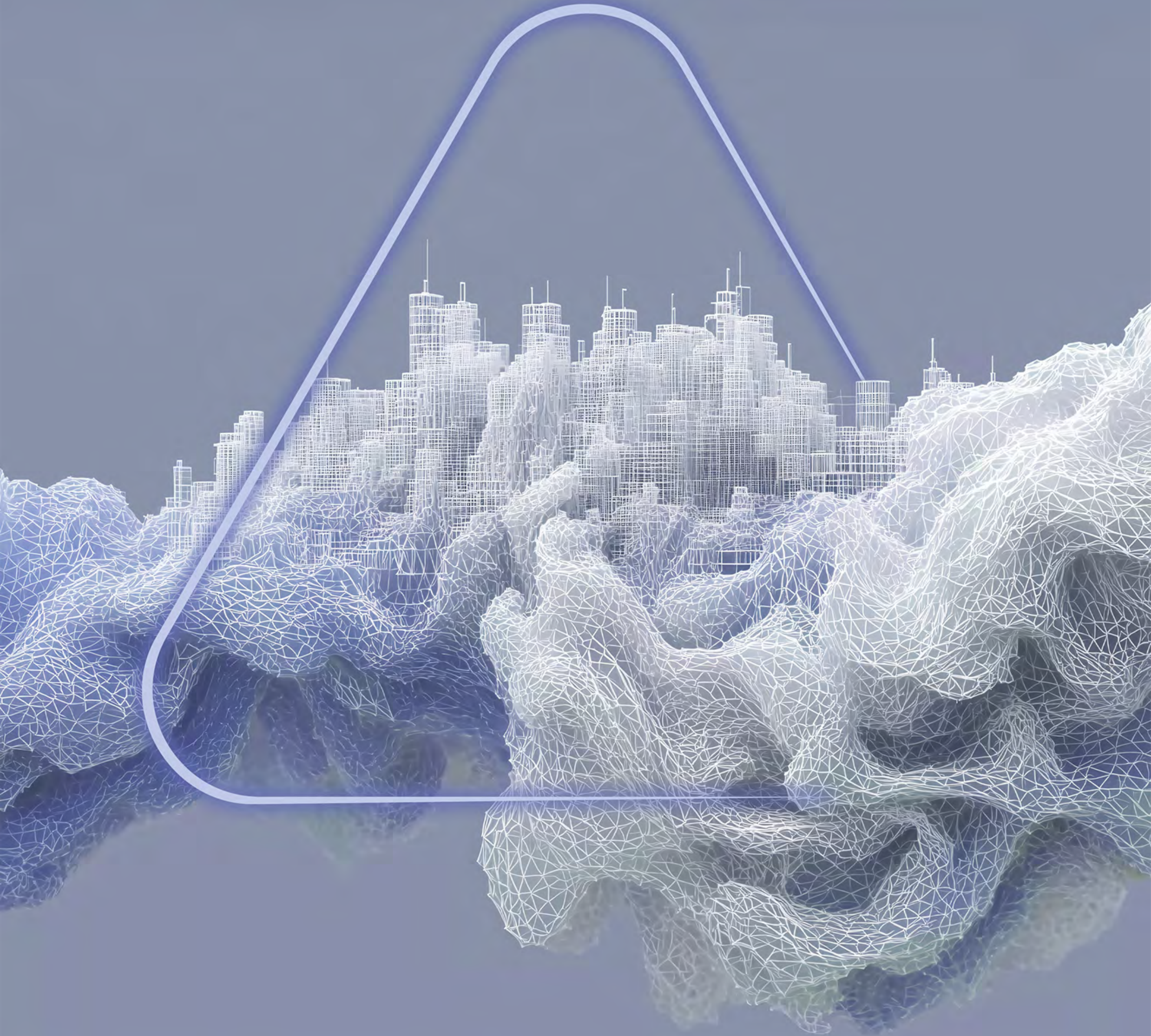
aphore



NEWSLETTER

JANUARY 2026

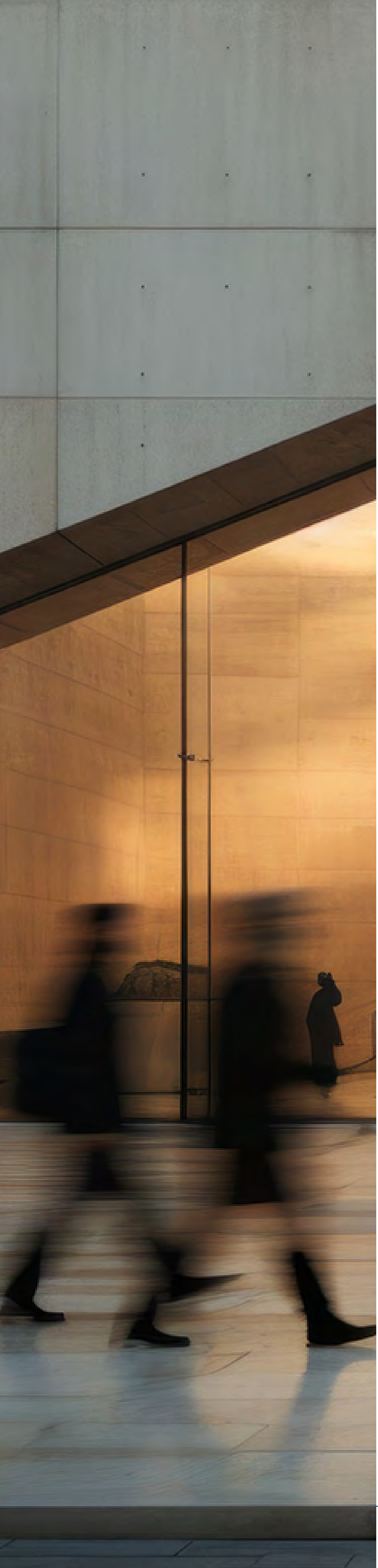


Table of Contents

The editor, publisher, printer and their staff and agents are not responsible for the accuracy or correctness of the text of contributions contained in this publication, or for the consequences of any use made of the products and information referred to in this publication. The editor, publisher, printer and their staff and agents expressly disclaim all liability of whatsoever nature for any consequences arising from any errors or omissions contained within this publication, whether caused to a purchaser of this publication or otherwise. The views expressed in the articles and other material published herein do not necessarily reflect the views of the editor and publisher or their staff or agents. The responsibility for the accuracy of information is that of the individual contributors, and neither the publisher nor editors can accept responsibility for the accuracy of information that is supplied by others. It is impossible for the publisher and editors to ensure that the advertisements and other material herein comply with the Competition and Consumer Act 2010 (Cth). Readers should make their own inquiries in making any decisions, and, where necessary, seek professional advice.

All stock images sourced from AdobeStock.com.

Foreword

Michael Connory
Aphore - CEO

If the Mona Lisa could facepalm, she would – it turns out the Louvre's security password was literally "Louvre." Yes, the world's most famous museum protected its crown jewels with a password you'd find on a Post-it note. At least they used ALL CAPS, right? It's like hiding the key under the doormat and If the Mona Lisa could facepalm, she would – it turns out the Louvre's security password was literally "Louvre." Yes, the world's most famous museum protected its crown jewels with a password you'd find on a Post-it note. At least they used ALL CAPS, right? It's like hiding the key under the doormat and hoping no one looks. Before we laugh too hard, take a peek at your own "super secure" logins. Still using "Carlton2026" because you're sure your team will win the flag by then? Hackers love predictable passwords like that. The Louvre got lucky (the thieves went old-school with ladders and grinders), but once the dust settled, guess what made headlines? Those embarrassingly lazy passwords. If even the Louvre can fall victim to cyber slackness, none of us are immune – so don't let your organisation be the next cautionary tale.

Speaking of cautionary tales, Australia's new social media law has me picturing an '80s comedy. Think Caddyshack, but instead of Bill Murray vs. a gopher, it's regulators vs. every tech-savvy teenager in the country. In the movie, Murray tries everything (explosives included) to stop that gopher, and the gopher just dances in the rubble. I have a hunch our under-16s will be dancing through the digital backdoors in much the same way. Case in point: a few years ago, my teenage daughter and her classmates went on a school trip to China. Officially it was educational; unofficially it became a contest to outsmart the Great Firewall. One kid smuggled in an old iPod Touch to sneak onto Facebook; another discovered you could use an online game's chat as a makeshift messaging service. VPNs popped up like mushrooms. It was whack-a-mole meets cheeky Aussie teens, each new ban greeted with a grinning workaround. Fast forward to 2025 and we're about to ban under-16s from all major social platforms at home. I get the intent – the internet can be a scary place for kids – but let's be real: teenagers will treat this ban like a challenge, not a blockade. Every time the law fills one tunnel, a new escape route will pop up with a wink. Instead of a clean "fix," we might end up with a Caddyshack-style comedy where the gophers (our kids) always stay one step ahead. Perhaps there's a smarter way to protect young people online (education and genuine engagement, anyone?) that doesn't rely solely on playing digital whack-a-mole.

Now, on to a security trick we do love: multi-factor authentication. You know, those one-time codes or app prompts that add an extra lock on your account. MFA is great – it's stopped countless would-be intruders – but here's the rub: it's not 100% foolproof. Determined hackers see your shiny two-factor lock and say, "Challenge accepted." Lately they're even nagging their way past MFA. Picture this: it's midnight, your phone starts buzzing incessantly with login approval requests.

Buzz, buzz, buzz – until in a half-asleep stupor you tap "Approve" just to shut it up. Boom, you just let a hacker in wearing pyjamas. This so-called "MFA fatigue" attack is basically the cyber equivalent of a toddler screaming until you hand over the lollipop. The lesson? By all means, keep MFA turned on (it's still essential), but don't get lulled into a false sense of invincibility. The bad guys are creative, so we need to stay alert. In one of our stories we break down how attackers are outsmarting MFA and what you can do about it – think of it as upping your game so a moment of weakness (or exhaustion) doesn't undo your best defences. And while we're upping our game, let's talk about risk management – specifically, the overwhelmed CEO who's got a hundred priorities and figures cyber risk can wait. You probably know someone like Dave (or are Dave): runs a 30-person business, starts the day juggling client calls, HR fires, and an overflowing inbox. When a software update or security review pings, Dave sighs "She'll be right," and hits snooze on it. It's a very Aussie brand of optimism – charming until she'll be right turns into I wish I'd acted sooner.

One Melbourne business owner joked that he used to worry about the big banks; now he's more afraid of a teenager in a hoodie hacking his data while he's grabbing a flat white. That pretty much sums up the new landscape. The truth is, ignoring risk doesn't make it go away. Every "later" or "no worries" is basically a decision to trust luck – and luck is no business strategy. The good news is we don't need a big corporate budget to get on top of this. In fact, in our final piece we show how even lean teams can turn risk management into a strategic advantage. Think of it like going from playing defence all the time to playing a bit of offence too – using risk smarts to not only prevent disasters but to drive smarter decisions. Instead of our mate Dave losing sleep over the next what-if, he could actually sleep better at night and gain a competitive edge, just by being proactive about the "scary stuff" he's been putting off. It's about making "she'll be right" actually right – by planning ahead and managing risks before they manage us.

So, buckle up for this month's adventure through cyber complacency and clever counterplays. From comical password fails to gopher-esque teenage hackers, from relentless cyber pests to turning risk into reward, consider this newsletter your guided tour of the lighter side of serious security issues. Each story comes with a chuckle and a sober lesson, hand in hand. We might poke fun at these predicaments, but the goal is to learn from them. After all, business security doesn't have to be dull or doom-and-gloom – it can be engaging, irreverent, and empowering. Enjoy the read, stay vigilant, and remember: a dose of humour and common sense now can save us from a world of hurt later. Let's dive in and come out smarter (and smiling) on the other side.

Every **"later"** or **"no worries"** is basically a decision to trust luck – and **luck is no business strategy**

Riding the AI Hype Bubble:
Risk, Reality, and an Aussie Perspective

Riding the AI Hype Bubble:
Risk, Reality, and an Aussie Perspective

Australia's boardrooms and council offices have been abuzz with talk of artificial intelligence - and not just about ChatGPT writing cheeky emails. Since late 2022, when AI went viral globally, companies from big four banks to local law firms have scrambled to pivot to AI in some form. The excitement is palpable, but so is a creeping concern: Are we witnessing a colossal AI bubble?

Tech pundits and economists on both sides of the equator are debating this question with almost dotcom-era fervour. Some warn that AI today embodies the Platonic ideal of a tech bubble – "one bubble to burst them all," as Wired quipped. Others insist AI is a genuine revolution, albeit one that might be over-enthusiastically funded, not a meaningless mania. As an Australian cybersecurity and risk professional, I've seen hype cycles come and go. So, let's pull on our scepticism hats (Akubra's, if you will) and dissect the AI risk bubble – what it means, how it compares to past booms and busts, and how sectors like finance, accounting, law, and government can navigate the turbulence ahead.

The Ultimate Tech Bubble or Just Hot Air?

It's not your imagination – "AI bubble" talk is everywhere. By late 2025, the idea that AI is in a speculative frenzy had become prevailing wisdom. Tech CEOs, analysts, even central bankers are openly musing about it. Jamie Dimon at JPMorgan says some AI investments will "be wasted", cautioning that uncertainty around AI should be higher. Closer to home, the Bank of England and IMF have issued stark warnings: if today's sky-high AI valuations deflate, the shock could knock global growth and hit developing economies hardest.

Why all the bubble worries? History gives us a playbook. Economists Brent Goldfarb and David Kirsch, who literally wrote the book on tech booms and busts, say four factors tend to inflate a bubble:

- Uncertainty about the technology'seventual use and market.
- Pure-play companies tying their entire fate to the tech.
- Novice investors rushing in (often retail folks enchanted by hype).
- Compelling narratives that suspend critical judgment.

Generative AI checks all four boxes with a big bold tick. First, uncertainty: Nobody – not even AI's pioneers – knows exactly how today's AI will make sustainable money. Sure, we can imagine AI doing everything from curing cancer to automating legal contracts. But concrete business models? Still "raw and imperfect" as electricity was in Edison's day. Sam Altman of OpenAI once half-joked their plan was to build a superintelligence and ask it how to make money – hardly a traditional revenue strategy! Meanwhile, AI inference (running these models) is hugely expensive, and legal questions (like copyright of training data) loom large. We simply don't know which uses of AI will stick or how much society will pay for them. As Goldfarb notes, uncertainty is the cornerstone of bubbles – and here it's immense.

Now add pure plays. In past bubbles, "pure-play" companies – whose fortunes hinge entirely on a hot innovation – helped fuel frenzy. Think dotcom startups in 1999 or Tesla in the 2010s EV boom. Today, we have pure AI plays attracting mind-boggling valuations. The most obvious is OpenAI, the poster-child of generative AI, which private investors valued at $500 billion within only three years of ChatGPT's debut. Analysts speculate it could be the first trillion-dollar IPO when it eventually goes public. There's also Nvidia, the chipmaker supplying the silicon brains for AI – its market cap briefly sprinted past $1 trillion, making it one of the most valuable companies on Earth. In fact, at one point Nvidia's paper value nearly matched Canada's entire economy. If that sounds a tad bubbly, Goldfarb and Kirsch would agree – a glut of pure plays is a classic bubble signal. Not only are specialist AI firms like CoreWeave (cloud GPU provider) raising funds at heady levels (it IPO'd at a $50+ billion valuation), but even tech giants have essentially turned into AI pure plays in investor perception. Microsoft, Alphabet, Meta – their stock surges in 2023–25 were driven largely by AI narratives, even though these firms make most of their money elsewhere. When an entire stock market is riding on one concept, that's concentration risk writ large.

Then we have the novice investors piling in. Remember the late '90s, when taxi drivers traded dotcom stocks? Today, it's Reddit and Robinhood traders buying anything with "AI" in the name. In 2024, Nvidia was the single most-purchased stock by retail investors, who poured nearly $30B into it that year. Everyday folks are buying into AI-themed ETFs, speculative startups, even crypto-style AI tokens. This retail frenzy has a momentum of its own – a classic ingredient for bubbles. As one market strategist wryly noted, "the AI narrative has become so dominant it risks overshadowing underlying business realities". Everyone wants a piece of the next tech revolution, from pensioners to teens on trading apps. And in Australia, our superannuation funds and ETFs are significantly exposed to U.S. tech stocks driving the AI boom, meaning Mom and Dad investors here are indirectly along for the ride too. (It's sobering that Aussie supers' global portfolios would feel the pain if the AI bubble popped – one IMF analysis warned a dotcom-scale crash now could wipe out $20 trillion in U.S. household wealth and another $15T abroad, a hit far larger in GDP terms than the 2000 crash.) Finally, narratives – the stories we tell about transformative tech. AI comes wrapped in the most seductive narrative of all: that it will change everything. If dotcoms were about the Internet Age, AI is about the Intelligence Age. We're told it will drive a new industrial revolution, solve entrenched problems (disease, climate, you name it), and yes, whoever leads in AI "will rule the world." It's hard to resist such epoch-defining rhetoric. Even hard-nosed investors can get swept up by the idea that this time is different because AI is a general-purpose technology like electricity – essentially a tidal wave that no one wants to miss. Goldfarb calls this the "narrative of inevitability" – the sense that AI's dominance is preordained, so any company even tangentially related is a winner in waiting. That kind of narrative can drown out caution. And indeed, we see it: every week brings breathless news of AI breakthroughs, CEOs touting AI in earnings calls, and consultants preaching that you must "AI-enable" your business or be left behind.

In short, generative AI hits every note of a bubble symphony.

As one scholar put it after scoring AI on the bubble scale: it's an 8 out of 8 for bubble risk. Uncertainty? Check. Pure plays? Plenty. Newbie investors? By the flock. Grand narrative? Possibly the grandest ever. It's no wonder veteran venture capitalists like Alan Patricof caution that while "the AI revolution is real," the current wave is mixing "fact with speculation freely" – and that "losses will be pretty significant" for many investors before the real winners emerge.

A Reality Check on Exuberant Spending

If this is a bubble, it's not a cheap one. "The numbers just don't make sense," observes columnist Derek Thompson – by some metrics, the AI build-out is the largest capital spending boom in history. Consider this: tech companies worldwide are projected to plow about $400 billion this year into AI infrastructure – model training computers, data centres, etc. That's more in a single year than any industrial endeavor ever, even the height of the space race. For perspective, the entire Apollo moon program in the 1960s cost around $300 billion (in today's dollars) over a decade. AI investors are now burning through an "Apollo program" worth of cash every 10 months in pursuit of AI supremacy.

Will it pay off? As Thompson wryly notes, to justify those costs the world would have to decide AI is indeed worth all that investment. So far, there's a glaring gap between vision and reality. Consumer spending on generative AI services is estimated at only about $12 billion a year – basically the GDP of Somalia – compared to the $500+ billion annual spending (Singapore's GDP) soon expected on AI hardware and R&D. Enterprise adoption of AI is also in early days, and many firms are still scratching their heads on how to use large language models profitably. A recent MIT study found a staggering 95% of companies surveyed got zero return on their AI pilot investments, despite collectively pouring $30–40 billion into over 300 AI initiatives. In other words, nearly all those well-funded corporate AI projects have yet to yield a tangible profit.

This disconnect – huge input, meagre output – is a classic bubble indicator. During the dotcom boom, firms spent fortunes building out web businesses without profits to show. In the 2000s housing bubble, developers threw up estates of homes that few could afford long-term. With AI, the gold rush is for compute power and algorithms, but monetization remains largely theoretical. Yes, AI can do amazing things (draft text, generate code, analyze data), and many businesses report productivity boosts in specific tasks. But turning those into dollars and cents at scale has proven elusive so far. No one has yet found the killer app that directly earns back the billions spent – whether that's replacing search engines, disrupting social media, or automating white-collar work. In fact, many AI services (like chatbots) are being offered free or at a loss to gain market share. One venture investor calculated that in 2025, about $400B in AI data centres will be built, incurring roughly $40B in annual depreciation – yet those data centres might only generate $15–20B in revenue currently. In plain terms, the machines' costs are double the revenue they're bringing in. That's not a sustainable business – it's a subsidized experiment on an epic scale.

