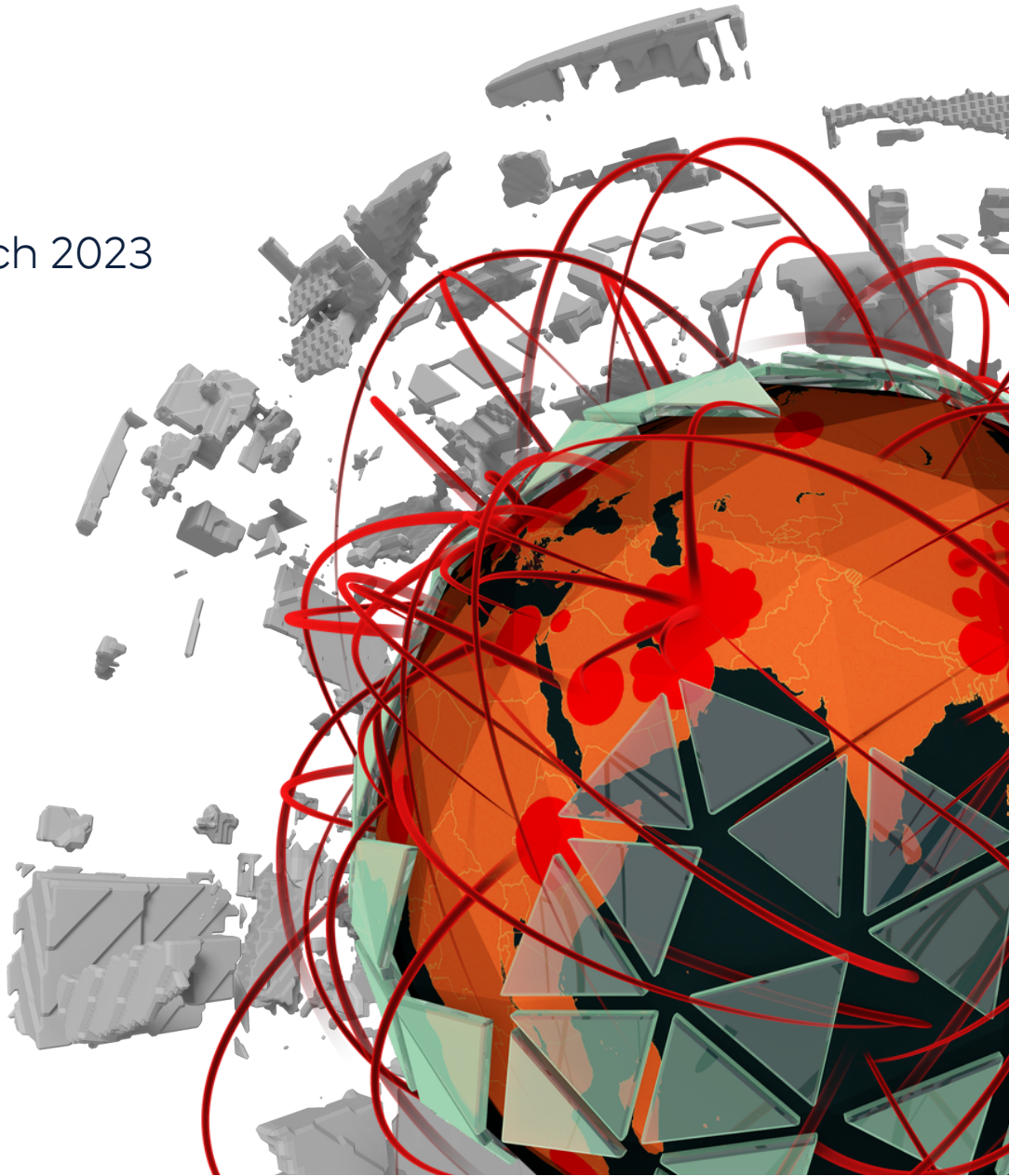
emqnet

OPERATIONAL RESILIENCE

Equipping businesses to thrive.

Published March 2023



COMPOSED BY

Dynamiq
Helping brave organisations thrive

Table of Contents

About this Paper

Operational resilience isn't a slogan eulogised at motivational TED Talks so that business can tick a KPI box once a year. Nor is it a simple business management plug-in executives can buy. Job done. Operational resilience is an all-of-enterprise business continuity framework that ensures global companies can not only survive in the face of adversity, but thrive.

