This quarter the chaos around global tariffs being imposed by the United States has taken a back seat to the recent bombing of Iran and threat of war. Let's hope it doesn't escalate any further! We wish more people would try to 'build' bridges… not 'blow them up'! Is it any wonder then that the Lowy Institute found that only 36 per cent of Australians trust the US to 'act responsibly', and that 2/3rds of us are 'pessimistic about the next several years with Donald Trump as US president'?!?!

AI stands for what?

Someone suggested AI might not actually stand for Artificial Intelligence, but perhaps '**Access Invitation**' (because it opens backdoors even when you didn't ask it to), or perhaps '**Autonomously Insecure**' (making your security team's job harder since deployment)? While cleverly funny, the first (Access Inviter) might actually have some basis for truth when we learned about 'EchoLeak' a few weeks ago, which is the first zero-click vulnerability enabling data exfiltration from Microsoft 365 Copilot.

Don't get us wrong – AI holds immense promise and potential! We might question if AI is 'more profound than fire', but being 'forewarned is forearmed', and it's good to go in with your eyes wide open. Therefore, the Governance Institute's paper on the'10 Guardrails for AI Safety' might be a good read. Why? It found that 88% of organisations have struggled to integrate Generative AI into legacy systems.

However, as with many things in large organisations, it's often about awareness and 'governance' as the old 'Shadow IT' takes a back seat to everyone of your company's employees trying every variation of AI to determine if it can help them do their jobs faster, better or quicker (and without understanding, evaluating or mitigating the risks). That was reinforced last quarter when we wrote that 65% of office workers bypass cybersecurity to boost productivity.

Don't fret though. There are some good models on what a sound Governance Framework and overall process looks like. So, if you think you're ready to consider what that means for you, reach out [here] – it might be better to get it defined now, then learn that one of your employees pasted proprietary code into ChatGPT in search for a bug fix!

While on the theme of being forewarned, we also found an impressive effort to catalogue all AI-based incidents in an "AI Incident Database". This database is "*dedicated to indexing the collective history of harms or near harms realized in the real world by the deployment of artificial intelligence systems. Like similar databases in aviation and computer security, the AI Incident Database aims to learn from experience so we can prevent or mitigate bad outcomes*". We applaud their objectives!!

It's high time to protect your customers from themselves

Marketing executives love espousing 'frictionless e-commerce' and exploring ways to make one's digital experience 'easy'. Heaven knows we can often make e-commerce easier, but NOT when it comes to employing fundamental protections like "Multi-Factor Authentication" or by helping them by using features like password complexity checking, geolocation techniques, or providing simple videos of the do's and don'ts when setting up an account.

Not your problem? In early April, we saw the major attack on Australian superannuation funds using exploited password credentials to gain access to their members' accounts. You could have the most secure system in the world, but if your customers access their accounts with poor / insufficient passwords (or reuse theirs like 78% who do), it might become your problem too.

How's that? AustralianSuper has vowed to refund members who had $500,000 stolen from their accounts for that reason. If you're working in a bank, you might take notice of that too – it sets a precedent which may not bode well for the current legal posture of many financial institutions when hackers exploit customer accounts.

It's no wonder that after that news, the Australian Prudential Regulatory Authority (APRA), sent a letter to all Licensee Board Chairs to "shape up, or else" when it comes to using robust authentication controls.

That's a positive step for our financial ecosystem, but what about the other MILLIONS (Tens? Hundreds? Or More?) of Software-As-A-Service (SaaS) businesses, or e-Commerce system owners who think such measures cause 'friction' and is 'frivolous functionality that might cause customers to go elsewhere'?

Well, seeing is believing! We recently helped an organisation 'decode' their passwords from the system that manages their staff's access to ALL their systems. Security professionals talk about password / phrase complexity 'until they're blue in the face'. BUT when you actually see a list of nearly 500 employees and scan your eyes across what is ACTUALLY being used to gain external access to your internal systems, we guarantee you that your toes will curl (at best!). For example, nearly fifty "Welcome1" passwords…. NO use of 'passphrases', and the 'oh so clever' use of Leetspeak by using "P@ssw0rd1" (for nearly two dozen accounts in this example, and which every hacker will try).

We could go on and on, but if you want REAL proof that your organisation should spend a bit of time improving passwords, just drop us a note [here]. We might be able to provide you with impactful insight that can significantly improve your exposure to this significant risk! If you haven't "looked under that rock" recently (or ever), it's high time to take a look before something nasty crawls out and bites you.

Reports, Reports and more Reports

This quarter it felt like we were getting barraged with updates to some of the key 'reports' that come from highly-regarded sources. For example;

Google's M-Trends 2025 found we still lack the ability to 'DETECT' if something has gone wrong inside our organisations, since over half (57%), first learned of a 2024 compromise from an external source.

The FBI's Internet Crime Complaint Center (IC3) shows that cyber crime is rising with nearly 860,000 complains last year and a 'staggering' US$16.6 BILLION in losses to businesses and individuals – the highest in 25 years, and since IC3's establishment in the year 2000.

Verizon's 2025 Data Breach Investigations Report (DBIR) analysed over 12,000 confirmed breaches and found a disproportionate impact on small and medium businesses, where ransomware appears in 88% of all breaches in that category (remember 3,2,1?). Also, don't forget about your third parties and external vendors who were a cause for 30% of all breaches (doubling from 15% the prior year!).

And finally, Economist Impact (sponsored by FTI) found that about 70% of organisations don't have an identified cross-functional crisis response team for when a crisis strikes (cyber or otherwise). Remember our favourite quote? "**Under pressure, you don't rise to the occasion – you sink to the level of your training.**" Resilience requires planning and practice. So... what level of training will your team 'sink to'? Consider our IMPROVED approach for conducting cyber incident response simulations.

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