Downtime: a rising challenge for organisations in Australia & New Zealand

Downtime can cost organisations up to AU$86 billion in Australia and NZ$75 billion in New Zealand

splunk>

In late 2024, Splunk conducted a groundbreaking report examining the direct and historically overlooked costs of unplanned downtime across the globe. I am pleased to extend this report to Australia and New Zealand. The research reveals a breakdown of the financial costs and time from cybersecurity incidents and system outages, as well as common causes and consequences of downtime in both countries.

Cybersecurity threats in ANZ are intensifying, with recent high-profile incidents underscoring the urgent need for stronger defences. Beyond the immediate risks to data and IT systems, these incidents often lead to unplanned downtime, which can result in financial losses and damage to reputation. Additionally, there is such a complexity in the environment and tech industry that is leading to talent shortage, employee burnouts and greater room for error.

In today's fast-paced digital landscape, downtime has evolved from a mere inconvenience to a critical vulnerability that businesses can no longer overlook. As artificial intelligence (AI) accelerates, the potential for disruption is greater than ever, and businesses must be prepared to manage these risks.

At the same time, regulatory frameworks are also evolving to keep pace with AI. For example, the Australian Government has proposed 10 mandatory guardrails for high-risk AI systems, demonstrating the increasing focus on responsible and ethical AI. These types of developments also highlight the need to embrace AI while ensuring compliance with new and forthcoming regulations.

Our research reveals that, despite claims from business leaders in Australia and New Zealand that they are prepared for unplanned downtime, they are not only facing financial losses but also experiencing productivity setbacks, which may hinder innovation and weaken customer trust as a direct consequence of downtime. The research also shows that while ANZ organisations are increasingly prepared for unplanned downtime, critical gaps still exist in ensuring true digital resilience.

Nevertheless, the Australian and New Zealand Governments are prioritising digital resilience and focusing on strengthening their cybersecurity frameworks to be global leaders in cybersecurity.

As the next few pages will uncover, understanding downtime will be crucial for any organisation aiming to thrive in an era of increasing uncertainty.

Craig Bates,
Senior Vice President & General Manager,
Asia Pacific

Contents

Understanding the impact of downtime on organisations

Downtime is identified as any service degradation or outage of a business system. The disruption goes beyond immediate financial losses, impacting an organisation's productivity, reputation and long-term growth.

Expanding on Splunk's global downtime report, this survey provides a comprehensive understanding of the impact of downtime on ANZ organisations. We conducted a survey among 551 Australian and New Zealand business leaders.

$250,700+
Lost revenue

Downtime is costing Australian businesses an average of A$250,754 and New Zealand businesses NZ$210,917

89%

of ANZ organisations have experienced a cybersecurity incident

Cyber threats drive downtime in ANZ

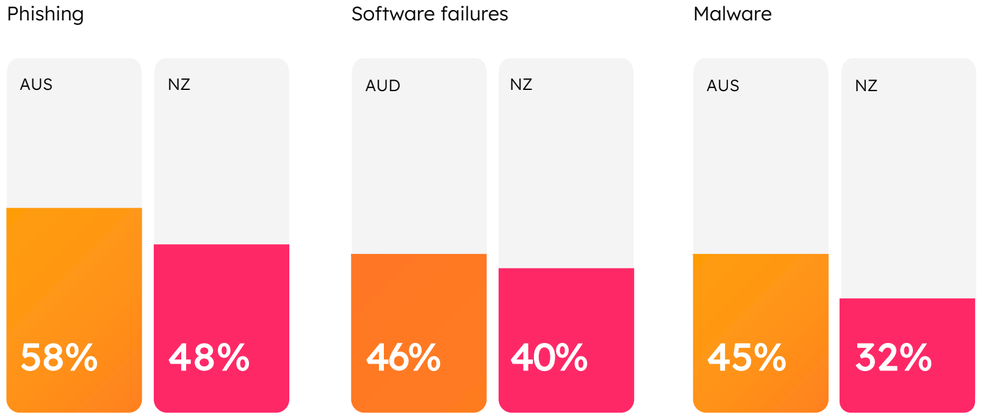
Cyber threats are reaching unprecedented levels, with 92% of Australian organisations and 85% of New Zealand organisations reporting that they have been exposed to a cybersecurity incident or system issue.

