The intro of an email from Wired Magazine summarised the situation in the world for this last quarter.

"*War is here. It's in Minnesota, with masked immigration enforcement agents pulling people out of cars in broad daylight. It's at sea, with solitary boats being bombed in the Caribbean. It's certainly in Sudan and Ukraine. And now it's in Iran and yet again across the Middle East. War is everywhere you look, with an acute onus on the American political apparatus: President Trump has dropped bombs on at least seven countries since he took office last year and has supercharged the defense tech industry in 18 short months*."

Strategic Shift?

We also noted a similar, more aggressive 'shift in philosophy' with the newly released 'Cyber Strategy for America', which makes a notable shift from a primarily 'defensive' posture (i.e., strengthen defences, share threat intel, and improve resilience after attacks occur), to emphasising an offensive posture (i.e., deterrence, disruption and a 'projection of capabilities').

There's a good summary here, which also aptly noted that "Historically, U.S. cybersecurity policy has largely followed the adage, "speak softly and carry a big stick"". Well, there's nothing 'softly spoken' in the 5-page strategy just released. The promise to "unleash the private sector by creating incentives to identify and disrupt adversary networks and scale our national capabilities" is both interesting and frightening at the same time! That shift is even bigger, given that the lead cyber Agency (CISA), "lost roughly one-third of its staff since Trump came into office, a period during which it has so far had three acting leaders."

So, what does that mean for us? The spill over from 'kinetic war' to cyber is inevitable – whether it's war motivated or just used as a distraction to try to defraud you. Also as things become more 'adversarial' expect the damage or impact of cyber incidents to become both larger and more detrimental. In short, keep your guard up, maintain focus and remain vigilant! Also, be PREPARED. If the 'inevitable' cyber incident does happen, make sure you've practiced your ability to respond and recover. Is it time your organisation ran a cyber incident simulation to improve your resilience?.

If you're in or part of Critical Infrastructure…

Last week the Minister for Home Affairs released a 'consultation' on two reforms to the Security of Critical Infrastructure Act 2018. There are lots of useful resources here too. Most changes are sound steps to improve the resilience of our Critical Infrastructure. They aim to strengthen the government's ability to manage national security risks, as well as introduce more prescriptive obligations for designated high-risk critical infrastructure asset classes across cyber, supply chain, personnel and physical security.

If you're in the Critical Infrastructure industry, it's worth considering how the proposed reforms would impact your organisation (or we can assist, if you need some help?). Submissions are due 1 May 2026.

Third parties as an 'Attack Surface'

We thought you might enjoy this piece from the 'Fair Institute' that proposes that our perspective on third parties is wrong and suggests it should be more of a question of 'ownership'.

For example, "When a supplier suffers a breach that exposes your customer data, whose data was leaked? **Yours**. When a software vendor ships a vulnerable component embedded deep in your stack, whose systems are compromised? **Yours**. When a payroll processor misconfigures a database and employee records are exposed, whose employees are affected? **Yours**.

The harm in every one of these scenarios' lands on the first party, the organisation, its customers, its regulators, and its shareholders. The third party is the mechanism, not the owner of the outcome. Calling it "third party risk" is a bit like calling a house fire a "match problem." The match may have started it, but the house is still yours."

Are cloud misconfigurations your biggest security threat?

When we reflect on our 20 years assisting more than 400 organisations, the following sentence rang loud and clear…. "It wasn't sophisticated cybercriminals… Instead, basic errors opened the door." It's a well written review of a Cloud Security Alliance report, that found misconfigured settings caused nearly every single breach investigated.

We've performed thousands of 'Penetration Tests" for a very diverse range of technologies and clients – overall, we have seen a marked decrease (improvement) in programming-based vulnerabilities. However, that improvement is often offset by incorrectly or poorly configured cloud environments.

Need more proof? What about WA Office of the Auditor General, which found a "litany of security shortcomings in how seven state entities manage their M365 environments" which were the reasons behind leaked personal information on minors and the theft of $71k in BEC / invoice fraud!

Given the essential role of the 'cloud' in today's business environment; reviewing and confirming your cloud configuration settings, is one of those BASICS. If nothing else, have your team review the benchmarks at the Centre for Internet Security. Yet, if you want either an independent perspective (don't let the fox check the hen house!), or want to leverage someone who has LOTS of experience reviewing (and prioritising) cloud configuration improvements, just drop us a note here.

Regulatory scrutiny increasing…

A review of this quarters' key cyber announcements shows that if your organisation faces Regulatory scrutiny, you will want to reevaluate your risk of increased scrutiny from Regulators of all types. For example, January's Victorian Education Department data breach triggered a formal investigation by OVIC. We also previously mentioned the Audit report from WA. And in February, the Federal Court (from an ASIC-originated lawsuit) ordered FIIG Securities to pay a $3 million penalty for cyber security failures in breach of their Australian Financial Services License AFSL obligations.

What can you do to reduce your risk of regulatory scrutiny? Considering having an INDEPENDENT Firm (like us - it's what we're all about), help you with a comprehensive 'maturity assessment' of your cyber capabilities, and have a defensible roadmap of improvement that can be measured over time to demonstrate your progress. It's prudent in today's 'tightly interconnected and AI accelerated' world!

Have you considered quantum yet?

An interesting Bain study found *"Some 90% of responding organisations say they are **not prepared** to defend against quantum computing related threats. That's **despite nearly three-quarters (71%) expecting quantum powered attacks** within five years and almost a third claiming it could be as soon as three"*. Just send us a note if you'd like to get ahead of that curve?

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