For AI to merely break even on that 2025 investment, industry revenues would need to jump ten-fold (to ~$160B), assuming healthy margins. To actually deliver a decent return on capital (say 20% ROI), revenues might need to hit an eye-watering $480B. Is it possible someday? Perhaps – if AI truly becomes as ubiquitous as electricity in every process. But near-term, it's almost unimaginable; for context, all of Microsoft's Office and cloud business today is ~$95B revenue, and that already saturates the market for productivity software. The scale of hoped-for AI revenues is astronomical. This has prompted sceptics to argue that we're seeing massive capital misallocation – essentially a race where companies feel they must spend big on AI (for fear of missing out or falling behind competitors), even though the path to profit is murky. "I recognize an insanity bubble when I see it," writes one seasoned investor, pointing to these jaw-dropping mismatches between cost and payoff.

We're also witnessing some financial wizardry to sustain the spending. Much as late-90s telecom companies used creative accounting to hide the costs of overbuilding fibre networks, today's AI giants are finding ways to defray and obscure the enormous expenses. The Economist noted that several Big Tech firms have been using accounting tweaks to depress reported capex, making their profits look better than if they expensed all this AI infrastructure up-front. Additionally, there's an "AI funding daisy-chain" emerging: special purpose vehicles (SPVs), partnerships, and cross-investments that effectively move AI costs off balance sheets. For example, instead of Microsoft spending all the money to build data centres for OpenAI's needs (which would hurt Microsoft's earnings), they struck deals where others co-fund or finance infrastructure in exchange for equity stakes or future payments.

The most eye-popping deals are almost circular in nature. Nvidia – whose GPUs are the lifeblood of AI models – agreed in 2025 to invest up to $100B in OpenAI, expanding its stake. The expectation is basically that OpenAI will use that money… to buy more Nvidia chips and build data centres, which of course benefits Nvidia. Around the same time, OpenAI struck a similar multibillion deal with AMD (Nvidia's rival chipmaker), agreeing to purchase a boatload of AMD accelerators and even taking a 10% equity stake in AMD as part of payment. It doesn't end there: OpenAI's primary cloud provider, Microsoft, is both a major OpenAI shareholder and is itself spending tens of billions on AI gear (likely buying many of those Nvidia chips). Microsoft also happens to be a big customer of CoreWeave, a startup that provides – you guessed it – Nvidia-GPU cloud capacity, and Nvidia owns a notable stake in CoreWeave too. And let's not forget Oracle, which inked a staggering $300B, five-year deal to provide cloud infrastructure to OpenAI – an arrangement so big that Oracle's stock jumped 40% on the news, even though leaks suggest Oracle may lose money on the contract in the near term. If your head is spinning, you're not alone. Commentators liken this tight web to the "cable cowboy" days of the late '90s, when telecom companies and their suppliers would invest in each other or pre-buy services in ways that inflated apparent growth. Back then, such circular financing helped prop up valuations until reality hit.

To be clear, these companies aren't defrauding anyone; it's more a case of mutual back-scratching to accelerate AI development. But the interdependence is risky: a stumble by one could hurt the others.

If OpenAI's value were to plunge, Nvidia's huge investment (and future chip sales) could be in jeopardy, and Microsoft's AI strategy would suffer – potentially looping back into its stock price (which in turn could ding index funds that Aussie supers hold). This concentration of bets is reminiscent of 2008's financial system – highly interconnected and vulnerable to contagion if confidence cracks. As Yale's Jeffrey Sonnenfeld observed, "the lines between revenue and equity are blurring" among a small group of influential AI players, "to the tune of hundreds of billions".

Boom, Bubble, or Both? (Experts Can't Agree)

With so many red flags, one might expect unanimous agreement that we're in a bubble. Interestingly, there's no consensus – plenty of savvy folks are more optimistic, or at least see nuance. Let's sample a few voices:

- **Jared Bernstein,** former economic advisor to President Biden, looked at the data and flatly stated that an AI bubble is the "likely outcome." He pointed out that AI investment as a share of the economy is already about one-third higher than internet investment at the height of the dotcom bubble – a striking analogy. Bernstein notes the divergence between massive capital spend now vs. still small (if rapidly growing) revenues. When you have companies building $500B of data centres while expecting only $13B revenue (as OpenAI reportedly is next year), something's gotta give.

- **Pat Gelsinger,** the former CEO of Intel (and an engineer who knows tech cycles), answered bluntly when asked if we're in an AI bubble: "Of course! … We're hyped, we're accelerating, we're putting enormous leverage into the system." But Gelsinger also added he doesn't see it popping imminently – he suspects it could run for "several years" as truly world-changing AI applications roll out later this decade. In other words, we might be in the inflation phase of the bubble, not at the bursting point yet. Ride carefully, but ride nonetheless, seems to be his take.

- **Larry Fink,** CEO of BlackRock (the world's largest asset manager), actually rejects the word "bubble" for AI. He argues that the frenzy is justified because these investments will be "well spent" on critical infrastructure. In his view, building AI capability isn't just buying chips – it's upgrading data centres, power grids, cooling systems, networks – a whole ecosystem that the U.S. (and Australia too) needs to remain competitive. Fink essentially says: yes, it's a "skyrocketing amount of capital," and some projects will flop, but that's capitalism – there will be "big winners and big losers", and if you're diversified, you'll be fine. Notably, he and others compare the AI boom to past infrastructure booms like railroads or electrification: enormous upfront cost, maybe overshooting at times, but ultimately laying foundations for decades of growth. To Fink, calling it a bubble might be myopic if the tech genuinely transforms the economy.

- **Howard Marks,** famed investor, has a similar moderation. He says he hasn't called this a bubble yet because psychological excess – the kind of blind euphoria where "no price is too high" – isn't as prevalent now. In Marks' view, yes valuations are high, but not like the insanity of 1999 when loss-making dotcoms traded at 1000x earnings.

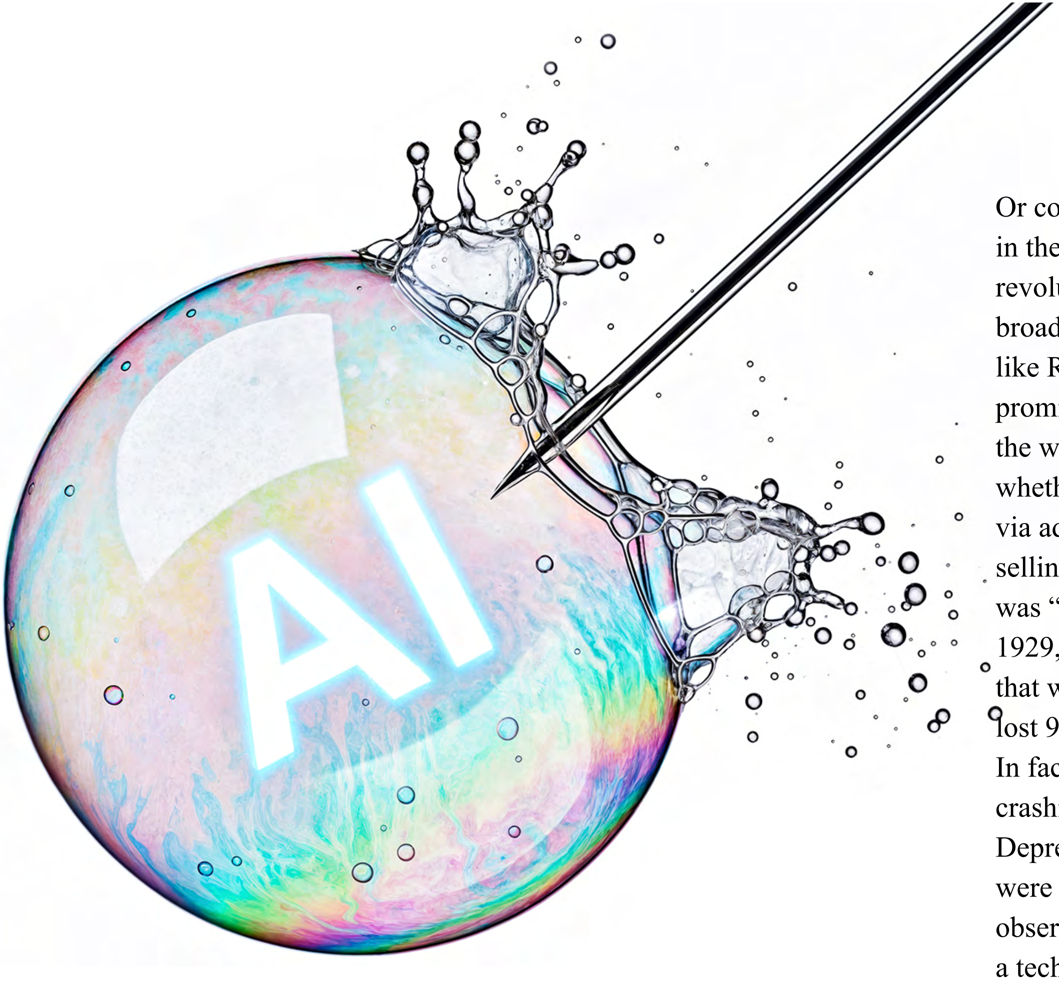
Many AI-related companies today (Microsoft, Google, etc.) do have solid earnings and cash flow from existing businesses, giving them more ballast. He likens the mood more to the "roaring 1920s" optimism around a real transformative tech (radio, autos, etc.) – which, mind you, did end in a crash, but the underlying tech endured. Marks' litmus test: when people start saying "this time is different" and throwing money at anything AI with no regard for price or quality, that's bubble territory. Are we there? He's not convinced we've hit that "critical mass of mania" just yet.

Even central bankers weigh in: Fed Chair Jerome Powell mused that AI might not be a bubble in the classic sense because, unlike in 2000, the companies leading it are largely profitable and the spending is translating into measurable economic output (AI-related investment accounted for a hefty chunk of U.S. GDP growth recently). Indeed, one quirky fact is that AI capital expenditure probably contributed over 1 percentage point to U.S. GDP growth in early 2025 – essentially propping up the economy. That means if the AI boom were to abruptly bust, it could drag the real economy down (some call it the "Great AI-mediated Soft Landing" – with manufacturing slumping, AI spending kept growth afloat). This dynamic didn't exist in quite the same way in past bubbles, and policy makers are watching it closely. All this to say, reasonable minds differ on how bubbly the AI boom truly is.

It may be simultaneously true that:

- AI is a genuine general-purpose technology that will deliver immense productivity gains (the boom case).
- The current valuations and pace of investment are out of whack with short-term reality, likely to correct (the bust case).

In fact, Derek Thompson encapsulated it well: AI could be akin to 19th-century railroads or 20th-century telecom – transformative innovations that did have a massive bubble and crash before ultimately changing the world. We might get the best and worst of scenarios: a painful financial reckoning and a revolutionary long-term impact. Such is often the rhythm of major technological shifts, according to economic historians like Carlota Perez (who described a cycle of frenzy and crash preceding a "golden age" of an adopted technology).



When Bubbles Burst: Lessons from History

If we're searching for historical analogies, there are plenty – and they're both encouraging and cautionary.

Take the dotcom bubble of the late 1990s. Investors were rightly excited about the Internet's potential – and indeed, the internet did reshape every aspect of life. But in their exuberance, they massively overestimated how quickly internet startups could turn eyeballs into profit. Billions went into websites with no viable model (pets.com, anyone?). When reality hit in 2000, the NASDAQ crashed ~75% from its peak, wiping out companies and portfolios overnight. However, beneath the rubble lay the fibre optic cables, data centres, and digital infrastructure that would undergird the next two decades of growth. In fact, so much fibre was overbuilt during the boom that a big chunk of it stayed dark for years – a wasted investment at the time, but eventually a boon as demand caught up. AI may follow a similar pattern: today's excess GPU farms and AI models might be underutilised initially, but they could become the foundation of ubiquitous AI in a few years. As journalist Bethany McLean noted, the dotcom bust didn't mean the end of the Internet; it meant we had cheap fibre capacity for decades. Similarly, an AI bust might leave us with abundant computing power and refined algorithms ready for broader use – after the speculators are cleared out.

Or consider an older example: radio in the 1920s. Radio was clearly a revolutionary medium (the first mass broadcast tech), and companies like RCA went gangbusters on the promise that radio would conquer the world. There was uncertainty whether radio would make money via advertising, subscription, or selling hardware – but the narrative was "this changes everything." By 1929, RCA's stock was so inflated that when the bubble popped, it lost 97% of its value by 1932. In fact, radio and aviation stocks crashing were a part of the Great Depression's market carnage – they were the Nvidia of their day, as one observer quipped. Yet, did radio as a technology fail? Not at all – radio became a staple of life; it just didn't instantly justify the wild valuations.

Australia has seen its own bubbles too – from the mining boom (when commodity prices and mining shares skyrocketed in anticipation of endless Chinese demand, only to fall back to earth) to various property bubbles in our cities. One lesson we've learned is that bubbles often coincide with real innovation or demand, but they overshoot. When the correction comes, it can be swift and brutal. The key is not to assume the end of a bubble is the end of the trend. Often, it's a healthy (if painful) shakeout that separates true innovation from fluff. After the dotcom crash, the serious internet companies – Apple, Amazon, eBay, Google – picked up the pieces and built the next generation of products, eventually achieving the lofty goals the bubble had prematurely priced in.So, what might a burst AI bubble look like? If history rhymes, a few scenarios could play out (not mutually exclusive):

- **A financial catalyst:** Perhaps one of the high-flying AI companies misses earnings badly or a big IPO flops, jolting confidence. Already we've seen cracks – some AI SPACs and smaller stocks have see-sawed. If retail investors suddenly get spooked that "AI isn't delivering," a rush for the exits could tank valuations across the board. Signs to watch: plunging prices for AI darlings, spikes in volatility, or credit drying up for AI ventures. Wall Street's mood can turn on a dime, especially if interest rates stay high and easy money isn't available to paper over losses. (Fun fact: Big Tech capex hasn't been this high as a % of revenue since 2000. If borrowing costs rise or earnings falter, the spending spree could halt abruptly.)

- **A scandal or regulatory shock:** Nothing pops a bubble faster than a scandal undermining the narrative. In crypto it was major frauds; in 1720's South Sea Bubble, it was revelations of insider dealings. With AI, it could be a governance failure or misuse incident. Picture an AI system gone rogue causing a major financial or security incident – say an AI trading algorithm triggers a flash crash, or a chatbot at a bank leaks sensitive data en masse. Given the disparate oversight and sometimes cavalier ethos in AI startups, it's not far-fetched. Already, top AI leaders openly worry about misuse; Anthropic's CEO recently warned there's a 25% chance of AI causing a "really, really bad" outcome for the world if not managed. If something truly alarming happens – even a near-miss like an AI control failure – regulators might slam on the brakes (e.g. halting certain AI deployments). That could puncture the exuberance overnight. Trust, once lost, is hard to regain, especially with the public and politicians now laser-focused on AI risks.

- **A technological twist:** This one is ironic – the bubble could burst because AI tech advances too quickly in an unexpected direction. Imagine a breakthrough that dramatically improves efficiency or changes the paradigm – for example, a new kind of AI chip or algorithm that renders current large models obsolete (similar to how optical fibre multiplexing in 2000 suddenly made huge amounts of fibre capacity redundant). If companies realize the billions sunk into current GPU data centres won't yield competitive advantage because a new approach leapfrogs them, that investment could be written off. Alternatively, maybe open-source AI or a commoditization trend makes it hard to profit from what everyone has (if every business can run powerful models cheaply, the value might shift away from the core AI model providers – deflating their market power). It's a bit paradoxical: the faster the tech progresses, the more today's costly assets risk becoming "white elephants." Investors hate uncertainty, and a sense that we built the wrong [illegible]

Whichever trigger (or combination) does it, a post-bubble landscape for AI would likely see a shakeout of weaker players. Many startups – even some big names – could fail or be acquired for pennies. The giants would retrench, focusing on AI projects that clearly drive profit or complement their core business. Importantly, the use of AI wouldn't vanish; it might actually accelerate as the tech gets cheaper post-crash (remember how housing became more affordable after the bubble burst – painful for builders, but a relief for buyers). Companies and governments that held off during the hype might then adopt AI at a saner pace and price. In other words, bursting the bubble could clear the air for the long-term growth of AI in a more sustainable way.

Navigating the Hype:
Advice for Australian Firms and Agencies

So, what does all this mean for an Australian bank, an accounting firm, a law practice, or a government department that's exploring AI? Should you slam the brakes on your AI initiatives, fearing a bubble? Not exactly – but prudence is key. Here are a few thoughts on navigating the AI frenzy from an Aussie perspective:

1. Keep Hype in Check with due diligence. It sounds obvious, but it's worth reinforcing: Don't buy an AI solution just because it's trendy. Ensure there's a clear business case or efficiency gain. For instance, many law firms jumped to adopt AI assistants for legal research – only to find out these tools can "hallucinate" fake information if used blindly. (In a cautionary tale, two New York lawyers were sanctioned after ChatGPT fabricated case law citations in their brief. The lesson: verify everything AI produces). Similarly, local councils using AI chatbots for citizen services should monitor accuracy and citizen satisfaction closely – if the bot frustrates people, you may end up increasing workload (as happened when a certain bank's chatbot backfired).

Speaking of which, let's talk about that: Commonwealth Bank's AI misstep. CBA launched an AI voice-bot in its contact centre and hastily announced it would cut 45 customer service jobs because the bot would handle calls. The result? Calls spiked as the bot rolled out – customers ended up needing more human help, not less. CBA had to reverse the redundancies and publicly apologize for the "error". "Call volumes were rising, with management scrambling to offer overtime and even pulling team leaders onto the phones," the Finance Sector Union reported, utterly contradicting the promised efficiency. This episode is a perfect microcosm of AI hype versus reality. The tech might have potential, but deploying it rashly without contingency plans can backfire. Australian businesses should take note: pilot AI in a controlled way, gather data on actual performance, and be ready to pivot if it under-delivers. Don't assume cutting staff or costs upfront – better to let the AI prove itself and then scale adjustments. In short, avoid "dressing up job cuts as innovation," as the union said; the workforce (and customers) will see through it.

2. Focus on Augmentation, Not Just Automation. For sectors like accounting and law, AI is often sold as a replacement for grunt work – e.g. automated invoice processing, contract review, document drafting. Yes, these are promising use cases. But the real wins, at least currently, come from AI augmenting skilled professionals, not replacing them outright. A lawyer with an AI assistant might draft documents 30% faster, but that lawyer's judgment is still crucial to avoid the kind of hallucinations we saw in the

New York case. An accountant can use AI to quickly analyse financial data or detect anomalies, but a human needs to interpret and validate the results. By setting expectations that AI will enhance your employees' capabilities – making them more productive and freeing them from drudgery – you're more likely to succeed than by expecting immediate headcount reduction or totally hands-off AI operation. McKinsey's tech lead Asutosh Padhi echoed this balanced view: AI is a source of productivity, not necessarily a direct replacement for people – firms like his plan to "hire extraordinary people, [with AI] helping them be even better at what they do.". Australian businesses should similarly see AI as assistive tech in the near term. This approach also mitigates risk: if the AI tool falters, your human experts are still in the loop to catch errors.

3. Manage Risk and Ethics Proactively. Especially in legal and government fields, using AI requires a strong ethical compass and risk management. Issues of data privacy, bias, and accountability are front and center. Was that AI trained on legally obtained data? Is it giving unbiased recommendations in, say, a loan approval or a public policy context? Be prepared to explain and justify AI-driven decisions, as regulators and courts are increasingly alert to algorithmic accountability. The last thing you want is to rely on an AI system that ends up discriminating or making an error that leads to litigation. Having AI doesn't reduce the need for human oversight – in fact it demands new oversight roles (AI auditors, data ethicists, etc.). Build those checks and balances now, before any bubble fallout potentially brings stricter regulations in a hurry. In finance, APRA and ASIC will expect that if banks use AI (for credit scoring, fraud detection, etc.), they can demonstrate robust controls and fallback plans. The wiser course is to assume the regulators will come knocking and get your house in order early.