Like global organisations, phishing was the most common threat and ANZ business leaders reported experiencing phishing attacks at a similar rate to the global average (56%), as highlighted in Splunk's 'Hidden Costs of Downtime' report.

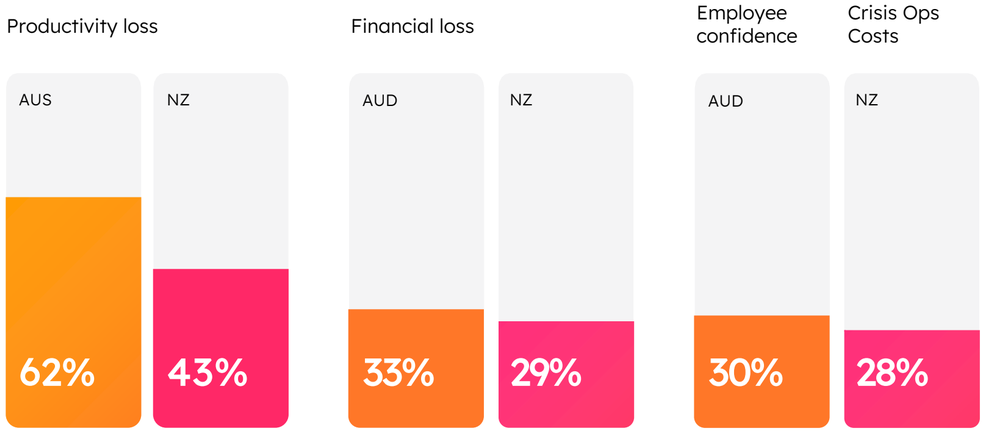
Of those ANZ business leaders that experienced a cyber security incidents or system issues, 75% say that this resulted in downtime.

Malware, software and phishing were the biggest drivers of downtime which lead to productivity, financial and operational losses for business across the region.

Most common incidents in ANZ



Business consequences of downtime



Slow recovery is impacting businesses

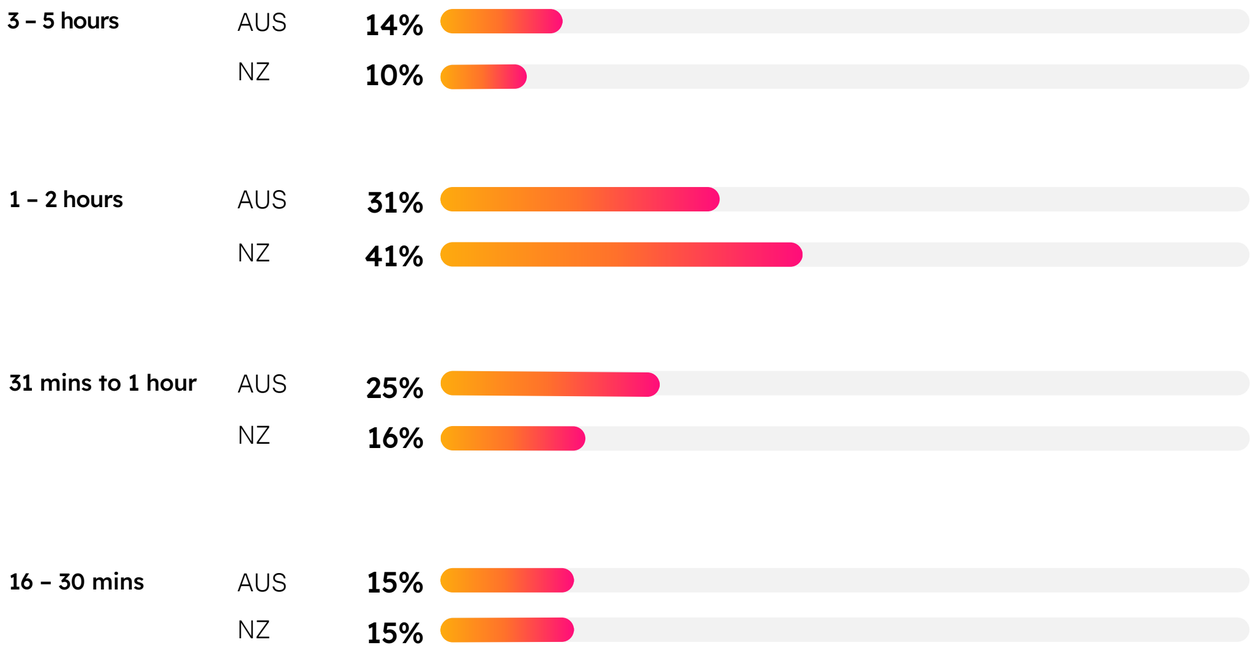
The slower the recovery time from a downtime incident, the bigger the financial, productivity and brand cost.

