Enterprise resilience

Boosting your corporate immune system

MAY | 2020

pwc

Organisations are increasingly vulnerable as business becomes more complex, virtual and interdependent. Building and sustaining a resilient business is a commercial imperative and therefore, in a post-COVID-19 environment, what organisations do next, will matter most.

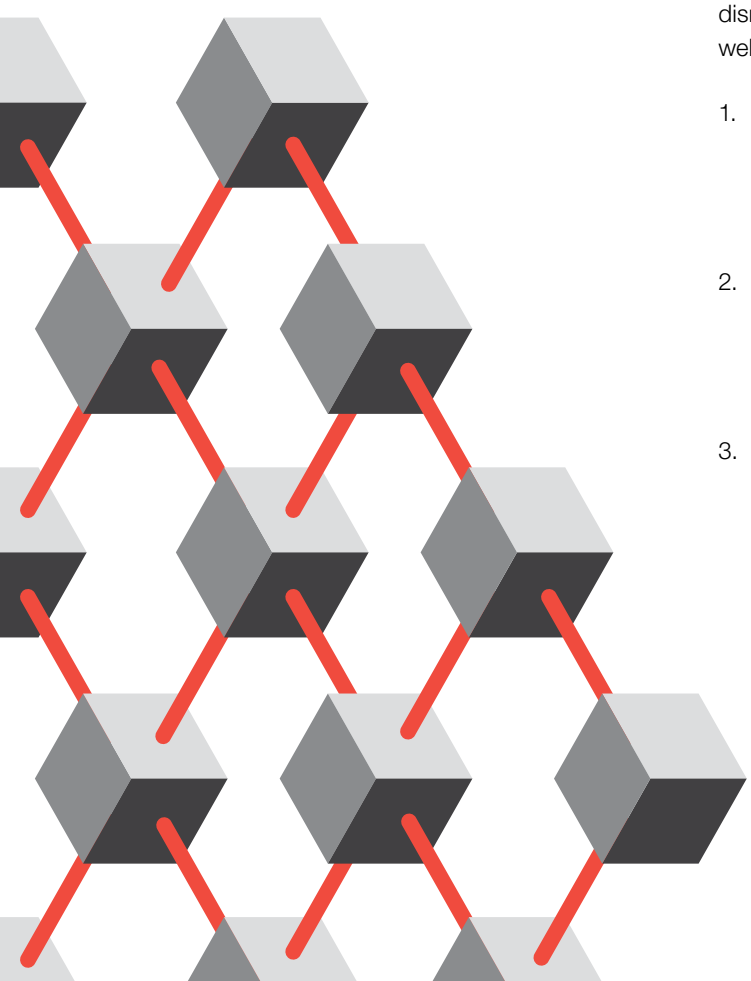
Your corporate immune system is what protects your business from illness – if it's in good shape and something strikes, you are ready to respond. Organisations that enhance their immune system are able to tackle challenges, fend off illness and bounce back more quickly. They also learn from incidents in order to prevent them from happening again.

The last decade has seen countless examples of businesses brought to their knees by a lack of foresight or poor management of a crises. 'Black swan' events have exposed the shortcomings of traditional risk management, putting resilience at the top of board agendas. Yet many are still not making the connection between resilience and success. While it's possible to survive in the short term, resilience is a fundamental pre-requisite for success over the longer term.

Successful enterprise resilience initiatives require an approach that's broader than traditional business continuity planning or disaster recovery, and permeates through all areas of the business across People, Processes & Operations, Technology & Cyber, Physical Assets & Facilities and Financial Resilience – underpinned by strategy and an adaptive culture.

In a post COVID-19 world, it will become more important than ever that leaders have a clear answer to a fundamental question: “How can my organisation be better prepared, next time this happens?”

Developing and sustaining enterprise resiliency requires a detailed understanding and prioritisation of the organisation’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, prioritised 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.