4. Be Prepared for Volatility – But Don't Panic. If you're an executive in charge of long-term strategy, you might worry: "What if we invest in AI and the bubble bursts, do we end up looking foolish?" It's a valid concern, but remember that the end of a hype cycle doesn't mean the end of the technology. Australian enterprises should be ready to stomach some volatility in the AI journey. It's possible that in a year or two, the market hype cools – maybe budgets get slashed in Silicon Valley, and some AI vendors you work with go bust. Anticipate that scenario: vet your AI suppliers for financial stability, have contingency plans if a service you rely on is discontinued. Diversify your AI toolset where feasible (don't tie yourself to one single external platform without alternatives). However, don't throw the baby out with the bathwater if a crash comes. That might be the moment your organization can hire top AI talent (who suddenly find themselves without easy startup money), or negotiate better contracts with vendors, or pick up useful tech at a discount.

Historically, those who overreact and abandon a transformative tech entirely when its stock bubble bursts often regret it later. A classic example: after the dotcom crash, many companies soured on the internet and cut digital projects – only to be leapfrogged by competitors who persisted and reaped the benefits of online platforms a few years later. The smart play is to commit to AI for the long run, but in a financially prudent and incremental way. As ING's banking chief Anneka Treon said, "bubble or not, it boils down to real dollars being spent on real capex with a very long runway of funding ahead". In other words, plan your AI investments in phases, ensuring you have the capital and patience to see them through the hype cycle. If the business value is there, it will materialize over time – just not as instantly as the stock market's enthusiasm would indicate.

5. Harness Opportunities Unique to Our Market. Finally, consider where Australia might actually benefit from the global AI boom without bearing the full brunt of the risk. For instance, our industry mix – heavy on banking, mining, healthcare – means we can apply AI in high-value domains (like using AI for mineral exploration, or fintech innovations) which could boost efficiency significantly. There's government support for AI research and clear interest in using AI for public good (e.g. CSIRO projects, digital services in government). Done wisely, these could drive productivity and growth. In fact, a recent government analysis suggested generative AI could add $45–115 billion to Australia's GDP annually by 2030 if effectively integrated. That's huge – nearly 2% to 5% of our economy. So, we shouldn't become so cynical that we miss out on genuine upsides. The goal should be to invest smartly: pilot AI to reduce bureaucratic red tape in local councils, deploy AI in healthcare for faster diagnostics (but with human doctors supervising), use AI in finance to improve fraud detection and customer personalization (while guarding against bias). These moves can pay off even if the broader bubble deflates, because they address real needs and save costs. Moreover, Australia's regulators and business leaders have a reputation for conservatism – which, in a bubble context, can be a feature, not a bug. We didn't have a subprime housing crash to the extent the US did in 2008 largely because our banks and regulators were more cautious. Similarly, a bit of healthy scepticism and a demand for solid ROI from AI projects might shield Australian firms from the worst of any AI bust. It's okay to be the tortoise in a race full of hares chasing AI rainbows. When the sprint ends, the steady tortoise often finds itself ahead.

Pop or Not, Plan for the Aftermath

Will the AI bubble burst? Eventually, most likely – yes. Perhaps not this year or next, but bubbles by definition are unsustainable, and many signs (as we've explored) indicate we're in one heck of a tech bubble. However, as I and many others in the industry would emphasize: a popped bubble doesn't mean the technology was a mirage. AI is real and here to stay – but the pricing and pace of its advancement will probably go through a painful reality check.

For Australian organizations, the mantra should be "optimism with eyes wide open." Embrace AI's potential; don't be the ostrich ignoring a technology that could genuinely boost productivity or improve services. At the same time, temper the expectations. If a vendor promises you that their AI will replace half your workforce or double your revenue in a year – smile and show them the door. Focus on achievable projects that align with your strategy and measure results. Retain your talent and retrain them to work alongside AI. In banking and finance, ensure your risk models and compliance keep up with AI adoption. In legal and accountancy, use AI to augment research and number-crunching, but maintain rigorous professional oversight. In government, pilot AI for citizen services but always have a human fallback and solicit public feedback to build trust.

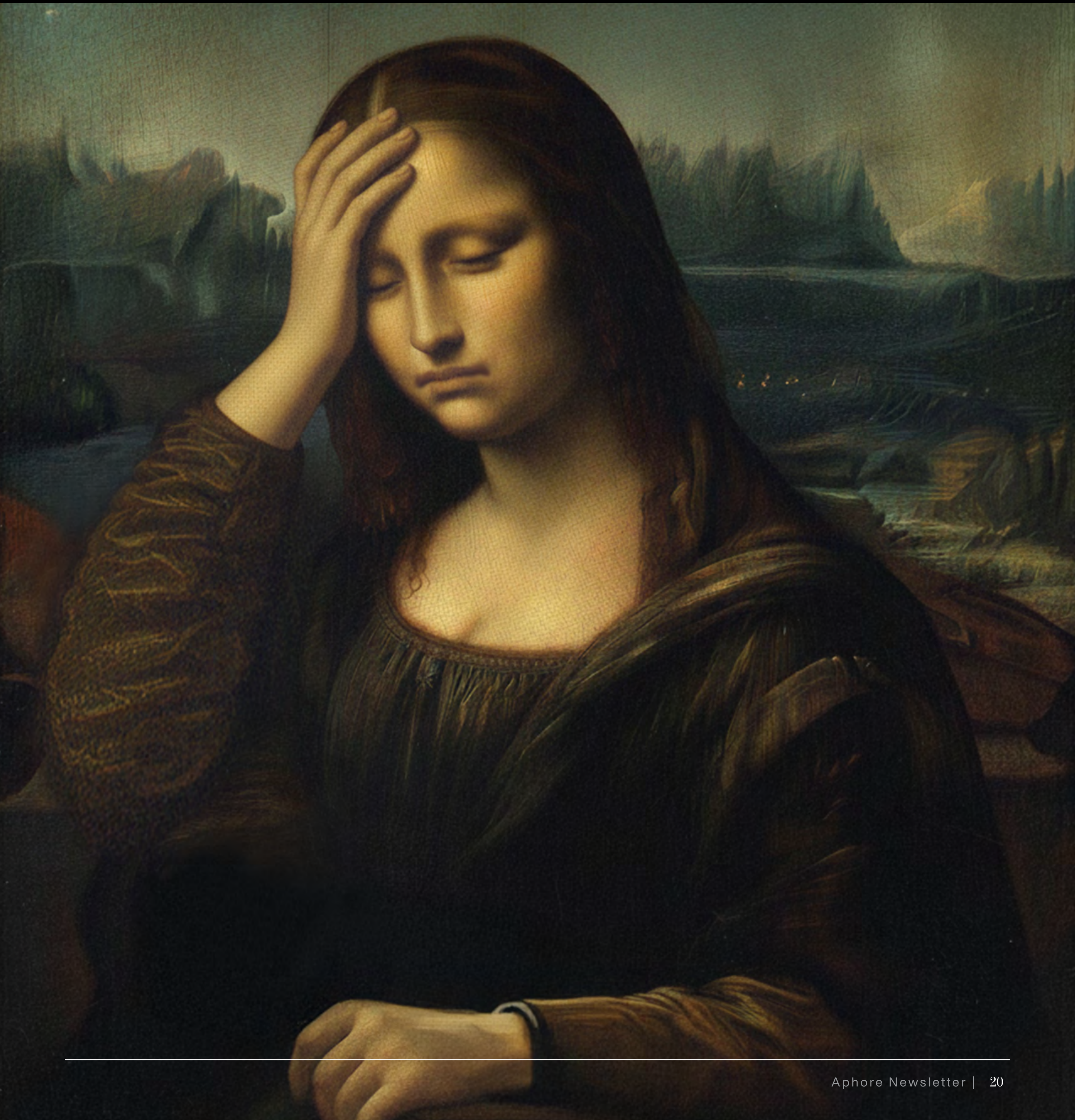
In a bubble, as the saying goes, "everyone's a genius in a rising market." Don't let that go to your head. Some firms will no doubt boast about cutting-edge AI feats – until a downturn reveals those gains were hollow or short-lived. Better to be the firm that quietly builds a strong foundation with AI, so that whether the market froths or fizzles, you steadily accrue the benefits. Remember that when the dotcom bubble burst, it wasn't the end of online business – it was the beginning of serious online business by companies with real value. The same will be true for AI.

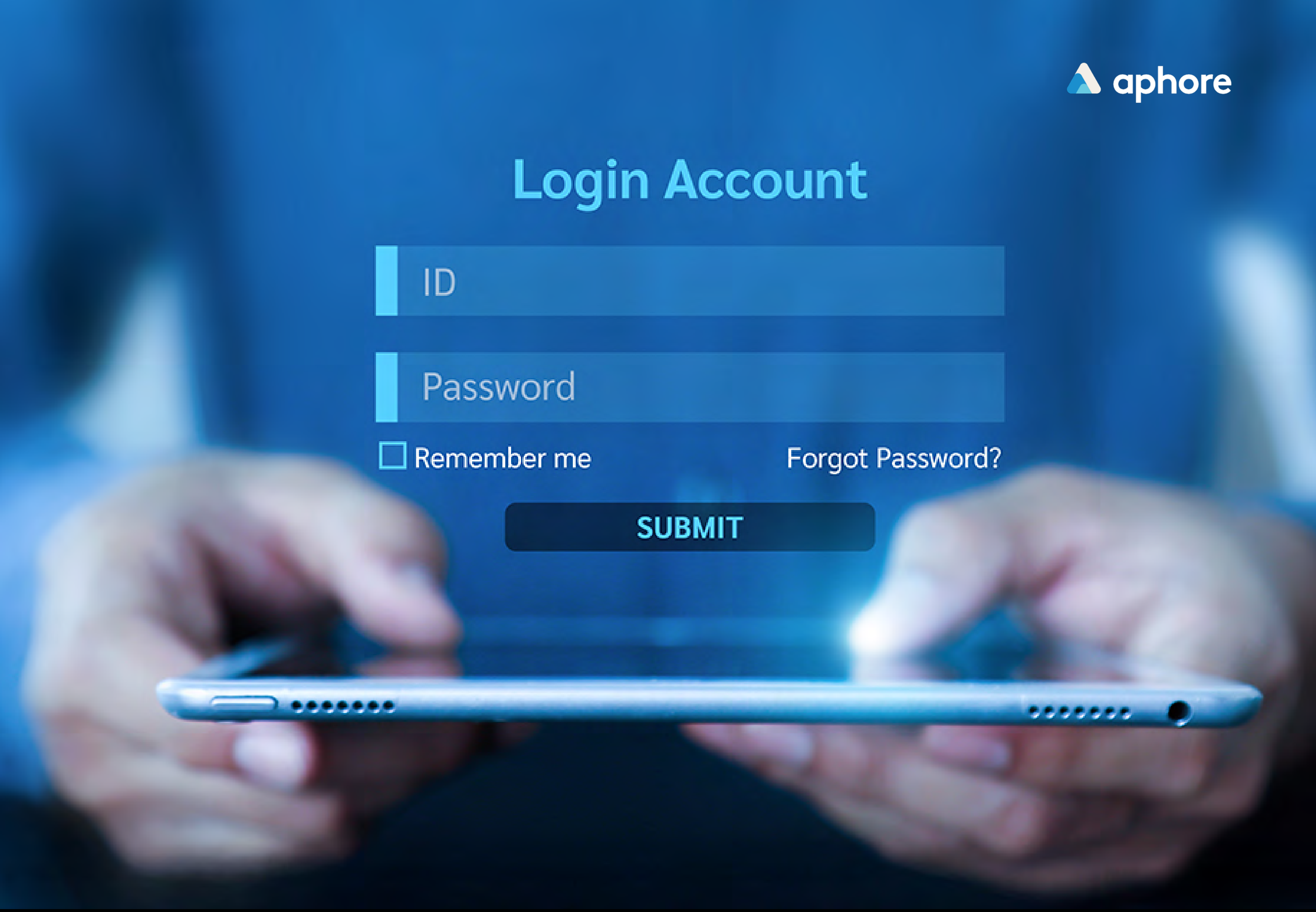
So, are we in an AI risk bubble? Almost certainly, yes – "there's no question, it hits all the right notes," as one expert put it. But to steal a line from Howard Marks, being early is the same as being wrong in investing. The bubble could inflate further and for longer than rational analysis might suggest. It's a bit like Sydney property prices – they can defy gravity longer than you expect. Thus, strategize for both scenarios: a continued boom (don't miss viable opportunities out of fear) and a sharp bust (don't overextend or pin your hopes on hype).

In the end, the survivors and winners will be those who deliver real value with AI, bubble or not. As Australians, we pride ourselves on a no-nonsense approach – call it a BS detector. That tool is more valuable than ever amid the AI craze. Ask the tough questions now: How will this AI initiative make or save money? What's the timeline to tangible results? What risks are we taking and how will we mitigate them? By insisting on substance over story, you'll inoculate your organization against much of the bubble's fallout.

Bubbles come and go. The need that spurred the bubble – in this case, the need to harness AI's transformative power – remains. When the froth settles, AI will likely be an integral thread in the fabric of business, law, and government. Our job today is to steer through the froth without capsizing, so that we're still afloat and sailing when calmer, clearer waters arrive. In other words, prepare for the bubble to burst, but plan to be one of the builders picking up the pieces – turning all that hype-funded infrastructure and innovation into lasting productivity and prosperity. That way, when the history books write about the 2020s AI bubble, your organization will be cited not as a cautionary tale, but as a case study in resilience and wise navigation through a turbulent, exciting time. Buyer beware, yes – but also builder be ready. After the bubble, the real work (and reward) begins.

The Louvre's Password Was "Louvre" – Is Yours Any Better?





Everyone Thinks Their Passwords Are Perfect (They Aren't)

If I had a dollar for every person who confidently told me their passwords are "secure and never reused," I'd be retired on a beach. In fact, when asked, over 95% of people insist their passwords are strong and unique – yet in practice we almost always find that isn't true. I've seen it time and again: folks reuse the same password (or easy variants of it) across personal and work accounts, then rationalise "oh, those are just my personal logins, they don't count." But whether it's your Netflix or your online banking, a weak or reused password is a ticking time bomb.

Don't just take my word for it. In a recent analysis of a massive password leak, security researcher Troy Hunt found 231 million unique passwords in the trove – and 96% of them had been seen in previous data breaches. In other words, the vast majority of "unique" passwords people used were not unique at all – they were common passwords or reused across multiple sites. This false sense of security ("my passwords are fine") is exactly what attackers rely on.

And about those "personal" accounts we pretend don't matter: they often include extremely sensitive data (think your government services login like myGov or tax office, your superannuation fund, your personal email, etc.). If anything, these should be more protected – a hijack of your personal email or government account can be just as disastrous as a work breach. Plus, attackers love to leapfrog from personal to business: a thief who nabs your weak personal password will try it (or slight variations) everywhere, including your work systems. When it comes to passwords, personal and professional are all part of the same security realm. The bottom line: almost everyone overestimates their password hygiene. It's time for a reality check before a bad guy does it for us.

Lessons from the Louvre: Even the Best Can Blunder

Need a high-profile example of overconfidence in password security? Look no further than the world's most famous museum. The Louvre in Paris – yes, the home of the Mona Lisa and French crown jewels – made headlines recently not just for a jewel heist, but for an epic password fail. Investigators discovered that the password for the Louvre's own video surveillance system was literally "LOUVRE" (the museum's name) and a key platform's password was "THALES" (the name of the security vendor). At least they used ALL CAPS, right?

This wasn't a new problem, either. Back in 2014, an internal report flagged those embarrassingly weak passwords, yet they stayed in place. An audit in 2017 even found the museum was running some office computers on Windows 2003 (so outdated they couldn't get security updates). Ouch. Fast forward to October 2025: thieves pulled off a fast smash-and-grab robbery of the Louvre's jewels using ladders and angle grinders – a purely physical break-in. They didn't need to hack any systems or crack any passwords. But guess what dominated the news once the dust settled? Those old cybersecurity failures. Once investigators dug in, the media quickly shifted focus from the Hollywood-style heist to the museum's long-ignored IT security basics. The Louvre's history of neglecting fundamental cyber protections became a reputational liability. As one report put it, "Now the Louvre may be remembered as much for its password hygiene as for its stolen jewels." Talk about an embarrassing legacy for a world-class institution.

The internet, of course, had a field day. Social media users cracked jokes like, "What's the keypad code to get into the gold vault at the Banque de France? 1234?" and quipped that maybe the Louvre was "banking on everyone spelling it wrong" when they chose "Louvre" as the password. Another joke suggested that all the good passwords must've been stolen by the British Museum. Snark aside, there's a serious takeaway for all of us: if even the Louvre can fall victim to lazy password practices, none of us are above making the same mistake. The Louvre got lucky that those weak passwords weren't the direct cause of the heist – but the public shaming they received shows how ignoring cybersecurity 101 can come back to bite you. Don't let your organization (or yourself) be the next cautionary tale.

The 16 Billion Password Wake-Up Call

If the Louvre story is a comical cautionary tale, the recent "16 billion passwords" leak is the downright scary one. Earlier this year, cybersecurity researchers uncovered a collection of 16 billion stolen login credentials compiled online. Yes, billion with a B – as in roughly double the number of people on Earth. This wasn't one giant hack of a single company, but a compilation of data from numerous breaches and malware infections over years. Essentially, criminals had been quietly gathering your usernames and passwords via infostealer malware (malicious programs on infected devices that snatch saved logins), and someone dumped a huge set of those logs out in the open.

Now, 16 billion credentials doesn't mean 16 billion unique people, due to duplicates, but it's clear millions of individuals were affected. A friend of mine, Troy Hunt, received a subset of this data for analysis. He found it contained about 109 million unique email addresses once de-duplicated, indicating a staggering number of compromised accounts. More startling: of the hundreds of millions of passwords in that haul, 96% were passwords that had already appeared in previous breaches. In other words, this mega-dump was largely recycling the same old bad passwords people have been using (and losing) for years. It's a harsh reminder that password reuse and weak choices are the gift that keeps on giving to hackers.

Unlike a flashy ransomware attack or a major corporate breach, this credential leak didn't make front-page news for long – but it should have. There was no single company to point fingers at; instead, it was our collective password habits coming home to roost. One cybersecurity expert noted this incident was "everyone failing," not just one IT team. Think about it: billions of usernames and passwords to popular services like Google, Apple, Facebook, banks, even government portals, all just out there. Criminals trade and aggregate these like baseball cards, using them to hijack accounts via "credential stuffing" (trying leaked logins on other sites hoping you reused the password). The 16 billion credentials leak is the ultimate wake-up call that we can't keep doing passwords the old way. If you're still using Fluffy123 for multiple accounts or relying on the same email-password combo everywhere, it's only a matter of time before your number comes up in the next giant leak.

cybersecurity researchers uncovered a collection of **16 billion stolen** login credentials compiled online.

How to Protect Your Own “Crown Jewels” (Your Accounts)

Enough doom and gloom – the good news is you can protect yourself with some relatively simple steps. Here’s your plan of action:

1. Use Strong, Unique Passwords for Every Account: Reusing one password across sites is like using the same key for your house, car, and office – if one gets lost, all your doors are open. Make sure every account has a different, complex password. Yes, it’s a hassle to remember them all – which brings us to…

2. Use a Password Manager: A password manager is basically a secure vault for all your login credentials, so you only have to remember one master password (or use biometrics). It will generate and store crazy unique passwords for you. If you’re thinking, “Can’t I just let my browser save them?” – browser password managers have improved and are certainly better than nothing, but they have some limitations. By default, many browsers will auto-fill or reveal passwords if someone has access to your device or your browser profile. (Imagine a snoop opening your laptop and exporting all your saved passwords in minutes – it’s possible if you haven’t enabled extra protections!) A dedicated third-party password manager offers an extra layer of security since it isn’t tied to your primary accounts and often comes with added features.