The average downtime is almost two hours in Australia (109.6 minutes) and New Zealand (117.8 minutes).

However, even when systems are back online quickly, ANZ business leaders report that on average it takes them 7.4 days to recover from an incident.

Lack of training is a major issue for ANZ businesses. Over 30% of organisations said employees within their organisation are not trained in cybersecurity preparedness.

Average time of unplanned downtime



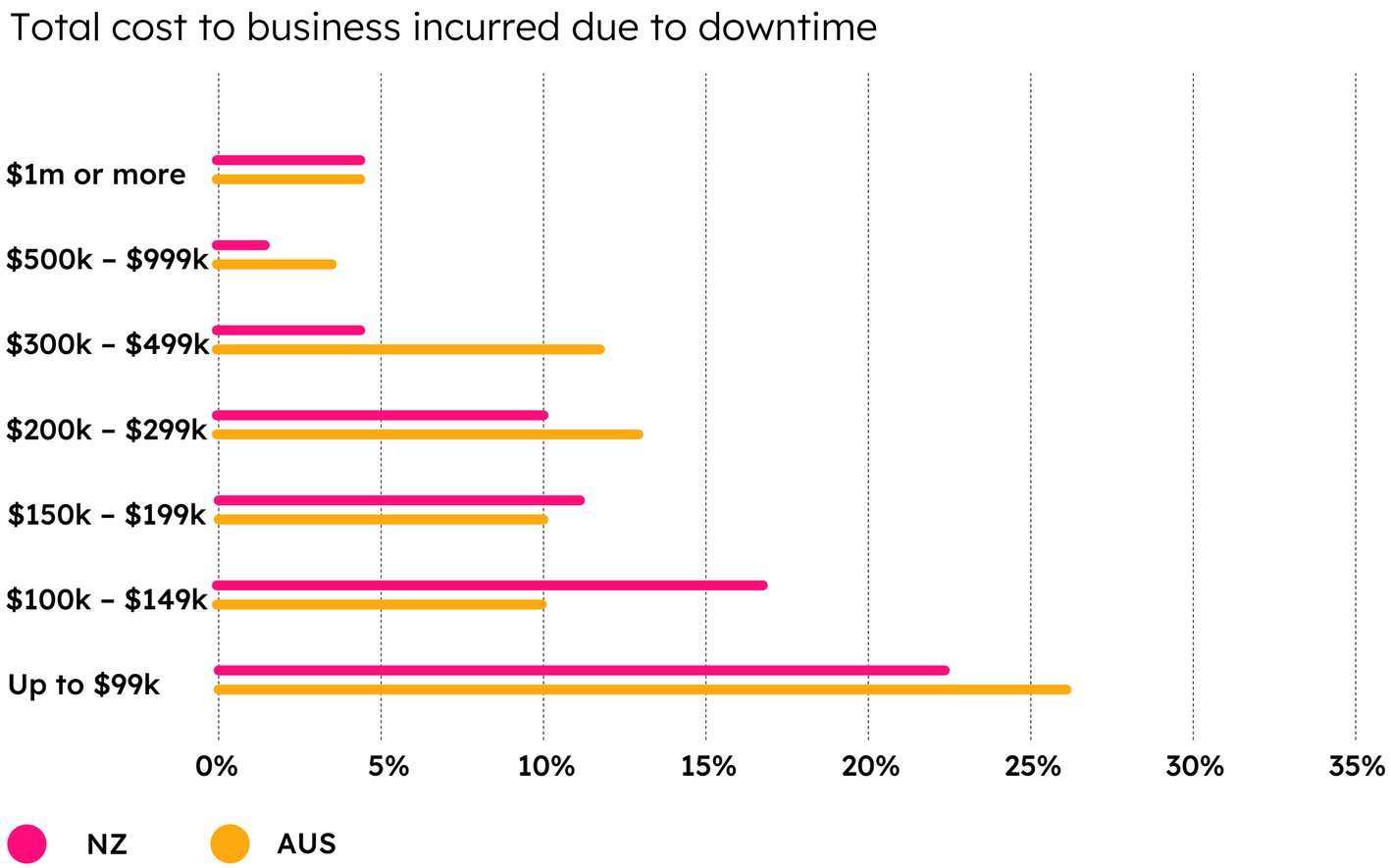
Downtime comes at a cost

Despite 93% of Australian and 89% of New Zealand business leaders claiming they are "prepared" for unplanned downtime, they have also conceded that they've experienced significant financial losses due to cyber threats and systems outages.

Australian business leaders reported an average of A$250,754 losses, which could potentially cost the economy A$86 billion dollars.*

