THE END OF TRADITIONAL RESILIENCE

THE MOVE FROM FIX ON FAILURE TO BUILDING FOR RESILIENCE

THE END OF TRADITIONAL RESILIENCE

The move from fix on failure to building for resilience

Our increasingly complex world demands a new approach

Traditionally, we have understood resilience as our ability to reduce faults and outages to acceptable levels. It meant a focus on recovery after an event. But the status quo has been upended due to the complex and globally interconnected nature of Australia's economy. The challenges have been further exacerbated by a paradigm shift in customer expectations, the increased scale of threats, rising collection and use of data, climate change, and natural disasters - all of which demand a greater need for agility and flexibility.

Paradigm shift in customer expectations driven by digitisation

> *"Australians have seen a new and emerging standard from the public sector and they won't easily accept a reverse of this, rather they will demand consistency across touchpoints and a culture of continuous improvement to ensure service delivery standards keep pace with increasing expectations."*
>
> **– KPMG Customer Experience Excellence Report 2021**

Digital service disruptions can have enormous cost. Kyle Duffy, VP Global Solutions at Pageduty noted some of the largest global retailers could lose up to half a million dollars in revenue per minute when digital services were degraded or disrupted[1]. We know even minor service degradations and short outages can cost millions. Further, the reputational impacts can be significant and instant. Outages can generate front-page news stories and dominate social media conversations.

Amid growing customer expectations for instant gratification and an "always on" response, digital outages can have far-reaching consequences. Customer experience can be regarded as the new competitive battleground for government and business, where service uptime and reliability are now some of the most important measures of success.

Increasing supply chain dependency

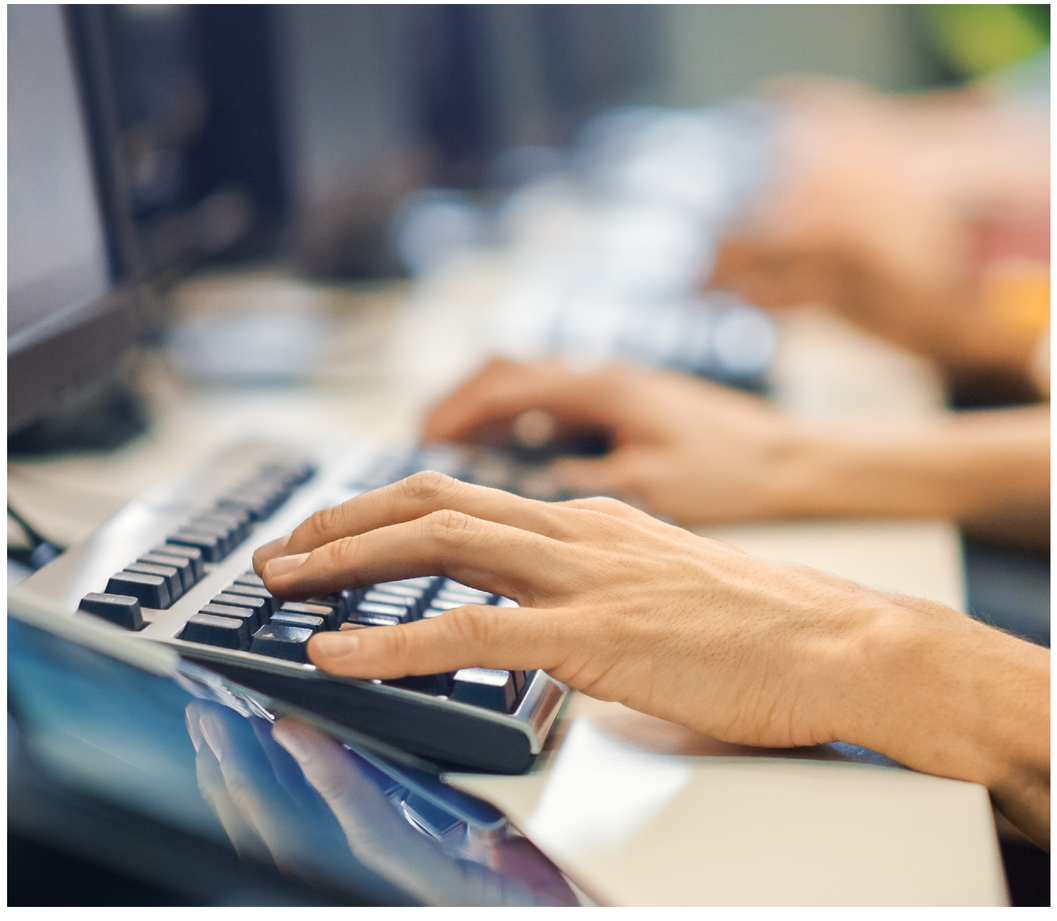
Supply chain viability means meeting changing demands and being able to survive in a potentially disrupted environment. In the case of extraordinary events, for example a cyber attack, supply chain resilience to disruptions needs to be considered at the scale of survivability or viability to ensure you can continue to deliver core outcomes.