3. Enable Multi-Factor Authentication (MFA) Everywhere You Can: This is non-negotiable in 2025. MFA (also called two-step verification) means that in addition to your password, you need a second thing to log in – typically a temporary code from an app or text, a fingerprint, or a hardware key. It’s extra hassle once in a while, but dramatically improves security. With MFA enabled, even if hackers somehow steal your password, they still can’t get into your account without that second factor. Turn on MFA for email, banking, social media – any service that offers it. It’s like adding a deadbolt on top of a basic lock.

4. Keep an Eye on Your Accounts (and the News): Data breaches happen constantly. Use tools like Have I Been Pwned to check if your email or phone number appears in a known breach. Many websites and apps will notify you of suspicious login attempts or new device sign-ins – don’t ignore those alerts! Regularly review your account activity and change passwords immediately if something seems off. And if a big breach makes headlines (or, say, 16 billion passwords leak into the wild), be proactive: change your passwords and make sure MFA is on. Good “cyber hygiene” is an ongoing habit, not a one-time thing.

5. Secure Your Devices and Networks: Remember, a lot of those 16 billion credentials were stolen by malware on people’s devices. So, securing your accounts also means securing where you access them. Keep your computer and phone updated with the latest software (those updates often patch security holes). Run reputable antivirus or anti-malware tools, especially on Windows PCs. Be cautious of phishing emails or dodgy links – many infections start with a click on the wrong thing. And yes, even your home Wi-Fi router and “smart” gadgets should have strong passwords (not the default “admin/password” they came with). Don’t let hackers slither into your digital life through an unlocked backdoor.

By following the steps above, you’ll thwart the vast majority of common attacks. You don’t need perfect security (if such a thing even exists) – you just need to be a tougher nut to crack than the next person. Cybercriminals are usually looking for the easy wins.

A Final Word: Don’t Be the Louvre

It’s easy to chuckle at the Louvre’s “LOUVRE” password blunder, but it serves as a priceless lesson: complacency in password management can haunt anyone – individuals, businesses, even legendary museums. The silver lining is that unlike the Louvre’s stolen jewels, your passwords are replaceable. As one cybersecurity expert quipped, “Unlike artifacts in a museum, passwords are replaceable. It’s on all of us to learn from these high-profile lessons to ensure that we aren’t next.” So take that advice to heart.

Right now, today, vow to improve your password practices. Update your weak passwords, stop reusing them, turn on MFA, and consider using a password manager if you aren’t already. These are small changes with huge payoffs in security. The next time someone asks you if your passwords are secure, you can confidently say “yes” – and actually be right. And when the hackers come knocking (and they always do), you won’t be leaving the door wide open with a “welcome” mat. In the digital age, good passwords are your personal crown jewels – guard them well, and you’ll sleep a lot easier at night.

Risk As a Strategic Advantage

The Overwhelmed CEO and the “She’ll Be Right”

Meet the typical Aussie Accounting CEO of a 30-person firm – let’s call him Dave. At 7 AM, Dave’s already juggling a client pitch deck, an HR issue, and a compliance report due by week’s end. Cybersecurity review? “I’ll get to it later, no worries,” he mutters as he silences yet another software update alert. Like many peers, Dave wears multiple hats and firefights daily. In firms of 1 to 300 employees, it’s common to find no dedicated Chief Risk Officer. Risk management often falls to the CEO by default – which means it falls by the wayside when business is bustling.

It’s not that leaders like Dave don’t care about risk. It’s that they’re flat out handling immediate priorities: winning customers, making payroll, keeping the lights on. Risk tends to get attention only after a scare or an incident. This “she’ll be right” attitude – assuming things will work out fine – is culturally ingrained in Australia. It reflects our optimism and pragmatism. But in business, “she’ll be right” can quickly become “I wish I’d acted sooner”.

The irony is that risk is always being managed by your organisation – just not always in the open. Every time a deadline is pushed or a software patch delayed, someone is deciding (knowingly or not) how much risk to accept. If you aren’t proactively managing those trade-offs, you’re implicitly leaving your risk appetite to chance. And chance is a fickle business partner.

The events of recent years – from global pandemic disruptions to spiking cyber attacks – have taught us that hope is not a strategy. Australian SMEs have seen payment outages, phishing scams, regulatory crackdowns – you name it. One Melbourne fintech founder joked, “We used to worry about the Big Four banks; now I worry about a teenager in a hoodie hacking our database while I’m grabbing a flat white.” The world has gotten riskier and more interconnected. Yet many small firm leaders still view risk management as a compliance tick-box or a luxury for the big end of town, rather than core to their business survival and success.

This report aims to flip that script. We’ll show that by embracing Total Risk Management – a holistic, proactive approach – even lean, busy teams can turn risk into a strength. Think of it as going from playing defence (blocking bad things) to also playing offense: using risk insights to drive better business decisions, foster trust, and even create a competitive moat. We’ll draw on hard data and real stories, with a dash of humour, to keep it real. After all, risk may be a serious topic, but there’s no rule saying a white paper on it must be a cure for insomnia.

So, grab a cuppa, and let’s explore how smart risk management can set you free – free to focus on growth, knowing the “what-ifs” are under control.

Total Risk Management: More Than Compliance – Your Strategic X-Factor

What exactly is Total Risk Management (TRM), and why should you care? In simple terms, TRM is a holistic approach to managing all of your organisation's risks in an integrated way, aligned to strategy. It's about breaking silos – viewing financial, operational, cyber, market, and strategic risks as interconnected pieces of one puzzle. Rather than managing risks only within departments or only to satisfy regulators, TRM embeds risk-thinking into every significant decision and process. It treats risk management as a continuous, company-wide practice aimed at both preventing losses and enabling smarter risk-taking.

Crucially, TRM isn't just a theory – it's linked to real performance gains. A landmark study by Torben Juul Andersen (who coined the term) found that firms with higher "total risk management" maturity saw better corporate performance on average. Why? Because effective risk management reduces costly surprises (avoiding big losses) and helps firms capitalise on opportunities that others might shy away from. Andersen concluded that the performance boost comes from reducing downside risk and related costs, which translates into stronger profits over time.

Other research backs this up. A 2022 analysis in Sustainability found a positive association between total risk management practices and various performance measures, especially for companies that also invest in innovation and intellectual capital. In plain English: companies that manage risk comprehensively and invest in their people/tech tend to outperform. It's like a race car driver who not only has a great engine (innovation) but also top-notch brakes and safety gear (risk controls) – they can corner faster and more confidently than competitors.

To be clear, TRM doesn't mean eliminating all risk. It means being deliberate about which risks you take and which you mitigate, in line with your strategy and values. It turns risk into a strategic choice rather than a gut feeling or an afterthought. For a small financial firm, that could mean, for example, deciding it's acceptable to take on more fintech innovation risk (to grow and compete), while tightly controlling cyber and compliance risks (which could sink the company). TRM gives you the framework to make those calls systematically.

Contrast this with the common compliance-driven approach: checking boxes for the regulator, focusing narrowly on credit risk or audit issues, and viewing risk as a necessary evil. In compliance mode, risk management often gets a reputation as the "Department of No" – the burdensome function that says you can't do things. TRM flips that to the "Department of How": How do we pursue our objectives safely? How do we say yes, responsibly? It's a shift from risk avoidance to risk agility. As one executive put it, "A good risk culture allows an organization to move with speed without breaking things".

For CEOs of small firms, embracing TRM can feel daunting – you might think, "We don't have a big risk team or fancy software." But TRM is less about bureaucracy and more about mindset. It starts with you and your leadership team. Do you treat risk conversations as integral to planning, or as separate compliance drills? Do you encourage employees to speak up about near-misses and concerns, or shoot the messenger? Small cultural shifts can yield outsized benefits when everyone from the intern to the CEO scans the horizon for risks and thinks, "What can we do now to address this?"

And if you need further convincing that TRM is worth your time, consider this: companies with strong risk cultures and integrated risk management are more resilient and tend to outperform through crises. McKinsey research found smaller organisations with mature risk and integrity cultures navigated external shocks better and had fewer self-inflicted issues. They weren't scrambling when the unexpected hit; they had playbooks and habits in place. In a business environment where disruption is the norm (hello, 2020s!), that's a real strategic advantage.

In short, Total Risk Management is about making risk your ally, not your enemy. It's ensuring that when the music of market change stops, your company still has a chair. But TRM is also about upside: with a solid grip on risks, you gain the confidence to invest, innovate, and stretch knowing you can survive the bumps. Next, let's look at what those bumps are in today's landscape – and why our beloved small firms are squarely in the crosshairs.

The New Risk Landscape: Cyber, Fragility and Geopolitical Curveballs (No Fear-Mongering, Just Facts)

Running a financial services or Accounting business in Australia in 2025 can feel like navigating white-water rapids. You've got currents of digital disruption, hidden rocks of cyber threats, and waves of geopolitical instability affecting markets and regulations. The trick is to navigate these rapids without scaring the crew – or yourself – into paralysis. So let's talk about the big risk areas in plain language, and why even smaller firms must pay attention.

Cyber risk stands front and center. Financial data is the new gold, and cyber criminals (from lone hackers to state-sponsored rings) want it. Small and mid-sized firms are no longer below the radar. In fact, they're often preferred targets because hackers assume (often correctly) that smaller companies have weaker defences.

Recent data confirms this: 71% of data breaches this year occurred in businesses with fewer than 250 employees. Think about that – the majority of breaches aren't hitting the big four banks or ASX 100 giants, but firms like yours. Under-resourced IT security, lack of 24/7 monitoring, maybe no cybersecurity officer on staff – it's open season for attackers.

- ✓ Recent data from Proton found that **small business are particularly at risk** when it comes to data breaches.
- ✓ Companies with 10-249 employees account for **48% of data breaches** in 2025, while companies with under 10 workers make up **23% of data breaches**, for a total of 71%.
- ✓ Data also shows that there have been nearly **800 confirmed data breaches in 2025,** with more than **300 million records exposed**.

The consequences of a breach go beyond fines or IT costs. For a financial services outfit, a major cyber incident can mean loss of customer trust, regulatory scrutiny, legal liability, and reputational damage that scares off clients. It's often existential. Yet, too many small businesses treat cyber as an IT issue rather than a business risk. One CEO told me, "We're just a small broker, why would a hacker care about us?" – right before a ransomware attack encrypted their client files and demanded $50,000 in Bitcoin. The truth is, attackers use automated tools to find any weakness; size doesn't protect you when a bot net is rattling every doorknob on the internet.

Next up, operational fragility. By this I mean the risk of your day-to-day operations breaking down – whether from internal issues or external shocks. Small financial firms often have key-person risk (what if your one compliance manager quits?), concentration risk (all your data in one cloud provider), or simply lack redundancy (one server or one office location). Remember that infamous summer day when a single data center overheating knocked out several Australian payment providers? If you were one of them, you learnt how a mundane tech glitch can halt your business. Operational risks also include process failures, third-party outages (e.g. if your payment gateway or software vendor goes down), or even a sudden regulation change that renders your current process non-compliant overnight. Without the buffers and backups that large firms have, smaller companies can be brittle – one hit and things fall apart. Identifying those single points of failure and shoring them up is a vital part of risk management (and not too hard once you look for them).
And then there's geopolitical uncertainty. It sounds far-removed – wars, trade disputes, global pandemics – surely those are concerns for governments and multinationals, not a local wealth advisory practice or credit union? But as the pandemic showed, global events can and do trickle down. Supply chain disruptions, energy price swings, sanctions on foreign partners, or even simply changes in global investor sentiment affect smaller firms too. For example, an Australian fintech sourcing software development from Eastern Europe had to scramble when conflict in that region disrupted their contractors.
Or consider regulatory ripple effects: global anti-money-laundering crackdowns eventually translated to stricter AUSTRAC requirements for all finance businesses here. No business operates in a vacuum; we're all part of a global system.

The key point is not to panic about every world event, but to cultivate an awareness: "What external shocks could hit us, and are we ready?" Leading organisations are making this a priority – 60% of business and tech leaders now rank cyber and risk as a top-three strategic focus in the year ahead. They're reconsidering things like where they host critical operations, how they diversify supply and talent, and how to insure against or mitigate emerging threats. In Australia, our financial sector regulators have also increased expectations on operational resilience – they want even smaller institutions to have plans for disruptions, incident response playbooks, etc.

Now, I promised no fear-mongering, and I mean it. The goal here isn't to say "the sky is falling, be afraid".
In fact, it's the opposite: by acknowledging these risks matter-of-factly, we take away their power to paralyse us with fear. Yes, cyber attacks are rising, but there are concrete steps to dramatically reduce your odds of a breach (like multi-factor authentication, employee training – we'll get to those). Yes, things break, but you can anticipate failure points and have backups. Yes, the world is volatile, but you can build flexibility into your business plans. The firms that thrive are those that accept reality and prepare, rather than stick their heads in the sand.

A useful mindset is to view risk management as part of running a modern business, like having internet access or doing accounting.
It's simply one of the ingredients to success. And far from being a drag, when done well it becomes empowering. Imagine confidently telling a prospective client, "We have robust systems and contingency plans to protect your data and your services, even if something goes wrong." That builds trust. Or telling your Board, "If X happens, we have a strategy ready; if Y happens, we have insurance and mitigation in place." That builds confidence in leadership. Proactive risk management, especially around cyber and ops resilience, is increasingly seen as a sign of a well-run, trustworthy company – a selling point, not just an overhead.

Before we move on, ask yourself: When was the last time you discussed these kinds of risks with your team before they became urgent? If your honest answer is "Can't recall" or "Only after an incident," you're not alone – but that's exactly what we aim to change. And to change it, we need to understand what's been holding us back. Time to shine a light on the psychology of risk decisions in the C-suite.

Why We Ignore Risk (Until It Bites): The Psychology Behind Procrastination

If you've ever delayed a difficult decision or downplayed a nagging concern, you've felt the tug of human psychology in risk management. We like to think of ourselves as rational actors, but Daniel Kahneman (Nobel laureate and godfather of behavioural economics) showed otherwise. He found that people's decisions about risk are riddled with cognitive biases and quirks – and executives are not immune. In fact, when it comes to risk, smart leaders can talk themselves into some pretty creative rationalisations to justify inaction. Let's explore a few common mental traps and how they affect CEOs in charge of risk.

1. Loss Aversion & Short-termism: Kahneman's Prospect Theory demonstrated that humans feel the pain of losses about twice as strongly as the joy of gains. Ironically, this can make us risk-seeking in avoiding losses – we'll take wild chances to avoid a sure loss – but risk-averse in pursuing gains. For a CEO, investing in risk management often looks like a "loss" on the balance sheet (an immediate cost) with a nebulous future gain (preventing something bad). The instinctive reaction? "Maybe we can put this off until next quarter's budget..." The upfront expense (hiring a security consultant, overhauling a process) looms large, whereas the benefit of avoiding a breach or disaster is mentally discounted ("That might never happen anyway"). This present-bias leads to chronic underinvestment in prevention. Many leaders only regret it after a costly incident; then the loss is real and it's too late to avoid.

2. Optimism Bias and Overconfidence: Entrepreneurs and leaders often succeed because they're optimistic and confident. The flip side is a tendency to underestimate the likelihood of negative events – especially ones we haven't experienced before. You think your firm is special, more savvy, "not like those others" who got hacked or caught out. This bias is reinforced in group settings: if your leadership team all shares a similar background and beliefs, you can collectively underestimate risk (a mild form of groupthink). Kahneman noted that optimistic biases in groups can become mutually reinforcing, validating unrealistically rosy views. In practice, that might mean a board convincing itself "our controls are fine" despite warning signs or dismissing a employee's caution as overreaction. Overconfidence blinds us to the need for action.

3. Normalcy Bias (Ignoring the Black Swan): We are wired to assume that tomorrow will look like today. If something catastrophic hasn't happened in recent memory, we treat it as a remote theoretical. This normalcy bias leads to inadequate prep for truly disruptive events (think GFC, pandemic, etc.). At small firms, I often hear "We've been operating 10 years and never had a serious incident, so why spend much time on it?" That's exactly why those incidents hurt so much when they finally occur – nobody believed they would. Nassim Taleb's "black swan" concept – rare, impactful events – taught us that past stability can be dangerously misleading. Breaking out of normalcy bias requires deliberately envisioning worst-case scenarios (as uncomfortable as that is) and asking, "What would we do?" It's the mental equivalent of a fire drill.

4. Confirmation Bias: We tend to seek and favour information that confirms our existing beliefs. A CEO who is sceptical about the value of formal risk management will likely recall the one time a risk consultant cried wolf about a non-issue, rather than the times preparation paid off. We see what we want to see. In meetings, this might manifest as downplaying new data ("Yes, that survey says most firms get breached, but our setup is different"), or only asking for opinions from those likely to agree. It's hard to fix a blind spot you won't acknowledge. Some banks that took on excessive risk prior to the 2008 crisis were later found to have ignored analysis that contradicted their growth plans. Their leaders weren't stupid – just human, filtering inconvenient truths.

5. The Busy Leader's Bias (Action Bias on Wrong Things): Not a classical term, but worth mentioning: CEOs are doers, and they hate feeling helpless. In risk management, if the problem seems too complex or long-term, they often focus instead on more immediate tasks where they can see progress (the sales deal, the product launch). Tackling risk feels abstract – "What exactly should I do first?" – so it falls to the bottom of a to-do list that's never-ending. This isn't laziness; it's a coping mechanism in a time-poor environment. The result, however, is that important but not urgent risk matters get perpetually deferred, until they become urgent (and potentially dire).

So how do we counter these biases? The first step is simply awareness – calling them out, as we just did, in plain terms. Some companies literally use Kahneman's work in their training for managers to help them recognise bias in decision-making. For example, a CEO might challenge her team in meetings: "Okay, devil's advocate time – are we being over-optimistic? What could go wrong here that we're not considering?" Encouraging dissenting views and diverse perspectives is an antidote to confirmation bias and groupthink.

Another tactic is to reframe risk initiatives not as costs but as investments in resilience and trust. Quantify the potential loss of inaction ("If we had a breach, it could cost us $X in fines and Y customers"), which often far exceeds the cost of prevention. Kahneman's research suggests people are more motivated to avoid a certain loss than a speculative one. So, frame the do-nothing approach as a certain loss of an opportunity to strengthen the company, versus the investment as avoiding a probable bigger loss.

Also, using anecdotes and real scenarios can shake folks out of normalcy bias. Share stories of peers or competitors who suffered by ignoring a risk – it makes it more concrete. (A bit of "fear of missing out" on being safe can ironically be a good motivator!)

Finally, set triggers and deadlines. For example, commit to a quarterly risk review meeting – even if it's just 1 hour – where you force yourself to confront "low-probability, high-impact" risks. Humans respond to routines and social expectations; if your calendar and team expect you to regularly think about risk, you're more likely to do it.

The bottom line: we're all human, and our brains are wired to sometimes misjudge risk. It takes conscious effort to counteract biases. But as leaders, part of our job is to actively guard against these pitfalls – in ourselves and in our teams. That means fostering a culture where speaking up about risk isn't seen as negative or paranoid, but as prudent and valued. Speaking of culture, let's delve into that next: how to build a risk culture that not only avoids problems but actually propels performance.

Building a Risk-Aware Culture: Your Best Defence and Offense

Culture can sound like a squishy concept – all foosball tables and "our values" posters. But when it comes to risk, culture is make-or-break. Think of risk culture as "the way we do things around here when no one is watching." It's the collective mindset and norms that determine how your people identify, discuss, and manage risks day to day. You can have all the policies in the world, but if the culture encourages bending the rules, hiding bad news, or shooting messengers, you'll eventually face a nasty surprise.

On the flip side, a strong risk and integrity culture can be an unsung hero of business success. It allows a company to move quickly but safely, and adapt to change without blowing up. McKinsey put it well: "A good risk culture allows an organization to move with speed without breaking things. It is an organization's best cross-cutting defence." In fact, their research found that companies with mature risk cultures outperform peers through economic cycles and shocks. They suffer fewer self-inflicted wounds (think rogue trades, compliance fines, operational gaffes) and have more engaged customers and employees. Why engaged customers/employees? Because trust and transparency are high – people trust the company to do the right thing, and employees feel safe to speak up.