New Zealand businesses are faring slightly better with an average loss of NZ$210,917, which has a potential to impact the economy by NZ$75 billion.**

With mitigating costs front of mind for ANZ business leaders, downtime is not only an inconvenience but also a risk to profitability and stability.



* Potential loss figure using average: Average ($250,754.37) X weighted count i.e. number of Australian business leaders from companies with 500+ employees according to the Australian Bureau of Statistics (342,969.28) = $86,001,045.34.

** Potential loss figure using average: Average ($210,916.89) X weighted count i.e. number of New Zealand business leaders from companies with 100+ employees according to Stats NZ (354,223.35) = $74,711,687,990.53.

Resilience leaders are investing in tools and training

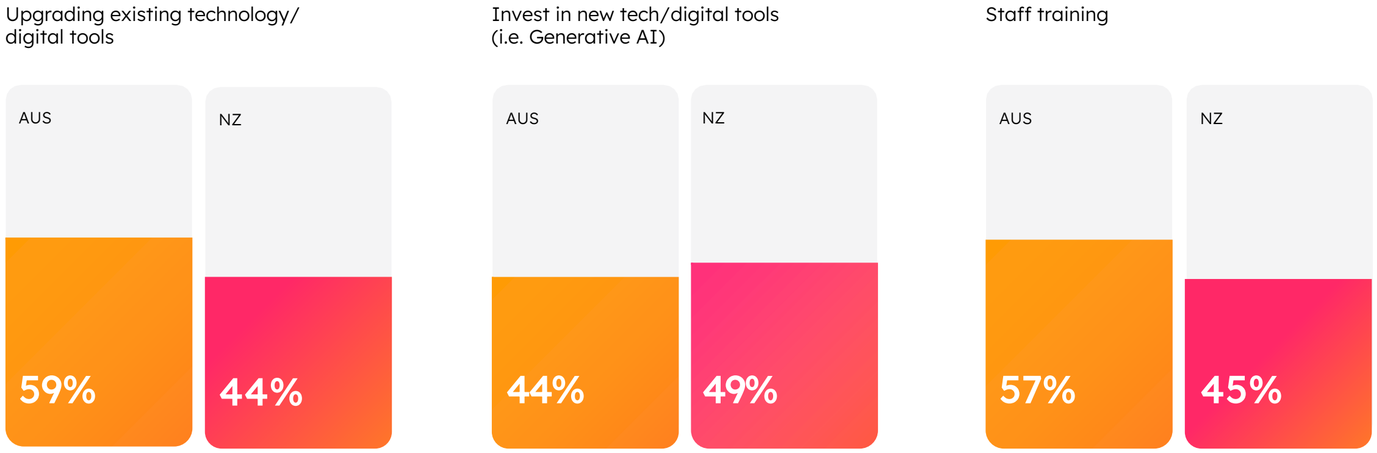
The most successful businesses at mitigating and recovering from downtime are those that align technology, processes and people. These organisations are what we define as resilience leaders.

