Enterprise resilience

Enabling competitive advantage and minimizing the impact of disruption

pwc
All too often, leading organizations around the globe experience significant, costly business disruptions and show up in less than flattering headlines. The common thread? A lack of enterprise resilience.

The International Organization for Standardization (ISO) defines enterprise resilience as the ability of an organization to absorb and adapt in a changing environment so that it can deliver its objectives and survive and prosper. Prioritizing resilience at an enterprise scale is no doubt challenging, but a future-proof organization recognizes the opportunities true enterprise resilience provides to excel beyond competitors.

Leaders of resilient enterprises view business service delivery from a customer point of view to address what’s most critical to success: customer satisfaction and today’s expectation of “always on, accessible from anywhere” reliability. Resilience is a key business performance enabler that helps enhance market competitiveness, brand reputation, profitability, regulatory compliance as well as operational efficiency.

Successful enterprise resilience initiatives require a plan that’s broader than traditional business continuity planning or disaster recovery (BCP/DR), also encompassing technology and cybersecurity resilience; crisis management; third-party risk management; and regulatory compliance.

Many enterprises are undergoing a digital transformation to increase profitability, customer satisfaction, and competitive advantage – all of which depend on enterprise resilience to succeed in the long term. Poorly governed innovation and unplanned growth can rapidly increase the complexity of the technology environment, erode resilience and put a premium on managing risk. These types of strategic initiatives bring opportunities to those first movers but also complexities to execute and risks to any organization. From globally diverse regulations to regional business models to increasing reliance on third-party providers to building upon platforms that have significant technical and security related debt—all of this requires diligent focus.

Today’s rapidly advancing technology can better enable business leaders to leverage a holistic, automated, on-demand view of their critical business portfolios, processes and supporting systems as well as their relative interconnectivity. Leveraging this detailed information about your ever-changing organization is a critical input to any enterprise resilience initiative. Many organizations consider the gathering of this information about their environment a “tax” to the planning of any critical business initiative, often gathering the same or similar information multiple times leveraging subjective interviews or tribal knowledge over what is occurring in an environment.

The resilient foundation you begin to build today will continue to evolve and benefit your organization in years to come, as organizations shift from enterprise resilience (focused on full business resilience) to digital resilience (in which technology is self-healing, business platforms and supporting applications are self-reliant, and resilience is designed into each system) to continue to evolve their sustainable competitive differentiators.

An incident at a data center spurs a nationwide ATM system outage that damages a bank’s brand credibility

A retailer’s supplier goes out of business, causing that company’s profits to drop 49% year-over-year

A cyberattack takes out a firm’s computers, creating hundreds of millions in losses insurance won’t cover
What effective enterprise resilience looks like—a 360-degree view

Resilient enterprises can effectively prevent and manage disruptions; rapidly triage incidents when they occur; and learn from incidents in order to prevent them from happening again. Their goal: improve the ability to continually deliver goods and services and achieve business objectives across an interconnected ecosystem of businesses and third-party relationships. Or, as Forbes magazine succinctly put it: “Risk is inevitable. Resilience is everything.”

We’ve entered a new era of hyper-competitiveness, enhanced corporate performance transparency and enterprise risk, all of which requires a new, overarching, top-down approach to enterprise resiliency. This new approach should provide a 360-degree view of enterprise resiliency across all key areas, including business competition, supply chain, technology, cybersecurity, regulatory compliance, and more.

Can your organization withstand the bankruptcy or natural disaster that has critically impacted one of your key suppliers?

Will a cyber breach, data center or public cloud outage significantly affect your brand credibility and financial performance? These and other possible disruptions to your business are why it’s critical to make enterprise resilience a top priority.

Developing and sustaining enterprise resiliency requires a detailed understanding and prioritization of the organization’s most important assets along with potential threats to those assets.

To address gaps and reduce the risk of disruption, a resilient enterprise has a well-funded, prioritized plan:

1. To avoid disruptive events whenever possible, especially those that can affect critical aspects of your business’ performance;

2. To catch disruptive events that occur as soon as possible and to have a proactive, well-understood plan in place to triage the disruption and mitigate its impact;

3. To learn from events that do disrupt business operations and develop a root-cause remediation to help prevent the disruption, or others like it, from happening again.
Five drivers for enterprise resilience

1. Stakes are high.
Governments and regulators have increasingly focused attention on resilience to avoid broad, systemic crashes or volatility. Organizations may be out of compliance with regulations, resulting in stiff financial penalties. Consider a financial services firm, which was hit with a $500 million penalty by the U.S. Office of the Comptroller of the Currency (OCC) after it found the firm had failed to maintain a compliance risk management program appropriate for its size and complexity.¹

2. Customer experience is everything.
In today’s 24/7 global business environment, consumers expect the companies to be available at any time, and competition has made switching more friction-less than ever. When a business experiences a disruption, its customers are often quick to share their disappointment and anger on social media channels, which can damage brand reputation and cause financial losses.