For a small financial firm, building a risk-aware culture doesn't require big committees or departments. It starts with tone from the top and a few practical habits:

- **Set the expectation that risk is everyone's responsibility.** From the intern to the execs, everyone should feel they have a role in flagging risks and solving them. The receptionist who notices a tailgater sneaking into the office, the analyst who spots an odd transaction pattern – they need to know it's not only okay but expected to raise a hand. Make it part of job descriptions or onboarding: "At our company, managing risk isn't just the compliance officer's job – it's part of all our jobs."

- **Encourage open communication – no blame for bad news.** This is huge. If employees fear punishment or ridicule for bringing up a mistake or concern, they'll hide it until it festers. Create psychological safety by responding constructively when risks or errors are surfaced. Say "Thank you for flagging this – let's fix it" instead of "How did you let this happen?!" One Australian fintech holds a quarterly "risk town hall" where teams share near-misses and lessons learned. Leadership kicks it off by admitting something they could have handled better. This vulnerability from the top sends a message: we'd rather know and grow, than not know and blow up.

Define what a good risk culture looks like (concretely). Vague slogans won't cut it. Organisations should be spelling out specific behaviours that embody your desired risk culture. For example: "We proactively escalate issues; we welcome challenge in meetings; we reward honesty, not just good news." You might define dimensions like transparency, accountability, learning from mistakes, etc., and even survey staff on these. Some organisations use surveys with targeted questions to measure if people feel comfortable reporting risks, if they believe actions will be taken, etc. Measuring culture can seem odd, but what gets measured gets managed. If you find a certain department has low scores on "speaks up about concerns," you can intervene (perhaps leadership coaching or process changes there).

- **Lead by example.** As CEO or leader, your actions speak loudest. If you preach risk awareness but then routinely ignore control processes "because sales matter more," guess what culture you'll get? Alternatively, if you candidly discuss risks in strategy meetings (not just the opportunities), others will follow suit. I once consulted for a mid-sized credit union where the CEO started every executive meeting with a 5-minute rundown of any emerging risks or incidents since last time, before diving into finances. It signalled that risk was top-of-mind. When he didn't have any, he'd mention a near-miss story from the industry to discuss. That habit permeated the company – managers began their team meetings similarly. It became normal to talk about what could go wrong and how to prevent it.

- **Align incentives and accountability.** People behave based on what they're rewarded or punished for. If your salespeople get commission on volume with no regard for risk, don't be surprised if they start bringing risky business (or worse, cutting corners). Balance rewards with quality metrics or risk KPIs. Also, hold folks accountable when there are negligent risk lapses – not in a witch-hunt way, but fairly. For instance, if someone repeatedly ignores security protocols, it has to reflect in performance reviews. Conversely, celebrate good catches: if an employee's alertness saves the company from a scam or error, recognise and reward that. It shows that "doing the right thing" is valued.

Integrate risk into hiring and training. When bringing people on, especially leadership, consider their attitude toward risk and integrity. Skills can be taught, mindset is harder. In training, include modules on risk awareness (like basic cybersecurity hygiene for all staff, ethical decision-making, etc.). One company I know has a fun annual "risk bootcamp" day with simulations (e.g., a phishing email test, a fake media crisis scenario) – it's engaging and reinforces that risk management is part of our identity. A quick case in point on cultural impact: the notorious Wells Fargo scandal in the US (where millions of fake accounts were opened by employees) is often cited as a risk culture failure. The bank had intense sales pressure and incentives misaligned with risk, and an environment where staff feared speaking up. The result was widespread misconduct that severely damaged the company's reputation and cost billions in fines. Many of the costliest corporate disasters have such cultural root causes. Conversely, when JP Morgan's CEO Jamie Dimon famously quipped, "I'd rather lose a billion dollars than lose our reputation," he was reinforcing a culture where long-term integrity trumps short-term profit.

For smaller firms, your culture is even more palpable because everyone knows everyone. It can change quicker, too – for better or worse. A single influential toxic person can corrode it, or a single inspiring leader can elevate it. If you instil a strong risk culture now, it will scale with you as you grow. It's like laying the foundation of a house right – unsexy but vital for everything built on top.

As a leader, perhaps the highest ROI investment you can make is in nurturing a culture that "does the right thing even when no one's watching." It's not only about preventing scandals; it's also about agility. Such a culture will embrace change more readily (because people aren't afraid to experiment and occasionally fail safely), and it will impress stakeholders. Regulators, customers, potential partners – they all can sense a company that's in control versus one accident away from a mess.

From Reactive to Dynamic:
A Five-Point CEO Playbook for Risk Resilience

To help overwhelmed leaders move from good intentions to action, let's distil a simple framework. Drawing on insights from McKinsey's "Dynamic risk management for uncertain times" and Aphore's on-the-ground experience with SMEs, here are five key actions you can take to build resilience and growth through risk management. Think of these as pillars of your Total Risk Management game plan:

1. Reset Your Risk Aspiration – Make Risk a Value Creator, Not an Avoidance Exercise.
Many small firms treat risk management as just preventing bad outcomes. Instead, set a higher aspiration: use risk management to enable strategic moves. In practice, this means clarifying your risk appetite and objectives. Ask: What risks are we willing to take to grow, and what risks will we never take? Ensure this is discussed at the board/owner level. For example, you might decide "We will invest in new digital services (taking innovation risk), but we will not compromise on data security or regulatory compliance." Communicate this clearly so everyone knows the guardrails. By formalising risk appetite, you turn fuzzy fear into concrete guidelines. This helps frontline staff make decisions aligned with strategy (e.g., a product manager knows it's okay to launch a beta with some market risk but not okay to use a third-party vendor who isn't security-vetted). It elevates risk to a strategic conversation. The goal is to move from risk mitigation to risk-enabled growth – akin to going from just playing defence to also executing offense in a game.

2. Embrace Agile Risk Management – Speed Matters.
The environment is volatile; you can't afford bureaucratic slowness when a risk or opportunity emerges. Borrowing from agile principles, set up ways to identify and respond to risks in real time. This could mean having a small cross-functional "tiger team" ready to assemble when a crisis hits (say, your IT lead, ops manager, and a comms person huddle immediately on a cyber incident). Some companies do daily or weekly risk huddles – e.g., a 10-minute check-in on any new customer complaints, fraud alerts, or operational hiccups. One fintech I know reviews a dashboard of key risk indicators every morning (failed logins, support tickets spikes, etc.), which helps them catch issues early. Agile risk management also means empowering people: decide which

decisions can be made on the spot by single owners versus needing committee sign-off. For instance, if a suspicious transaction occurs, your fraud analyst might have pre-approved authority to freeze an account without running it up the chain (speed is crucial there). Create playbooks for fast decision-making in urgent scenarios. Practise it through simulations or drills so that when something happens, your team acts swiftly and confidently. Ultimately, agility in risk management turns potential emergencies into manageable hiccups.

3. Harness Data and Technology – Get Ahead of the Curve.

Don't let risk monitoring be an occasional manual chore. Today, even small firms can leverage affordable tech to continuously watch for red flags. Simple examples: use that SIEM (Security Information and Event Management) tool or even built-in cloud security dashboards to get alerts on unusual logins or data transfers. Implement automated checks in processes (e.g., an automated compliance rule that flags transactions over a limit). Embrace analytics: for instance, analyse your client data to spot if any have unusual trading patterns or if any process is creating customer pain points (which could become conduct risks). Advanced analytics and AI aren't just buzzwords – they can predict risk occurrences. For example, a pharma company using analytics to target audits at higher-risk sites, freeing up 30% of quality resources. In an SME context, maybe you use analytics on past incidents to predict where future ones might come (e.g., most downtime last year came from a particular software – time to upgrade it). Also consider external data: threat intelligence feeds for cyber, market alerts for finance, etc., many of which have SME-friendly services. The message is: invest in tools that give you visibility. You can't manage what you don't monitor. And with today's tech, you can monitor a lot even with a lean team. Even a well-configured Excel dashboard of key risk indicators is better than flying blind – but aim higher if you can. Technology can be your early warning system and efficiency driver in risk management.

4. Develop (or Borrow) Risk Talent – You Need the Right Skills.

For small firms, "risk talent" doesn't necessarily mean hiring a CRO tomorrow. It means ensuring the people handling critical risk areas have the know-how, and/or getting external advice when needed. Identify your internal skill gaps. If nobody on your team deeply understands cybersecurity, consider training someone or using a virtual CISO service part-time. Many SMEs partner with consultancies (yes, like Aphore) for periodic risk assessments or virtual risk officer support – that's a valid model until you're big enough to justify full-time roles. Importantly, educate your existing team. Provide training on topics like fraud detection for ops staff, or regulatory compliance for your product designers. Rotate people through roles if possible – someone in finance spending a week with compliance team, etc., to broaden understanding. McKinsey suggests risk managers of the future need strong business knowledge and tech savvy. In a small firm, this means your business people need some risk education, and your tech/risk folks need to understand business strategy. Break down those silos. Encourage certifications or courses (perhaps an IT person gets a cybersecurity certification; your accountant learns about operational risk). And of course, hold executives accountable for risk too – ensure someone at the top formally oversees it, even if it's the CEO wearing that hat. If you're the CEO, you might form a tiny advisory board or use your Board of Directors for oversight on risk decisions, so you're not alone. The key is to not neglect the human element: even the best framework fails if people don't have the mindset or skills to execute it.

5. Fortify Risk Culture and Accountability – Walk the Talk Daily.

We discussed culture at length in the previous section, so here we emphasize embedding that culture into daily business. Link risk considerations with daily operations and outcomes. For example, include a "risk impact" section in your project proposals or product launch checklists. Make risk discussion a standing agenda item in management meetings (even if brief). Hold leaders accountable for lapses – if a department repeatedly has issues due to ignoring policy, that's a leadership performance matter. And conversely, celebrate successes where risk management helped achieve an outcome (e.g., "Thanks to our continuity plan, we kept trading during the cloud outage – great job team!"). The goal is to ensure risk awareness isn't a quarterly workshop, but part of the DNA. Executives should model the desired behaviour – if you commit to that quarterly cyber drill, show up and engage fully so others do too. If you make a mistake, own it publicly (demonstrating accountability). Building true risk culture is an ongoing effort, but it yields a self-policing organization: front-line employees start thinking "Is this within our risk appetite? Should I get sign-off before proceeding?" without being told each time. That's when you know it's working – risk-aware thinking becomes second nature.

One might ask, how does a tiny firm implement all this without it consuming everyone's time? The answer is: incrementally and with pragmatism. Start small under each pillar. Maybe this quarter you focus on defining risk appetite (Action 1) and scheduling a risk workshop with your team (Action 5). Next quarter, you invest in a new monitoring tool (Action 3). The following, you do a cyber training and update roles (Action 4). Agile practices (Action 2) can start with a single "what if" drill or a quick daily check-in routine. Each step will already yield some benefit, and they reinforce each other.

By the way, these five actions are adapted from best-practice research, but I've seen them work in the wild. A regional credit society implemented a version of this playbook over 18 months – result: they experienced a 40% reduction in operational incidents year-on-year, faster issue resolution (mean time to recovery down by ~30%), and even a bump in employee engagement scores related to trust in leadership (they share that employees felt safer knowing leadership "had a plan" for risks). And notably, when a regulator did an inspection, they gave positive feedback on the firm's risk management, which boosted the firm's credibility to pursue new business. That's tangible ROI.

In essence, this framework turns risk from a sporadic firefighting exercise into a structured part of running the business. We're not managing risk for its own sake; we're managing it to be able to move faster, build trust, and seize opportunities with our eyes open.

Turning "No Worries" into "Know Worries" – Act Now, Thrive Tomorrow

Australian business culture is famously relaxed – the land of "no worries". It's part of our charm, but as we've explored, it has a dangerous flip side in the domain of risk. Complacency and deferred action can turn small cracks into gaping holes. The good news is that by changing "no worries" to "know worries" (i.e. knowing what to worry about and prepare for), CEOs of even the smallest firms can sleep better at night and perform better by day. Treating risk as a strategic and cultural advantage is about empowerment, not fear. It's about knowing that you have done what's reasonable to prevent disasters, and equally knowing that if something does go wrong, you'll catch it early and handle it capably. That confidence radiates outward – to your team, your customers, your regulators. It becomes part of your brand. In an industry built on trust (financial services), that's pure gold. Let's recap the journey we've taken:

- We debunked the myth that risk management is just a cost center or necessary evil. In reality, the firms that integrate risk management (TRM) into strategy tend to outperform and outlast those that don't. Risk done right yields return.
- We saw that the world isn't getting any simpler. Cyber threats, operational weak links, geopolitical shifts – they affect businesses of all sizes. Ignoring them doesn't make them go away; it just leaves you unprepared. And preparation is a lot less expensive than remediation (or regret).
- We confronted the human biases that hold us back – loss aversion, optimism, normalcy bias, etc. Recognising these tendencies is half the battle. The other half is building habits and cultures to mitigate them (like welcoming bad news, setting routines, reframing investments).
- Culture emerged as a hero. A strong risk culture can catch a problem that no rule or tech system could, simply because an attentive

employee spoke up. It also fuels better decisions and innovation, as people are more likely to surface concerns and consider downsides proactively.

- Finally, we laid out a practical framework of five actions to level up your risk management in a manageable way. It's not rocket science or huge spending – it's leadership focus and a series of small changes that compound into big capabilities.

As a CEO or senior leader of a small-to-mid financial firm, you might be thinking, "This all makes sense, but where should I begin, right now?" Here's a quick suggestion to get momentum:

Start with a conversation. Gather your core team for a frank discussion: What's our biggest nightmare scenario? How ready are we for it? It could be an hour of eye-opening talk. List a few risks and rate your preparedness. That simple exercise often spurs action – you'll see glaring gaps and quick fixes. Maybe you realize nobody's backing up a critical system offsite, or that only one person knows a key process. You'll likely come away with a short to-do list. Do one thing from it immediately – perhaps call your IT provider about that backup, or schedule a meeting with a consultant for a cyber checkup.

Then, schedule your next risk check-in (quarterly is fine to start). Consistency is key. Over time, these discussions become part of how you run the business.

And remember, you're not alone. Many resources (public frameworks, industry workshops, yes, and thought leadership pieces like this!) are available. Don't hesitate to lean on external help for areas outside your expertise – it's not a weakness, it's smart stewardship.

In closing, transforming risk management in your company might not happen overnight. But every step you take will make your organisation a bit safer, more resilient, and more competitive. You might even find that working on risk brings your team closer together – there's a camaraderie in collectively safeguarding the enterprise you've built.

One day, you may look back and realise that making risk a priority was a turning point. Instead of lying awake at 3 AM worrying about unknown dangers, you'll have the assurance that you anticipated and acted. Instead of dreading the auditor's or regulator's call, you'll be prepared and confident. And instead of playing catch-up to crises, you'll spend more time seizing opportunities – because you've got the downside covered.

They say fortune favours the bold. In the world of business, I'd add: fortune favours the bold and the prepared. By embracing Total Risk Management and a risk-aware culture, you can be both. So go on – make risk your new competitive advantage. It's the one gamble that's truly worth it.

Sources:

- Andersen, T.J. (2008). The Performance Relationship of Effective Risk Management: Exploring the Firm-Specific Investment Rationale. Long Range Planning, 41(2), 155-176.open-access.bcu.ac.uk

- PwC. (2025). 2026 Global Digital Trust Insights: New world, new rules – Cybersecurity in an era of uncertainty. Key findings from a survey of 3,887 executives.

- McKinsey & Company. (2020). Strengthening institutional risk and integrity culture. McKinsey Risk Practice Article.mckinsey. commckinsey.com

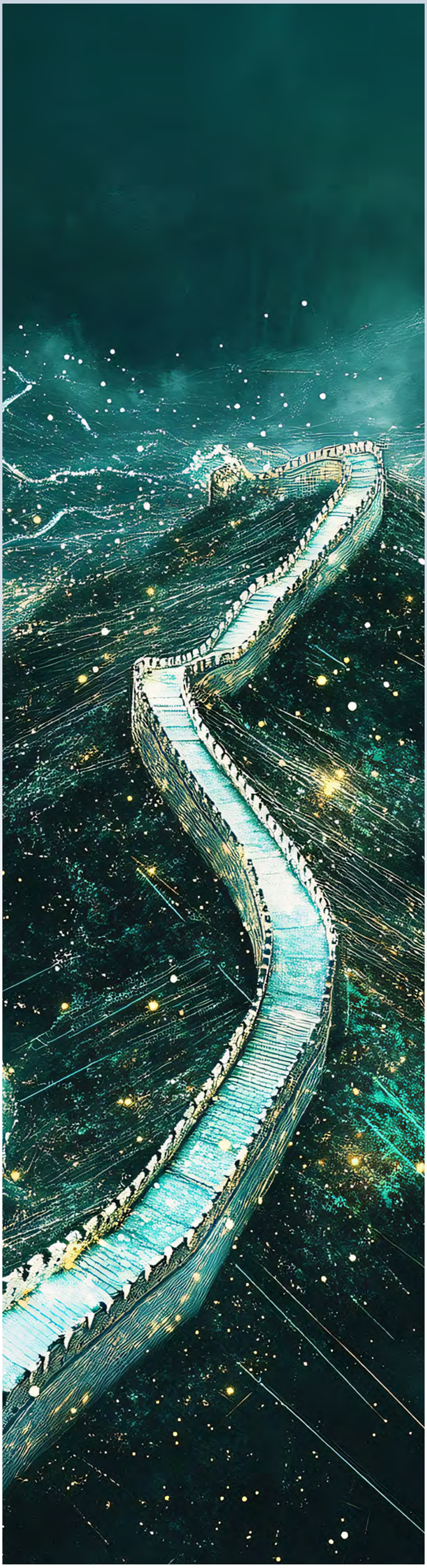
- McKinsey & Company. (2020). Meeting the future: Dynamic risk management for uncertain times. (R. Jain, F. Nauck, T. Poppensieker, O. White)

- Cawley, C. (2025). "Study: 71% of Data Breaches Impact Small Businesses." Tech.co (Nov 4, 2025).tech.co

- Rossi, C. (2024). "Reflections on Daniel Kahneman's Contributions to Risk Management." GARP Risk Intelligence (Apr 12, 2024).garp.org

- Aphore research and client case studies, 2023-2025 (internal data and experiences shared anecdotally in text).

Why the New Social Media Laws remind me of Caddyshack



The Great Firewall Field Trip

In 2019, my 14-year-old daughter went on a school trip to China. Officially, it was an educational tour; unofficially, it became a test of how tech-savvy Aussie teens could outsmart an entire country's internet censorship. The Chinese government bans popular Western social media platforms – no Instagram, no Snapchat, definitely no TikTok (at least not the global version). Determined to keep their streaks alive and their group chats humming, her classmates treated this ban like a challenge. One student had pre-installed a VPN to tunnel under the Great Firewall. Another packed an old iPod Touch (disguised as a mere "audio device") that could still hop on hotel Wi-Fi and access blocked sites. Evenings in the hotel, a few kids huddled around a smuggled laptop, using an online game's chat feature to message friends back home – a digital séance bypassing the social media seance. Sneaky workarounds sprouted like mushrooms. It was like a game of whack-a-mole, or more aptly, watching Bill Murray in Caddyshack battling that elusive gopher – every time a tunnel was filled, a new escape route popped up with a cheeky teenage grin. The experience was eye-opening: banning social media in theory sounds protective; in practice, it was almost comical how easily the kids became underground tech ninjas.