During peak times of the COVID-19 outbreak, we saw global supply chains impacted in an unprecedented and extraordinary manner. This led to highly visible shortage of goods and services on a scale not experienced in Australia for decades, and highlighted a need to build stronger resilience mechanisms and practices into our supply chains. Among the high-profile impacts was the worldwide shortages of semi-conductor chips, which paralysed the global automotive and consumer-electronics appliances industry. According to an analysis by Goldman Sachs, the semiconductor shortage touched 169 industries in some way.

The rising risk of cyber incidents and the role of state actors

Malicious activities are increasing and no sector is immune. The Australian Cyber Security Centre's **Annual Cyber Threat Report** highlighted 34.7 per cent of the cyber security incidents were reported by Australian government[2]. In Australia, high-profile cyber incidents have impacted organisations from hospitals and healthcare networks, to logistics providers, retailers, not-for-profits, and government agencies. The Australian Federal Police have estimated losses from cyber security incidents totalling $33 billion a year. Further, losses reported to the Australian Competition and Consumer Commission's Scamwatch between January and May this year have totalled $205 million, an increase of 166 per cent on the same period last year. These figures are considered significant underestimates of the true losses.

Imagine what would happen if your organisation was the target of a cyber incident? Would you be forced to shut down your network, as others have? Would you operate with limited capability? Computing operations at shipping giant Maersk were crippled within 15 minutes across 60 nations after they were hit by a cyber incident in June 2017. Within an hour, the $50 billion company had lost all digital capability globally. This "extinction event" left the business incapacitated.



1. "How can digital services keep up with customer expectations in this new 'always on' world?", Anthill, **https://anthillonline.com/how-can-digital-services-keep-up-with-customer-expectations-in-this-new-always-on-world/**, accessed August 2022.

2. Australian Cyber Security Centre, ACSC **Annual Cyber Threat Report - 2020-2021.pdf,** accessed August 2022.

Growing data collection and use at unprecedented scale

> *"The amount of digital data created over the next five years will be greater than twice the amount of data created since the advent of digital."*
>
> **– Dave Reinsel, IDC Global DataSphere Senior Vice President[3].**

The global data boom is well underway. Businesses are not only generating more data than ever, but due to regulation and auditing obligations, they are now required to store it for years, or even decades. In today's digitised economy there is an increased dependence on data to enable customer experience. Any compromise of this data or disruption to its availability, leaves businesses vulnerable and the trustworthiness of systems open to question.

Citizens are at risk personally, too

Despite growing efforts to prevent cyber incidents, the threats are real and rising. Telstra's Cleaner Pipes initiative to reduce cyber threats through phishing, ransomware and malware blocked 200 million scam calls between September 2020 and June 2022, including 10 million in May 2022 alone. Just under half of all incoming BigPond emails are blocked, around 2.4 billion a month and 29 billion from September 2020. Further, about 5000 Australians are protected each week from accessing spoof and potentially malicious websites through DNS blocking of more than 32 million malicious sites each month. All it takes is one to get through and there can be significant damage wreaked.

