While we were delighted to hear of a formal, but fragile ceasefire in Gaza this quarter, it was significantly offset by the tragic event at Bondi on the 14th of this month. Our sympathies go to all of those who lost friends or family and who were negatively impacted by this horrific event. Let's hope that 2026 will be a year of less conflict!

Resilience is an operating discipline.

When we asked the 'AI' what was a key learning from the last quarter's cyber headlines, it gave us:

Q4 2025 underscored that resilience is an operating discipline.

A pretty good line that was reference from the ASD's 2024-25 Annual Cyber Threat Report that was released in November. This year, the Australian Cyber Security Centre (ACSC) responded to nearly 85,000 cybercrime reports, or one every SIX minutes. While that the number of incidents is still very big, it is pleasing to see that there was a decrease of 7% when compared to the previous year. There's always a wealth of information in that report, so it's worth a read if you haven't done so already.

The wealth of statistics in that report all support the statement that cyber resilience is essential. Don't forget that resilience requires not just planning, but practice too. One of our favourite sayings has always been that "Under pressure, you don't rise to the occasion, but sink to the highest level of your training"! What level of training would your organisation 'sink to'? If you think you could be better prepared, consider our unique approach for cyber incident response simulations, and just drop us a note here

Only 40 per cent of organisations integrate cyber security during the planning stage of digital initiatives.

Wow! Why does the old adage of 'stitch in time saves nine' come to mind when reading that headline!?! While we always thought that the number would be low, we didn't realise it was SO LOW, until we read about a survey released by IDC this quarter. The lead paragraph says it all:

The disconnect between digital transformation (DX) ambitions and cybersecurity execution is widening. While organizations invest in AI/ML, cloud, and analytics to drive growth, only 40% integrate cybersecurity during the planning stage. As a result, cyber incidents frequently delay or derail key IT and business projects, undermining time to value, eroding stakeholder confidence, and jeopardizing future competitiveness in an increasingly digital world.

Many 'seemingly innocent' design decisions – if not considered from a privacy or security perspective – can have major 'downstream' cost, risk and privacy implications. That issue came to life when we helped a Charity with the design of a unique online system. While it seemed like a good idea at the time, one small design change meant the system went from hosting extremely sensitive information (and the associated cost needed to protect it from loss), to a system that was relatively low risk.

Drop us an email here if you want the details behind that story. Also, if you need help thinking through the issues, don't hesitate to reach out. If nothing else, take a look at the Australian Signals Directorate, Secure by Design if you're undertaking any kind of digital transformation in your organisation!

Don't look up

Our imagination was captured when we read that "Satellites Are Leaking the World's Secrets: Calls, Texts, Military and Corporate Data". The researchers said "It completely shocked us. There are some really critical pieces of our infrastructure relying on this satellite ecosystem, and our suspicion was that it would all be encrypted… [The Satellite operators] assumed that no one was ever going to check and scan all these satellites… They just really didn't think anyone would look up".

In addition, there was a video embedded in that same article titled "6 of the worst data breaches in U.S. History" is worth a quick watch as well! What's the lesson? It's a shining example why Secure by Design is worth doing at the start of a new idea or transformation!

World's first large-scale cyberattack executed by AI

This quarter, Anthropic apparently detected the use of agentic AI in a "highly sophisticated" espionage campaign out of China. By manipulating Anthropic's own AI coding assistant Claude Code, the hacker(s) reportedly attempted to infiltrate approximately thirty global targets. In a small number of cases, they succeeded. There's a lot in the reference article and even more in the linked report.

The important 'so what' was summarised as: Overall, the threat actor was able to use AI to perform 80-90% of the campaign, with human intervention required only sporadically (perhaps 4-6 critical decision points per hacking campaign). The sheer amount of work performed by the AI would have taken vast amounts of time for a human team. At the peak of its attack, the AI made thousands of requests, often multiple per second—an attack speed that would have been, for human hackers, simply impossible to match. Hold onto your hats – it's going to be windy in the world of cyber!?

Reframe cybersecurity as a strategic driver of value

If you're a current CISO or aspiring CISO, you should have a look at The World Economic Forum's paper on Elevating cybersecurity: Ensuring Strategic and Sustainable Impact for CISOs. We were impressed by the '**strategic collaboration network**' that the report defines where the CISO needs to interact well with a very large number of diverse external and internal stakeholders. Also, if your role is in the 'C-Suite', you should have a look at it too, because it does a good job defining what 'good looks like' from both sides of the relationship.

SolarWinds Dismissal and what it means for you?

In late November, the US Securities and Exchange Commission decided to dismiss its lawsuit against SolarWinds and it's CISO Tim Brown. It was enlightening to hear his side of the story at the AISA 'CyberCon' in Melbourne earlier this year. It also highlights the core issue of 'responsibility without authority', which is worth thinking about if you're a 'head of' cyber. We thought this quote summarised it all:

"Brown had to live through five years of this, first, investigation and, then, litigation… And I assume that comes with a significant personal toll, psychological toll, and physical toll. [Brown suffered a heart attack during the litigation.] If CISOs don't have the necessary indemnification agreements or directors and officers [D&O] insurance protections via the bylaws or by agreement, it can also mean that even if you win, it carries a significant financial toll."

'Tis the season to reflect on things that are important. You're one of those and we appreciate you being connected with us. However you celebrate the season, we hope you create some positive memories with friends and family, and may your New Year be full of peace, joy, prosperity and good health!

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