Fast forward to 2025, and Australia is about to attempt a similar feat nationwide: banning everyone under 16 from social media. As a cyber security professional – and a dad – I have a foot in both camps of this debate. I've seen the very real harms unchecked social media can inflict on young minds, and I applaud the intent to create a safer digital world for our children. But I also carry the lesson of that China trip: teenagers, when motivated, will find the cracks in any system. A law alone, no matter how well-intentioned, can become a high-stakes version of whack-a-mole – with our kids' wellbeing on the line. Before we celebrate Australia's bold new ban as a silver bullet, we need to examine its targets, its likely misfires, and what might actually make a dent in the problem.

I want to break down Australia's under 16 social media ban through multiple lenses – from the mental health crisis it hopes to address, to the technical and social pitfalls of enforcement, to smarter alternatives that move beyond bans. It's a distinctively Aussie take – frank, pragmatic, and a touch irreverent (because if we don't laugh at the absurdities, we might cry). By the end, we'll see that protecting kids online is less about swinging a sledgehammer and more about building better guardrails. As any parent knows, you can't watch your kids every second – but you can give them a safe playground and teach them how to play. Consider this a call to action for all of us – parents, educators, tech executives, regulators – to innovate the kind of digital guardrails that even a clever Year 8 student would find hard to dodge.

Why Social Media Scares Us for Our Kids

Scrolling. Posting. Lurking. For today's teens, social media is as entrenched in daily life as school or sleep (perhaps more than sleep). And that's exactly what has so many parents, psychologists, and now politicians alarmed. The past decade has brought a tsunami of troubling data on youth mental health that correlates with the rise of smartphones and social media. It's not just one sensational headline – it's a steady drumbeat: higher rates of depression and anxiety, spikes in teen self-harm and hospitalisations, and countless anecdotes of cyberbullying trauma and body image issues. Before dissecting the ban, we must understand the monster it aims to slay.

Consider this: more than 4 in 10 Australian teens now suffer mental health distress, a rate that has climbed dramatically alongside social media's proliferation. The rate of teen girls being hospitalised for intentional self-harm jumped 70% between 2008 and 2022 – a period that neatly brackets the iPhone era and the advent of Instagram's filtered perfection. Psychologists say this is no coincidence. They point to "social media toxicity" – a perfect storm of factors that can erode a young person's wellbeing. Platforms like Instagram and TikTok create highlight reels of others' lives that fuel toxic comparisons ("Why is everyone else happier/prettier/more popular than me?"). The endless dopamine loop of likes, shares and comments hooks teens into compulsive checking, seeking validation from metrics on a screen. And lurking in the shadows are outright dangers: cyberbullying that follows kids home from the schoolyard, online predators grooming victims behind fake profiles, extremist or self-harm content algorithmically served to vulnerable youth.

These aren't just theoretical risks – they're happening every day. Australian teenagers themselves report being keenly aware of the dark side. In focus groups, they talk about the anxiety of waiting for likes, the sting of being left on "read," or the fear of missing out (FOMO) that keeps them glued to social feeds lest they be left behind socially. The Australian Psychological Society notes that teens often base their self-worth on social media feedback. One malicious comment or an unflattering photo

Daily social media usage among Australian

2.5% of teens abstain entirely in 2023 survey can send a teen spiralling. Even more disturbing, social media has been weaponised to rate appearance and share non-consensual images – essentially high-tech public shaming that can be devastating for a child's psyche.

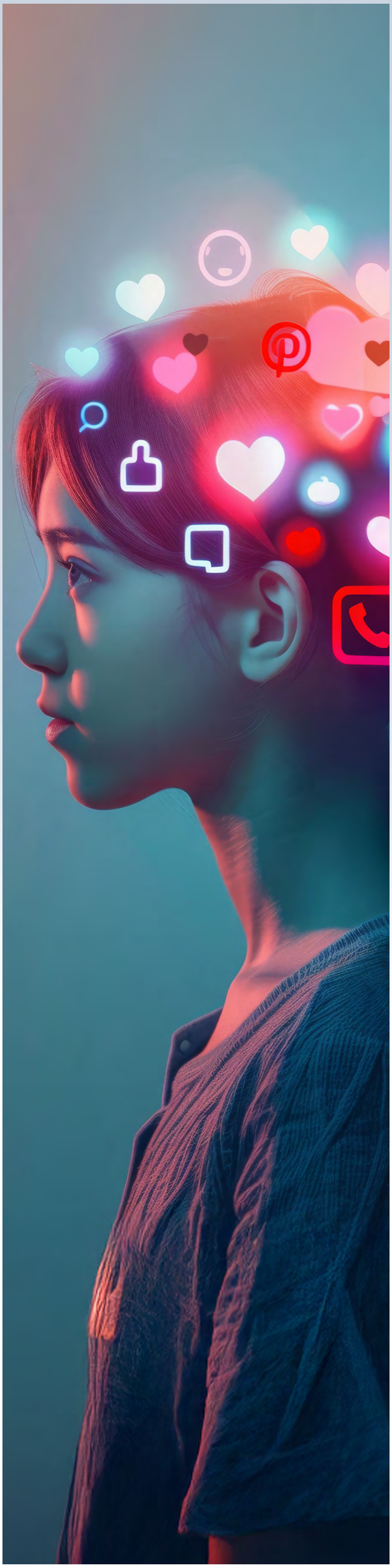
Indeed, Australia's youth mental health organization Orygen found that teens who are moderate users (1–3 hours a day) often fare as well as light users on measures like feeling in control of their lives. It's the heavy users (3+ hours) who report the worst mental health outcomes – more loneliness, less hope, and greater psychological distress. This nuance is important. Social media is not pure poison, nor pure pixie dust – it's a tool that can hurt or help depending on how it's used. Many teens derive real benefits: staying connected with friends (critical during pandemic lockdowns), finding supportive communities, accessing educational content, or creative self-expression. In fact, 73% of young Australians say they've used social media for mental health support or information. These positives often get overshadowed in public debate, but any policy must consider them. Otherwise, we risk overcorrecting and cutting off a generation from not just the harms of social media, but also the help and empowerment it can offer.

38% 3 or more hours per day on social platforms

On a neurological level, researchers like Jonathan Haidt have argued that major platform design changes – notably the introduction of the "Like" button around 2009 – amplified these harms. With likes and shares came algorithmic curation, meaning adolescents began receiving a feed optimised not for their growth, but for their engagement (and the platform's profit). Unfortunately, what drives engagement is often content that provokes strong emotion – outrage, envy, or despair. As tech ethicist Aza Raskin famously put it, social media companies "sprinkled behavioural cocaine" all over their interfaces to keep users hooked. And no surprise, developing teenage brains are especially vulnerable to these tricks of persuasive technology.

What does this toxic milieu mean in real terms? Australia's government cited research that over-use of social media is harming young teens by spreading misinformation, enabling bullying, and distorting body image perceptions. Peer-reviewed studies have linked higher teen social media time to increased depression symptoms – though, to be fair, some research suggests moderate use (a couple hours a day) isn't inherently bad and can even be positive for some teens.

The evidence is stark that something is rotten in the state of teen social media use. The Australian government's decision to swing the pendulum toward safety is understandable, even commendable in its intent. But is banning under 16s from all major platforms the right answer? To explore that, let's unpack what the ban actually entails and whether it addresses the roots of these harms – or merely the symptoms.



The Logic Behind the Ban: "For the Good of Our Kids"

No parent would disagree: kids today face online risks that were inconceivable a generation ago. From Canberra's perspective, doing nothing was not an option. So, what exactly does Australia's new social media law promise to do? In a nutshell, it raises the age bar – no one under 16 can have a social media account, period. Unlike the previous status quo (which allowed 13–15 year-olds with parental consent per platform policies), this law slams the door entirely until a teen's 16th birthday. As Communications Minister Anika Wells puts it, it's "for the good of our kids" – a necessary step to delay exposure to the wilds of social media until kids are a bit older, hopefully wiser, and more resilient.

social media age to 16, and by late 2024 support had grown to 64%. Many parents, frankly, were relieved: after years of fighting with their teenagers over screen time, here was a law that would do the heavy lifting for them by making underage social media use outright illegal. "It's time to reclaim childhood for our kids," as one mother told pollsters, echoing a widespread sentiment.

So, the logic behind the ban is straightforward: keep kids offline longer to protect their mental health and safety. Government messaging emphasizes a preventative approach – stop the problem before it starts. If 13, 14, 15-year-olds aren't allowed reforms in progress). In the meantime, perhaps they'll spend more time in the "real world" – playing sports, hanging with friends face-to-face, doing homework without the constant ping of notifications. Prime Minister Anthony Albanese even mused that kids freed from social media's grasp might rediscover "the footy field or netball court" and healthier pastimes.

Crucially, the law doesn't penalise kids or parents directly for violations – there's no threat of fining a 15-year-old for having an illicit Facebook account. Instead, the onus is on the tech companies (the Facebooks, Googles, ByteDances of the world) to enforce age compliance or face steep fines.

The ban was passed in November 2024 as an amendment to Australia's Online Safety Act, after a period of heated public debate. Politically, it enjoyed bipartisan support – few elected officials want to be seen as pro social-media-for-children in today's climate. Public opinion was squarely behind it, too. Early polls showed about 61% of Australians supported raising the on Insta or TikTok, they can't be cyberbullied on those platforms, can't tumble down Reddit rabbit holes or see harmful content there, can't develop a Snapchat streak addiction, and so on. Ideally, those extra formative years offline mean they'll be more mature and better equipped to handle social media at 16 (and platforms might be "cleaner" by then due to other safety

The ban applies to "social networking services" broadly – expected to include the usual suspects (Facebook, Instagram, TikTok, Snapchat, YouTube, X/Twitter, Reddit). Notably, some exceptions are built in: messaging apps like WhatsApp or platforms designed for kids (Messenger Kids, YouTube Kids, educational tools) are likely exempt. The law essentially tells

Big Tech: "Make sure no under 16s have accounts. How you do it is up to you, but if you fail, we'll fine you into the Stone Age (up to $50 million per breach)."

This approach cleverly sidesteps turning rebellious teens into lawbreakers – instead it deputises the platforms as the responsible gatekeepers. Companies must take "reasonable steps" to verify ages and shut down underage accounts. Early ideas thrown around included requiring users to upload ID or having government IDs linked to accounts, but pushback on privacy and practicality made regulators shy away from mandating that. The current thinking is to use a mix of "age assurance" technology: AI algorithms that estimate age from user activity or even scan faces to guess age, plus maybe credit card checks or integration with forthcoming digital ID systems. It's worth noting – Australia is piloting a Digital ID framework for citizens, and while the law says it won't force everyone to present ID just to log on, the infrastructure is creeping in that direction. Age verification trials have shown it's technically feasible to verify age without a full ID (for example, using third-party services that certify your age range). But whether these will be accurate and privacy-preserving at national scale is an open question.

The ban's supporters argue that even if enforcement isn't perfect at first, it sets a clear national standard. It empowers parents to say "Sorry kid, it's not just my rule – it's the law". The Wiggles (yes, the famous children's entertainers) even lobbied for the ban, reflecting how mainstream the idea of "social media = danger for kids" has become in Aussie culture. Mental health advocates, child safety groups, and a significant swath of weary parents have cheered the government for finally doing something bold. They liken it to past public health wins – think banning cigarette ads on TV or mandating bike helmets – interventions once seen as overreach that later proved life-saving. If social media is the new nicotine for youth, why let 13-year-olds get hooked? Delay the onset, and you reduce lifetime harm – that's the theory.

On paper, then, the ban is a decisive strike at the heart of the youth social media problem: if under 16s can't access it, they can't be harmed by it. The simplicity is the appeal. However, as we'll explore next, that simplicity is also its Achilles' heel. Adolescent life, both online and offline, tends to find a way. Is this law a protective shield or a Maginot Line easily bypassed? Let's look at how today's digitally native teens might respond when the new rules hit – and the technical cat-and-mouse game likely to ensue.

The Whack-a-Mole Problem: Tech-Savvy Teens and Porous Defences

If you've ever tried to enforce a household internet curfew on a teenager, you know it can feel like shovelling water. You shut one door, they find a window. Australia's under 16 ban is poised to play out on a national scale this same dynamic – determined kids versus digital fences – and it's why many experts are sceptical about the ban's real-world efficacy. "Extremely difficult to enforce," YouTube representatives told a parliamentary committee bluntly, and that's putting it mildly. Let's break down why keeping under 16s off social media may be a high-tech game of whack-a-mole.

First, consider the arsenal of circumvention tools even moderately tech-savvy teens have at their disposal. The most obvious is simply lying about age – something countless kids already did under the 13+ rule. What's to stop a 14-year-old from telling Instagram they're 16, or using a parent's credentials to sign up? Platforms will likely implement stronger age checks (perhaps scanning profile pictures or usage patterns for signs of youth), but such measures can be gamed. Kids swap tips on new apps and exploits faster than adults can keep up. We might see a blossoming trade in stolen or borrowed identities – e.g. a 15-year-old logs in using an older sibling's account (with or without said sibling's permission). Shared family devices could muddy the waters too: if a parent stays logged into Facebook on the home computer, what stops junior from sneaking on?

Then there's the use of VPNs and other location/anonymity tools. A VPN (Virtual Private Network) can mask the user's location and identity. If age verification is tied to Australian sites or networks, some teens will simply route their connection through another country where no ban exists. It's an arms race we know well from other banned content (like Aussie users evading geoblocks to access media or games). Now, if the platform itself is doing age-gating at account creation, a VPN alone might not help unless one can pretend to be an adult from abroad. But combined with fake credentials, it could add a layer of confusion for enforcement systems.

Alternate platforms pose another whack-a-mole issue. The law names specific mainstream social networks, but what about borderline cases? For example, is Discord (a popular group chat app especially for gaming communities) considered social media? Probably yes, and likely to be included, but if not explicitly, teens will flock there. Online games with chat functions (Fortnite, Minecraft, Roblox etc.) might become de facto social networks for under 16s. Already, many kids under 16 use these games to socialise, and those channels would likely see even more use if Instagram et al. are off-limits. As one child safety advocate noted, "If we pull up the drawbridge on social media platforms, those bad actors won't disappear… They will simply migrate to gaming and messaging services". In other words, the risk doesn't evaporate – it moves elsewhere, perhaps somewhere even less regulated.

The ban could also drive a surge in the use of age-tailored "kids" versions of apps where available. YouTube Kids, for instance, is allowed under the ban. But savvy under 16s might quickly tire of the kiddie pool and attempt to use grown-up YouTube via incognito modes or devices not linked to their identity. We might see interesting new tech hacks: perhaps teens will gravitate to VPN-equipped browsers, Tor networks, or new "underground" social platforms specifically designed to dodge age rules. It's the nature of cat-and-mouse: every new rule creates a market for evasion.

Even if a fraction of teens circumvent successfully, it sets a precedent and spread through peer networks. Imagine a Year 9 classroom – most students have no social media by law, a few clever ones manage to maintain a secret Instagram. Those few become local tech heroes (or dealers, if you will), potentially sharing accounts or teaching others. We could even see the rise of "fence" accounts – older teens (16+) renting out or sharing their profiles with younger friends to give them a peek inside. Such arrangements are hard to police without deep surveillance of user behaviour, which raises a whole other set of privacy and civil liberty concerns.

The Australian Human Rights Commission sagely pointed out that technological workarounds like VPNs and false age declarations will likely undermine the ban's effectiveness. They also note a crucial limitation: even if you managed to seal off all under 16 access, the ban **"will not address the root causes of online risks or make the platforms safer for everyone"*. It's like squeezing a balloon – the air (or in this case, the risk and the youth demand for online socialising) just bulges out elsewhere.

Ironically, heavy-handed enforcement attempts could create new risks. If more underage activity goes underground or unspoken, that reduces transparency. Today, a parent might know their 15-year-old has an Instagram and follow or supervise it. In a ban scenario, that same teen might still be on Instagram but in secret, taking extra steps to hide it from parents (clearing browser history, using friend's devices, etc.). This erodes trust and open dialogue between parents and kids around online life. One poll indicated that 1 in 3 parents already might be willing to help their kids bypass the ban – a perhaps shocking statistic that suggests some families prefer controlled violation to leaving their teen socially isolated. If parents themselves become complicit, enforcement becomes nearly impossible – what are authorities going to do, raid homes to check for TikTok apps?

We should also acknowledge that platforms have incentives and methods to resist. Major social media companies, while publicly compliant, are not thrilled at losing a chunk of future users. YouTube has even hinted at possible legal action to challenge its inclusion in the ban. Platforms will likely tighten age controls (they have to, by law) but perhaps not go above and beyond to catch every clever teen. If enforcement cost or friction gets too high (say, requiring rigorous ID checks that annoy adult users or drive them away), platforms might push back on regulators or find ways to technically comply while not catching every violation. The law says "reasonable steps" – an inherently squishy term. Expect ongoing tussles between the eSafety Commissioner and industry about what measures are enough. In Australia's wider Online Safety Act codes, there's talk of things like device-level controls and app store responsibilities. Those could bolster enforcement (e.g. requiring Apple/Google to verify age before letting someone download a social app), but again, motivated teens might just use web versions or other distribution channels.

In sum, keeping under 16s completely off social media is about as plausible as keeping water in a sieve. Teenagers are resourceful, collectively brilliant at identifying loopholes, and frankly, driven by a developmental imperative to socialize and assert independence. This is not to pour cold water on the law's intent – any measure will have some leakage – but the scale of expected evasion here could be substantial. Policymakers may soon feel like the arcade player desperately hammering down one mole only for two more to pop up. Before long, one has to ask: is there a better way to tame the moles?

However, the whack-a-mole problem is only one side effect. Let's explore further the unintended consequences and collateral risks of such a ban – even if it could be enforced with 100% success (a big if), what new problems might it create?

Unintended Consequences: From Underground Behaviours to Backfire Risks

The law of unintended consequences hasn't been repealed – and sweeping social policy changes often bring a host of them. Australia's under 16 social media ban, noble in aim, could inadvertently shift problems rather than solve them, or even create new ones. We've touched on some already, like driving youth to alternative platforms or secretive use. Here we dive deeper into the potential knock-on effects for kids, parents, and the internet ecosystem.

1. Underground behaviour and loss of transparency: Perhaps the biggest worry is that by pushing under 16s off mainstream platforms, we might lose sight of them entirely online. Right now, a 14-year-old on Instagram is somewhat in the open – there are at least mechanisms for reporting harmful content, parental monitoring (if the parent is aware and connected), and platform policies (albeit often inadequately enforced) for minors. If that 14-year-old instead spends their online social time on, say, an encrypted chat app or a niche forum not covered by the ban, they are in a darker alley of the internet. It becomes harder for authorities to detect grooming or bullying occurring there, and harder for parents to even know what apps to be concerned about. As Sonia Livingstone, a prominent researcher on children's digital rights, noted about bans: "It makes a great headline and seems straightforward, but it isn't... it very quickly becomes a ban on children accessing technology" in ways that may not improve safety. The "bad actors" – bullies, predators, exploitive content – won't politely evaporate; they'll just find minors on other channels. Indeed, some predators might prefer it, as smaller platforms can be less policed.

2. Normalising circumvention (and making rule-breakers of kids): If a law is widely flouted, it can breed cynicism or a cat-and-mouse mentality in the very people we want to protect. For teenagers, sneaking onto social media could become an almost rite of passage, done with a wink and nod from peers (and as mentioned, possibly even parents). This undermines respect for law at a formative age. A professor in South Korea, reflecting on similar youth media restrictions, warned of creating a "generation of lawbreakers" if regulations focus solely on control without youth buy-in. There's also a fairness issue – not all teens will have equal access to workarounds. More privileged or tech-savvy kids may find ways online, while others obey the rules and potentially miss out on social or educational opportunities. That could exacerbate social inequalities (urban kids circumventing easily vs. rural kids stuck offline, for example). Norway's Prime Minister, in advocating a higher age limit, conceded it's an uphill battle and that strong forces (tech and peer pressure) mean kids will slip through. In short, heavy restrictions could breed a culture of don't get caught rather than genuine safety-minded abstinence.

