The first quarter review
March 2025

There's an ”old Chinese proverb (curse?)" that says "may you live in interesting times". Well, wikipedia says it's a misattribution, but we definitely are living in interesting times. Trump… Musk… DOGE… Tariffs… Gaza the 'Monaco of the Middle East'… Canada, Greenland?? Can it get any more bizarre? The answer is almost certainly YES. We have no idea what, but just when you think it can't get crazier with US politics, it does.

This article and this one, also explains how the American Cyberdefense program will have some significant challenges during the Trump Presidency. And just when you thought it's better to be in Australia, similar tones were heard when Treasurer Jim Chalmers delivered his federal budget. In short, "the 2025 budget is remarkably light on investing any further in protecting the nation from a growing raft of cyber threats**"** or said more bluntly "For anyone with an interest in the digital economy or its associated data infrastructure, Jim Chalmers' federal Budget will be remembered as a flatliner, dead on arrival.

Brian Krebs summarised the state of the American Cybersecurity and Infrastructure Security Agency (CISA) in relation to the new American Political Administration here. The article notes that the Secretary of Homeland Security's nominee believes the CISA has 'gotten far off its mission' and should be focused more on 'hardening federal IT systems'.

That topic resonated locally when the Commonwealth Cyber Security Posture for 2024 was released this quarter. Three years ago, our country announced the 'most significant single investment in the Australian Signals Directorate's history' (RedSpice), but even with that, somehow the proportion of Commonwealth entities that reached an overall 'Maturity Level 2' (and not overly impressive goal, mind you) across the Essential Eight mitigation strategies actually **DECLINED** from 25 percent to just 15 per cent in 2024.

Really? It feels a bit sanctimonious then when we then read that the Australian Securities and Investments Commission (ASIC) started a lawsuit against FIIG Securities for 'systemic and prolonged cybersecurity failures over a four-year period that led to the 2023 data breach'. We're (rightfully) suing our companies for lax cyber, yet only 15% of Commonwealth entities are barely scraping by with cyber fundamentals?

IoT security – Voluntary?

As noted here, for the professional security industry, the conversation surrounding the security and reliability of connected devices is nothing new. Our industry has long been aware of the risks – unsecured devices acting as potential network entry points, vulnerabilities in communication protocols, even some manufacturers prioritising convenience over security. Therefore, the announcement of the US Federal Communications Commission's "U.S. Cyber Trust Mark" was a breath of fresh air.

However that quickly dissipated when we read that "Voluntary is [the] key word here"… a great step to improve one key area of risk, but a 'voluntary program' will likely be met with tepid acceptance. If your organisation makes connected devices or any sort, it's worth having a look.

WHEN, not if!

New data from a global survey says that Australian companies are beginning to understand that facing a cyber attack is not a matter of if you get attacked, but rather when. 75 per cent of Aussie businesses expecting to face a cyber breach in 2025. Admission is the first step, but remember that expecting is one thing, while preparing is another. One of our clients quoted:

"Under pressure, you don't rise to the occasion – you sink to the level of your training".

Resilience requires planning and practice. What level of training will your team 'sink to'? If you think you should be better prepared, consider our unique approach for cyber incident response simulations.

$190,000 for not calling to confirm details?

Does your organisation physically call and confirm details when someone (supplier, customer, OR employee) establishes or changes bank account details? If you don't, you should because almost $84 million was lost by businesses through BEC scams.

And even if you do, you should also make sure you don't just go through the paces, as Inoteq learned this quarter. While a judge said they had been 'prudent' in trying to call a supplier, they didn't actually confirm the change because there was a 'poor phone line'… because they made no further telephone call, a judge ruled that they failed to protect itself and ordered Inoteq to pay $190k. That's 190,000 good reasons to make a second call!

Better developing, but worse fixing.

Veracode released the 'State of Software Security 2025" this quarter and it supports what we have found for the last 19 years – in short, our developers are better at writing software. Now over half (52% - up from 32%) of programs pass the 'OWASP Top 10'. That's great news!

But sometimes we forget the priority is not just finding the issue but fixing them. The report says that the average days to fix these issues increased from 171 days to a whopping 252 days! That's more than 8 months to resolve a known issue.

With examples like ASIC's lawsuit against FIIG, it's hard to believe that a legal defence would be very strong if you found an issue, but then took over 8 months to fix it! Also, check your third party software libraries! 70% of "critical security debt" comes from third party code. If you think you might need some help, testing is a full time endeavour for us – just drop us a note here.

Shadow IT 'on steroids'?

We used to talk a lot about 'shadow IT' as a HUGE organisational cyber risk. Well, as Bachman Turner Overdrive would say "You ain't seen nothing yet" – at least when it comes to Artificial Intelligence. We were reminded of that when we read that 65% of office works bypass cybersecurity to boost productivity.

Do you have a policy on how to utilise AI in your workplace? That's the first (easy) step, but it's really about education, awareness, and effective governance. If you haven't started thinking about the risk of your staff using AI, it's probably time to start. We've been helping a few organisations with it – just drop us a note if you think it might be worth exploring how we could help you with this risk?

We appreciate you being connected with us and taking the time to read this quarter's update. If you're not already, please 'follow us' on LinkedIn and/or X (Twitter), and feel free to send this to others (or have them subscribe here).

Kind regards,

TrustedImpact
PROTECTING DIGITAL

we're **independent** consultants – it's about **your** business and **your** success
with a **singular focus** – cyber security is all we do
leveraging **experienced** professionals – credentials, not checklists