How leaders of highly resilient organisations describe themselves

Prepared for uncertainty

We understand our organisation and likely futures. We acknowledge we cannot predict everything, and must create optimal conditions to identify and respond to change.

Protecting what's important

From customers and people to assets and processes, we focus on what is important. We have processes in place to protect them, but we know there are risks and we're ready to manage them.

Consistently creating advantage

We use our resilience to create and exploit opportunity. We understand how our everyday decisions and activities, as well as our strategies and processes, manage risk and opportunity.

Avoiding major remediation

Major change, total transformation and even minor remediation costs time and money, and means we've not been as good as we could have. We avoid remediation by investing in getting it right the first time.

Identifying and acting on weak signals

We monitor key risk indicators (KRIs) across our business that serve as resilience signals – positive and negative – and address them before impact. These KRIs are measured against dynamic risk appetite tolerances to assess performance and risk at the same time.

Building trust

Our stakeholders trust us; our customers rely on us; people like working with us. They know they can count on us, they bring us opportunities and they forgive us because we always work hard to consistently honour them.

"Resilience isn't just about surviving in the present, it's about having the foresight, capability and agility to adapt and evolve; to identify and take advantage of opportunities as well as address challenges; to thrive as well as survive."

A framework for thinking about Enterprise Resilience

The International Organisation for Standardisation (ISO) defines enterprise resilience as the ability of an organisation to absorb and adapt in a changing environment so that it can deliver on its objectives, survive and prosper. Enterprise Resilience is more than business continuity. It is an opportunity for organisations to build resilience throughout the whole business. For example – building resilience only into financial aspects (such as working capital and cash flow) will be of little help if failed technology or cyber incidents create reputational damage that is hard to repair. Thinking about resilience 'enterprise-wide' means that when the next disaster, pandemic or crisis hits, the organisation **as a whole** can both thrive and survive.

People are the life-blood of every organisation. Resilience in the workforce is one of the key components that supports an organisation's sustained success. Some of the risks include:

- Workforce cost management
- Health & Safety
- Capacity planning
- Contingency planning

Process and operations include **all the functional areas, processes and operational disciplines** in the organisation that are relied upon for sustained operations. Some of the risks include:

- Supply shortages, supply chain interruptions and delays
- Data management & quality
- Insufficient risk management practices

Facilities and physical assets play a pivotal role to ensure **sustained business operations.** Disruption to the access and safety of physical assets in one or more locations can have a severe impact on an organisation's ability to operate continuously. Some of the risks include:

- Breakdown of critical infrastructure
- Access to and safety of critical infrastructure
- Loss of physical assets due to extreme events or climate change

The **sustainability and ongoing flexibility of technology** in an organisation is critical to not only respond successfully in times of crisis, but help organisations to flourish. Some of the risks include:

- Technology & cyber risks
- Infrastructure & tools
- Remote working demands

With often **rapid impact on economies and individual businesses,** organisations need to consistently have oversight over micro-level financial impacts including identifying new risks and opportunities. Some of the risks include:

- Accurate forecasting
- Cashflow
- Working capital
- Scenario analysis and stress testing

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. Organisations may fail to comply with regulations, resulting in stiff financial penalties. Consider a financial services firm, which was hit with a $700 million penalty by the Australian Transaction Reports and Analysis Centre (AUSTRAC) after it found the firm had failed to carry out an appropriate assessment of the money laundering and terrorism financing (ML/TF) risks.

2. Customer experience is everything

In today's 24/7 global business environment, consumers expect 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

Organisations 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 realisation 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.

5. Cyberattacks are more sophisticated, destructive and targeted

One growing concern is that tech-savvy nations have the resources and motivation to create extremely destructive cyberattacks that can threaten any organisation. 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.

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 organisations, 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 organisation's resilience at risk, occur across a number of the operating model components we mentioned earlier.

Financial/business issues could include significant swings in an organisation'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.

