+44 345 094 0945
www.waterstons.com

Article

Jul 2025

Cyber security chaos or cautionary tale? Why Australian businesses must rethink their cyber strategy

In recent months, cybersecurity attacks have surged globally, but Australia has been hit particularly hard. From major corporations to essential services, no sector has been spared. As someone who's spent years in the trenches of cybersecurity, I want to offer a grounded perspective, not panic, not hype, but a reality check.

Let's be clear: I don't believe most affected organisations were careless. I don't think decision-makers knowingly underinvested in cybersecurity risk management. In most cases, they simply didn't realise how exposed they were. Like all of us, you often don't know what's missing until it breaks.

Even when businesses are following "best practices," those efforts often go unnoticed until something goes very, very wrong.

What's going wrong? Here's my take:

1. The dangerous comfort of "we're fine"

Overconfidence is one of the most persistent and silent threats in cyber risk management.

I've worked with hundreds of organisations, some with advanced infrastructure, others just starting their digital journey. And ironically, it's often the ones who believe they're "secure" that are most vulnerable. Why? Because they stop looking.

Meanwhile, those who know they're underprepared tend to be the most cyber resilient. They're testing, learning, and adapting. They document vulnerabilities. They close gaps proactively. They're not waiting to be perfect; they're aiming to be prepared.

In contrast, companies relying on a "silver bullet" cybersecurity solution or a "brilliant IT guy" are often sitting ducks.

Here's the truth: even billion-dollar defence departments can't fully prevent attacks. Absolute security doesn't exist. But awareness, agility, and consistent action? That's what builds true cyber resilience.

2. Misguided investment: flashy tools vs. fundamental controls

Let's stop confusing cybersecurity spend with security maturity.

Too many businesses fall for expensive, over-engineered solutions that look impressive on paper but miss the mark in practice. These "Golden Dome" platforms promise total protection, but breaches are rarely stopped by magic.

They're stopped by unsexy basics done well.

Take the UK's Cyber Essentials Scheme. Five basic controls. Less than $4,000. It blocks up to 80% of common cyber threats. Not glamorous, but it works.

Security operations centres (SOCs), threat intelligence platforms, MDR/XDR, these are powerful. But they only work when layered on top of robust fundamentals: security hygiene, embedded processes, and a security-first culture.

Cybersecurity is not just a technology problem. It's a people and process problem, too.

3. Weak regulation = weak response

Without clear rules, many businesses simply won't act. It's not laziness, it's human nature. Think about the history of workplace safety, minimum wages, or seat belts. Change came because regulation forced the issue.

Europe's GDPR fines of up to 20% of turnover raised the bar. The UK followed. But Australia? We're still catching up.

Efforts like the SOCI Act, privacy reforms, and Cyber Security Strategy 2030 These are steps in the right direction. And organisations like the Australian Signals Directorate (ASD) You are doing excellent work with frameworks like the Essential Eight.

But awareness is still low. And enforcement? Often toothless.

To create real change, Australia needs mandatory cybersecurity frameworks, regular cyber audits, and meaningful consequences for negligence. It's not about punishment, it's about accountability and setting clear expectations.

4. Supply chain: the hidden vulnerability

Your organisation's weakest security link might not even belong to you.

Today, every business depends on SaaS tools, cloud services, and third-party providers. But how often do you assess their security posture?

- Who holds your data
- Where is it stored?
- What's the breach response plan?

Remember the aquarium thermometer hack in a Las Vegas casino? That $100 IoT device bypassed enterprise-grade defences.

Supply chain attacks aren't fiction; they're one of the biggest real-world cybersecurity threats today. Just ask Maersk (who lost $800M in 10 days) or Qantas, still reeling from the reputational and financial fallout of recent breaches.

Start doing real cybersecurity due diligence with suppliers. Make it a business norm, not an exception.

5. Employee training: from tick-box to transformation

Your people are your first line of defence, or your easiest way in.

Unfortunately, cybersecurity awareness training often becomes a once-a-year box to tick. People skim a compliance video, guess their way through a quiz, and forget it instantly.

What works better?

- Frequent micro-learning
- Interactive simulations
- Phishing drills
- Real-life context (protecting families, not just company files)
- Gamification

We once ran a security resilience workshop as a competitive board game. Teams ran their business under cyber stress, learned through failure, and made real-time decisions. It changed their mindset. Because when learning is fun and meaningful, it sticks.

6. Choose honest cybersecurity partners

Let's be honest: the cybersecurity consulting industry is full of flattery.

Too many providers focus on upselling instead of challenging. They show only green dashboards, praise IT teams, and avoid hard truths. That's not partnership, that's performance.

At Waterstons, we chose a different path. For example, we mandate vulnerability management in every managed services contract. It's non-negotiable. With over 280,000 new vulnerabilities published every year, you can't afford to ignore them. Some clients walked away. But those who stayed? They saw 10x more value.

Honesty beats comfort. Choose providers who challenge you, not just cheer you on.

Final thoughts: from reaction to resilience

Here are five actions the Australian cybersecurity ecosystem needs right now:

1. Be humble

Admit what you don't know. Awareness is the foundation of security.

2. Take action now

Businesses: Implement the ASD Essential Eight or Cyber Essentials.

Regulators: Offer both incentives and enforcement.

3. Secure your supply chain

If your third parties aren't secure, you aren't either.

4. Rethink training

Make it relevant. Make it regular. Make it stick.

5. Work with honest experts

Seek partners who give you hard truths, not just nice reports.

Get ahead of the game.

Want to stress-test your cybersecurity strategy or just start with the basics? Whether you're looking to build resilience, audit your supply chain, or make training stick, reach out to our experts at **cyberaus@waterstons.com**. No fluff, just honest advice.