RSIS COMMENTARY

23 July 2026

Why Singapore's AI Push Needs a Cyber Layer

Gaurav Keerthi

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSiS 30

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 158 – 23 July 2026

Why Singapore's AI Push Needs a Cyber Layer

By Gaurav Keerthi

SYNOPSIS

Singapore's digitalisation and AI-adoption grants subsidise small enterprises to build software they cannot secure, generating risk the same public spending leaves unaddressed. Framing SME cybersecurity as a public good, this article proposes an effective policy intervention: government digitalisation and AI subsidies should have a component that is ring-fenced for cybersecurity protection.

COMMENTARY

Singapore has spent the better part of a decade helping its small and medium-sized enterprises go digital, supporting more than 88,000 through the SMEs Go Digital Programme since 2017. It is now funding the next wave: a S$150 million (US$116.2 million) Enterprise Compute Initiative to put AI tools within reach of local firms, and a National AI Impact Programme to move 10,000 enterprises up the AI-adoption curve. The economic case is sound.

But Singapore is now paying small firms to build with AI, and many of them have no concept of what building securely means. There is a real risk that the state has funded something that will increase risks yet is not requiring the mitigation of those risks.

The cost of prevention, by contrast, is neither high nor a mystery. Mature firms spend around 11 per cent of their IT budgets on cybersecurity, according to the IANS and the Artico Security Budget Benchmark survey of chief information security officers. A policy norm of one dollar of protection for every ten dollars of digitalisation subsidy would simply translate that private-sector practice into industrial policy.

The New Risk that Arrives with AI-built Software

A new class of generative-AI software, informally called “vibe coding”, lets people with no engineering background build working applications by instructing an AI in plain language. Platforms such as Lovable, Bolt, and Replit are marketed squarely at small businesses, and no engineers are required; with AI coding assistants such as Copilot and Cursor, they have tens of millions of registered users. Even the Government Technology Agency of Singapore (GovTech) is moving in that direction.

These tools have a poor security record, for a reason built into the way they are used. The person building the application is usually not an engineer and cannot read the code well enough to judge whether it is safe. The AI writes it for them, and the whole appeal of the tool is that they never have to look.

When the model produces insecure code, as it frequently does, nothing catches it before the application goes live. Veracode’s 2025 GenAI Code Security Report tested more than 100 models and found that 45 per cent of the code generated introduced known vulnerabilities. The failures are not theoretical and exist systemically: Lovable, a platform valued at around US$6.6 billion, exposed user data and database contents across more than 170 applications because of a basic access-control flaw.

These applications will run retailers’ checkouts, clinics’ appointment books and law firms’ document sharing: the long tail of the digital economy. The Cyber Security Agency of Singapore’s (CSA) Cyber Landscape 2025/2026 report found that more than eight in ten enterprises here experience a cyber incident each year, with smaller firms the most exposed and hardest hit by ransomware. To subsidise these firms to adopt AI tools without a protective layer is to expand the volume of insecure software online, and to pay for the consequences twice: once through the grant and again in the breach.

Cybersecurity is a Public Good

The natural objection is that each business should secure itself. But the state is already “subsidising the car”, and it is entitled, arguably obliged, to insist that the “car comes with seatbelts”. Responsible grant-making accounts for the harm the spending predictably invites, not only the productivity it unlocks.

The economic answer runs deeper. A breach rarely stays where it starts. The 2025 ransomware attack on the printing vendor Toppan Next Tech exposed the data of more than 11,000 DBS and Bank of China Singapore customers, many of whom had never dealt directly with that vendor. CSA calls supply-chain compromise a defining feature of the 2025 threat landscape: well-defended institutions are reached through vendors with weaker cyber hygiene.

The reverse also holds. Once enough firms in a network are secured, the whole system becomes harder to attack, a form of herd immunity in which everyone benefits from protection they did not individually pay for. That is the textbook signature of a public good: a condition in which markets under-provide and the state must act.

Singapore accepted this logic long ago for clean water and street lighting; digital security belongs in the same category.

What every current intervention lacks is operational capacity. Awareness campaigns address a knowledge gap that is not the binding constraint. Certification marks work for the medium-sized firm with a compliance officer and are ignored at the small end: by early 2026, fewer than one in 400 of Singapore's roughly 357,000 SMEs had earned the Cyber Essentials mark. Genuine protection is continuous work, performed by people who do it for a living, and small firms can neither employ them in-house nor afford enterprise prices.

Building Security in from the Start

The deeper problem is conceptual. Digitalisation and its security are funded as two separate budgets, when they are properly one thing. A digitalisation programme that does not pay for its own security is not a cheaper programme; it is incomplete. The seatbelt is not an optional extra on the car.

The policy shift that is needed: for every ten dollars of digitalisation or AI-adoption grant a business receives, at least one dollar must be ring-fenced for cybersecurity. That figure is what mature firms already spend, written into the grant condition rather than left to the recipient's discretion, where it is invariably the first line to be cut. Whether that dollar flows through accredited providers, pooled schemes or shared services is for the market and regulators to settle. The policy point comes first: the money has to be there, and spent on protection that is actually operated.

Singapore is unusually well placed to make this shift, and to set an example for other countries. It has the digital-statecraft tradition to treat security as part of building well, and the most to lose if its programmes run on as they are. The bill is coming due on every grant the government writes. The only question is whether it is paid now, while it is still a line in a budget, or later, when it is an incident in the headlines.

Gaurav Keerthi is the founder of StrongKeep, a managed cybersecurity service for small and medium businesses. He previously served as Deputy Commissioner of Cybersecurity and Deputy Chief Executive of Cyber Security Agency Singapore.

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.