



ECLIPSE TECHNOLOGY SERVICES

The Hidden Cost of Downtime

What an Hour Offline Really Costs Australian SMEs

INTRODUCTION

In any given week, thousands of Australian small and medium-sized enterprises start their work day to find that something isn't working. Email is down. The accounting system is refusing to load. A cloud platform is throwing an error. Whatever the cause, work stops, and the meter starts running on lost time, lost revenue, and lost trust.

Downtime is one of the most expensive things that can happen to a small business, yet it's also one of the least understood. While most business owners can quote their rent and their wages to the dollar, very few can answer an equally important question: what does an hour offline actually cost their business?

This whitepaper examines the real cost of IT downtime for Australian SMEs. It covers the most common causes, the direct and indirect costs that follow, and why the hours accumulate much faster than most business owners realise.

01 Defining Downtime in Practical Terms

Although a full outage, where a server fails or the internet is completely offline, is the most visible form of downtime, partial degradation can be just as detrimental over time. The accounting system runs, but takes two minutes to load each invoice. The Wi-Fi drops every fifteen minutes. Files open eventually, but slowly. Staff can technically work, but at a fraction of their normal pace.

THE WORKING DEFINITION

For the purpose of measuring impact, downtime should be defined broadly. If a critical system is unavailable, or running so poorly that productive work is meaningfully slowed, the business is experiencing downtime, whether or not anyone calls it that.



02 The Real Causes of Downtime

It's easy to see downtime as mostly a cybersecurity story. While it's true that cyber incidents cause downtime, they're just one cause among many.

Hardware failure remains another leading cause of downtime. Servers, hard drives, and network equipment all have a finite lifespan, and failure rates climb sharply once equipment moves beyond its warranty period.

Internet and telecom outages affect almost every business at some point. The 2023 nationwide Optus outage demonstrated this at scale. For around twelve hours, more than 400,000 Australian businesses lost access to mobile and fixed-line services, and in many cases the EFTPOS systems that depended on them. The economic impact was estimated at approximately two billion dollars.

2023 OPTUS OUTAGE

\$2bn

Approximate economic impact, with more than 400,000 Australian businesses affected across around twelve hours.

Cloud service outages have become a regular feature of business life as more applications move from local servers to platforms such as Microsoft 365, Xero, and Amazon Web Services. In July 2024, a faulty update from cybersecurity vendor CrowdStrike caused roughly 8.5 million Windows devices worldwide to crash and refuse to restart, with major impacts across Australian aviation, banking, retail, and media. In October 2025, a domain name system failure in a single Amazon Web Services region disrupted services globally for around fifteen hours.

Finally, key person unavailability is the cause SMEs are least likely to plan for. When a business relies on one person, whether a staff member or an external contact, to manage every IT issue, a badly timed holiday, illness, or resignation can leave systems unmaintained and problems unresolved for days.

03 Direct and Indirect Costs of Downtime

The direct costs of downtime are relatively easy to quantify. They include the wages paid to staff who can't work, the lost revenue from sales that can't be processed, the overtime required to catch up afterwards, and the fees paid for emergency IT support. These costs can scale up quickly. In a forty-person Australian office with an average loaded staff cost of \$45 per hour, three hours of downtime will cost \$5,400 in lost productivity alone, before any consideration of lost sales.

Indirect costs are harder to count but often greater. Among these are customer trust when calls go unanswered or orders unfulfilled, and reputational damage when word spreads that a business is "having IT issues", particularly in industries where reliability is part of the value proposition. Finally, there are the missed deadlines, frustrated staff, and management time spent dealing with the fallout.

Research by Splunk has estimated that Australian organisations collectively lose around \$86 billion each year to unplanned downtime and cybersecurity incidents combined. To imagine what this looks like for an individual SME, divide annual revenue by approximately 2,000 working hours to get a rough hourly revenue figure. Then add wages for staff who would be sitting idle, plus any direct cost of recovery. This yields the approximate cost of one hour of downtime, most owners are surprised by the result.

\$5,400

Lost productivity from three hours of downtime in a forty-person office.

