Cyber and AI: ASIC Recommends Going Back to the Future

Ravi Nayyar

2 June 2026

On 8 May 2026, the Australian Securities and Investments Commission (ASIC) flagged for its regulated entities the increasingly complex cyber risks introduced by artificial intelligence (AI), particularly large language models (LLMs). In an open letter, Simone Constant, an ASIC Commissioner, called for licensees, market participants and their directors to act.

ASIC was not the first and will not be the last financial or corporate regulator from a major economy to warn of the cyber resilience implications of frontier AI. What was notable about its open letter, however, was its recommending that regulated entities, in essence, go back to the future to navigate an increasingly turbulent cyber risk landscape.

Two key AI-related drivers of that risk landscape warrant particular attention: threat actors' use of AI and organisations' accelerating in-house deployment of AI.

Multiple cyber resilience vendors (including Google, Microsoft, CrowdStrike and Sophos) have reported rapid growth in a range of threat actors' using LLMs to automate development, troubleshooting and execution of attack chains, particularly since late 2025. Such malicious use included that for: researching targets; discovering vulnerabilities; developing exploit chains and malware; drafting more convincing phishing lures; and analysing exfiltrated data. Little wonder that Commissioner Constant warned that LLMs are 'lowering the barrier to sophisticated cyber activity, [and] increasing the speed and scale of attacks'.

At the same time, organisations across sectors continue to rapidly integrate LLMs and agentic systems into their operations. In January 2026, Proofpoint surveyed 1,453 security professionals, located worldwide, including in the US, UK, Australia and Singapore. It found that 87% of the respondents' organisations had rolled out AI assistants beyond the pilot stage while 76% were 'actively piloting or rolling out [AI] agents'.

Why regulators like ASIC would particularly be concerned is the absence of decent cyber risk management governing that rollout. Of the organisations represented in Proofpoint's survey, only 48% said 'security was embedded from the start 'while 52% said security was 'catching up, inconsistent or reactive'.

A particular problem is employees deploying unauthorised AI systems, a growing incarnation of shadow IT (employee use of unauthorised and unprotected software). In 2025 (and for the first time), CyberCX responded to a number of incidents in client environments that stemmed from their

employees uploading sensitive corporate data to such systems . Similarly, when auditing certain large Australian banks, insurers and superannuation trustees in late 2025, the Australian Prudential Regulation Authority found unauthorised staff use of AI, failures to calibrate AI rollouts with organisational risk appetites and reactive security postures.

Such factors arguably drove ASIC to declare its concerns on 8 May.

Notable about that declaration were ASIC's underlining the importance of foundational cyber hygiene and explicitly urging against 'panic or reactive overreach'.

ASIC eschewed dramatic rhetoric, rather preferring to stress 'first principles'. Stating that '[s]trong cyber resilience is not built on novel tools', Commissioner Constant flagged the risk landscape's changing due to AI, not the creation of 'entirely new categories of risk'.

Eleven of the twelve steps that ASIC thus recommended regulated entities take in response are existing categories of cyber resilience controls. Those included prioritising business-critical assets, regular review of controls, vulnerability management, business continuity planning and supply chain risk management.

A major theme of ASIC's open letter was corporate governance, with a section dedicated to it. Echoing the retiring ASIC Chair, Joe Longo's, speeches from recent years, Commissioner Constant conveyed ASIC's expectation that corporate officers are proactive in overseeing cyber risks from AI. Hardly radical stuff, but clearly requiring restatement.

ASIC's open letter is a welcome sign of regulatory sanity, sorely needed amid exasperation and exaggeration from stakeholders generally about AI's implications for our societies and economies.

Commissioner Constant's closing sentence captures the matter quite elegantly: "'The time to act is now, not by reinventing your approach, but by ensuring the basics are robust, resourced, and working effectively".