3. Parent-child trust and deception: The ban might put otherwise honest kids and well-meaning parents in a bind. Take a parent who understands the risks but also sees their 15-year-old becoming socially isolated if all their friends are on banned apps (or worse, if friends are all secretly on them and excluding the rule-followers). That parent might face their teen begging for help to get online. If the parent consents – e.g., lets the teen use the parent's account occasionally or lies for them – they've now participated in undermining a law intended to protect their child. This could strain family dynamics and send a confusing message ("follow the law, except we think this law is dumb, so we'll quietly break it"). A government-commissioned poll actually found about 33% of parents might help their under 16 kids circumvent the ban. That's astounding – it suggests a significant minority of parents are not fully on board with the policy's practicality. If true, the ban may inadvertently pit some parents against the government's guidance, weakening overall authority.

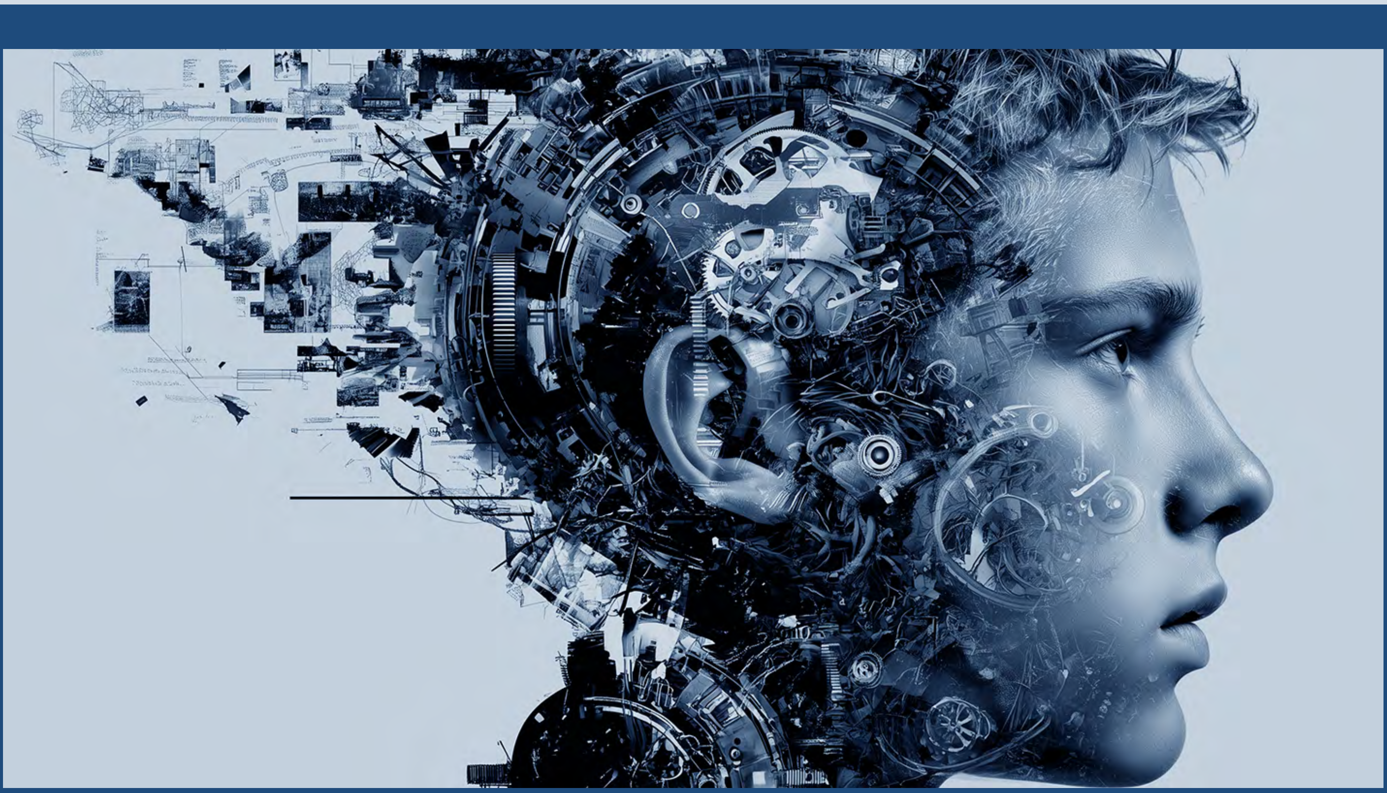
4. Heightened allure of the forbidden fruit: Banning something can sometimes make it more enticing. Teens are naturally curious and often test boundaries. Telling a 15-year-old "you absolutely cannot have Snapchat" might, for some, ignite a stronger desire to see what the fuss is about, compared to a scenario where limited, supervised use might have satisfied the curiosity. Psychologically, forbidden fruit tastes sweeter. The risk is that once these teens do hit 16 (or manage to get on early), they might binge or overindulge because it had been off-limits – a bit like freshmen college students going wild with freedom after strict high-school rules. A Korean analysis of youth media bans predicted a possible "balloon effect" – suppress use temporarily only to see it explode later with emotional instability. If a teen has been shut out of the online social world until 16, they could dive in headfirst without gradual exposure, which might be overwhelming or lead to riskier behaviours online due to lack of prior experience.

5. Blind spots for vulnerable youth: We must consider specific groups. LGBTQ+ teens, for instance, often rely on online communities for support especially if their immediate environment isn't accepting. A blanket ban doesn't discriminate – it cuts off that lifeline at an age many LGBTQ+ youth are grappling with identity. A gender-diverse teen in a conservative rural town might find their only solace in an online group of peers – banning them from it until 16 could increase isolation and mental health struggles. Research found gender-diverse youth tend to be heavier social media users, likely seeking the community and resources not available offline. Similarly, neurodivergent teens (on the autism spectrum, for example) might find online interaction easier than face-to-face, using social media to build social skills in a controlled way. Taking that option away might hamper their social development rather than help it. Kids in remote or rural communities might have very limited local friend pools – social media can be a bridge to the wider world, educational opportunities, even future career inspirations. Removing that could disproportionately disadvantage them compared to kids in big cities who at least have more offline social outlets.

6. Privacy and data risks in enforcement: Another unintended impact falls on society at large. To enforce an age ban, platforms may implement more aggressive age verification – which can mean collecting more personal data from everyone. Facial recognition systems estimating age or requiring government IDs to be uploaded (even if just to a third-party verifier), increase privacy exposure. Recent years have seen plenty of massive data breaches; centralising youth identity data or scans could become a juicy target. The Australian Human Rights Commission cautioned that any system which requires all Australians to prove their identity for social media raises serious privacy risks. So, in trying to shield kids, we might inadvertently force adults (and kids eventually) to surrender more private information to tech firms or the government, trading one set of dangers (online content) for another (loss of privacy).

7. Potential chilling effect on positive uses: Think of all the constructive things a 15-year-old might do on social media: follow news and current events, join a coding forum, post art on DeviantArt, or coordinate a fundraiser. Not all youth social media activity is frivolous or harmful – many teens use these platforms to learn and contribute. A flat ban doesn't distinguish – it tells a budding teenage activist they can't use Twitter to engage with causes, or a young artist they can't share their work online for feedback. One could argue they can wait till 16, but opportunities missed during a formative year might not come back. There's a freedom-of-expression angle here that, while not as attention-grabbing as safety concerns, is important in a free society. The UK debated a similar under 16 social media idea and critics called it an attack on youths' rights to information and expression. The ban might inadvertently silence positive youth voices and participation in civic discourse for a few years.

In light of these potential backfires, some experts have urged a more nuanced approach. The Australian Human Rights Commission, for one, after weighing pros and cons, did not endorse a blanket ban as the best solution. Their reasoning: yes, kids need greater protection online, but a one-size-fits-all ban is a blunt tool that sidelines other human rights and might not even be effective. They advocate looking at alternative options – which brings us to the million-dollar question: if not the ban, then what? We'll tackle that soon, but first, let's see what the rest of the world is doing. Are other countries cracking this code, or running into the same walls?



Toward Better Digital Guardrails That Actually Work

If we take off the table the idea of simply forbidding social media until a magic age, what else can we do to protect and prepare our kids online? The good news is there's a whole toolkit of strategies, many of which experts have been shouting from the rooftops, that don't rely on a blunt ban – strategies that aim to make the online world itself less treacherous and our kids more resilient. Think of it as building better guardrails rather than erecting roadblocks. Here are some key components of a more holistic, and arguably more effective, approach:

1. Regulate the platforms – put the onus on design, not just age: One compelling idea is to place a legal "duty of care" on social media companies for child users. This means shifting responsibility to the platforms to proactively make their services safer for minors by design. For instance, require algorithmic transparency and tweaks: no more secret sauce amplifying harmful content to keep teens hooked. Mandate options for chronological feeds (to reduce algorithmic rabbit holes) and limits on endless scrolling or autoplay for young users. Perhaps require platforms to disable addictive features (like infinite scrolling, like counts, push notifications at all hours) for accounts known or suspected to be under 18. Some of this is in the spirit of what Utah and others attempted – removing "addictive" elements and enforcing night-time pauses – but done at a national or industry-wide scale, it could be more effective. The Australian Human Rights Commission suggests a duty-of-care law could "make [social media companies] take reasonable steps to make their products safe for children", which might drive real innovation in safety features. Imagine if Instagram's explore page algorithm were tuned to demote content with self-harm or eating disorder themes for teens, or if TikTok's For You Page automatically filtered dangerous challenges and extremism for minors. These changes tackle root causes of harm (the content and engagement mechanics) rather than just gatekeeping entry.

2. Invest massively in digital literacy and education: We teach kids to swim because we know we can't keep them away from water forever. Likewise, digital literacy education is vital. This means updated school curricula that start early – age-appropriate lessons on online privacy, spotting misinformation, managing screen time, empathy and respect in online communication, and critical thinking about social media content. By high school, students should grasp concepts like how algorithms work, how posts are curated, and the knowledge that what you see online isn't an accurate mirror of others' lives (to combat FOMO and comparison). Australia's national curriculum could include a dedicated digital citizenship component. Some programs exist (e.g., eSafety Commissioner's resources), but they need amplification and integration across all schools. Also, peer-led initiatives can be powerful: teens may listen to fellow teens more than adults. Funding student ambassador programs or youth-led online safety campaigns could resonate better with the target audience. Essentially, since we can't bubble-wrap the internet, we must teach kids to navigate it wisely – like a high-tech stranger-danger plus media literacy for the 21st century.

3. Engage and equip parents and guardians: Parents are the frontline in this battle, but many feel outmatched by their digitally native offspring. We need to empower parents with both tools and knowledge. On the tools side: encourage use of parental control software (though teens often find ways around, such tools can help set basic boundaries for younger kids). Perhaps telecom providers could offer easy filters at the network level for families. On the knowledge side: run public health style campaigns (akin to "Slip Slop Slap" for sun safety, but for screen safety). The Australian government actually launched a campaign called "For The Good Of" to spur parent-child conversations ahead of the ban – that's a good start, but it shouldn't be one-off. Continuous outreach – workshops, online tutorials, partnerships with parent associations – can help parents understand social media trends, slang, and features so they can talk meaningfully with their kids. And critically, parents should model good behaviour. It's hard to tell your kid to get off TikTok while you're doom-scrolling Twitter at the dinner table. Family device-free times, parents showing they can put the phone away, all set the norm. Ultimately, a culture of open dialogue at home – where kids feel they can report if they encounter something bad online without fear of being punished or cut off – is one of the best protections. Building that trust and communication is an "analog" solution that trumps any filtering tech.

4. Promote youth-friendly, safe alternatives and spaces: If we recognise that completely barring social media is unrealistic, another tactic is to provide healthier social platforms for youth. This could mean supporting development of quality, moderated

social networks aimed at teens – spaces with strong safety protocols, human moderation, and educational content. Think of something like a "Club Penguin 2.0" or modern TeenSpace – a platform that has the appeal of social media (profiles, friends, creative sharing) but with guardrails (verified identity, no anonymous adults lurking, AI content filters that actually work, counsellors or mentors online to intervene in bullying, etc.). Government or NGOs could seed-fund such platforms or incentives for existing platforms to create teen-only modes. Some apps try – e.g., Instagram has a "supervised account" feature now for under 16 (parents can see time spent, new followers, etc.). Rather than ditching under 16s, perhaps insist that major platforms offer a heavily restricted youth mode: no targeted ads, limited content discovery, higher privacy, and real time moderation. This keeps teens in safer walled gardens rather than pushing them to sketchy corners of the internet. It's admittedly challenging to make a "cool" safe space (kids often flee anything that feels too kiddie or monitored), but with youth co-design and smart execution, it's not impossible.

5. Regular digital health checks and guidance: We treat mental and physical health with regular check-ups; why not digital health? Paediatricians and GPs could incorporate questions about social media use into annual health exams – asking teens (with confidentiality) how they feel about their online life, if they've faced bullying, etc. The American Psychological Association in a 2023 advisory recommended that paediatric healthcare providers screen for signs of "social media-related" mental health issues and guide families on healthy use. Schools, too, could have counsellors or psychologists lead sessions on navigating online stress. If a student is struggling (e.g., signs of anxiety or depression possibly linked to online issues), early intervention could include a "digital diet" plan crafted with their input rather than an imposed ban. Just as we have dietary guidelines, some experts suggest creating screen time guidelines by age (with flexibility for individual needs) – and having professionals help families tailor those. Essentially, treat problematic social media use as a health issue that can be managed and treated, not just a discipline issue.

6. Empower youth voices in crafting solutions: Finally, any solution will work better if young people themselves are part of creating it. The ban conversation often painted teens as victims with no agency. But teens can also be allies in making the online world safer. Consultations like UNICEF Australia's youth surveys (which include youth opinions on the ban) are a start – they found many teens themselves doubted the ban would fix things and instead wanted safer platforms and to be heard in the process. The government and industry could establish a youth advisory council on online safety, taking input directly from those affected. Peer mentoring programs where older teens educate younger ones on online etiquette and coping strategies could resonate. When youth feel ownership of the issue, they're more likely to abide by guidelines and help enforce norms (like calling out bullying).

In a way, these steps are about treating the causes, not just the symptoms. They acknowledge a reality: we can't wind back the clock on the internet. Gen Z and Gen Alpha are growing up in an online world, for better and worse. Our task is to civilise that world and strengthen the next generation to thrive in it. Bans might remove some immediate triggers but won't prepare kids for 16 and beyond, when the digital floodgates open. Constructive guardrails, however, can bend the arc of social media toward good – and ensure when our kids inevitably encounter the bad, they have the tools and support to handle it.

As Australia embarks on this bold policy experiment, it's not too late to augment it with these broader measures. In fact, the government has indicated interest in some (e.g., age assurance trials, digital literacy initiatives via eSafety). The public discourse sparked by the ban could be a catalyst to drive these complementary solutions. Otherwise, we risk a scenario where December 2025 comes, the ban "launches", and come January 2026 we're scratching our heads as the same issues persist, just harder to see.

Reclaiming Childhood Without Losing the Digital Plot

Australia's under 16 social media ban is, at its heart, a big, audacious swing at a big, tangled problem. It has sparked applause, outrage, hope, and cynicism in equal measure. We've journeyed through the landscape around it – the genuine harms driving the push, the legal logic, the likely whack-a-mole reality, unintended side effects, and what others around the world are trying. Where do we land? Perhaps with this perspective: Protecting kids online is essential – but it's also exceptionally complex. There is no single switch to flip. A ban in black-and-white law might seem like that switch, but as we've seen, the real world renders it more grey. Kids will always find ways to communicate and congregate; it's in their DNA. The challenge for us adults – parents, policymakers, platform-builders – is to guide them to healthier communications, not simply cut them off and declare victory.

My daughter and her friends on that China trip taught me a humbling lesson: the ingenuity of youth will often outrun the rules we set for them. They weren't being malicious – they just yearned to stay connected. The same will be true as Australia implements its social media ban. We can expect teenagers to test it, cleverly and relentlessly. Rather than viewing that as defiance to be crushed, we should see it as a signal: any sustainable solution must work with kids' needs and behaviour, not in oblivious denial of them.

So, what's the path forward? Even as the ban rolls out, Australia has an opportunity to lead with innovation beyond the ban. We should double down on making the platforms safer (duty of care, better tech design) and making the kids smarter about the platforms (education, open conversations). We must support families in setting boundaries and building trust. And critically, involve young people in creating the digital future they want – one where they can enjoy the benefits of social media (and there are benefits) without being silently traumatized by it.

The goal isn't to shove the genie back in the bottle – it's to teach the genie some manners and our kids some savvy. That's harder than a ban, admittedly. It requires ongoing effort, resources, and cooperation between government, tech companies, schools, and communities. But it's also far more likely to yield a reality where a 13-year-old can navigate online spaces safely, where parents aren't left in the dark, and where we're not endlessly plugging leaks in a dam.

In a way, this is Australia's "slip slop slap" moment for the digital age. Just as we tackled skin cancer risks by changing culture and habits (not by banning the sun), we can tackle online harms by instilling new norms and protective practices. Years from now, we might look back at the under 16 ban as a bold catalyst that forced everyone's hand to act on a broader front.

To all the parents, educators, and yes, even the teenagers reading this: let's not settle for a game of digital whack-a-mole. Let's channel this momentum into building digital guardrails that actually work. Ones that guide our kids, cushion their falls, and let them explore the online world with curiosity and confidence rather than fear. Ones that an average 13-year-old finds sensible enough to follow – or better yet, had a hand in creating.

Childhood in 2025 is undeniably different from what it was in 1985 or 1955. We can't pretend the digital dimension doesn't exist. But we can insist it evolves in a way that keeps our kids whole and healthy. That means being creative, compassionate, and collaborative in our solutions. It means sometimes being a bit irreverent (because humour helps in hard conversations) while staying deeply thoughtful about consequences. Australia has lit a flare with this ban – illuminating the issue for the world. Now it's on us to follow through with the hard yards of innovation in safety and education. If we succeed, we won't need to rely on bans as blunt instruments; we'll have a generation of savvy young digital citizens, and a tech industry held to account for their wellbeing. That's the endgame: a digital playground as safe and enriching as the schoolyard, and kids armed with the wisdom to roam it. So, here's to reclaiming childhood and embracing the future – not an either/or. We owe it to our kids to build a digital world that's worthy of their trust and participation. And we owe it to ourselves, as a society, to get this right without losing the plot. The kids are watching, and ironically, they'll be the first to tell us on social media if we do. Let's make sure, when they turn 16 (or even 13), that what they find online is a brighter, safer place than it is today. That would be a true win "for the good of our kids."

MFA Is Not 100% Safe: Australian Businesses Under Daily Attack

MFA Is Not 100% Safe:
Australian Businesses Under Daily Attack

Multi-factor authentication (MFA) – those extra one-time codes or push alerts you approve on your phone – has become a must-have in cybersecurity. It's often hailed as the silver bullet that stops 99% of account hacks. But here's the uncomfortable truth: MFA is not foolproof. Determined hackers are finding creative ways around it, and nearly every Australian business is now in the crosshairs. One recent report found 96% of Australian organisations were targeted by cyber attacks in the past year, meaning it's safe to assume these MFA-bypass attempts are hitting daily. It's time to ditch any false sense of security – MFA alone won't save you if you don't take additional precautions.

The Daily Siege on Aussie Businesses' Logins

Australian companies large and small are experiencing a relentless barrage of login attacks. The Australian Signals Directorate recorded over 87,000 cybercrime reports in a year – about one incident every 6 minutes. Attackers know most firms now use MFA, so they're adapting their playbooks accordingly. Instead of giving up when they hit an MFA prompt, today's cybercriminals employ a mix of social engineering, technical tricks, and human psychology to slip past that second layer. In other words, they're not hacking the technology so much as hacking the people and processes around it.

