

Tough online safety rules are Singapore's competitive advantage

Digital safety protects consumers' trust in businesses, increasing competitiveness

By Ben Chester Cheong

IN JUNE, Singapore regained first place in the 2026 IMD World Competitiveness Ranking. Eleven days later, the Online Safety Commission began operations.

The two developments may appear unrelated. One is a survey run by the Institute for Management Development (IMD), an international organisation that assesses economic performance. The other is a government agency that provides victims with faster relief from online harassment, doxxing, stalking and image-based abuse.

But they are connected by a principle. In an economy conducted through digital platforms, safety, institutional credibility and competitiveness cannot be separated.

That wider policy direction was reinforced at the National Day Rally on Aug 23, when Prime Minister Lawrence Wong announced stronger safeguards, including robust and reliable age checks, for young social media users. This comes as Singapore continues to embrace technology while managing its risks.

Singapore's digital economy was worth S\$128.1 billion in 2024, accounting for 18.6 per cent of gross domestic product, up from 18 per cent in 2023. Two-thirds of that value came from digitalisation outside the information and communications sector.

Digital trust therefore affects finance, retail, logistics, professional services and every business interacting with customers online.

The policy challenge is to protect Singapore's digital economy while keeping obligations targeted, proportionate and predictable.

Singapore's framework recognises that effective regulation supports investment by reducing the substantial costs that online disorder otherwise imposes on consumers, businesses and public institutions.

Digital disorder has an economic cost

Singapore recorded 41,974 scam and cybercrime cases in 2025. Scam losses amounted to S\$913.1 million. The median loss per case increased to S\$1,644 from S\$1,389 in 2024.

These are not merely private misfortunes. Banks investigate fraudulent transfers. Businesses strengthen payment checks, and respond when scammers impersonate them. Employers lose time and productivity. Legitimate advertisers compete with fraudulent operators.

Every successful scam weakens confidence in the channels through which businesses sell and communicate.

Without proportionate regulation, these costs are borne by consumers, financial institutions, legitimate businesses and public agencies.

The Online Criminal Harms Act 2023 allows authorities to require higher-risk services to introduce specific anti-scam safeguards. These can include verifying sellers and advertisers, offering



safer payment options or preventing accounts from masquerading as government agencies.

Evidence suggests that targeted safeguards can make a difference. Following six-month enhanced verification pilots in the second half of 2024, e-commerce scam cases fell by about 11 per cent on Carousell and about 55 per cent on Facebook Marketplace.

The point is not to prescribe one design for every online service, but to place responsibility on businesses able to reduce a particular risk.

For firms, this changes online safety from a public relations concern into an operational issue. Platforms need reliable systems for identity checks, suspicious-account detection, complaint handling and engagement with authorities.

Banks, marketplaces and other businesses should review how quickly they can detect impersonation, preserve evidence, suspend transactions and warn customers.

The Online Safety (Relief and Accountability) Act 2025 complements these anti-scam measures by giving victims faster and more effective routes to stop serious personal harm.

For businesses, the practical message is simple: online harm requires a prepared response. Platforms need clear reporting channels and teams capable of assessing complaints and acting quickly.

Faster action protects employees, limits business disruption and gives customers greater confidence in Singapore's digital economy.

Faster action protects employees, limits business disruption and gives customers greater confidence in Singapore's digital economy. PHOTO: YEN MENG JIIN, BT

strengthens that predictability.

The Republic has built its framework in stages: Pofma and stronger Poha remedies in 2019, systemic duties for major social media services from 2023, anti-scam requirements under the Online Criminal Harms Act from 2024 and faster individual relief through the Commission from 2026.

This gradual approach allows regulation to respond to distinct risks without repeatedly replacing the entire framework. It also gives businesses time to build reusable compliance capabilities.

A platform that has already developed reporting channels, moderation procedures and regulator-engagement teams can adapt them as targeted duties evolve.

By contrast, abrupt reversals after each political change can leave firms redesigning products and compliance systems before earlier investments have matured.

Businesses may ask why global platforms should redesign systems for a market of fewer than six million people. The answer is that access to a jurisdiction has never carried an entitlement to transfer the costs of an activity to that jurisdiction.

Banks comply with anti-money-laundering rules. Pharmaceutical companies meet local safety requirements. Transport operators are subject to licensing and operational standards.

Digital intermediaries should not be treated as categorically different merely because their infrastructure and corporate headquarters are located elsewhere.

Responsible businesses also benefit from such a regulatory floor. It prevents firms investing in safer systems from being undercut by competitors that monetise engagement while passing the consequences to others. It also gives companies greater certainty about the standards expected of them.

While no framework can eliminate every scam, falsehood or instance of abuse, Singapore's calibrated approach places responsibility on platforms where they are best placed to prevent or address harm.

By ensuring that the benefits of digital commerce are matched by appropriate responsibilities, the framework strengthens trust among users, businesses and public institutions.

For an economy built on confidence, connectivity and institutional reliability, online safety is not a concession to competitiveness. It is part of what makes Singapore competitive.

The writer is a law lecturer at the Singapore University of Social Sciences. He is also a counsel at a Singapore law firm and an associate academic fellow at the National University of Singapore's Asia-Pacific Centre for Environmental Law.

Regulation can strengthen a market

The Protection from Online Falsehoods and Manipulation Act (Pofma) and the Protection from Harassment Act (Poha) also safeguard the conditions on which commerce depends by upholding reliable information, individual security and confidence in online interactions.

Pofma principally requires false statements of fact to carry correction notices linking readers to the government's clarification; it ordinarily does not require the original post to be removed.

Reliable public information matters to businesses because false claims about a disease outbreak, public measure or essential service can alter consumer behaviour and disrupt operations.

Poha, meanwhile, addresses harassment, stalking and false factual statements. It matters when falsehoods damage a person or business.

The framework's strength lies in using tailored laws for different forms of harm. Pofma addresses false statements of fact affecting public interest, Poha addresses harassment and related conduct, and the newer online safety legislation addresses defined forms of personal or criminal harm.

Applying the appropriate legal test to each situation provides businesses and users with clarity while preserving confidence in legitimate online activity.

A fair regulatory floor for all

Singapore's political and institutional continuity