Resilience leaders make up only the top 10% of organisations. They suffer less downtime, therefore having lower total direct costs and experiencing minimal impacts from hidden costs.

Resilience leaders are also more mature in their adoption of AI, expanding their use of embedded AI features in existing tools more than at four times the rate of other organisations.

Resilience leaders are investing in technology and people to better prepare for unplanned downtime and boost digital resilience.

Top areas for investment



Downtime is a major setback for any organisation striving for success in an increasingly digital and connected world. Beyond the financial impact, it undermines trust with partners, shareholders, customers and employees – trust that takes time and effort to rebuild. It also disrupts productivity, weakens business performance, and in highly regulated industries, introduces compliance risks.

What sets resilience leaders apart is their ability to anticipate risks, adapt to uncertainty, and build organisations that not only withstand disruption but emerge stronger from it.

Craig Bates,
Senior Vice President & General Manager, APAC

Pro tips for strengthening resilience

Most businesses understand there is too much at stake to not invest in protecting themselves and their customers from cyber incidents and system outages.

However, with varying budgets, time and capabilities, it can be challenging to steer clear of downtime and its costly consequences.

Here are our top four tips for Australia and New Zealand organisations to become more resilient:

1. Have a down plan

When it comes to downtime, there is no such things as too prepared. It's not just the tools and the technology. Instrumenting every app, following a runbook for outages and identifying owning engineers — and ensuring everyone knows who's on point — is good corporate hygiene.

To strengthen your plan and modernise your IT infrastructure, perform regular tabletop exercises with your SecOps, ITOps, and engineering teams, running through hypothetical scenarios to practice and verify responses to downtime events.

2. Root out the root cause

Downtime is inevitable, but understanding what caused downtime is essential.

Effective incident response relies on root cause analysis to identify the underlying problem and point to fix. Invest in observability tools to help reduce both the time it takes to detect an issue (MTTD) and the time it takes to resolve it (MTTR). Integrating data from across your environment into one centralised location can isolate root causes more easily, fix and fix problems faster, ensure reliability, and gain control over your data and costs.

3. Get AI on the case

AI can help you recover from downtime quicker and ease the tech talent gap by automating routine processes and accelerating response times. Resilient business leaders use AI tools at four times the rate of other organisations. AI empowers organisations with visibility and speed, allowing them to effectively detect and mitigate security issues and deal with downtime while reducing reliance on limited resources.

4. Bring everyone together

Downtime comes from anywhere. It's important to start by identifying a specific business challenge or problem to solve. Once this is clear, bring together all relevant stakeholders - IT operations, security teams, legal and compliance, engineering teams – to collaborate on addressing this issue. A unified approach will help to swiftly identify and address both cybersecurity breaches and system failures, ensuring greater resilience and supports best practices.

About Splunk LLC.

Splunk, a Cisco company, helps build a safer and more resilient digital world. Organisations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation.

Methodology

Lonergan Research surveyed 435 Australian business leaders in companies of 500+ employees and 116 New Zealand Business Leaders of 100+ employees. These business leaders were mid-level management, executive/business unit manager, senior management and business owners and founders. In addition, respondents were from 20+ industries, including manufacturing, construction, retail trade, transport, information media and telecommunications, financial and insurance services, and public sector/government.-After interviewing, data was weighted to the latest population estimates sourced from the Australian Bureau of Statistics and Stats NZ.

Discover how to strengthen your resilience here:

splunk>