3. Digital transformation increases complexity.
Enterprises are investing in digital transformation to dramatically improve business outcomes. In a complex, highly distributed environment, it’s challenging to architect resilient business platforms that can blend the best of the new with the current proven business systems and platforms.

4. Downtime is expensive.
There’s a growing realization that system, network or key supplier downtime, whatever the cause, is extremely costly, with some estimates totalling $5,600 a minute—or $300,000 per hour.¹

5. Cyberattacks are more sophisticated, destructive and targeted.
One growing concern is that tech-savvy nation states have the resources and motivation to create extremely destructive cyberattacks that can threaten any organization. The 2017 WannaCry ransomware attack was believed to have infected more than 300,000 computers in 150 countries and caused $4 billion in financial losses.³

What non-resilience looks like—angry customers and financial fallout

Threats to your resilience can manifest themselves in many ways and can occur anywhere, at any time. For unprepared enterprises, the threats can upend business-as-usual continuity and may cause significant damage to the brand and the bottom line.

Disruptive events, service interruptions and other adverse conditions that may put an enterprise’s resilience at risk can be grouped into four major impact areas—business/financial, technology, security, and business processes.

The expectation of a zero-defect environment is unreasonable. When the inevitable disruption occurs, the resilient enterprise catches and manages it early, so critical business operations can be restored quickly, regardless of the cause of the disruption or the underlying technology impacted.

**Business/financial** includes significant swings in an enterprise’s business, such as a recession; changing business models, such as a disruptive competitor; or an unexpected event causing financial loss not covered by insurance.

**Example:** In 2017, a ransomware attack impacted operations for a multinational food and beverage company. Its $100 million insurance claim was denied—with the insurer stating the attack was a “hostile or warlike action” excluded from coverage. Litigation is ongoing.

**Business process** issues include a disruption stemming from a third party, as when a key supplier goes out of business, or natural disasters such as a hurricane that causes a prolonged power outage in one or more facilities.

**Example:** In 2019, a supplier going out of business resulted in a supply chain disruption for a retailer, causing its shares to fall 16 percent and profits to plunge 49 percent. The primary culprit: a natural disaster such as a hurricane.

**Security** challenges include ransomware, social engineering, data breaches, physical security and other cyberattacks.

**Example:** A transport/logistics enterprise suffered a devastating ransomware attack in 2017 that forced it to reinstall 4,000 servers and 45,000 PCs, creating major business disruptions that resulted in some $300 million in losses.

**Technology** challenges are anything that adversely impacts the operating environment that support global business functions and processes.

**Example:** In 2019, smoke in a data center caused an extended outage at a US financial services firm, preventing many financial transactions. It was the bank’s second outage in a month. The two events damaged the bank’s brand reputation, with customers venting on social media.
Roadblocks to achieving enterprise resilience

Matching your organization’s most important business assets and processes to potential disruptions is the starting point toward becoming a resilient organization. The next step is to identify the hurdles that stand in the way of enterprise resilience, so that you can develop a plan for mitigating or overcoming them. The following are common roadblocks to enterprise resiliency.

**Fragmented, incomplete views of information.** One of the biggest challenges with enterprise resilience is the inability of enterprises to know all the technology they have and how things relate to each other. Many organizations, especially those launched decades ago, accrue a significant amount of technical and security debt over time. They’re running on an IT infrastructure of legacy hardware, software and tools. But it’s difficult to obtain a complete, near-real-time view of the technology landscape using legacy tools. Typically, these tools are difficult to maintain and only produce point-in-time snapshots.

Further, obtaining a holistic view can be especially challenging when business processes incorporate many disparate internal systems, supporting technologies and infrastructures, different data structures and multiple third-party suppliers. Most organizations have significant complexity in the number and type of automation and tools to support their business processes, increasing the difficulty to establish this foundational holistic view.

Enterprises need comprehensive, validated, automated, up-to-date maps of their business functions, processes and supporting technology and security environments that break down the silos. Without that, they may be unaware of all the software, hardware and networks that support each of their critical business systems; the changes that have been made to those technologies; and their various interdependencies, making true enterprise resilience impossible.

**Security disparities with third parties.** Today’s enterprise works with multiple third parties, including supply chain relationships, outsourcers, managed service providers and public cloud providers. However, vulnerabilities in your third parties’ systems and operations can expose your enterprise to risks it might not otherwise faced or fully prepared for.

**Sustained funding may be a low priority.** Too often, no one at a Board of Directors or C-suite level is advocating to make enterprise resilience a high priority. Consequently, there may be no budget allocated to support the proper resiliency business architecture and supporting technology. Even enterprises that have lost millions of dollars from outages may only triage the incident or get back to normal operations and not leverage it as an opportunity to uplift their overall resilience posture and competitiveness. Despite these obstacles, there’s growing interest among board members and C-level executives in prioritizing – and appropriately investing in – enterprise resiliency.

