produce complex events. A traditional recovery plan that sits in a notebook or on a hard drive and is reviewed each year or two (if at all) can scarcely keep pace with today's quickly developing and rapidly escalating challenges.

Mastering this world of risk and achieving resilience requires data — and lots of it. That's what enables organizations to make better decisions about necessary investments that help limit risks. Data also enables resilience by providing ample information to enable fully informed decision making during incidents and "glitches."

What kinds of data? Each organization will have different priorities and resources. But a balanced mix usually includes data on business processes, interdependencies, financial and operational impacts, certain support systems, and third parties.

These domains each track and use substantial quantities of data, which may not be readily accessible or in a form that's useful for discussing risk and resilience. Therefore, to guide both long-term planning and short-term resilience, it's important to identify specific potential sources of data and develop a plan for keeping it accessible and interpretable.

Traditional information from risk, business continuity, disaster recovery, and emergency response disciplines can also be assessed and, if possible, supplemented with geospatial information about facilities, business partners, and service providers. And as systems are refined and data is aggregated in a repository, mobile should be a component.

Mobile devices not only help provide visual information, but they can also guide real-time decision making. Social media platforms can provide additional timely information about events and individuals to improve decision making and reveal the outcomes of decisions already made.

In contrast to the sedate vision of BCM that has predominated for so long, today's risk picture demands both speed and a response capability that isn't an afterthought or an add-on. While it might once have been acceptable to frame risks around a laundry list of familiar natural or human-caused mishaps, such as fires and floods, that's no longer enough. Delivering resilience in a 21st century context means having some kind of "decision engine" that enables an efficient and effective response to the risks and threats to which a company is exposed.

Getting there can take effort, but it should pay substantial dividends.

Moving toward resilience

Key risk indicators, number of disaster plans created and catalogued, and frequency of updates were the foundation of BCM. Counting things may provide some metrics, but those plans rarely inform executives of their actual ability to respond to and recover from disruptions. A clearer indication is needed that the data "counted" reflects the critical elements of the organization and its risk exposure. Data needs to be transformed into information that enables decision making.

People are also part of the strategy. Risk and resilience belong to everyone in the organization. Tapping into the organization's collective wisdom and orchestrating the results can make resilience part of the fabric of the business. Risk professionals need to engage at many levels in the organization to carry this message.

For example, there are often many individuals who are cognizant of potential risks but have no established means of sharing that information, usually because it isn't something measured or rewarded. These risks could be challenges that are imminent or could emerge in the foreseeable future. Someone in the field may be aware of market sentiments that are on the cusp of gaining a troubling political dimension. Or an individual in purchasing may understand how a sourcing decision made elsewhere is leaving the organization vulnerable to a supply disruption. The point is that risk awareness, impact assessment, and resilient thinking should permeate the organization at least as much as awareness of profit and loss—perhaps even more so, since the consequences of risk can be so immense.

While risk needs to become everyone's job, awareness and knowledge of risk issues should flow upward in the organization, so they can be assessed on a strategic level and dealt with effectively, with the best possible resources.

The new resilience model also requires connecting people with data. A common problem is that some of the information needed to support resilience efforts is typically managed and accessed by only a small pool of people. Furthermore, there is typically plenty of data. But because it often isn't organized as effectively as it needs to be, it isn't immediately usable. Organizations typically have good information about their staff and facilities, their vendors and service providers, and their systems and applications. They may even have information about some specific kinds of risks and their potential impacts. However, that data has been created by different parts of the organization and resides in native files, share file sites, or proprietary databases. The data housed across the entity is not correlated to create meaningful information that can be used to assist the organization in understanding risk and composing resilience. It should also be noted that organizations have often acquired or developed point solutions — application inventories, risk databases, and business continuity systems abound — to address specific needs. But they typically don't integrate the data, and they lack an organizing principle tied to resilience. If an organization actually looked at each of those point solutions and made a concerted effort to integrate that data into usable information, it could provide executives with greater insight into their strategic and operational risk profile while helping point the way to resilience.

The bottom line is that companies are resilient when they are truly confident in their program, predictive about potential disruptions, and ready to be proactive in response.

Resilience confidence

The end result of resilience thinking should be *resilience confidence*: an objective, risk-based measurement, unique to each organization, which provides a clear sense of a company's ability to respond to disruptive business events, while also offering clear guidance on correcting underperforming areas. The starting point in this process should be visibility into risk. Various existing business continuity-disaster recovery, supply chain, and cyber information documentation and plans often contain useful information that can start the process. By themselves, they lack dynamism and offer comparatively limited response options. Together, they can be foundational elements for building resilience.

What does resilience confidence look like? It involves not only assessing risk but also determining what should be required to recover, replace, or rebuild critical business processes in the wake of business disruption and, in particular, the ability to meet recovery objectives. It's both a plan and a tool kit. But developing resilience confidence is a two-way street. For example, the loss of a single functional area might justify rapid recovery of that area—almost without regard to cost. Where multiple sites, functions, or facilities are affected, however, recovery may require tradeoffs, greater economies, or perhaps less rapid recovery goals. These possibilities and all reasonable recovery scenarios should be considered in advance. This prepares the organization to "weather the storm"; it also helps clarify dependencies among different sites and organizations, between and among technologies, and within the organization and its ecosystem of suppliers and customers.

Getting to resilience confidence can start with a simple checklist approach. But it should advance to include planning and discussion about potential scenarios, notification and activation processes, and descriptions of ultimate responses.

Boards of directors, with legal obligations regarding governance, should seek the kind of certainty that a resilience confidence approach can provide. Put another way, there are no longer valid excuses for not anticipating specific kinds of disruptions or even combinations of disruptions. And boards will likely be held to the highest standards regarding how they have guided advanced preparations.

Executives, for their part, should be working to build resilience confidence, leveraging assets that are already in place whenever possible. This may yield rewards with modest efforts.

The great truth about resilience is that, as an attribute with day-to-day business value, it isn't helpful only when disasters strike—it can strengthen an organization and help improve agility at every level. Resilience is an attribute to strive for. And it may well be a requirement for the successful 21st century organization.

How Deloitte can help

Deloitte Advisory can assist organizations at several points in their journey to achieve resilience. Operating model labs have been used by many organizations to collaboratively develop the roadmap for bringing together disparate risk data and organizations. Our professionals have also been instrumental in designing and implementing those integrated systems that help convey resilience confidence. Further, Deloitte Advisory can assist an organization in transforming its traditional BCM programs, built on 1990s' standards, to a much more modern and technology-enabled approach.