WONG PARTNERSHIP

Cybersecurity

CSA Releases *Singapore Cyber Landscape 2025/2026* Publication

On 30 June 2026, the Cyber Security Agency of Singapore (**CSA**) issued a press release announcing the release of the *Singapore Cyber Landscape 2025/2026* publication, which concerns initiatives to strengthen Singapore's cyber resilience against an increasingly complex and AI-enabled global threat landscape. The publication covers key cybersecurity trends observed over the past year and outlines how CSA is working with industry, critical sectors and the public to address evolving cyber risks.

We summarise below the key highlights of *Singapore Cyber Landscape 2025/2026* as set out in CSA's press release.

AI is Reshaping the Cyber Threat Landscape

Threat actors are increasingly harnessing artificial intelligence (**AI**) to conduct cyber-attacks at greater speed, scale and sophistication. Agentic AI can potentially automate significant parts of the cyber kill chain, lowering barriers to entry for less sophisticated threat actors and compressing attacks that previously unfolded over days into hours.

Anthropic's Mythos has demonstrated how AI can accelerate vulnerability research and exploit development, while the misuse of OpenClaw, a legitimate open-source agentic AI tool, has shown how such technologies can be weaponised to breach development pipelines at scale.

Concurrently, AI presents opportunities for defenders. AI-enabled cybersecurity capabilities can improve threat detection, accelerate incident response and help security teams identify and remediate vulnerabilities more quickly. By automating routine tasks and enhancing security testing, AI enables cybersecurity professionals to focus on more sophisticated threats requiring human expertise and judgement.

As organisations increasingly deploy AI across enterprise networks and Critical Information Infrastructure (**CII**), AI systems themselves are also becoming attractive targets. Vulnerabilities in AI systems could have wider security implications beyond the AI applications themselves, making the secure deployment of AI an increasingly important priority.

To support organisations in adopting AI securely, CSA has introduced several initiatives:

(a) **Guidelines on Securing AI Systems**: CSA has published the Guidelines on Securing AI Systems and its accompanying **Companion Guide**, which provide practical recommendations for system owners to safeguard AI systems.

(b) **Discussion paper on agentic AI**: Recognising the unique challenges posed by autonomous AI, CSA also published a discussion paper on securing agentic AI systems in October 2025.

(c) **International standards**: CSA will continue working with international partners to advance AI security standards.

Phishing Evolves as AI Lowers the Cost of Deception

AI is also reshaping phishing and scam operations, enabling threat actors to generate convincing phishing lures at scale, produce realistic voice clones and video deepfakes, and develop tools capable of bypassing multi-factor authentication.

To strengthen public resilience against increasingly sophisticated scams, CSA, with the support of the Ministry of Home Affairs, launched the pilot run of the National Simulated Scams Exercise in March 2026. The exercise simulated AI-enabled Government Official Impersonation Scam calls to help members of the public better recognise and respond to emerging scam tactics.

Botnets, Ransomware and APTs Continue to Threaten Organisations

In 2025, instances of infected infrastructure detected in Singapore rose significantly to 284,300, a 142% increase from 2024. CSA attributes this primarily to persistent malicious infrastructure activity and improved detection of infected botnet devices. The continued profitability of Malware-as-a-Service operations, coupled with the widespread use of consumer Internet-of-Things (**IoT**) devices with weak security configurations or unpatched firmware, has created more opportunities for botnet operators.

Ransomware also remained a significant threat in 2025, with reported cases increasing slightly from 159 in 2024 to 165 in 2025. Small and Medium Enterprises (**SMEs**) continued to be disproportionately affected due to comparatively lower cybersecurity maturity and limited resources.

CSA has introduced the following measures in response:

(a) **Consumer IoT devices**: All residential routers sold in Singapore must meet Cybersecurity Labelling Scheme Level 2 requirements by end-2027. These requirements include stronger authentication mechanisms and more secure storage of sensitive data. Singapore was involved in establishing common requirements and guidance for developing labelling schemes internationally through the ISO/IEC 27404 standard.

(b) **SME resilience**: CSA supported the establishment of the Cyber Resilience Centre (CRC) with industry partners to provide cybersecurity health checks and recovery assistance following cyber incidents. Eligible SMEs can also receive up to 70% co-funding for cybersecurity advisory services under CSA's Chief Information Security Officer-as-a-Service (CISOaaS) programme.

(c) **International cooperation**: As a member of the Counter Ransomware Initiative (**CRI**), Singapore hosted the fifth CRI Summit in October 2025 during Singapore International Cyber Week, at which CRI members endorsed the Singapore- and United Kingdom-led Guidance for Organisations to Build Supply Chain Resilience Against Ransomware.

Advanced Persistent Threat (**APT**) activity continues to pose a serious threat to Singapore. One of the most significant incidents in 2025 involved an attempted cyber intrusion by APT actor UNC3886 targeting Singapore's four major telecommunications operators. Singapore responded through Operation CYBER

GUARDIAN, the nation's largest coordinated cyber incident response effort to date, which successfully contained the incident with no disruption to telecommunications services and no evidence of customer data being compromised.

Strengthening Cyber Resilience Across Singapore

CSA has introduced several further initiatives to strengthen cybersecurity across critical sectors, businesses and the wider community:

(a) **Cyber Trust mark for CII owners**: CSA has required all CII operators to attain Cyber Trust mark (**CTM**) certification by end-2027. While the Cybersecurity Act 2018 already regulates designated CII systems, the CTM requirement extends good cybersecurity practices across the broader enterprise environments supporting CII operations.

(b) **Guidance on frontier AI**: In May 2026, the Commissioner of Cybersecurity issued guidance to all CII owners on the cybersecurity implications of frontier AI developments. CSA will continue working closely with CII owners to implement the recommendations and has begun rolling out specialised technical training for cybersecurity practitioners within CII sectors.

(c) **Exercise Cyber Star**: National cyber readiness was further strengthened through the sixth and largest Exercise Cyber Star in 2025, which involved close to 500 participants from CSA, the Singapore Armed Forces' Digital and Intelligence Service, and CII owners across 11 critical sectors. The exercise tested Singapore's ability to coordinate responses to large-scale cyber incidents affecting national critical infrastructure.

(d) **Expanded certifications**: CSA expanded the Cyber Essentials and CTM certifications in 2025 to include mandatory cloud and AI security requirements. As of early 2026, more than 800 organisations have attained at least one Cyber Essentials certification.

CSA continues to advance Singapore's National Quantum-Safe initiative, working with industry, academia and international partners to raise awareness of quantum risks, support migration planning and accelerate the adoption of quantum-safe technologies.

If you would like information and/or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:

LAM Chung Nian
Head – Intellectual Property, Technology & Data

Kylie PEH
Partner – Intellectual Property, Technology & Data

Connect with WongPartnership.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Cheang & Ariff
Advocates & Solicitors
Loke Mansion
273A, Jalan Medan Tuanku
50300 Kuala Lumpur
t +60 3 2691 0803
f +60 3 2693 4475
w cheangariff.com
-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous Advocates and Legal Consultants
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com
-
Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
Gruba Law
27/F 88 Corporate Center
141 Valero St., Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w grubalaw.com