In today's volatile business landscape, operational resilience has never been more important. Recent events such as the global pandemic, natural disasters and the war in Ukraine illustrate how operating conditions are becoming harder. The world is becoming a more complex place in which to do business, and this will only intensify as enterprise grapples with the new world order. Those businesses that transform, adapt and embrace change will flourish, while those that don't will founder.

Operational resilience is a mindset and a skillset. A next-generation operating paradigm that prescribes how businesses – forward-thinking businesses – will respond in a crisis. It's about being on the front foot. Reacting with decisive, structured intent to unseen events, and being proactive in anticipating and preparing for those you can. Operational resilience gives global businesses agency to operate with certainty and communicate their value proposition to the market.

The evolving threat landscape

As world economies recover from the pandemic, smart businesses will not be resting on their laurels. They will be evaluating their performance during the COVID years, forensically analysing their response methodologies, learning from their mistakes, and preparing for the next market shock. The threat landscape is continually evolving as risks become more frequent and more complex. Leading the threat index going forward are cyber attack and natural perils.

The research topics addressed in this paper are;

1. **CYBER ATTACK**
Cybersecurity incidents are increasing due to the rapid uptake of new digital technologies.

2. **NATURAL PERILS**
Natural perils present the biggest risk to operational continuity.

3. **WHAT IS THE ROLE OF OPERATIONAL RESILIENCE?**
To ensure a return to business as usual with minimal loss to assets, revenue and reputation.

4. **OPERATIONAL RESILIENCE DONE RIGHT**
The framework that enables enterprise to prepare, respond and recover, no matter the event.

5. **CHANGING THE 'RISK' MINDSET**
Whilst identifying and mitigating risk is important, it's how you respond to the risks that become incidents that really counts.

