It's nice to finally be in Spring. It was an impressive Summer Olympic outcome for Australia this quarter with a ranking of #4 in gold medals, and #5 in total medals. That against a total of 206 "National Olympic Committees" makes it even more impressive given our small size! The Olympics is a great example of what 'mankind' can achieve when cooperating.

Unfortunately the opposite is also true, and we saw far too many examples of turmoil and continued violence – whether it was assassination attempts on US presidential candidates, the continued conflict in the Ukraine, or exploding pagers and walkie talkies which killed 32 and injured over 3,000.

"The wakeup call that is not waking up anybody"

That quote nailed one of the most important issues this quarter. While technically considered by many to not be a cyber 'incident' it clearly falls in the cyber domain if we think about protecting Confidentiality, Integrity and AVAILABILITY. Who will forget when CrowdStrike 'bricked' 8.5 million Windows devices globally, grounded 1,500 flights, disrupted banking transactions and caused various media services to go offline, we (again) learned just how important DIGITAL is to our world. It's ironic that the technology that is meant to protect us from cyber threats was the source of the problem!

The business impact was massive. The US airline Delta says it lost $380 million in revenue, and incurred an additional $170 in expenses (total growing at $550 million) due to the disruption. Just in the 'Fortune 500' companies alone, losses are estimated at a staggering $5.4 billion! In Australia, it's estimated to cost local businesses over $1 billion. While many felt that CrowdStrike would face "a tsunami of lawsuits", outside of one shareholder class action suit, we find it perplexing that (at least so far) CrowdStrike says there have been NO lawsuits registered as of September.

So what can we learn? It reminds us that we need to refresh our thinking about Business Continuity, Disaster Recovery and Cyber Risk. Some of the key lessons were summarised well by Mike Gillespie

> Over-reliance on major providers like Microsoft or Amazon can lead to several challenges for organisations, including vendor lock-in, reduced negotiating power, and increased security risks. It can also stifle innovation and limit customisation options due to the standardised nature of these platforms. Dependence on a single provider heightens vulnerability to service outages and can result in cost increases over time. Additionally, organisations may face difficulties ensuring data privacy and compliance across different jurisdictions. To mitigate these risks, it is advisable for organisations to diversify their technology stack and adopt a multi-vendor strategy to enhance flexibility and resilience.

The business use of technology has structurally shifted an in the last 10 years and we need to shift and update our thinking on technology risk as well. We've gone from 'on prem' to 'the cloud', and frequently use other 'Software-As-A-Service' providers for fundamental business processes. The news is littered with examples where we haven't considered the loss of these technologies – remember the 90,000 public servants in South Australia who could not get paid thanks to Frontier Software's ransomware problem? How about UniSuper's near miss catastrophic event last quarter that happened when the 'isolated, one of a kind occurrence' happened with Goggle Cloud? If you do use the cloud, we put together some additional suggestions (here) when we interpreted input from some of the key leaders using cloud technologies.

Is ASIC about to show their teeth?

Speaking of cyber-related lawsuits, it was interesting to read this quarter that most of the SolarWinds court case was dismissed because the Security Exchange Commission's (SEC) charges "impermissibly rely on hindsight and speculation."

Of particular note was that the company AND their Chief Information Security Officer (personally), is still charged with fraud for their role in allegedly lying to investors by "overstating SolarWinds' cybersecurity practices and understating or failing to disclose known risks".

This lines up closely with local conversations when Australian Securities and Investments Commission's (ASIC) Simone Constant spoke at a recent conference about investigations underway into directors and executives at (Australian) organisations deemed to have neglected their duties to guard against hackers… "*We don't want to see the rise of cyber washing… If you are on a board you need the curiosity and gumption to make executives prove that they aren't doing a poor job on cybersecurity, she said. "Don't allow yourself to be told but insist on being shown.""*

The message? The broad brush 'everything is fine' doesn't cut it any longer. Be careful what you say to your shareholders and the public, and when you do, be willing to back it up. In fact, that's what we're all about, so if you need some 'proof' or independent validation, please don't hesitate to reach out.

AI and CoPilot - have you read the small print?

A good friend of the firm (thank you Ben!), was curious about the 'terms' of Microsoft's CoPilot. Most of us glance (at best) over terms like these and often don't get into the detail. In short; while Microsoft does not claim ownership of your Artificial Intelligence (AI) 'prompts', they certainly act as though it's theirs, their third party partners, and that you have no ownership rights over them. Read section 5.

But what can go wrong you say? A local story highlighted just one concern when a Safety Trainer used CoPilot's chatbot to generate FICTIONAL examples of sexual harassment that employees might face, when they were delivering a course at Bundbury Regional Prison. Everything seemed fine until someone in the room said "That's not fictional, that's real". Apparently, CoPilot gave the full details of real people at that prison who are currently involved in an active Federal Court case!.

Have you taken a moment to consider the types of AI risk that your organisation faces? As a simple first step, do you even have a company policy on the use of AI? How about defined governance structures? Packaged or integrated AI tools come with risks, including biases or 'hallucinations' in the AI models, data privacy issues, and the potential for misuse. A considered AI governance framework will help mitigate these risks by establishing guidelines and controls that align with the ethical standards and values of your organisation. You need to consider one. Drop us a note if you'd like to discuss some ideas on how to establish a simple foundation NOW rather than when someone says "That's not fictional, that's real"!

The Stats Say "VALID ACCOUNTS"

The American Cybersecurity & Infrastructure Security Agency (CISA) released their Analysis of "FY23 Risk and Vulnerability Assessments this month – 143 Assessments across multiple critical infrastructure sectors. VALID ACCOUNTS was the most prominent technique used…really? Still? We've been trying to say that for the last 18 years! If you need hard stats to do what's important, you can find their analysis here, or the 'infographic' here.

———

Thank you for investing the time to catch up with us this quarter! 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