Process & Operations issues could include a disruption stemming from a third party, such as when a key supplier goes out of business, or failure to leverage key business data as a result of insufficient data & quality management practices.

> Example: In 2019, a retailer saw its shares fall 16 percent to their lowest point in 18 months after the company reported sales had dropped 3 percent and **profits plunged 49 percent.** The primary culprit: a supply chain disruption resulting from the retailer's major supplier going out of business.

Cyber & security such as 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 supports 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.

→ 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.

Roadblocks to achieving enterprise resilience

Matching your organisation's most important business assets and processes to potential disruptions is the starting point toward becoming a resilient organisation. 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 resilience that we see from a technology perspective.

Fragmented, incomplete views of information. One of the biggest challenges with enterprise resilience is the inability of organisations to know all the technology they have and how things relate to each other. Many organisations, 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 organisations 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.

Organisations 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. Organisations today work 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 face or be fully prepared for.

Sustained funding may be a low priority. Too often, no one at a Board or C-suite level is advocating to make enterprise resilience a high priority. Consequently, there may be no budget allocated to support the proper resilience business architecture and supporting technology. Even organisations 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-suite executives in prioritising – 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 organisations 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 and daunting 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 'set-and-forget' 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, reorganising employees, teams or third-party suppliers.

Enterprise resilience isn't a 'set-and-forget' project. It's not a point-in-time checklist that can be addressed and marked as complete – or worse, forgotten.

Success strategies for becoming a more resilient organisation

Resilient organisations share a number of traits and behaviours that span across their lines of business and management layers:

Priorities

No organisation can be completely resilient all the time. It's important to prioritise your enterprise's most important competitive advantages, differentiators and assets to clearly understand what your risk tolerance is across all parts 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.

Sponsorship

Resilience must be top-down. A relevant senior executive, with Board-level support, should be responsible for building resilience by delivering on prioritised resilience improvements across a reasonable timeframe (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 organisation 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.

Business Engagement

Too often, resilience is viewed through the supporting technology, cybersecurity and third-party risk lens. To succeed, business leaders must drive resilience in an integrated and prioritised manner. 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 organisation can tolerate for each. Ensure that contributions from all parts of the business are considered – this way everyone will own their resilience obligations.

Culture

Resilient organisations have successfully instilled a focus on designing the lifecycle of resilience into company DNA and culture – building an adaptive capacity. It's part of organisational and individual annual performance criteria, business and technology architecture principles and is as much a factor in compensation as revenue and profitability.

Data-driven Mindset

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 are inline with the way you actually run the business, your supporting technology, cybersecurity and third-party supplier ecosystems. The end product of your plan should be an expansive, dynamic, complete view of the organisation's business processes; the underlying technologies that support them; and the interactions with other applications and systems across the organisation's global technology environment.

Find out how PwC can support you on your enterprise resilience journey

We offer a range of diagnostic, technology and service-based solutions that can help you increase resiliency and mitigate negative future impacts. To talk to our experienced professionals about our pragmatic approach to helping New Zealand businesses become more resilient, please get in touch:

Chloe Gallagher
Partner: Risk & Resilience
chloe.v.gallagher@pwc.com
+64 21 051 6699

David Nalder
Partner: Risk & Resilience
david.w.nalder@pwc.com
Tel: +64 21 380 889

Hennie van der Watt
Director: Governance, Risk and Compliance
hennie.j.vanderwatt@pwc.com
Tel: +64 20 4142 1060

Parth Patel
Director: Technology & Cyber Risk
parth.c.patel@pwc.com
Tel: +64 21 856 842

Ian Curry
Director: Technology & Cyber Risk
ian.j.curry@pwc.com
Tel: +64 21 829 603

Yoonyoung Lee
Director: Business Assurance
yoonyoung.y.lee@pwc.com
Tel: +64 21 134 9352

www.pwc.co.nz