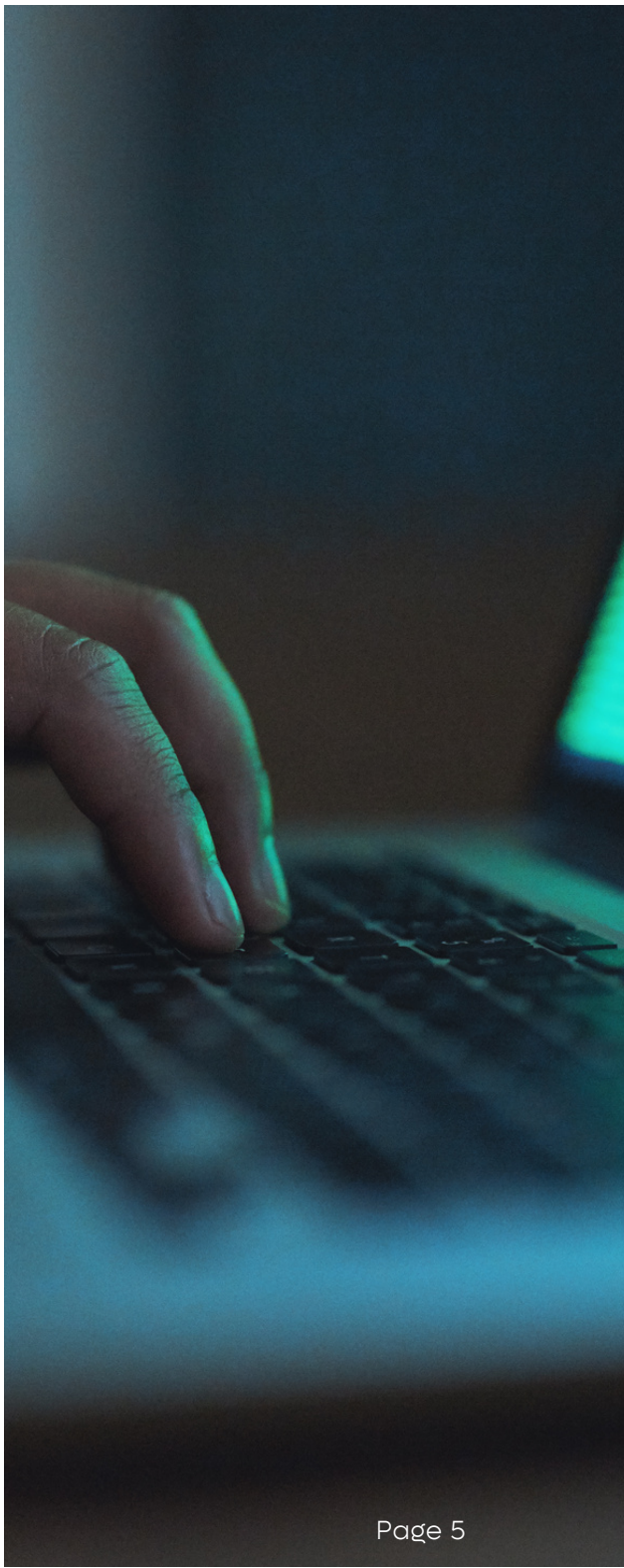
Cyber Attack

The World Economic Forum (WEF) predicts a "catastrophic" global cyber attack could occur in the next two years.

In its Global Cybersecurity Outlook 2023 report, the WEF warned the rapid uptake of new digital technologies, coupled with geopolitical tensions, would be exploited by cyber attackers seeking to cause disruption and reputational damage.

"The impact of cybersecurity incidents can cascade from organization to organization and across borders. The risks this creates are potentially systemic, often contagious and frequently beyond the understanding or control of any single entity," the report states. "Cybersecurity experts are themselves only beginning to grasp the extent and consequences of the technological interdependencies being created by their organizations' digital transformation."

The report stated that while business leaders and boards of directors are increasingly attuned to the risk of cyber attack, their response to the threat is lacking. "In many organizations, questions about the most recent cyber news continue to drown out conversations on the most important initiatives and investments needed to meaningfully reduce cyber risk," the report said.



Natural Perils

After malicious human-made threats, natural perils present the biggest risk to operational continuity.

Climate change has seen an increase in extreme weather events globally, and the trend is set to continue, jeopardising critical infrastructure, labour security, transport, supply chains – and even lives.

The World Meteorological Organization (WMO) reported in August 2021 that extreme weather events had stripped US$3.64 trillion from the global economy in the 50 years since 1970. On average, one weather-related disaster occurred every day, equating to $US202 million in daily losses. The economic impact increased sevenfold in half a century.

"The number of weather, climate and water extremes are increasing and will become more frequent and severe in many parts of the world as a result of climate change," WMO Secretary-General Professor Petteri Taalas said in a statement.

"That means more heatwaves, drought and forest fires such as those we have observed recently in Europe and North America. We have more water vapor in the atmosphere, which is exacerbating extreme rainfall and deadly flooding." Prof Taalas added that economic losses were mounting as exposure to these events increased, saying there was a need for greater investment in disaster risk reduction and a "multi-hazard approach to disaster risk management".