\$86bn

Lost each year by Australian organisations to downtime and cybersecurity incidents combined.



THE PATTERN THAT HIDES

04 The Surprising Cost of “Slow” Downtime

A single major outage tends to be remembered. The more dangerous pattern, however, is the slow accumulation of smaller events. Ten minutes lost to a frozen application. Twenty spent waiting for the internet to come back. An hour lost to a poorly timed Windows update. None of these feels significant in isolation, but across a year, and across an entire workforce, they add up to a substantial figure.

This cost is invisible for three reasons. First, no one is measuring it. There’s no log of small outages, no record of slow performance, and no calculation of cumulative impact. Second, the cost is borne by everyone in small amounts, so no single person feels the full weight. Third, owners and managers gradually normalise the problem. After enough months of dealing with the same slow file shares or spotty network access, the experience starts to feel like the way things are, rather than a cost that can be reduced.

05 What Good Practice Looks Like

Dealing with downtime doesn't mean trying to eliminate failure, failure will always occur somewhere in the chain. Instead, businesses can reduce the frequency of failure, limit its duration when it does happen, and ensure the business can keep functioning while issues are being resolved.



Proactive monitoring of critical systems means that problems are often detected, and hopefully resolved, before they become visible to staff. Routine maintenance and patching, applied on a consistent schedule, reduces the risk that an unsupervised automatic update will cause an outage at the worst possible moment.



Sensible redundancy ensures that the failure of any single component doesn't stop operations. This might mean a second internet connection from a different provider, a backup power supply on critical equipment, or cloud services accessible from any device.



Tested backups, and a real recovery plan, mean that when data loss does occur, the business knows how it will recover, which systems need attention first, and how long recovery should take. An untested backup is not a backup; it's an assumption. Documented procedures for common failures allow whoever is on hand to take sensible action, rather than waiting for the one person who knows the system.



Finally, a capable IT partner with clear response time commitments turns the question of "Who's going to fix this?" into a known process. The difference between a four-hour response and a four-day response is often the difference between an inconvenience and a serious financial event.

06 A Simple Framework for SMEs

Resilience doesn't need to be expensive, but it does need to be deliberate. A practical framework for any Australian SME involves three steps.

1

The first is to identify which systems will actually halt business operations if they go down. Email, the accounting platform, the customer database, the point-of-sale system, and any industry-specific applications should be on the list. Other systems may be useful, but tolerable to lose for a day.

2

The second is to set realistic targets for how quickly each system needs to come back, and how much data your business can afford to lose. These targets, known in IT planning as recovery time and recovery point objectives, don't need to be technical. If your business can't run without email for more than two hours, email needs to recover within two hours. If a day's worth of sales data being lost would be a serious problem, then sales data needs to be backed up more often than once a day.

3

The third step is to invest in resilience in proportion to the cost of downtime. A business losing \$500 an hour can't justify the same level of investment as one losing \$5,000 an hour, but both need a plan. The goal is to spend less on resilience than your business would lose without it.



Conclusion

Downtime is not a technical problem; it's a business problem with a technical cause. For Australian SMEs, the cost of being offline is consistently higher than owners assume, and the hours add up in ways that are easy to miss.

Major events such as the 2023 Optus outage and the 2024 CrowdStrike incident demonstrate that even well-resourced organisations can be brought to a halt by failures outside their direct control. However, the most expensive form of downtime is the one no one measures. Recurring small outages, slow systems, and unresolved performance issues quietly drain productivity, frustrate staff, and chip away at customer experience. Luckily, these smaller, daily incidents are well within an SME's control.

The businesses that handle downtime well aren't necessarily the ones with the largest IT budgets. Instead, they're the organisations that have decided downtime is worth understanding and worth planning for. They've measured what it costs, identified what they cannot afford to lose, and enacted proportionate measures to reduce both the likelihood and the duration of outages. For Australian SMEs operating in an increasingly digital economy, that level of intent is no longer optional.

GET IN TOUCH

Helping Australian businesses stay resilient.



02 9071 2345



info@etsau.com



etsau.com