**Becoming resilient can seem daunting.** A plan that preserves the value of a company across all its business and supporting technology can be highly complicated to develop. How are you identifying all the important vulnerabilities across cyber, operational, business processes, crisis management and compliance? Many organizations have built up significant "lock in" with legacy business processes and systems and have built up a large amount of technical debt that makes it difficult to protect an ever-changing ecosystem. How have you brought all these pieces together into an integrated framework and process that helps your enterprise be resilient and meet regulatory expectations?

Above all, enterprise resilience isn’t a ‘one-and-done’ project. It’s not a point-in-time checklist that can be addressed and marked as complete or worse, forgotten. It needs to be an ongoing focus. And moving toward enterprise resilience itself can be disruptive. It might require adding new leaders and roles, reorganizing employees, teams or third-party suppliers.

Enterprise resilience isn’t a ‘one-and-done’ project. It’s not a point-in-time checklist that can be addressed and marked as complete—or worse, forgotten.
Resilient enterprises share a number of traits and behaviours that span across their lines of business and management layers:

No organization can be completely resilient all the time. It’s important to prioritize your enterprise’s most important competitive advantages, differentiators and assets to clearly understand what your risk tolerance is for your most important assets and other aspects of your business. This analysis, including a true understanding of interconnectivity of your internal business processes, systems and third-party providers, should form the foundation of your enterprise resilience program.

Resilience must be top-down. A Chief Resilience Officer or someone with similar responsibilities should have board-level support to issue a mandate for achieving resilience and a proposed timeline for accomplishing its initial target (usually in two or three years). While the mandate for resilience is top-down, championing resilience should also come from the bottom-up. Everyone in the organization must be conversant with the value and believe in the goal of becoming resilient; integrate it into their daily responsibilities and long-term planning; and share in its ownership.

Too often, resilience is viewed primarily through the supporting technology, cybersecurity and third-party risk lens. But to succeed, business leaders must drive resilience in a prioritized manner vs. a bottoms-up blanket approach. With input from business leaders, develop an action plan for how to safeguard against disruptions within each business unit/process, based on the maximum allowable outage your enterprise can tolerate for each.

A data-driven approach to resilience is essential, because it’s repeatable, scalable and starts with your critical business services and processes. This approach leverages analytics and real-time data flows that overlap with clearly defined business contexts within your supporting technology, cybersecurity and third-party supplier ecosystems. The end product of your plan should be an expansive, always-updated, complete view of the enterprise’s business processes; the underlying technologies that support them; and the interactions with other applications and systems across the organization’s global technology environment.

Resilient organizations have successfully instilled a focus on designing the lifecycle of resilience into company DNA and culture. It’s part of organizational and individual annual performance criteria, business and technology architecture principles, a primary concern of product lines, and is as much a factor to compensation as revenue and profitability.
An automated, on-demand view of everything the enterprise does

Resilient enterprise leaders understand that while their business processes might not change as frequently, the infrastructure that supports them can shift minute-by-minute. They’re no longer willing to rely on manual processes that can’t provide a complete picture of the enterprise interconnectivity.

Given the crucial importance of technology to today’s business success, resilient enterprise leaders recognize that static, point-in-time snapshots of the IT environment can’t serve their needs. Today’s advanced discovery technology makes it possible to observe and aggregate communications between systems to achieve an understanding of the interdependencies of critical business systems and processes that simply wasn’t possible before.

Business leaders can now leverage a holistic, automated, on-demand view of every system they have in place. Combined with a trusted resilience platform, infused with its provider’s years of experience in cybersecurity, compliance, and other risks, every organization now has within its reach the foundation it needs to thrive for years to come.

The resilient foundation you build today will pay big dividends in coming years. Organizations will inevitably evolve from today’s enterprise resilience, which is focused on business resilience during and after failover, to digital resilience, in which technology is self-healing, applications are self-reliant, and failovers will no longer be necessary because resilience is designed into each system.
Find out how PwC can help you achieve enterprise resilience

PwC offers technology and service-based solutions that can help you increase resiliency and mitigate negative impacts. To speak to our experienced professionals to discuss resilience strategy and solutions for your enterprise, email us at US_enterpriseresilience@pwc.com.
Contact us

Chris Morris
Principal, US Cybersecurity and Privacy Practice
christopher.morris@pwc.com
Tel: +1 (617) 530-7938

Julien Furioli
Principal, Advisory
julien.furioli@pwc.com
Tel: +1 (646) 247-0608

Christian Iantoni
Principal, US Cloud Transformation Co-Leader
christian.iantoni@pwc.com
Tel: +1 (312) 833-6373

Charlie Latch
Director, PwC New Ventures
charlie.latch@pwc.com
Tel: +1 (214) 616-3281