Extreme weather events stripped

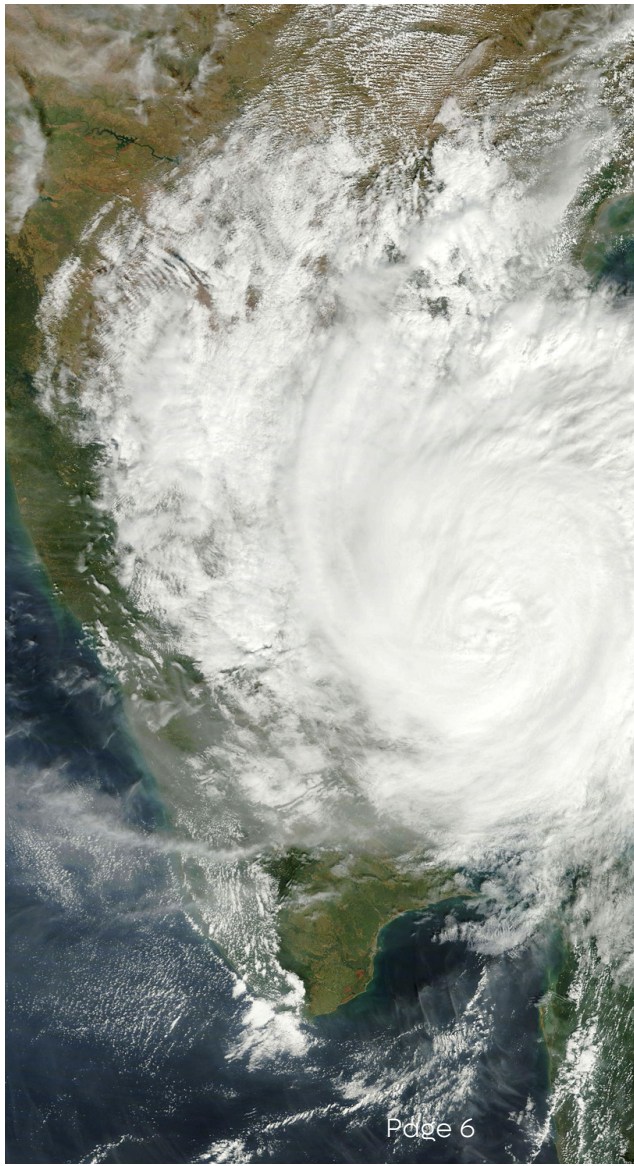
US $3.64 trillion

from the global economy in

50 years

since

1970



What is the role of operational resilience?

Operational resilience won't stop a cyclone hitting critical infrastructure in Papua New Guinea, or take the heat out of a forest fire encircling an open-cut mine in California. But it will insulate business from the fallout of a disruptive event or major crisis – ensuring a return to business as usual with minimal loss to assets, revenue and reputation.

Devastating floods in the Australian state of Queensland laid bare the imperative of having a robust business continuity plan.

The disaster inundated more than 3,500 businesses, damaged 19,000km of road and destroyed almost one third of the rail network in Australia's second-largest state.

The total damage bill was estimated at more than $6 billion.

emqnet had clients in the flood zone and conducted an analysis comparing businesses with a mature operational resilience program in place, and those without. The results were startling. The analysis compared two manufacturing enterprises in the same industrial complex. Both lost mains power, landline phone connections and air-conditioning, and suffered significant damage to their factory floors, offices, storerooms, IT infrastructure and fire control panels. The premises were both no-go zones for 48 hours.

During those two days, the emqnet client wasted no time activating their continuity plan. An off-site recovery coordination centre was immediately established and suppliers and tradespeople rapidly engaged. The business recommenced basic work activities within four business days and full operations resumed within two weeks. By comparison, the business without an operational resilience plan was completely out of action for two weeks. It took a further two months before normal operations resumed, causing significant financial strain.

Their mistake? Lack of crisis management preparedness.

While the emqnet client was quickly and methodically engaging trades and materials, the other business waited two critical days until they could inspect the flood damage before launching into recovery mode. By this time demand for materials and services was extreme. The delay was a failure that cost the business dearly in time and weeks of lost productivity.

