MEMO: Leadership Roundtable on Regional Cybersecurity Policy in Asia Pacific 2025
24 Oct 2025 830-1030am @ Australia High Commission to Singapore

Context and background: The increased deployment and use of artificial intelligence (AI) technologies in business and government systems, and increasing consumer familiarity with AI tools, creates a new class of cybersecurity risk for policymakers in Asia Pacific. These risks include exposing new attack surfaces, accelerating threat vectors, all of which contribute to new and sophisticated forms of cyberattacks that can target individuals, organizations, and states. Policymakers today are already grappling with the ethical and legal challenges that AI poses to cybersecurity policy, such as working through how to ensure accountability, transparency, and human rights in the use of AI for cyber operations. This landscape requires a coordinated and comprehensive responses from policymakers in the region.

This memo provides a snapshot of participant views of the current cybersecurity landscape in Asia Pacific (as of Oct 2025). This breakfast roundtable discussed AI, and other key cybersecurity topics relevant to Asia Pacific stakeholders, with three questions guiding the discussion:

- What do you currently see are the cyberthreats faced, and where do you think you are prepared, and could deal with more assistance?
- How does the addition of agentic AI into cyberthreats change anything? How should our postures change? e.g. should govt start putting out guidelines and rules around use of agentic ai?
- Are there areas of AI governance and regulatory coordination which exist now - particularly in Asia Pacific - which could be capitalised on and/or grown?

The discussion started with the launch of CCAPAC's annual trend report for 2025, AI Security in 2025 and Beyond: Emerging Threats and Solutions. The report builds on identified AI threats from the CCAPAC 2024 report on AI and Cybersecurity, which highlighted threats such as (1) data security risks, (2) model security risks, (3) infrastructure risks, and (4) application risks.

The 2025 Annual Report adds two additional risks from the developing AI landscape: (1) agentic AI security risks, and (2) AI-powered social engineering risks, and examines how governments and industry are responding to these transformative changes. The annual report is available for free at the CCAPAC website at https://ccapac.asia/research

From the discussions, participants made several key observations of the current cybersecurity and AI landscape.

1. **AI and Agentic AI – aiding both attackers and defenders.** First, there was a general observation that organizations are clearly investing in developing or acquiring new solutions

that leverage AI for security. The primary focus of these AI-enabled capabilities so far is in detection, analysis, and remediation efforts where traditional processes are either too-slow or incomplete resulting in ongoing breaches and compromise exploiting known vulnerabilities.

The introduction of AI into cybersecurity accelerated the speed and impact of threats and attacks but also empowered defenders to detect attacks and build stronger defences. Some examples shared included the observation that the ready availability of AI tools meant it was cheaper for bad actors to mount attacks, and that the barrier to entry for new threat actors was also lower with the introduction of AI tools. Conversely for defenders, the ready availability of AI tools made it easier to improve security postures through AI-generated reviews and suggestions, or through performing in the role as the red-team for cybersecurity exercises.

However, participants also cautioned that this readiness also increased the "defender's dilemma" burden (where defenders have to be right all the time, and a single mistake for cybersecurity incidents negates all previous protection and defence postures.)

2. **AI and Agentic AI – acceleration but not a novel threat as yet.** A second observation was that there did not (currently) appear to be a "novel threat" from agentic AI or frontier AI in cybersecurity, and there was no significant difference in the type of cyberattacks as a result of agentic AI. Participants shared that there was research that showed that in some samples of cyberattacks, the overall number and type of cyberattacks had not increased (e.g. DoS attacks), but the significance and impact of the attacks had risen.

   Some other participants also pointed out that cybersecurity fail points continued to remain the same as the pre-AI era, such as the threat from ransomware, or from machines running on unpatched/outdated legacy software poses, or from misconfigured and therefore insecure IoT and other connected digital devices. Some other participants noted that attack attribution was difficult, i.e. it was hard to identify where AI had been deployed and what it did in most attacks, although they could be inferred from attack acceleration where some defenders are seeing cyberattacks at speed, or from other indicators such as spikes from energy consumption.

   Addendum note – There were some differing opinions to this discussion point, raised after the official session in informal communications. Some participants noted that their industry experience was that many organisations are now rushing to implement CEO-mandates to deploy enterprise AI by leveraging frontier models, purchase AI-enabled solutions that use specialised models, or develop their own AI models in-house. This has resulted in a situation where cyberthreats arising from AI are new and novel threats, and that defending deployed AI solutions against novel attacks like data manipulation, prompt injection, model poisoning, model theft, non-human identity attacks cannot be entirely dealt with without upskilling existing cyber teams and developing a dedicated AI governance and security effort.