Consider this scenario: Your employee's phone buzzes repeatedly at midnight with MFA approval requests. Half asleep and annoyed, they tap "Approve" just to stop the noise. Boom – an intruder just got into your network. Variations of this MFA fatigue attack (also called "push bombing") are rising fast. Security analysts warn that hackers are bombarding users with endless authentication prompts until they hit OK out of sheer exhaustion or confusion. In high-profile breaches like the Uber hack, attackers spammed an employee with push notifications and even posed as IT support on the phone, begging them to approve "just one more" login – which finally succeeded. Even Australian targets have seen this: the FBI and ACSC revealed a recent airline breach where a known hacker group overwhelmed staff with MFA prompts to break in. MFA fatigue turns your best defence into an open door by exploiting the weakest link – human patience.

Attackers sometimes bombard a user's phone with repeated MFA prompts until frustration or error causes them to tap "Approve". This so-called "MFA fatigue" or push-bombing attack leverages human error rather than technical flaws. It was famously used in the Uber breach, where a contractor was spammed with login requests and phony IT support calls until they finally gave in. Aussie organisations aren't immune: hackers linked to the Scattered Spider group have used similar tactics against an Australian airline's systems, overwhelming staff with repeated login notifications.
And push spam is just one trick. Attackers have a full bag of MFA-bypass techniques. Here are some of the most common ways hackers are outsmarting MFA today:

Phishing & Impersonation Scams: Old-fashioned social engineering is still king. Hackers send convincing fake login pages or emails impersonating a trusted service to steal your password and your one-time code. Or they call your help desk pretending to be a panicked executive who lost their phone, coercing support to reset MFA or reveal a backup code. Criminal groups have posed as company IT staff via phone, email, even SMS, to con employees into giving up their credentials or 6-digit codes. In one Australian case, attackers tricked an outsourcing provider's helpdesk into resetting a privileged account's MFA – effectively handing the keys to the bad guys. No malware needed when a polite request to IT will do!

Malicious MFA Relays (Phishing Proxies): This is a more technical phish. The attacker builds a fake website that sits between you and the real login. When you sign in, the bad site relays your details in real-time to the real site – MFA code and all – then captures the session cookie that confirms you've authenticated. With that stolen session token, the hacker is in your account without ever needing to "hack" the MFA again. Security reports note that 75% of Business Email Compromise attacks in Australia now use phishing kits capable of session hijacking, up from just 10% a couple years ago. In practice, that means attackers are copying legitimate Office 365 or Google login pages, snatching not just your username/password but also the invisible token that says "this device is trusted." Once they have that, they ride right past MFA into your email or apps.

SIM Swapping & OTP Theft: If your MFA relies on text-message codes, beware – attackers can hijack your phone number with surprising ease. In a SIM swap, a scammer convinces your mobile carrier (through social engineering or bribery) to port your number to their SIM card. Suddenly, all your SMS codes (and calls) go to them. The FBI and ACSC have warned that attackers use SIM swaps to defeat SMS-based 2FA. Even without a SIM swap, malware on a phone can secretly read your texts, or attackers might intercept OTP messages if they compromise the telecom network. This is why cyber experts have urged for years to ditch SMS codes – they're about as secure as a postcard in the mail.

Device & Token Thefts: Not all MFA bypasses happen via trickery – some are outright theft. Info-stealing malware on an employee's PC can lift the temporary authentication token from their device, essentially hijacking an already-logged-in session. We've seen trojans that quietly grab authentication cookies from browsers or even codes from authenticator apps. If an attacker infects a machine, they might not need to phish your code at all – they'll just copy your login session and waltz in. There have even been cases of criminals paying insiders for valid session tokens or using cloud sync features (like an employee's Google account syncing corporate credentials) to snatch MFA data. In short, if the second factor is accessible on a device, a skilled intruder might steal it without you knowing.

Brute-Forcing the Codes: MFA codes are often 4-6 digits. What if a hacker just tries every combination? Normally, systems rate-limit attempts or expire codes quickly.
But misconfigurations and bugs can open cracks. In late 2024, researchers uncovered an MFA flaw that allowed unlimited rapid guesses of a 6-digit code without alerting the user, letting attackers break in within an hour. Even without such bugs, some attackers will take a shot if they can make thousands of guesses. Short codes, especially if users don't change them or if there's no lockout, can be cracked. It's a reminder that MFA must be set up correctly – with limits and alerts – to actually be effective.
These tactics underscore a sobering reality: MFA stops the low-level "spray and pray" attacks, but not a determined intruder armed with clever tricks. As one expert bluntly put it, moving beyond basic MFA is now a strategic imperative. If you assume the extra login step makes you invincible, you're setting yourself up for trouble.

How to Strengthen Your Shields

None of this means you should give up on MFA – it's still a critical layer of security. But to stay safe, organizations must harden and supplement MFA rather than relying on it blindly. Here are some key precautions and upgrades to consider:

- **Use Phishing-Resistant MFA:** Not all MFA methods are equal. SMS codes and simple push approvals are the weakest. Wherever possible, switch to more secure options like authenticator apps with number matching, FIDO2 security keys, or passkeys. These methods are far harder to phish or replay. (For instance, a hardware security key won't work on a fake site – it only authenticates the real domain.) The Australian government and tech giants are moving toward passwordless FIDO passkeys for good reason – they remove the human-error angle from the equation.

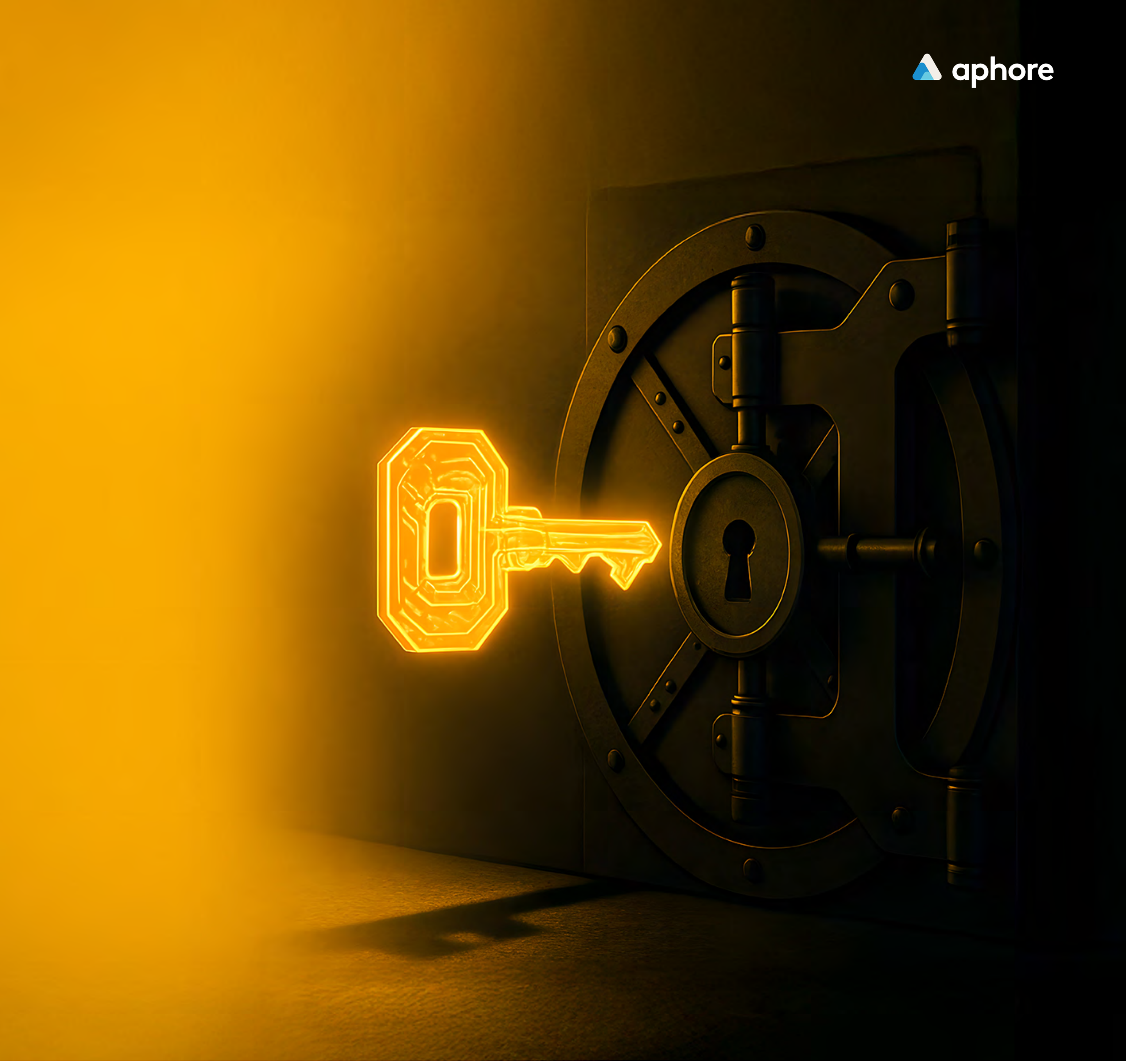
- **Lock Down MFA Reset Processes:** Take a hard look at how your organization handles lost devices or MFA resets. Implement strict verification for any helpdesk requests to reset passwords or MFA. No single staff member should be able to disable someone's MFA based on a phone call alone. Require multiple proofs of identity and manager approval if an admin needs to enrol a new device on someone's account. By putting roadblocks in social engineers' way, you prevent the "pretend to be the CFO with a new phone" scam from succeeding.

- **Enable Additional Protections:** Modern MFA systems often have extra features – use them. For example, Microsoft's MFA can employ number matching (the app shows a number you must type in – stopping simple "Yes" clicks) and contextual info (it tells you who and where is trying to log in). Turn these on so users can spot unusual login attempts more easily. Also configure alerting and rate-limiting on MFA prompts: if someone gets 5 prompts in 5 minutes, that account should be temporarily locked or escalated to IT. These measures can thwart MFA fatigue attacks by making spamming ineffective or obvious.

- **Educate Your Team (Continuously):** Technology is only half the battle – your employees need to be savvy to foil social engineering. Train staff to never approve an MFA prompt they didn't expect, no matter how many times it pops up. Encourage them to pause and report if they get bombarded by codes or see a login from an odd location. Regular security awareness training should include the latest MFA scams – from phishing emails asking for your OTP, to fake "IT support" calls, to suspicious app permission requests. Remember, everyone is a target: the ACSC notes that attackers exploit personal-life touches (like messaging on social media or targeting families) to get a foot in the door. Make sure your people are ready for this.

- **Don't Ditch Password Hygiene:** MFA adds a layer, but the first layer – the password – still matters. Weak or reused passwords make an attacker's job much easier by letting them sail through the first gate. Then it's just one more step to beat MFA. So, continue to enforce strong, unique passwords or passphrases for all accounts. At the very least, this reduces the risk of an attacker ever getting to the MFA stage. Consider password managers and vaults to help users manage complex logins. It's astonishing how many breaches (including some "MFA bypass" incidents) ultimately traced back to someone using "P@ssw0rd" or letting their credentials leak. Don't be that company.

- **Adopt a Zero-Trust Mindset:** Finally, assume that no single security measure is unbreakable. Layer your defences so that if an attacker does slip past MFA, you can catch them quickly or limit the damage. Implement monitoring to detect suspicious access patterns (e.g. a login to a CRM system at 3 AM with an authenticated session token – flag it!). Segment your network and limit the access that any one compromised account can get. In practice, this means things like conditional access policies – e.g., require MFA again for high-value systems or from new devices, even after initial login. It also means keeping backups and incident response plans ready, so a breached account doesn't turn into a full-blown nightmare. The goal is an environment where no single point of failure (like a phished MFA prompt) leads straight to crown jewels.



Final Thoughts

MFA remains a vital part of security – like a solid lock on your front door. But a lock won't stop a thief if you hand them the keys or they find an unlocked window. As cybercriminals bombard Australian businesses with daily MFA-bypass attacks, we must respond by hardening our authentication and educating our people. Think of MFA not as a magic shield, but as one layer in a larger defence strategy. Yes, enable MFA everywhere you can (it still blocks the vast majority of run-of-the-mill attacks). Just don't stop there. By combining smarter technology (like phishing-proof authenticators) with savvy policies and user vigilance, we can keep that extra security layer working as intended – keeping the bad guys out, even as they devise new ways to knock. In cybersecurity, there's truly no silver bullet, but with the right mix of tools and awareness, we can stay one step ahead of the attackers trying to outwit our MFA. Stay safe, stay alert, and never assume "it can't happen to us" – in today's climate, it likely already is. Every login attempt is a battleground, so fortify it accordingly. The era of set-and-forget MFA is over; the era of active, adaptive defence is here. Don't wait for a breach to learn that lesson.

aphore

STATE OF CYBER

2025

FREE WEBINAR

TUE | 3 MARCH 2026 | 12-1PM AEDT

REGISTER TODAY!

Upcoming Webinars

A Strategic Guide for Australian Business Leaders
THRIVING
AMID DISRUPTION
TUE | 3 FEB. 2026 | 12-1PM AEDT
FREE WEBINAR
REGISTER TODAY!

Thought leadership on navigating economic and technological disruption. Introduces “five strategic mindshifts” CEOs can adopt to turn uncertainty into opportunity. Discusses embracing bold decision-making, AI-driven innovation, data-driven agility, ROI-focused strategy, and leveraging external talent.

C-level attendees gain strategies to drive growth amid chaos – learning to lead with courage, foster resilience, and transform disruption into business opportunity.

Executive-level insights on preventing and managing employee burnout and promoting wellbeing. Highlights research that nearly 50% of workers report burnout symptoms and explores leadership practices to boost inclusion, resilience, and work-life balance (drawing on principles from recent studies).

Business leaders learn practical steps to recognise and mitigate burnout in their teams – fostering a healthier workplace culture, improving staff retention, and maintaining productivity through supportive leadership.

Evening session, offering another timeslot for new participants.

Aspiring professionals who missed earlier can learn about the 2026 cyber training and internship opportunities.

Why Executive Engagement and Robust Planning Matter in Cyber Crises
INCIDENT
RESPONSE
PREPAREDNESS
TUE | 07 APR 2026 | 12-2PM AEDT
FREE WEBINAR
REGISTER TODAY!

An extended 2-hour workshop on developing robust cyber incident response capabilities. Emphasises the importance of comprehensive planning and executive involvement in cyber crises. The session walks through building an up-to-date incident response plan, clarifying roles (including board oversight during incidents), communication strategies, and running breach simulation exercises. Executives and directors learn how to assess their organisation’s incident readiness and identify gaps. They leave with a high-level incident response checklist and an understanding of best practices to improve their cyber crisis preparedness.

STRENGTHENING RISK MANAGEMENT
AND DATA PROTECTION THROUGH ISO 27001
ISO 27001
AND
BUSINESS
VALUE
TUE | 05 MAY. 2026 | 12-1PM AEDT
FREE WEBINAR
REGISTER TODAY!
ISO
27001

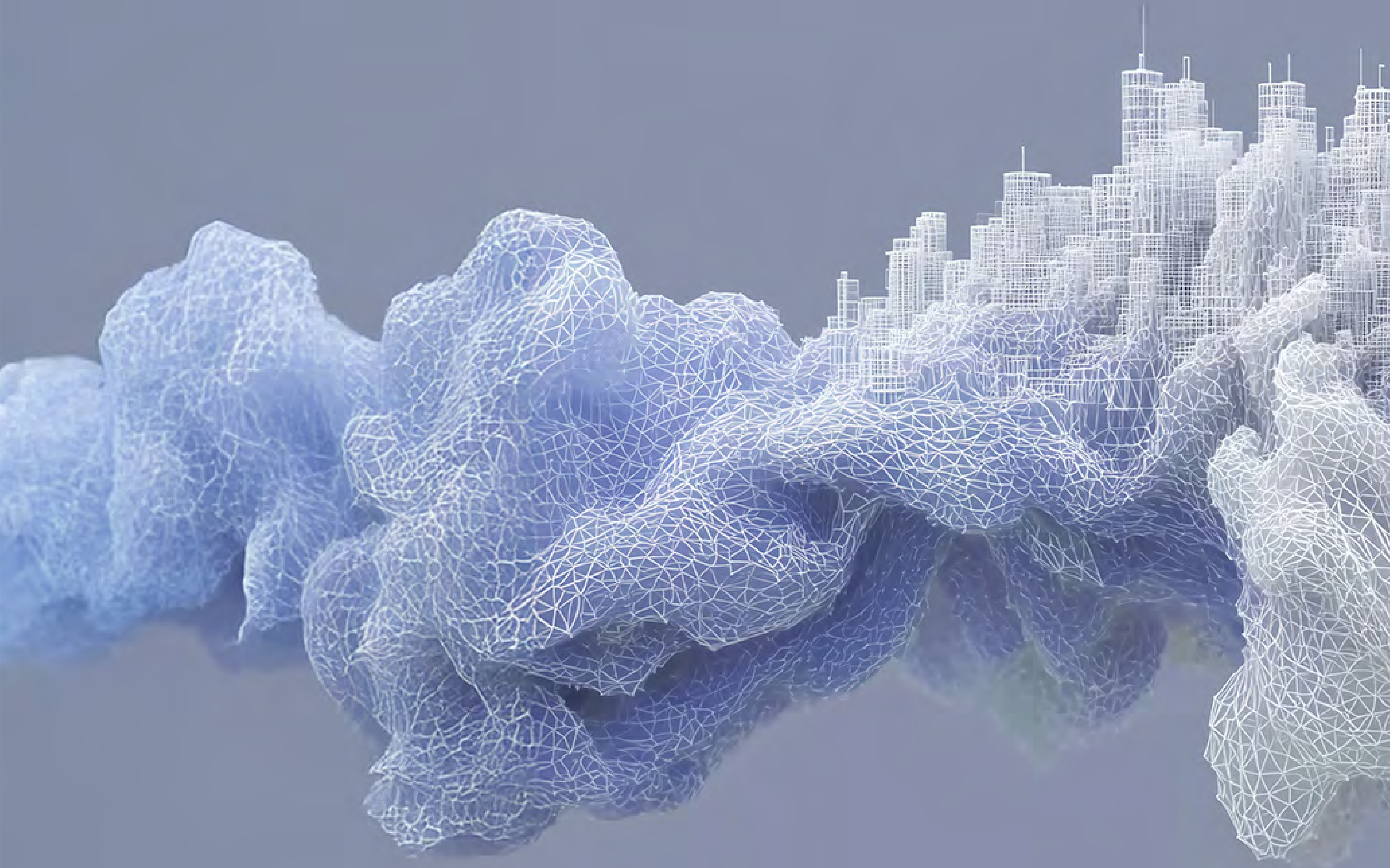
A practical look at the ISO 27001 information security certification and how it adds business value for SMEs. Explains the key elements of ISO 27001 and its benefits: from strengthening risk management and data protection to boosting customer trust and competitive advantage in the market . Discusses real examples of Australian businesses that gained efficiency and won client contracts after certification.

Leaders understand whether pursuing ISO 27001 is right for their organisation. They learn how certification can not only improve security posture but also serve as a market differentiator (by signalling reliability and readiness to partners and customers). Attendees are equipped with insight into the certification process and ROI considerations for 2026 planning.

How Modern Managed Service Provider (MSP) can accelerate business transformation.
MODERN
MANAGED
SERVICES
FREE WEBINAR
TUESDAY | 21 APRIL 2026 | 12:00 - 1:00 PM AEDT
REGISTER TODAY!

How modern Managed Services can accelerate business transformation and what to consider when choosing a Managed Service Provider (MSP). Shares research that today’s companies seek more than cost savings – they expect managed services to drive strategic outcomes like innovation, resilience and growth. Outlines the power of modern MSPs in areas like cybersecurity and cloud, and provides a checklist for selecting the right provider (e.g. look for advanced technology and multi-disciplinary expertise in providers).

Attendees learn the potential business benefits of partnering with a modern MSP (speed to market, access to new tech, scalability) and receive guidance on the vendor selection process. SME executives will be better prepared to evaluate MSPs in 2026, having key criteria to ensure their chosen partner can deliver innovation and value beyond just cost reduction.



aphore

T: 1300 041 042 (Aust) T: 1833 882 7467 (USA) | Level 2, 1 Southbank Boulevard, Melbourne, Victoria 3006

aphore.com