APAC Cybersecurity Fund

The Asia Foundation

INVISIBLE THREATS, VISIBLE IMPACT

Securing MSMEs in the Scam Economy

in partnership with Protect.ngo GLOBAL CYBER ALLIANCE

with support from Google.org

Acknowledgments

This report was authored by Protect.ngo, in collaboration with The Asia Foundation, supported by Google.org.

Research

Protect.ngo team: Adrien Ogee, Jim Boevink

Project Management

APAC Cybersecurity Fund Policy team: Anthea Mulakala, Rukshanie Vidyaratne, Diya Nag, Sandy Walsh, Sharifah Shahirah Idid, Syasya Roslan

Design

Syasya Roslan

Cover photo: Image altered using Canva AI tool.

INVISIBLE THREATS, VISIBLE IMPACT
Securing MSMEs in the Scam Economy

KUALA LUMPUR, MALAYSIA, June 2026.

Executive Summary

Micro, small, and medium enterprises (MSMEs) are driving the Asia-Pacific region's digital commerce boom. Across the region, online retail markets are expanding at double-digit rates, with Vietnam's e-commerce sector alone growing by 18 percent in 2024, to reach an estimated USD 22 billion (Google, Temasek, & Bain, 2024).

This transformation is opening markets, boosting inclusion, and fueling post-pandemic recovery. Yet it also exposes MSMEs and their customers to a surge in scams, fraud, and cyberattacks – exposing MSMEs to a systemic risk rather than a series of isolated incidents. Scamming itself has become a lucrative business model for malicious actors, exploiting the rapid digital transformation of MSMEs.

This digital expansion is unfolding alongside the rapid growth of a transnational scam economy, that increasingly targets MSMEs through business email compromise, fake suppliers and buyers, and brand impersonation – turning e-commerce itself into an attack surface. While governments, platforms, and regional bodies have strengthened cybersecurity frameworks and fraud detection systems, these efforts largely bypass micro and small firms.

The result is a structural policy gap: digitalisation has been actively promoted, but protection has not kept pace, leaving MSMEs the weakest and least supported link in the region's digital economy.

With timely and coordinated action, the coming years present an opportunity to reinforce the resilience of the region's digital economy. Strengthening cybersecurity systems and practices can help sustain consumer confidence in online markets, protect increasingly digital regional supply chains, and consolidate recent gains in financial inclusion.

By reducing systemic vulnerabilities, policymakers and industry partners can avert rising insurance and compliance costs that disproportionately affect MSMEs and ensure their continued participation in digital commerce.

This brief focuses specifically on cybersecurity risks arising from MSME participation in digital commerce and online marketplaces, with particular attention to scams, fraud, and forms of cyber-enabled deception that exploit e-commerce channels. By building a secure and trusted e-commerce ecosystem, the Asia-Pacific can ensure that digital growth remains both inclusive and resilient.

"Scams are rising across the region and, if left unchecked, risk eroding trust in the digital economy – particularly for MSMEs that rely on confidence to grow and participate online. This makes it critical to **advance security approaches that are effective, affordable, and seamlessly embedded into digital commerce.**"

Rajat Maheshwari, Chair, Global Anti Scam Alliance (GASA) Singapore
Senior Vice President, Strategic Growth (AP), Mastercard

Problem Overview and Context

The Cybersecurity Challenge Facing MSMEs in APAC :
Digitalization Without Protection

The COVID-19 pandemic accelerated MSMEs' shift online, driving an e-commerce revolution across Asia and the Pacific. Affordable smartphones, social commerce, and accessible logistics platforms now enable even micro-entrepreneurs to sell their products nationwide or globally.
Key drivers of MSME digitalization include:

Mobile-first economies: Most MSMEs operate directly via smartphones and social media storefronts ("F-commerce").

Platform-driven reach: Regional marketplaces (Shopee, Lazada, Tokopedia) have lowered entry barriers for sellers.

Consumer behavior shifts: Online shopping has normalised across age groups during and after the pandemic.

Expanding attack surface: Each new seller account, payment integration, and platform dependency adds a node that scammers can exploit.

WHY THIS IS A POLICY PROBLEM ?

Governments across the Asia-Pacific region have actively promoted digital transformation through programs such as Indonesia's "MSME Go Online," India's "Digital Saksham Initiative," and the ASEAN Strategic Action Plan for SME Development 2016–2025 (APEC, 2020), now replaced by the ASEAN SMEWG Strategic Plan 2026–2028. Yet cybersecurity capacity-building has not kept pace. While national strategies prioritise connectivity and market access, they lack corresponding investments in MSME cybersecurity training, incident response systems, or accessible security tools. This underinvestment creates a structural vulnerability gap.

THREE dynamics define the policy problem:

Governments promote access, not protection. Public programs accelerate online entry but rarely build in security baselines.

Cybersecurity capacity-building lags market penetration. Training, response systems, and affordable tools are not scaling with adoption.

MSMEs are the weakest link in digital supply chains. Their vulnerabilities cascade upward to platforms, payment providers, and larger buyers.

Evidence Snapshot:
Scale, Cost, and Exposure

The data paint a consistent picture: cyber incidents targeting MSMEs are widespread, awareness is low, and the economic consequences are concentrated on the firms least equipped to absorb them.