It is no longer enough to assume a stable operating environment and manage risk defensively. There is a fundamental need to ***move from fix on fail to fix before fail.***

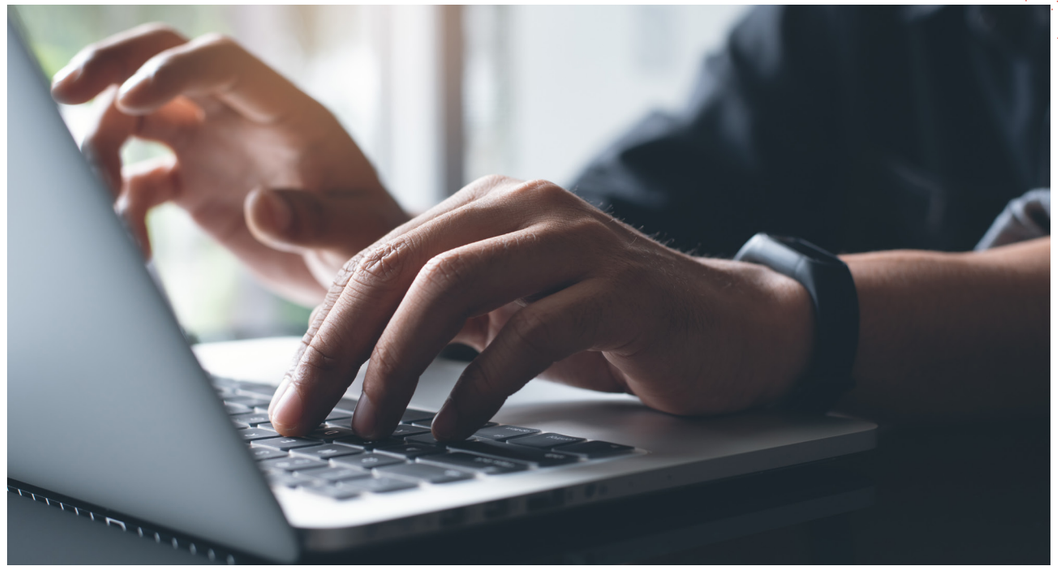
> *"Given the prevalence of malicious cyber actors targeting Australian networks – which is often under-reported to the ACSC – there is a strong need for greater resilience, and for Australian organisations and individuals to prepare to respond to and recover from any cyber attack to their networks."*
>
> **– ACSC Annual Cyber Threat Report 2020-2021**

Rethinking resilience – what does it take

A resilient organisation has a proactive approach to its operations and processes front of mind. Its technology and processes are built and maintained to have the capability to anticipate, prevent, detect, respond and recover from any and all events securely, reliably and expediently. It collaborates across domains to achieve the right end-to-end resilient outcomes and meet the expectations of customers, the community and shareholders.

Business is complex and disruption is inevitable. Amid geopolitical shifts, lingering pandemic impacts, climate change and rapid digital transformation, resilience is essential as a foundation for business operations and growth. It is about making considered investments in key areas to ensure your business can minimise the impact of disruption. A forward-thinking and multifaceted approach to resilience is focussed on ensuring readiness ahead of when it is required.

3. IDC, "Worldwide Global DataSphere Forecast", https://www.idc.com/getdoc.jsp?containerId=US46410421, accessed August 2022.



Understanding your resilience posture

Building resilience is key to an enduring business. Understanding an organisation's resilience goes far beyond a simple "do we have it" or "don't we have it" approach. It is important to know what is critical to a business - the "Crown Jewels". Know the value of your data, to yourself and those who may wish to do you harm. With this knowledge comes an understanding of the threat, and a focus on areas that could be considered vulnerabilities or gaps. These areas will require the strongest resilience posture.