3. **People and behaviours continue to be a large cybersecurity risk.** With the introduction of agentic AI and generative AI, participants observed that in many instances of cyber breaches, it was human behaviours and errors which led to insecurity, which are

increasingly exploited by AI-enabled attacks. Examples raised included phishing emails, or through misconfiguration of devices, or other "human-centric" vulnerabilities. Participants observed that there is a need to continue efforts to improve resilience in this arena, with aids such as stronger access controls, or "prevent nudges" which prompt and check risky behaviours (e.g. "did you mean to send that?"), or through education (e.g. ChildFund Australia's SwipeSafe app which helps children encounter and identify risks online and on mobile.)

4. **Increased regulation may not resolve/improve current cybersecurity postures.** While there are governments who have released policies and regulations around improving cybersecurity postures, we must be careful not to overregulate and stifle innovation and creativity. In addition, in some instances, regulation may be premature or inappropriate due to the specificity of some cyber technologies being used. Differences and inconsistencies of rules across jurisdictions are also a concern. Risks like supply-chain, hallucination, poisoning, etc require attention but cannot be managed alone by model-users. Capabilities like AI-governance, testing of AI agents, version control etc are probably more relevant to enterprises to implement and be held accountable for. Giving the technology time to settle down and taking a principles- and risk-based approach for agentic AI regulation may be a more appropriate stance to take.

5. **Coordination and cooperation around supply chain security.** A final observation was around the areas of cooperation, particularly through public private dialogue that includes all stakeholders affected. Some participants felt that there was an important need to ensure safe and secure communication network infrastructure as well as to shore up the resilience of small and medium enterprises (SMEs) who lack the resources to tackle the increasing complex cybersecurity threat landscape. Other participants highlighted the opportunity for cooperation and information sharing around securing the cybersecurity supply chain, particularly around reducing the risk for a single point of failure.

The roundtable concluded with the moderator thanking all participants for their contributions and welcoming their feedback on the CCAPAC Annual Report 2025.

ABOUT CCAPAC - The Coalition for Cybersecurity in Asia-Pacific is a group of dedicated industry stakeholders who are working to positively shape the cybersecurity environment in Asia through policy analysis, engagement, and capacity building. To find out more on how to join us, visit our website at https://ccapac.asia

---

Please note that participation in this discussion is not indicative of individual or corporate agreement with the views presented.

Roundtable discussants (alphabetical, by organisation)

1. ASEF - Mr Donny Sandjaya Suparman
2. Asia Pacific Medical Technology Association (APACMed) - Ms Su Fen Ong
3. ASUSTeK Computer Inc - Mr Robert Chin
4. Bank of America - Ms Lee Kaishi
5. Becton Dickinson & Co - Mr Paul Chua
6. Cellebrite - Mr Nur Azhar Ayob
7. Cisco - Mr Goh Seow Hiong
8. Cisco - Mr Lilian Rogers
9. Cloudflare - Ms Carly Ramsey
10. Collaborative, Robust & Explainable AI-based Decision-making Lab (CARE.AI), School of Computing and Information Systems, Singapore Management University - Dr Pradeep Varakantham
11. Crowdstrike - Mr Brian Fletcher
12. Cyber Security Agency (CSA) Singapore - Ms Sonya Chan
13. Cybr - Ms Jasmin Ilic
14. ICANN - Ms Angela Wibawa
15. Internet Society - Mr Adrian Wan
16. INTERPOL - Mr Gan Seng Tark
17. KnowBe4 - Ms Caroline Mikaella Soo
18. Lee Kuan Yew School of Public Policy, National University of Singapore - Ms - Mae Chow
19. Nokia - Mr Charles Chew
20. Palo Alto Networks - Ms Nicole Quinn
21. Paypal - Mr Phoram Mehta
22. Qualcomm - Mr Adrian Choong
23. Salesforce - Ms Chan Yan Xi
24. Schneider Electric - Mr Andre Shori
25. Schneider Electric - Ms Charmaine Ng
26. School of Information operations - Mr Craig Harris Simpson
27. SentinelOne - Mr Kris Day
28. United Kingdom Government (Gov.UK) - Mr Oliver Brian Murray
29. Vericent - Mr - Mohammed Kazmi
30. WEF - Mr Filipe Beato

Co-Hosts

31. Access Partnership (CCAPAC Exec Director) - Ms Lim May-Ann
32. Access Partnership - Mr Sam Charlton
33. Access Partnership - Ms Wu Xiaomeng
34. Australia - Landing Pad - Mr Allen Teo
35. Australia - Gov of South Australia - Ms Natalya Twohill