INCIDENCE AND EXPOSURE

- **78%** of MSMEs in Asia-Pacific have experienced at least one cyber incident in the past year (Cloudflare, 2023). At this exposure rate, cyber incidents are no longer exceptional events – they are an operational certainty.
- Asia-Pacific accounts for **31% of global cyberattacks**, with potential costs reaching USD 3.3 trillion by 2025 (The Commonwealth Cyber Journal, 2023).
- **One in five adults** in Southeast Asia fell victim to an online scam in 2024, with estimated regional losses of **USD 23.6 billio**n (Global Anti-Scam Alliance, 2025).

AWARENESS AND PREPAREDNESS GAPS

- 92% of MSME owners in Bangladesh report no cybersecurity awareness despite widespread online sales (The Business Standard, 2022).
- In Korea, only 27% of SMEs have a cybersecurity policy, even though 92% of attacks target small firms (Korea Times, 2025).
- 75% of Indian MSME e-commerce apps contained security risks such as misconfigured networks (The Asia Foundation, 2024).

ECONOMIC CONSEQUENCES

- Globally, organisations suffering ransomware attacks report combined losses of USD 1–10 million, with average downtime of 24 days (The Commonwealth Cyber Journal, 2023; Statista, 2023).
- In ASEAN, 50% of SMEs report operational difficulties due to cybersecurity issues, and 31% report reputational damage and customer loss (ASEAN Foundation, 2024).
- In Japan, 52% of ransomware victims in the first half of 2022 were small and medium-sized enterprises (Statista, 2025).
- For MSMEs operating on thin margins, a single breach can erase months of profits or force permanent closure.

The Scam Economy:
A Structural Threat

From Opportunity to Exploitation

As MSMEs move online, fraudsters follow. Across Asia and the Pacific, fake buyers, counterfeit suppliers, and digital impersonators exploit MSMEs' limited defenses. Fraud is no longer an external shock to e-commerce – it is increasingly embedded inside normal business transactions, hidden in supplier emails, payment instructions, marketplace listings, and customer-service interactions.

This shift matters because it changes the nature of the risk. MSMEs are not occasional victims of opportunistic crime; they are operating in marketplaces where deception is a routine cost of doing business.

Industrialisation of Scams

These are not isolated incidents – they represent organised, networked criminal economies operating across borders. Scam operations function as sophisticated businesses, complete with infrastructure, specialised roles, and coordinated tactics that exploit regulatory gaps between jurisdictions (UNODC, 2024; CSIS, 2025). Criminal compounds employ workers drawn from 56 countries, with specialised roles including recruiters, "romance specialists," and technical teams deploying deepfake and AI-generated content (UNODC, 2025; Fortune, 2025).

Three features define this industrialisation:

- **Organised, cross-border networks.** Operations span multiple jurisdictions and are coordinated as enterprises rather than ad-hoc crimes.
- **Specialisation, AI use, and impersonation.** Distinct roles, scripted playbooks, and synthetic media (deepfakes, cloned voices, AI-written messages) raise the credibility and scale of attacks.
- **Enforcement asymmetries and jurisdictional gaps.** Cross-border enforcement remains fragmented; criminals routinely shift operations between countries to evade detection (USIP, 2024). Recent crackdowns have prompted "agile" organised crime groups to expand regionally and globally rather than cease operations (U.S. Treasury, 2025). Scammers consistently pivot tactics faster than regulators can coordinate responses.

"From a regulatory standpoint, we strongly advocate for safety by design and shared responsibility with digital platform providers. Protection, security, and content moderation should not be placed entirely on MSMEs. While we continue to improve MSME digital literacy, we also encourage platforms to fulfill their responsibilities through measures such as safety by design."

Nanci Laura Sitinjak, Head of the Legal and Cooperation Team, Secretariat of the Directorate General of Digital Space Supervision, Ministry of Communications and Digital (Komdigi)

From MSME Constraints to Cyber Vulnerability Pathways

MSMEs face a critical convergence of vulnerabilities when operating in online marketplaces: constrained financial resources that deprioritise cybersecurity investments, informal operational systems that lack standardised protective measures, and limited technical capacity that creates exploitable security gaps. These constraints translate into specific, predictable pathways through which scams and fraud penetrate MSME operations.

Key Vulnerability Pathways

MSME Contraints	Cyber Vulnerability Pathway	Typical Manifestation
Limited resources	Weak authentication & controls	Limited MFA on seller, payment, and platform accounts, reused passwords, no password manager.
Informality	Lack of regulatory protection	Selling through informal channels and messaging apps outside formal seller protections and dispute mechanisms.
Platform dependence	Account takeover & impersonation risk	Reliance on single platform identity, brand and seller pages are easily cloned across social and marketplace channels.
Low cyber maturity	Delayed detection & response	No incident response plan, no monitoring of mentions or listings, slow recognition of BEC and payment-redirection scams.
Thin third-party oversight	Supply-chain and data exposure	Dependence on payment providers, logistics partners, and digital service vendors with weak defenses, unencrypted customer and order data.

Illustratively: 75% of Indian MSME e-commerce apps contained security risks such as misconfigured networks (The Asia Foundation, 2024), in Japan, 52% of ransomware victims in the first half of 2022 were SMEs (Statista, 2025).

Political Economy of MSME Cyber Risk

Technical solutions alone cannot close MSMEs' exposure to e-commerce scams. Structural factors continue to limit the adoption of even basic protections:

INFORMALITY AND REGULATORY REACH

Many MSMEs sell online through informal or semi-formal channels, often without formal registration. This places them outside traditional regulatory and support frameworks and makes compliance-based approaches ineffective – particularly in markets where online selling has outpaced business formalisation.

COMPETING GOVERNMENT PRIORITIES

Governments often prioritise expanding digital access, platforms, and connectivity over securing online transactions. As a result, MSME participation in e-commerce has grown faster than investment in scam prevention, seller protection, and marketplace security.

ENFORCEMENT GAPS

Cross-border scam networks exploit jurisdictional fragmentation and weak coordination, allowing fraud, impersonation, and payment diversion schemes to scale across platforms and borders faster than enforcement responses.

INSURANCE AND RECOVERY GAPS

Cyber insurance products for MSMEs remain scarce or unaffordable, leaving small online sellers to absorb the full financial impact of e-commerce scams and fraud, with no structured recovery pathway.

Individually, these constraints weaken MSME defenses. Together, they contribute to a broader erosion of trust in digital marketplaces – undermining the confidence on which MSME e-commerce participation ultimately depends.

Case Study:
When One Scam Breaks a Business

The following composite cases, drawn from documented attack patterns across the region, illustrate how the vulnerability pathways above translate into concrete losses for individual MSMEs.

THE EMAIL THAT ERASES A QUARTER'S PROFITS — BUSINESS EMAIL COMPROMISE (PHILIPPINES)

A garment manufacturer in the Philippines receives what appears to be an email from their longtime fabric supplier in China, requesting payment to a new bank account due to an "audit." Without verification protocols in place, the business transfers USD 12,000 – nearly its entire quarterly margin – before discovering the email was fraudulent. Three months of work, gone in an afternoon.

THE REPUTATION THAT TAKES YEARS TO BUILD AND DAYS TO DESTROY — BRAND IMPERSONATION (THAILAND)

A family-owned handicraft business in Thailand discovers that scammers have created fake social media accounts using their photos and brand name. Dozens of customers who paid for products that never arrived flood the legitimate business with complaints and negative reviews. The damage to their online reputation could take months or years to repair – if customers ever trust them again.

THE ATTACK WITH NO ONE TO CALL — RANSOMWARE WITHOUT RECOVERY (INDONESIA)

A ransomware attack locks the inventory management system of a small e-commerce retailer in Indonesia. The owner spends days searching for help, but affordable cybersecurity support is nowhere to be found. Facing mounting losses from halted operations, they pay the ransom – with no guarantee their data will actually be recovered or that attackers won't strike again.

REGIONAL CONTEXT:
SOUTHEAST ASIA'S SCAM COMPOUND ECONOMY

These individual cases sit within a far larger criminal infrastructure. The industrialisation of online scams has reached unprecedented scale in Southeast Asia. Criminal compounds – many converted from pandemic-shuttered casinos – now employ **an estimated 220,000+ workers** across Cambodia, Myanmar, and Laos (UN Human Rights Office of the High Commissioner, 2023).

The UN Office on Drugs and Crime reports that workers are drawn from 56 countries, with many trafficked under false pretenses of legitimate employment (UNODC, 2025; Fortune, 2025). **For MSMEs, these networks pose multiple threats:** as direct fraud targets, as unwitting intermediaries in money laundering schemes, and as victims of impersonation when scammers hijack their brand identities to defraud consumers.

Common Cyber Threats Affecting MSME E-commerce

The vulnerability pathways outlined above manifest through a relatively small set of recurring threat categories. Most fraud and impersonation incidents affecting MSMEs in the region map to one or more of the following:

KEY THREAT CATEGORIES

- **Fake buyers and suppliers.** Fraudulent accounts place bulk orders, send fake receipts, or vanish after payment; counterfeit suppliers offer goods that never ship or do not match samples.
- **Business Email Compromise (BEC).** Fraudsters spoof or hijack supplier and partner email accounts to redirect legitimate payments to attacker-controlled accounts.
- **Account takeover and credential theft.** Weak or reused passwords and missing multi-factor authentication allow attackers to seize seller, payment, and admin accounts and to alter listings, payouts, or customer data.
- **Brand impersonation and fake reviews.** Cloned social-media pages, look-alike storefronts, fake reviews, and SEO hijacking divert customers, harvest payments, and damage MSME reputations.
- **Counterfeit listings.** Criminals copy MSME brands and product photos to sell knockoffs, eroding customer trust in the legitimate seller.
- **Ransomware and data extortion.** Attackers encrypt order, customer, or inventory systems and demand payment for restoration – often with no realistic alternative recovery path for an unprepared MSME.

These threats rarely operate in isolation. A typical scam pattern combines impersonation, credential theft, and payment redirection, exploiting MSMEs across several pathways simultaneously.

Systemic Impact:
Trust Erosion in Digital Marketplaces

Why Marketplace Trust Matters

In digital marketplaces, trust – not location – determines who sells and who succeeds. When reviews, search rankings, and social-media signals are manipulated through scams and impersonation, the integrity of e-commerce itself is undermined. Major reputation risks include:

Fake reviews. False reviews discredit or unrightfully promote products, leading customers to mistrust reviews in general, the product itself, or the seller.

Search Engine Optimisation (SEO) hijacking. Fraudulent sites mimic MSME brands to divert traffic and intercept transactions.

Social impersonation. Scammers pose as customer service to harvest data and payments.

Brand sabotage. Organised campaigns post false negative reviews to damage competitors.

85% of consumers suspect reviews are fake "sometimes or often" (Capital One, 2025). This widespread skepticism undermines the entire digital commerce ecosystem. For MSMEs that rely on trust to compete with larger corporations, a single coordinated false campaign can devastate sales and brand credibility. Unlike large companies with dedicated reputation management teams, MSMEs often lack the resources to counter disinformation at scale or navigate platform dispute processes effectively.

Trust losses also affect MSMEs disproportionately because their brands have less reach to absorb shocks: **a single viral negative campaign or wave of fake listings can erase years of customer-base building.**

A COMPETITIVENESS ISSUE

The integrity of digital marketplaces directly affects national competitiveness. Trusted e-commerce ecosystems attract investment, enable MSME growth, and strengthen consumer confidence. Conversely, persistent scam exposure raises the implicit "risk premium" of buying from local sellers, depresses cross-border consumer demand, and over time can shift market share toward a small number of large platforms perceived as safer – at the expense of the MSME segment that policy is trying to grow. Marketplace trust is therefore not only a consumer protection issue but a strategic determinant of digital competitiveness.

Regional Policy Landscape and Gaps

Existing Initiatives

Beyond initiatives supported by the APAC Cybersecurity Fund, **regional and national efforts are already underway** to address cybersecurity risks linked to online commerce.

ASEAN-level coordination

The Working Group on Anti-Online Scams has become a key platform for cross-border coordination, while the ASEAN Regional CERT, operationalised in 2024, strengthens collective incident response. The ASEAN-Japan Cybersecurity Capacity Building Centre and the ASEAN Recommendations on Anti-Online Scams provide a regional framework relevant to e-commerce fraud and scam prevention (ASEAN Digital Ministers' Meeting, 2025).

National Cybersecurity Strategies and Laws

Recent legislation includes Malaysia's Cyber Security Act 2024, the Philippines' National Cybersecurity Plan 2023–2028, and Singapore's amended Cybersecurity Act, reflecting growing policy attention to cyber risks (US-ASEAN Business Council, 2025).

Platform Investments in Fraud Detection

Major e-commerce platforms have expanded AI-enabled fraud detection, seller verification, and proactive takedown mechanisms.

Regional CERT and Coordination Mechanisms

Incident response capabilities are increasingly networked across the region, supporting faster identification of cross-border patterns.

Persistent Gaps

Despite this progress, the policy landscape continues to leave MSMEs underserved:

GOVERNANCE POLICY GAPS

- **Focus on large firms and critical infrastructure.** Most national strategies prioritise systemically important sectors and large enterprises rather than the long tail of MSMEs operating in marketplaces.
- **Limited MSME reach**. Training and support mechanisms cover only a small share of the region's estimated 70 million MSMEs, and informal sellers are often outside the reach of compliance-based instruments.
- **Enforcement lags scam innovation.** Cross-border enforcement still trails the speed and adaptability of organised scam networks (USIP, 2024), legal definitions, evidence rules, and takedown processes evolve more slowly than scam tactics
- **Fragmented data sharing.** Scam typology, payment-trail, and threat-intelligence sharing remains uneven across markets, limiting collective response.

Market Maturity Lens for Policy Action

E-commerce maturity shapes both scam exposure and marketplace trust risks, and therefore the calibration of the actions in Section 8. Nascent markets face payment fraud and informal seller vulnerabilities; emerging markets confront scale-driven fraud and platform-trust gaps; advanced markets must address sophisticated impersonation and cross-border scam networks.

The table below maps one defining e-commerce feature and one priority scam/trust implication per country to guide application of the recommendations.

Country (Tier)	Defining E-commerce Feature	Priority Scam / Trust Implication
Bangladesh (Nascent)	Informal e-commerce dominant, low payment security	Payment fraud from weak verification, basic scam awareness needed
Pakistan (Nascent)	COD dominant, limited digital payment adoption	Consumer protection gaps enable scams, counterfeit products, fake sellers, misleading advertisements, non-delivery fraud payment infrastructure security priority
Sri Lanka (Nascent)	Low retail digitisation, growing fintech sector	Informal sellers lack protections, formalising e-commerce needed
India (Emerging)	Massive scale with persistent rural digital gaps	Fraud detection capacity lags growth, public-private partnerships needed
Indonesia (Emerging)	Largest SEA market, rising mobile commerce	Scam volume increasing with platform scale, incident response mechanisms needed

Country (Tier)	Defining E-commerce Feature	Priority Scam / Trust Implication
Philippines (Emerging)	Young digital consumers, rapid e-commerce growth	Fraud incidents outpacing awareness, scalable training programs needed
Malaysia (High-Emerging)	High mobile commerce penetration, complex regulations	SME skill gaps create impersonation risk, compliance support needed
Thailand (High-Emerging)	The second largest Southeast Asia (SEA) market, 25% of SMEs lack adequate security	Sellers vulnerable to account compromise, online product scam, sector-specific guides needed
Vietnam (High-Emerging)	Rapid growth (38% annually), rural and small sellers gaps persist	Rapid adoption outpaces security capacity, escalating impersonation, and payment-related scams, capacity building, platform-integrated payment safeguards, and shared fraud-response mechanisms needed
Korea (Advanced)	Highly digitised, innovative MSMEs but low internal policies	Weak internal cyber policies persist despite growing digital maturity, AI-enabled phishing, account compromise, and data breaches are becoming more common, stronger MSME cybersecurity governance, regulation, and incident response capabilities are needed.
Japan (Advanced)	Mature e-commerce market with high consumer trust and well-established payment/logistics systems	Impersonation, phishing, and scam ads exploit established consumer trust, stronger platform accountability, reporting mechanisms, and public-private information sharing are needed
Singapore (Advanced)	Highly digital & Near-cashless, strong SME support ecosystem	Sophisticated impersonation and AI enabled fraud targets high-value transactions, threat intelligence sharing needed

Nascent markets (Bangladesh, Pakistan, Sri Lanka)

Initial priorities include enabling safer entry into online selling through trusted payment channels, basic scam awareness for MSMEs, simple seller protections, and gradual formalisation of informal e-commerce activity to improve oversight and support.

Emerging markets (Malaysia, Thailand, Vietnam, Indonesia, Philippines, India)

Policy focus areas include scaling practical protections alongside rapid e-commerce growth: platform-based scam detection, accessible incident-response channels for MSMEs, public–private fraud intelligence sharing, and affordable security tools embedded in marketplaces.

Advanced markets (Japan, Korea, Singapore)

Priority areas include strengthening MSME protections within mature online marketplaces – enhanced seller verification, faster removal of impersonation, improved cross-border sharing of scam typologies, threat intelligence sharing and deeper integration of fraud detection across platforms and payment systems.

Aligning regional cooperation with uneven capabilities

Cross-border scam networks exploit gaps between markets with different enforcement and technical capacities. Regional cooperation can therefore benefit from flexible, tiered approaches:

- **Tiered participation** in information-sharing and enforcement cooperation, allowing all markets to engage at appropriate levels.
- **Capacity support** from more advanced markets to emerging and nascent economies.
- **Minimum regional baselines** for e-commerce scam reporting, takedown processes, and payment tracing.
- **Resource pooling** to support rapid response to large-scale, cross-border scam incidents.

Advanced economies tend to emphasise consumer protection and data privacy; emerging markets focus on fraud mitigation and MSME capacity; nascent markets prioritise basic trust and safe digital participation. A secure regional e-commerce ecosystem depends on recognising these differences while progressively strengthening the weakest links.

Recommendations

Achieving digital trust in online marketplaces requires coordinated action by MSMEs, platforms, and governments. The actions below focus specifically on securing MSME participation in e-commerce – where scams, impersonation, and transaction fraud pose the fastest-growing risks – and require localisation to national contexts.

For MSMEs: Secure online selling and transactions

Many MSMEs operate informally, lack technical support, or underestimate scam risks, limiting adoption of even low-cost protections. The actions below indicate priority steps, the rationale, and how to overcome typical barriers.

Priority	Action	Why this matters	Barrier / Unlock
HIGH 	Enable multifactor authentication (MFA) on all accounts (seller, payment, admin)	Blocks automated account takeovers and payment-redirection scams.	**Barrier:** Low awareness; fear of login friction or account lockout. ***Unlock:*** Platform-default MFA with guided setup and recovery support.
HIGH 	Use trusted payment gateways only	Protects customer data and reduces fraud liability.	**Barrier:** Higher fees; cash-on-delivery norms; informal sales channels. ***Unlock:*** Platform-integrated gateways, fee subsidies, buyer-protection incentives.
HIGH 	Train staff to recognise phishing and fake-buyer scams	Staff are the first line of defense against BEC and impersonation.	**Barrier:** Time constraints; high staff turnover; low perceived relevance. ***Unlock:*** Short, platform-delivered micro-training tied to onboarding or payouts.
MEDIUM 	Keep all software updated; enable automatic updates	Closes known security vulnerabilities.	**Barrier:** Disruption concerns; compatibility fears with existing tools. ***Unlock:*** Enable auto-updates during off-hours; platform notifications for critical patches.
MEDIUM 	Back up critical data weekly (customer lists, financial records, orders)	Enables recovery after ransomware or data loss.	**Barrier:** Unclear responsibility; lack of technical confidence. ***Unlock:*** Automated cloud backups bundled with e-commerce tools.
MEDIUM 	Use a password manager for all staff	Prevents credential theft and reuse.	**Barrier:** Staff resistance; perceived complexity; subscription cost concerns. **Unlock:** Free-tier options for small teams; browser-integrated setup.
MEDIUM 	Monitor online mentions and respond to reputational threats	Early detection prevents reputation damage from impersonation and fake reviews.	**Barrier:** Limited capacity; unclear payoff until damage occurs. **Unlock:** Platform alerts and simple monitoring tools embedded in seller dashboards.
LOW 	Draft a simple one-page cybersecurity polic	Establishes clear security expectations across the team.	–
LOW 	Create a basic incident response plan (who to contact, what to do)	Reduces damage and downtime during incidents.	–

For Platforms: Protect marketplace integrity and sellers

Priority	Action	Timeline	Investment	Impact	Barrier / Unlock
HIGH 	Deploy AI-powered fraud detection for unusual transactions and logins	Short-term	High (initial); Medium (ongoing)	Real-time protection for thousands of MSMEs.	**Barrier:** High upfront investment; false-positive rates affecting legitimate sellers. ***Unlock:*** Phased rollout with human-review escalation for flagged transactions.
HIGH 	Offer built-in seller verification (identity verification, business registration checks)	Short-term	Medium-High	Reduces fraudulent seller accounts.	**Barrier:** Added friction; onboarding drop-off concerns. ***Unlock:*** Risk-based verification triggered by transaction volume or anomalies.
HIGH 	Send regular scam alerts to sellers via dashboard/ email	Immediate	Low	Keeps MSMEs informed of emerging threats.	**Barrier:** Alert fatigue; low engagement rates. ***Unlock:*** Targeted alerts based on seller category and regional threat patterns.
MEDIUM 	Accelerate dispute resolution for MSMEs (dedicated fast-track)	Mid-term	Medium (staffing + systems)	Reduces MSME losses from delayed resolutions .	**Barrier:** Cost and staffing burden; low MSME leverage. ***Unlock:*** Tiered fast-track for verified MSMEs and repeat scam patterns.

Priority	Action	Timeline	Investment	Impact	Barrier / Unlock
MEDIUM 	Proactive removal of fake listings, counterfeit sellers, and review farms	Ongoing	Medium-High (AI + human review)	Maintains marketplace integrity.	**Barrier:** High monitoring cost; risk of removing legitimate sellers. ***Unlock:*** Automated detection backed by human review and clear takedown timelines.
MEDIUM 	Integrate cybersecurity training modules into seller onboarding	Mid-term	Medium	Scales security awareness across the platform.	**Barrier:** Low completion rates; content relevance across diverse seller types. ***Unlock:*** Bite-sized modules with seller incentives tied to completion.
LOW 	Create an MSME cybersecurity helpdesk/ hotline	Long-term	Medium-High (staffing)	Provides ongoing support and guidance.	–

For Governments: Enable safe and trusted e-commerce

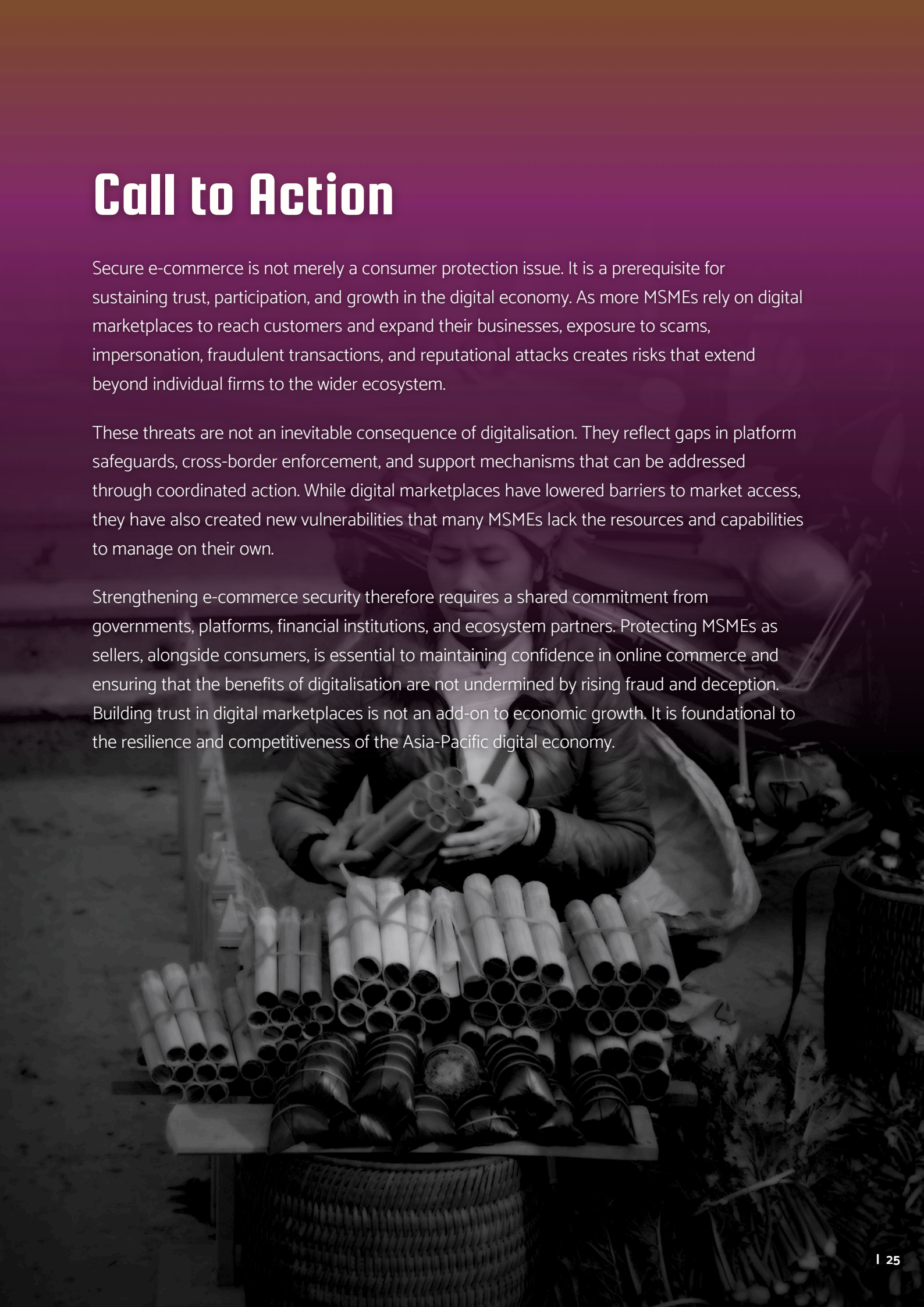
Priority	Action	Barrier / Unlock
HIGH 	Launch nationwide MSME cybersecurity awareness campaigns (digital + traditional media)	**Barrier:** Generic messaging; poor reach to informal sellers. ***Unlock:*** Delivery via platforms, payment providers, and MSME associations.
HIGH 	Facilitate cross-border agreements and fraud data-sharing with neighbouring countries	**Barrier:** Jurisdictional fragmentation; trust and capacity gaps. ***Unlock:*** Bilateral MOUs focused on scam typologies and payment trails.
HIGH 	Provide tax incentives, subsidies, or vouchers for MSMEs adopting secure tools (MFA, training, certified software)	**Barrier:** Administrative burden; low MSME uptake. ***Unlock:*** Voucher models redeemable directly through platforms or vendors.
MEDIUM 	Strengthen laws on e-commerce scams, counterfeit goods, and marketplace fraud	**Barrier:** Lengthy legislative timelines; enforcement capacity gaps. ***Unlock:*** Leverage existing consumer protection frameworks with e-commerce amendments.
MEDIUM 	Develop national digital trustmark schemes to certify secure small sellers	**Barrier:** Low MSME awareness; certification costs for small sellers. ***Unlock:*** Platform integration with subsidised certification for first-time applicants.
LOW 	Establish national cybersecurity training centres with MSME-focused programs	–
LOW 	Create government-backed cyber insurance programs for MSMEs (subsidised premiums)	–

Call to Action

Secure e-commerce is not merely a consumer protection issue. It is a prerequisite for sustaining trust, participation, and growth in the digital economy. As more MSMEs rely on digital marketplaces to reach customers and expand their businesses, exposure to scams, impersonation, fraudulent transactions, and reputational attacks creates risks that extend beyond individual firms to the wider ecosystem.

These threats are not an inevitable consequence of digitalisation. They reflect gaps in platform safeguards, cross-border enforcement, and support mechanisms that can be addressed through coordinated action. While digital marketplaces have lowered barriers to market access, they have also created new vulnerabilities that many MSMEs lack the resources and capabilities to manage on their own.

Strengthening e-commerce security therefore requires a shared commitment from governments, platforms, financial institutions, and ecosystem partners. Protecting MSMEs as sellers, alongside consumers, is essential to maintaining confidence in online commerce and ensuring that the benefits of digitalisation are not undermined by rising fraud and deception. Building trust in digital marketplaces is not an add-on to economic growth. It is foundational to the resilience and competitiveness of the Asia-Pacific digital economy.



References

ASEAN Foundation (2024). Call for Applications.

Capital One (2025). Shopping Data Research.

Center for Strategic and International Studies (CSIS) (2024). Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories.

Center for Strategic and International Studies (CSIS) (2025). Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories.

Cloudflare (2023). Securing the Future: Asia Pacific Cybersecurity Readiness Survey.

Fortune (2025). Inside the compounds of Asia's $10 billion scam industry.

Global Anti-Scam Alliance (GASA) (2025). State of Scams in South East Asia 2025.

Google, Temasek, & Bain (2024). e-Conomy SEA 2024 Report.

Korea Times (2025). Step Up Korea's Cybersecurity Readiness.

PR Newswire (2024). ASEAN fintechs GCash and DANA doubling down on support for MSMEs.

PwC (2024). Global Digital Trust Insights.

Statista (2023, 2025). Ransomware impact and SME victim share, Japan.

The Asia Foundation (2024). From Vulnerability to Resilience: Cybersecurity Challenges for MSMEs in the APAC Region.

The Business Standard (2022). 92% MSME entrepreneurs unaware of cyber security: Study.
The Commonwealth Cyber Journal (2023). Cybercrime in the Asia-Pacific Region.

U.S. Department of the Treasury (2025). U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia.

UN Human Rights Office of the High Commissioner (2023). Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a human rights response.

United Nations Office on Drugs and Crime (UNODC) (2024). Billion-Dollar Cyberfraud Industry Expands in Southeast Asia as Criminals Adopt New Technologies.

United Nations Office on Drugs and Crime (UNODC) (2025). Reports on transnational scam operations.

US-ASEAN Business Council (2025). Regional Cybersecurity Policy Update.

USIP (2024). The Latest on Southeast Asia's Transnational Cybercrime Crisis.

ASEAN Digital Ministers' Meeting (2025). Outcomes and Recommendations on Anti-Online Scams.

APEC (2020). ASEAN Strategic Action Plan for SME Development 2016–2025.

The APAC Cybersecurity Fund

The APAC Cybersecurity Fund is an initiative by The Asia Foundation, supported by Google.org, Google's philanthropic arm, designed to build inclusive and sustainable cybersecurity ecosystems across the Asia-Pacific region. Through cyber hygiene training, policy research, and stakeholder engagement, the program helps micro and small businesses, nonprofits, and social enterprises strengthen their cyber resilience. It also invests in long-term capacity by establishing more than 20 university-based cyber clinics to expand outreach and develop the region's cybersecurity workforce. The initiative spans across 13 countries including Australia, Bangladesh, India, Indonesia, Japan, Korea, Malaysia, Pakistan, Philippines, Singapore, Sri Lanka, Thailand, and Vietnam.

The Protect.ngo Foundation

Protect.ngo exposes harm and defends at-risk communities in cyberspace with talent, technology, and data.

The Asia Foundation

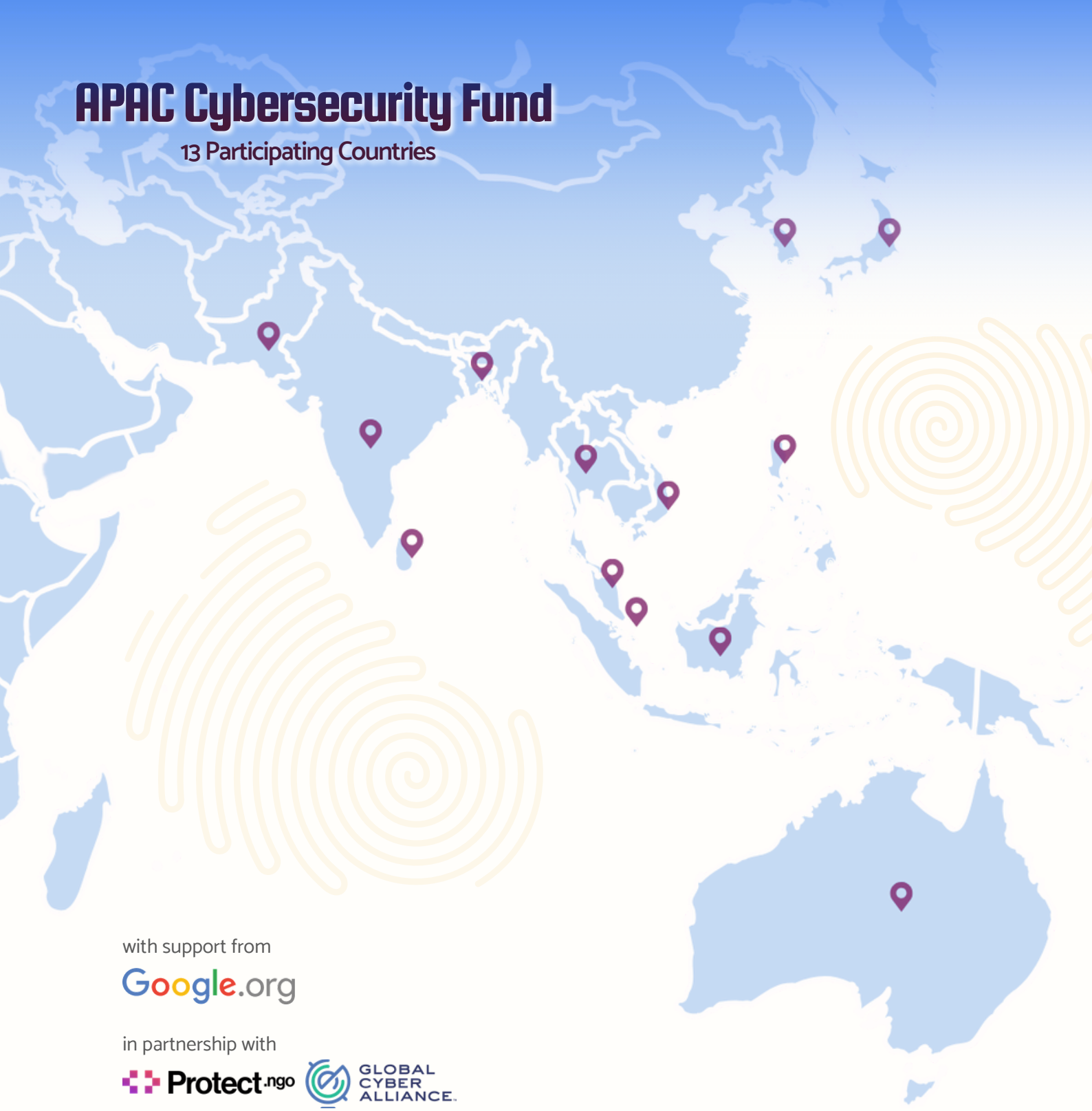
The Asia Foundation is an international nonprofit organization working to solve the toughest social and economic challenges in Asia and the Pacific. Informed by more than 70 years of experience and deep local knowledge, we work with partners across more than 20 countries to improve lives and expand opportunities.

Google.org

Google.org, Google's philanthropy, brings the best of Google to help solve some of humanity's biggest challenges combining funding, product donations and technical expertise to support underserved communities and provide opportunity for everyone. We engage nonprofits, social enterprises and civic entities who make a significant impact on the communities they serve, and whose work has the potential to produce scalable, meaningful change.

APAC Cybersecurity Fund

13 Participating Countries



with support from

Google.org

in partnership with

Protect.ngo

GLOBAL CYBER ALLIANCE

The Asia Foundation

The Asia Foundation
www.asiafoundation.org