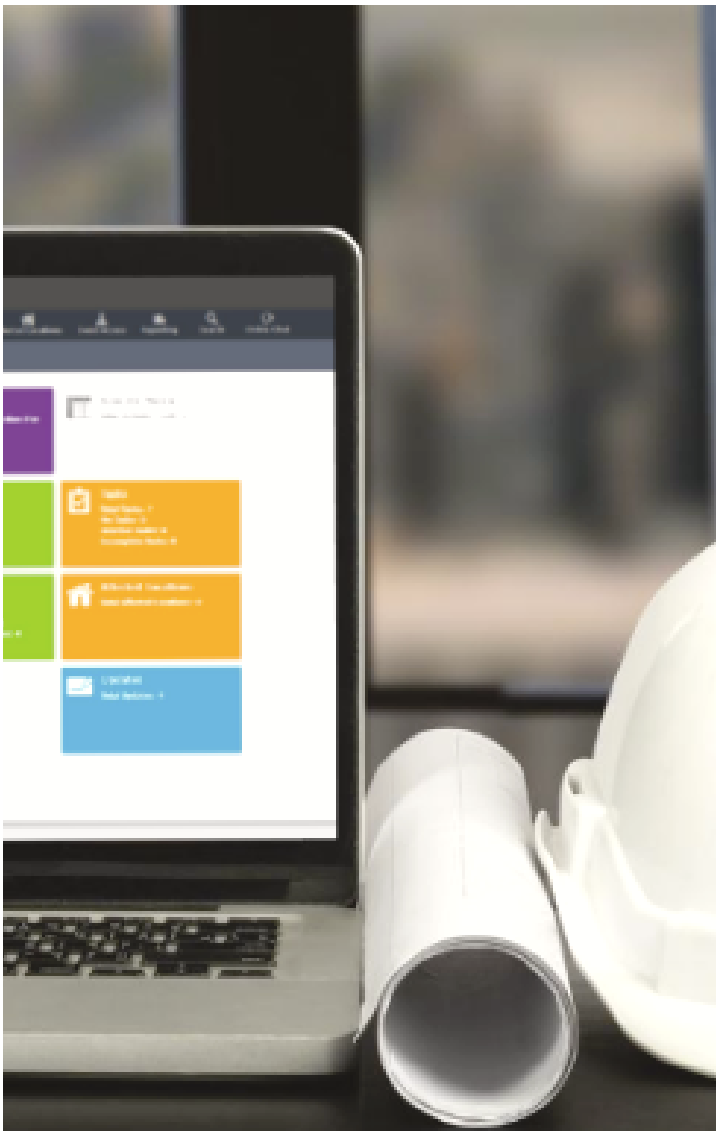
Operational resilience done right

SO, WHAT DOES GOOD OPERATIONAL RESILIENCE LOOK LIKE?

In simple terms, it's a framework that enables enterprise to prepare for, respond to and recover from a shock, no matter the severity.

The same principles apply regardless of the threat – be it a cyclone, workplace accident, cyber attack or civil unrest – and irrespective of the business. It doesn't matter if a company is a single-site manufacturing enterprise or a multinational resources conglomerate. The frameworks and methodologies underpinning a robust operational resilience strategy are the same. However, the larger the enterprise, the greater the liability if the business gets it wrong.

Operational resilience starts at the top. It's about quality leadership driving a top-down, organisation-wide approach to business continuity. It's about arming individuals and teams with the capability to prepare for, and respond to, incidents promptly and effectively, in a way that minimises the impact to the business. Crisis management teams may activate for hours, days, weeks or even years. .



Central to the incident response is a rigorous process, backed by clear and decisive decision making, rigid chains of command and stakeholder engagement. Data capture is also crucial. How can a business measure their performance in a crisis if they don't have a centralised platform for recording information, actions and communications that tell the story of how they fared under pressure?

These metrics provide invaluable, actionable insights that can be leveraged to enhance an organisation's resilience capability going forward. Data also tells an important story outside the business; to capital providers, regulators and insurers with an interest in how well a company can minimise the impact of a major disruption on their day-to-day operations.

So, how do your measure operational resilience?

There are various response metrics and data points that, when captured together and collated, provide an objective insight into an organisation's resilience profile. These data points measure things like response capability and capacity; gauging a business's ability to respond effectively to a single event or multiple disruptions.

Data also measures the capabilities of people; assessing personnel knowledge and experience, performance under pressure, and their ability to make good decisions quickly and in line with the organisations expectations. Together, these performance indicators will dictate how quickly normal operations can be restored after an incident.

Changing the 'risk' mindset

"INCIDENTS WILL OCCUR, REGARDLESS OF ANY RISK MITIGATION EFFORT"

For too long, operational resilience has focused squarely on risk management. But this is a superficial approach to a much more complex challenge. Whilst identifying and mitigating risk is important, it's how you respond to those risks that really counts. The reality for enterprises operating in dangerous environments is that incidents will occur, regardless of any risk mitigation effort. It's therefore imperative to shift the resilience narrative from risk to response; to focus on building a proactive incident management framework that enables teams to respond swiftly, act decisively and minimise any impact to business operations.

Key to any response plan is personnel. Who will coordinate your crisis response? When it comes to cyber threat, the burden can no longer rest solely with the IT team or cyber taskforce, nor can any other parts of the business operate in silos. Each must be integrated into a broader enterprise-wide response solution. One centralised platform for inputting information, coordinating tasks, sharing information and managing stakeholders.

Cyber breaches tell us that every business needs a digital redundancy plan, so this platform must be a standalone application, with no dependencies on other data sources or IT providers. This way, if systems access goes down, the business can continue to operate, and sites communicate effectively with each other, through a standalone resilience platform.

The Takeaway

Act today.

The only thing worse than an industrial disaster is not having an operational resilience program in place to manage the fallout. Too many businesses continue to lose time, resources, money and public confidence because they are not adequately equipped to manage an incident that impacts the core operations of their business.

In today's challenging threat landscape, that is akin to walking blindfolded through a minefield without body armor.

Building operational resilience needn't be an arduous internal process. There are resilience experts who live and breathe risk and response planning. They have the experience and capability to help the most threat-exposed businesses grow their resilience profile.

Investing in your people and an expert-led resilience program could be the best financial decision your enterprise makes.

For more information contact us at resilience@dynamiq.com.au

emqnet