Consider your resilience capability against the following key areas:

Technology resilience – Technology resilience means understanding the value of systems and their interconnections to prioritise security, triage, recovery and adaptions. Could any of these systems, or outages within them, threaten your organisation? Is your business geared for digital continuity, with systems in place to minimise disruption and support redundancy for telecommunications, computing, storage, software and enabled equipment? Do you know where your data is stored, how often it is saved and backed up? How could it be recovered in the event of a cyber incident or other interruption?

Supplier resilience – Supply chains should be assessed end to end, including staffing, parts and distribution. What suppliers is your organisation dependent on? Consider who has access to your data and where this data is located across your supply chain. How can disruption be avoided and continuity ensured? Amid a changing geopolitical environment, sovereign options should be considered.

Business resilience – Is it a blind spot in your organisation's business continuity? Are there individuals, services, equipment, or products that would create business interruptions if they were unavailable or otherwise impacted?

An awareness of an organisation's risks to the Crown Jewels is essential to establish its current resilience posture. It also guides an understanding of where resources need to be distributed or where extra attention must be paid to uplift the posture to the desired levels.

Where to focus across the resilience spectrum

The resilience spectrum operates across:

Prevention – This involves technology and processes that are built and maintained to have the capability to anticipate and prevent incident.

Reducing impacts – By using a more considered, distributed architecture, resilience can be enhanced by creating smaller "blast zones" in the event of an issue or incident. Taking this approach to a network architecture for example, if one part of the network goes down, the network automatically reconfigures to reduce the impact and number of services affected.

Response and recovery – This refers to a known response plan to enable recovery from any and all events securely, reliably and expediently.

While an organisation needs all parts of the resilience spectrum, it can choose to focus on specific areas depending on the organisation's aspirations and capabilities. An organisation can also choose to apply different parts of the resilience spectrum to different risks, for example, prevention of cyber threats, response and recovery for supplier risks.

"Advancing cyber resilience requires the public and private sectors to collaborate in new and innovative ways."

– World Economic Forum, Cyber Resilience: Playbook for Public-Private Collaboration

Resilience is a culture

For resilience to be sustainable and not a "point in time" exercise, organisations must understand the behavioural and cultural aspects. Is resilience core to your culture? For an organisation to ensure its products and services are resilient, all employees must adopt a resilience mindset and embed the approach into everyday activity. It requires a company-wide effort, driven by a strong executive focus and sponsorship to support resilience activity. A collaborative environment across disciplines goes a long way to supporting a resilient culture.

To build trust, employees must feel comfortable with disclosing errors, for example clicking on a dodgy link, or leaving their laptop behind on a train. Disclosure and transparency are key to responding effectively and mitigating further risk and damage. If employees are embarrassed or fearful of how they might be perceived by others, it can exacerbate problems. A culture of learning, support and trust is vital to achieving resilience.

Organisations should be focussing on resilience behaviours, as they move from a fix-on-fail approach to ensure everyone at every level of the organisation has resilience front of mind – a fix-before-we-fail approach.

It is important to have a simple, standardised and consolidated way of working where resilience is built into everything we do – and resilience is not a 'hero' activity after an event. This includes ensuring that resilience is not compromised because of a deadline and the organisation knows and understands the business and personal consequences of non-conformance.

It is important that organisational leadership focus on creating an environment of psychological safety, using a positive reinforcement approach to ensure this collaboration, focus and cultural shift occurs.

"Approximately 75% of Commonwealth entities include cyber resilience in their business continuity plans and have developed incident response plans, an increase from the 51% reported in 2019."

– The Commonwealth Cyber Security Posture in 2020[4]

4. ACSC, "The Commonwealth Cyber Security Posture in 2020", The Commonwealth Cyber Security Posture in 2020 | Cyber.gov.au, accessed August 2022.

KEY TAKEAWAYS:

Know your Crown Jewels
understand the data and systems that hold the most value to you and your organisation

Articulate the gaps in your resilience posture
(technology, supply, business resilience)

Make clear investments across the resilience spectrum

Nurture a resilient culture

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE