



APAC Cybersecurity Fund



The Asia Foundation

CLOSING THE REPORTING GAP

Cyber Incident Transparency for MSMEs in Asia and the Pacific



in partnership with



Protect.ngo

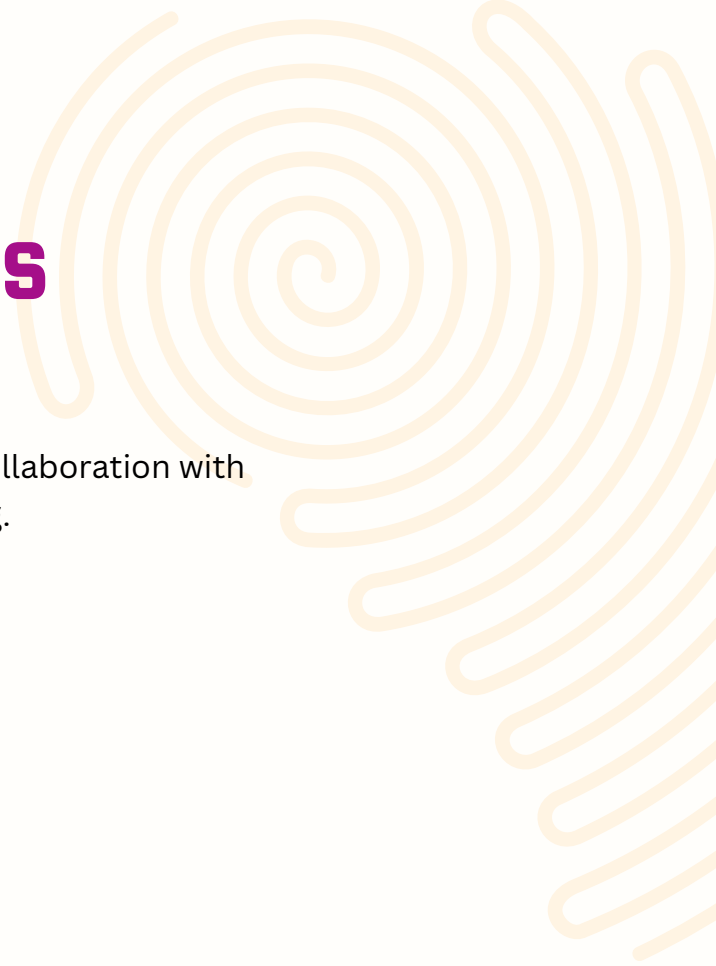


GLOBAL
CYBER
ALLIANCE.

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 Iddid, Syasya Roslan

Design

Syasya Roslan

Cover photo: Image altered using Canva AI tool.

CLOSING THE REPORTING GAP:

Cyber Incident Transparency for MSMEs in Asia and the Pacific

Kuala Lumpur, Malaysia, October 2026.

© The Asia Foundation 2026.

All rights reserved. No part of this report may be reproduced without written permission from The Asia Foundation.

Executive Summary



Micro, small, and medium enterprises (MSMEs) account for 99.8 percent of all businesses across the Asia-Pacific (APAC) region, employ over half of its workforce, and contribute a substantial share of regional gross domestic product according to the Asian Development Bank (Asia SME Monitor, 2025). Over the past five years, these firms have digitalized at extraordinary speed, adopting cloud services, mobile payments, social commerce, and generative AI tools to compete in increasingly online markets.

This brief addresses a paradox at the heart of APAC cybersecurity: MSMEs are simultaneously the most exposed segment of the economy and the least visible in official cyber incident data. Industry surveys suggest that roughly two in three APAC organizations experienced at least one cybersecurity incident in the past year, and 61 percent of those suffered a data breach (Cloudflare, 2024) — though those surveys reach only firms far larger than the region's typical MSME. Where smaller firms do appear in incident data, the attacks against them are harsher: ransomware features in 88 percent of small-business breaches against 39 percent for large enterprises (Verizon Business, 2025). Many of those affected never report the event to any authority (The Asia Foundation, 2024b).

The result is a regional blind spot: national Computer Emergency Response Teams (CERTs) see only a sliver of the threat landscape, policymakers cannot design well-calibrated interventions, and supply-chain partners cannot anticipate where compromises come from next.

Closing this reporting gap requires meeting MSMEs where they are: running businesses from their phones, managing customer calls without dedicated IT departments, and often navigating formal systems they do not fully trust. This brief examines why the current reporting architecture does not work for these firms, what incident response actually looks like inside a five-person workshop in Surabaya or a family-run logistics firm in Chennai, and what governments, platforms, and MSMEs themselves can do to make reporting feel useful rather than risky. Its central argument is that reporting is not an end in itself: it is the gateway to incident response — faster recovery, technical assistance, restored business continuity, and the shared threat intelligence that protects the next firm in the chain.

The brief concludes with three sets of recommendations, each designed to be actionable within the next 12 to 24 months. First, MSMEs should be supported to build simple incident response plans, have clear points of contact, accessible reporting channels, and stronger peer knowledge networks. Second, governments and policymakers should strengthen the enabling environment for reporting by establishing simple and multilingual reporting systems, incentives and protections for good-faith reporting, stronger regional cooperation, and a non-punitive approach to breached businesses.

Third, industry and service providers should embed "one-click" reporting and basic security measures into currently used platforms, providing affordable security services, sharing anonymized threat intelligence, and strengthening post-incident support.

“Creating a safe, trusted, and inclusive digital space is a shared responsibility. MSMEs face increasingly complex challenges in navigating the digital environment, and our support should go beyond one-off training. Continuous mentoring, listening to MSMEs, and helping them address their challenges are essential to strengthening digital resilience.”

Nanci Laura Sitinjak

Head of the Legal and Cooperation Team,
Secretariat of the Directorate General of Digital Space Supervision,
Ministry of Communication and Digital (Komdigi), Indonesia

The Digital Landscape for MSMEs in APAC

MSMEs are the structural backbone of the APAC economy, but their digital transformation has outpaced their ability to manage the risks that come with it. Understanding the speed, scale, and uneven nature of this transformation is essential to understanding the reporting gap.

Key Statistics

99.8%

of enterprises across APAC are MSMEs. MSMEs also provide more than half of total employment across APAC economies (ADB Asia SME Monitor, 2025).

68%

of organizations in the region reported experiencing at least one cybersecurity incident in the prior year* (Cloudflare, 2024).

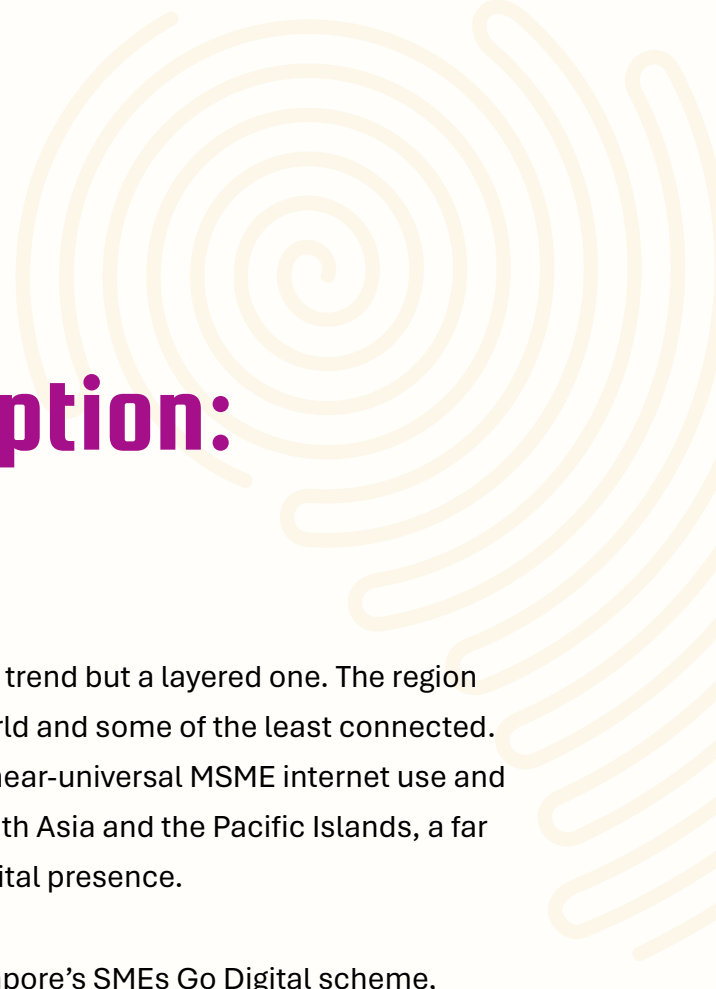
88%

of breaches among small businesses involved ransomware compared with 39% among large enterprises* (Verizon Business, 2025).

92%

of APAC organizations that experienced a data breach reported consequences beyond the breach itself, with regulatory action being the most common* (Cloudflare, 2024).

*Neither survey reaches the MSME segment as this brief defines it: Cloudflare surveyed only organizations of 250 employees or more, and Verizon defines small business as fewer than 1,000 employees.



Rapid Digital Adoption:

At Different Speeds

Digital adoption among APAC MSMEs is not a single trend but a layered one. The region spans the most mature digital economies in the world and some of the least connected. Japan, South Korea, Singapore, and Australia have near-universal MSME internet use and well-developed cloud markets, while in parts of South Asia and the Pacific Islands, a far smaller share of small firms has any meaningful digital presence.

National programs have accelerated the shift. Singapore's SMEs Go Digital scheme, Indonesia's E-Smart Industri Kecil dan Menengah (small and medium industries), Malaysia's SME Digitalization Grant, the Philippines' digitalJobsPH, India's Udyam registration and the Open Network for Digital Commerce (ONDC), Vietnam's Go Online program, and Japan's IT Donyu subsidy have together onboarded millions of micro and small firms. The MSME Trade Enablement and Marketing (MSME-TEAM) Initiative in India aims to onboard 500,000 micro and small enterprises onto ONDC between 2024 and 2027, with half the targeted beneficiaries being women-owned MSMEs (Ministry of MSME, 2024).

The mix of tools is consistent. Across markets, MSMEs rely overwhelmingly on a small set of platforms with limited awareness on secure use of these tools, such as: WhatsApp, Telegram, Line, or Zalo for customer communication; Facebook, Instagram, and TikTok Shop for sales; Shopee, Lazada, Tokopedia, Flipkart, or Rakuten for e-commerce; GoTo, Grab, or PayPay for payments; and Google Workspace or Microsoft 365 for productivity.

This concentration means that a vulnerability in any one of these platforms has cascading consequences for large numbers of small businesses simultaneously.

Asia and the Pacific

Digital tools MSMEs rely on

Common platforms across five areas of business activity.

01



Customer Communications

Messaging customers, responding to enquiries and coordinating orders

WhatsApp . Telegram .
Line . Zalo

02



Sales and Marketing

Promoting products, reaching customers and generating sales

Facebook . Instagram .
TikTok Shop

03



E-Commerce

Listing products, managing orders and transacting online

Shopee . Lazada .
Tokopedia . Flipkart
. Rakuten

04



Payments

Receiving customer payments and managing transactions

GoTo . Grab . PayPay

05



Business Productivity

Creating documents, storing files and collaborating on daily operations

Google Workspace .
Microsoft 365



Microsoft 365



Disproportionate Exposure

MSMEs are exposed through two distinct channels. The first is direct. Small businesses now absorb a distinct and harsher form of attack: ransomware features in 88 percent of their breaches, against 39 percent for large enterprises, and 99 percent of small-business breaches are financially motivated (Verizon Business, 2025). They are attractive precisely because they are soft: under-resourced, less likely to hold current backups, and useful to attackers as a low-risk environment in which to rehearse tooling.

The second channel is indirect, and arguably more consequential across APAC: even an MSME that is never itself targeted inherits the vulnerabilities of the shared public infrastructure it depends on. The June 2024 ransomware attack on Indonesia's Temporary National Data Center 2 (PDNS 2), located in Surabaya and attributed to the Brain Cipher group, disrupted hundreds of public services, including immigration, business licensing, and student registration. Although MSMEs were not the direct target of the attack, many experienced operational disruptions because they relied on these digital public services for permits, licensing, and cross-border business activities (BSSN, 2024).

Third-party involvement in breaches doubled over the past year, from 15 to 30 percent of cases (Verizon Business, 2025), and supply-chain attacks rank fourth among attack vectors reported by APAC organizations, at 35 percent (Cloudflare, 2024). That exposure travels through private supply chains as well as public infrastructure: when a large upstream firm is knocked offline, the small suppliers around it absorb a shock that rarely surfaces anywhere.

VARTA, INDONESIA (BATAM) — FEBRUARY 2024

A cyberattack forced the Batam site of German battery maker Varta offline alongside its plants in Germany and Romania. Recovery was handled inside the multinational; the downstream effect on the small local suppliers around it — canceled orders, delayed payments, idle capacity — was not captured by any reporting system. Business-continuity harm of this kind illustrates the MSME-level impact that may go unreported to a CERT. (The cascade to smaller suppliers is a general illustration of business-continuity risk, not a documented finding.)

Source: SecurityWeek (2024); Security Affairs (2024).

A Widening Reporting Gap

The gap between rising cyber threats and actual national threat visibility is widening, driven by a fundamental disconnect in how MSMEs engage with state defense apparatuses. Further, despite rising incidence, MSME representation in national CERT data cannot even be measured. India's CERT-In tracked roughly 1.4 million cyber incidents in 2021 alone, but the published figures are not disaggregated by firm size (Ministry of Electronics & Information Technology, 2022) — the segment comprising 99.8 percent of enterprises cannot be located in the data at all.

Industry bodies have flagged a related problem: in a September 2022 representation to CERT-In, National Association of Software and Service Companies (NASSCOM) and Data Security Council of India (DSCI) warned that the compliance obligations under the Cyber Security Directions — including the six-hour incident reporting requirement — would fall disproportionately on MSMEs (NASSCOM & DSCI, 2022).

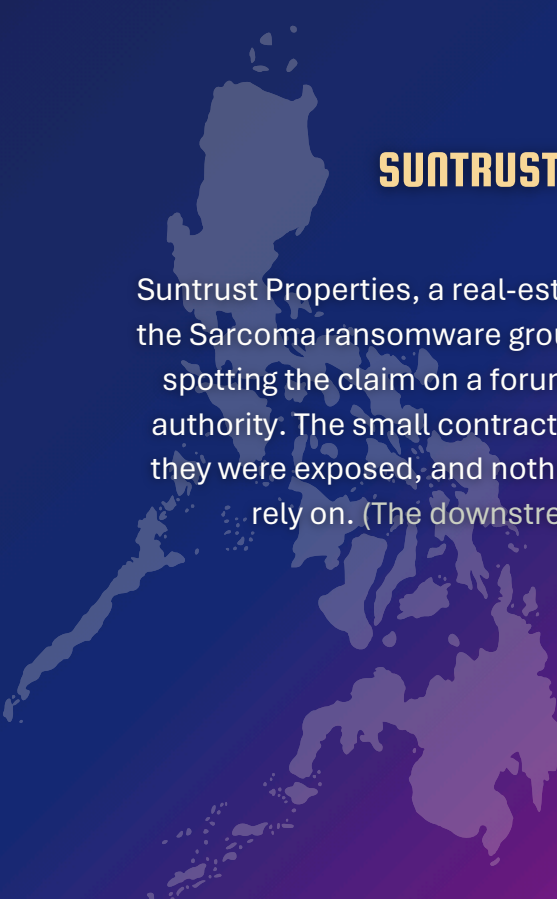
Japan's long-running Security Action program, run by the Information-technology Promotion Agency (IPA), passed 300,000 self-declared SME participants by October 2023, but the 2023 IPA program survey found that participation is often motivated by subsidy eligibility rather than sustained engagement (IPA, 2023). A self-declaration scheme of that scale therefore indicates how many firms have signed a pledge, not how many incidents those firms have experienced or disclosed.



The gradient is visible even inside surveys that never reach the MSME segment. Cloudflare's 2024 APAC survey found incident rates rising with organization size — 36 percent among its smallest respondents, 46 percent among medium and 51 percent among large firms — and reads this as attackers favoring larger targets (Cloudflare, 2024). Verizon's data points the other way: where small firms do appear, ransomware features in 88 percent of their breaches against 39 percent for large enterprises (Verizon Business, 2025). Smaller organizations report fewer incidents while suffering more severe ones. That is the signature of a detection and disclosure gap rather than a safety advantage, and it holds even at 250 employees — well above the size at which most MSMEs operate.

The Asia Foundation's 2024 study of MSME cybersecurity across 12 APAC countries identified widespread under-reporting as one of its central findings, attributing it largely to fear of reputational damage (The Asia Foundation, 2024b). The true picture of MSME cyber risk in APAC is therefore largely invisible to the policymakers who would need to act on it. This invisibility is not a data problem alone, it is a design problem, and the rest of this brief is about what design choices have produced it.

That invisibility holds at the level of individual incidents as well, where an entire compromise can pass without ever entering official data.

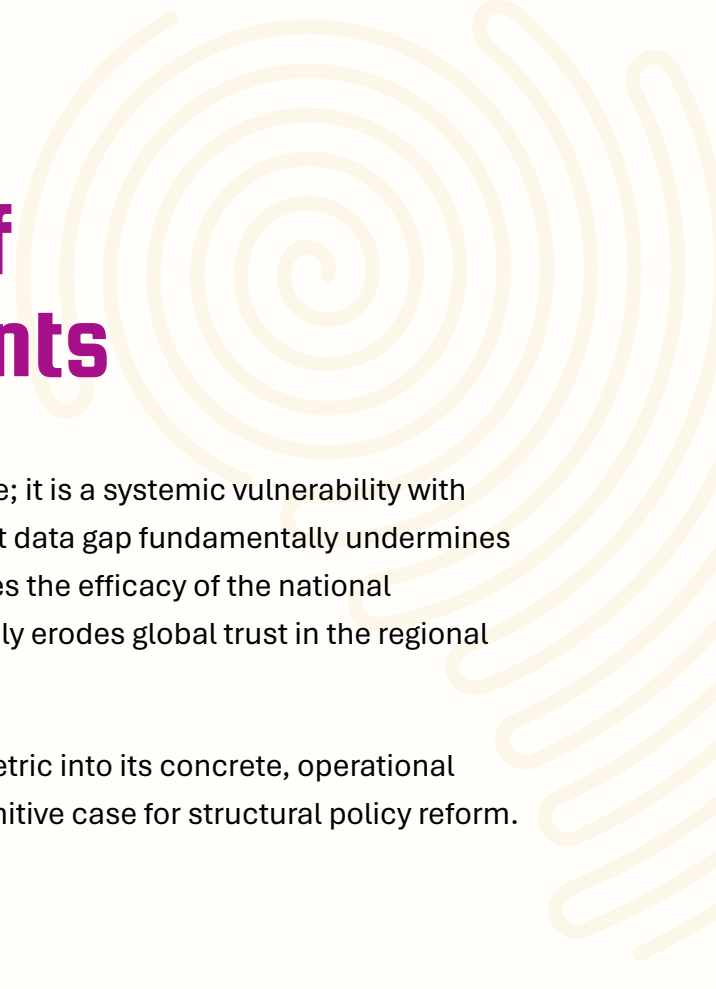


SUNTRUST PROPERTIES, PHILIPPINES — OCTOBER 2024

Suntrust Properties, a real-estate subsidiary of Megaworld Corporation, was claimed by the Sarcoma ransomware group. The only public signal was a threat-intelligence vendor spotting the claim on a forum; no leaked data was revealed and no report reached any authority. The small contractors and suppliers in its orbit therefore had no way to know they were exposed, and nothing about the incident reached the data that policymakers rely on. (The downstream impact on connected SMEs is a general illustration of supply-chain risk, not a documented consequence.)

Source: CYFIRMA (2024).

The Hidden Cost of Unreported Incidents



Under-reporting is far from a neutral statistical figure; it is a systemic vulnerability with cascading real-world consequences. This persistent data gap fundamentally undermines the resilience of individual enterprises, compromises the efficacy of the national institutions mandated to defend them, and ultimately erodes global trust in the regional digital economy.

Translating this reporting deficit from an abstract metric into its concrete, operational harms is the critical first step toward building a definitive case for structural policy reform.

Why MSMEs Stay Silent

Surveys consistently identify a handful of reasons MSMEs choose not to report. Fear of reputational, regulatory, and financial consequences consistently emerges as a primary barrier to cyber incident reporting among MSMEs, as disclosure may result in financial losses, legal exposure, and reputational harm (Sangari et al., 2022). At the same time, underreporting is reinforced by a perception that reporting offers little practical value: reporters are seldom acknowledged or told what came of a report (Ebert et al., 2025), and firms experience reporting as bureaucratic and unrewarding — disclosure is felt to invite regulatory scrutiny rather than protect the business (Lydon, 2022).

The fear is not misplaced. Among APAC organizations that suffered a data breach, 92 percent reported consequences beyond the breach itself, and the most common was regulatory action, cited by 26 percent — ahead of further attacks using the stolen data (17 percent) and reputational damage (16 percent) (Cloudflare, 2024). For firms that already regard the state as an auditor rather than a defender, that is the outcome they are avoiding.

These reasons share a common shape: in the absence of a clear, immediate benefit, the rational decision for a small business owner is to absorb the incident quietly and move on. The incentive structure does not reward transparency, and in many cases actively punishes it.

The "Dark Figure" of Cybercrime

Cybercrime is widely understood to be one of the most under-reported categories of crime globally, with UNODC and national crime victimization surveys both documenting reporting rates well below those for comparable offline offenses (UNODC, 2013; UNODC Education 4 Justice module 5). In APAC, that pattern is likely amplified. Cultural norms around public disclosure of failure, the strong reputational cost of being publicly identified as a victim, and limited legal protection for those who come forward all combine to suppress reporting further. In Japan, surveys by the market-research firm Teikoku Databank found that around a third of companies had experienced a cyberattack.

Still in Japan, repeated surveys have found smaller enterprises being attacked at rates at or above those of large firms, and being used as stepping-stones into the larger corporations they supply (Teikoku Databank, 2022; 2025). The clearest illustration is the February 2022 compromise of Kojima Industries, a Toyota parts supplier, which halted output across Toyota's domestic plants for a day (Reuters, 2022).

Impact on National and Regional Defense

Unreported incidents prevent CERTs from mapping attack patterns, which in turn starves regional threat-intelligence mechanisms such as the ASEAN Regional CERT, launched on October 16, 2024 in Singapore, of the data they need to be useful (CSA Singapore, 2024). It also negatively impacts the capability of law enforcement agencies to fight cross-border cybercrime. MSMEs are frequently the entry point into larger supply-chain compromises.

When a small accounting firm in Hanoi or a logistics SME in Karachi is breached, and the incident goes unreported, the threat intelligence that would have allowed a downstream multinational to defend itself never enters circulation. The same failure runs in the other direction, from a large supplier down to the small firms beneath it.

Policy Takeaway:

Under-reporting is not a measurement quirk; it is lost defense. Every silent incident is intelligence that never reaches a CERT and a warning that never reaches the next firm in the chain. Across the cases above the mechanism is the same: harm travels downstream to smaller suppliers, and in none of them was that harm recorded anywhere. The fact that this brief must label those downstream effects as illustrative rather than documented is not a weakness in the evidence — it is the phenomenon the brief describes. Building that connection — between reporting and a response the reporting firm can feel — is the task of the reforms set out in Section 5.

THONBURI ENERGY STORAGE SYSTEMS (TESM), THAILAND — AUGUST 2023

The Qilin ransomware group listed TESM, a Thai battery manufacturer and joint-venture partner in Mercedes-Benz's local production; when the firm declined to engage, the attackers published its exfiltrated contracts and design files. There is no public record of a report to any national CERT — the ecosystem learned of the compromise only when the stolen data appeared for sale. The warning that could have told the connected sub-suppliers to expect invoice fraud never entered circulation. (Downstream harm to sub-suppliers is illustrative supply-chain risk, not a documented consequence.)

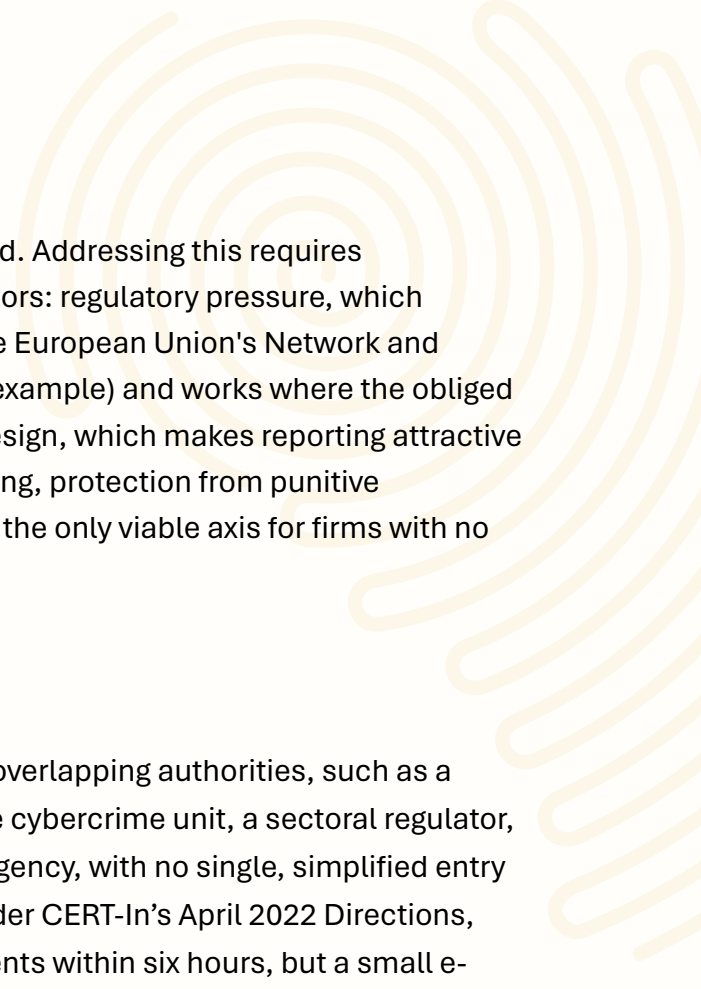
Source: The Cyber Express (2023).

Weak Links in the Reporting Chain

The reasons MSMEs do not report are not only motivational. They are structural, and they sit inside an institutional architecture that was not designed with small businesses in mind. The previous section explained why owners hesitate to report; this section explains why, even when they decide to act, the system makes acting difficult.

Across organizations, a strong reluctance to report cyber incidents persists, driven in part by a perception that reporting yields little tangible benefit. Firms experience reporting mechanisms as bureaucratic and unrewarding — reports are felt to vanish into a "data lake" rather than produce a constructive response — while engagement with regulators is associated more with the risk of scrutiny, investigation, and penalties than with protection, concerns compounded by the documented financial, legal, and reputational consequences that follow disclosed incidents (Lydon, 2022).

Reporting rates are low where they have been measured, though the measurement itself is concentrated outside the region: the UK's Cyber Security Breaches Survey found external reporting to be relatively uncommon, with organizations unclear both about whom to report to and about the impact of doing so (UK Government, 2020). No APAC-wide equivalent exists — which is both a limitation on the evidence here and an illustration of the visibility problem this brief describes.



The incentive structure is fundamentally misaligned. Addressing this requires intervention along two axes applied to different actors: regulatory pressure, which compels reporting through statutory obligation (the European Union's Network and Information Security Directive 2 being the leading example) and works where the obliged entity has the capacity to comply; and incentive design, which makes reporting attractive by offering concrete benefits — confidential handling, protection from punitive consequences, free technical assistance — and is the only viable axis for firms with no compliance function at all.

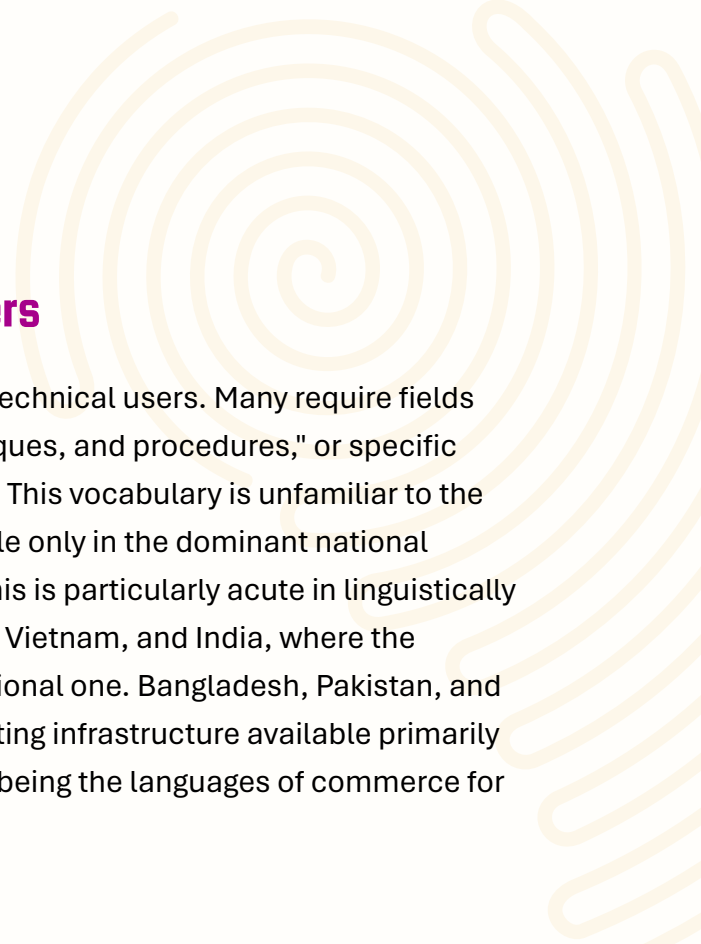
No Clear Front Door

In many APAC jurisdictions, MSMEs face multiple overlapping authorities, such as a national CERT, a data protection authority, a police cybercrime unit, a sectoral regulator, and sometimes a separate consumer protection agency, with no single, simplified entry point. India offers a particularly stark example: under CERT-In's April 2022 Directions, regulated entities must report a broad set of incidents within six hours, but a small e-commerce seller hit by an account takeover may simultaneously need to interact with the local cyber police cell, the Reserve Bank of India's payment fraud channels, and the relevant platform's own dispute mechanism (CERT-In, 2022). Even larger firms struggle to navigate this; for a micro-enterprise, the burden is functionally prohibitive.

Disconnect Between Agencies and MSMEs

Law enforcement is widely perceived by MSMEs as slow, unable to recover losses, and oriented toward investigating offenders rather than supporting victims. CERTs, where they are known at all, are typically seen as "for big companies." In India, the DSCI–Seqrite India Cyber Threat Report 2025 documented almost a million ransomware detections in 2024 across 8.44 million endpoints, with manufacturing among the most-targeted sectors, while industry commentary consistently notes that the great majority of Indian MSMEs lack a formal cybersecurity policy (DSCI & Seqrite, 2025).

In Japan, the IPA's Security Action program has reached over 300,000 self-declaring SMEs since 2017, but IPA's own 2023 survey notes that participation is frequently tied to subsidy eligibility rather than sustained, voluntary engagement with reporting and improvement (IPA, 2023).



Digital Literacy and Language Barriers

National reporting forms are typically designed for technical users. Many require fields such as "indicator of compromise," "tactics, techniques, and procedures," or specific Common Vulnerabilities and Exposures references. This vocabulary is unfamiliar to the majority of MSMEs. Further, forms are often available only in the dominant national language, excluding minority-language speakers. This is particularly acute in linguistically diverse markets such as Indonesia, the Philippines, Vietnam, and India, where the working language of small businesses is often a regional one. Bangladesh, Pakistan, and Sri Lanka face parallel challenges, with much reporting infrastructure available primarily in English despite Bangla, Urdu, Sinhala, and Tamil being the languages of commerce for most small firms.

Absence of Standardized Protocols

There is no common regional taxonomy for what counts as a "reportable incident". An owner who clicked a phishing link but caught it before transferring funds, a shop whose Instagram account was briefly hijacked, a clinic whose appointment system was locked for an afternoon, none of these may know whether they have experienced a reportable event. Academic work on safety-science-inspired reporting systems identifies definitional clarity as a core design requirement that most national regimes have not met (Ebert et al., 2025).

Fragmented Regulatory Landscape

Data protection and breach notification laws differ sharply across the region. Singapore's Personal Data Protection Act, India's Digital Personal Data Protection Act (2023), South Korea's Personal Information Protection Act each set different thresholds, timelines, and definitions for breach notification (Ooi & Teong-Lian, 2023). A cross-border MSME such as a Vietnamese seller fulfilling orders to Singapore, or an Indian Software-as-a-Service firm with customers in Australia, can face four or five overlapping regimes for a single incident. The rational response, for many, is to report to none.

What Reporting Actually Looks Like for an MSME

It is worth being concrete about what these structural failures mean in practice. The journey below follows a single composite incident through the eyes of an MSME owner — drawn from documented experiences across the region — to show how each barrier compounds the last and where the chance to protect other firms is lost. The real quotes and cases that follow then ground those friction points in evidence.

A Reporting Journey:

How an incident disappears

Consider a five-person online homeware seller, run by its owner from a phone between customer orders.

Day 0 — Discovery.

A staff member notices the marketplace account is logging in from an unfamiliar device and that the payout bank details have been changed. The owner realizes money may already have moved.

Hour 1 — Where do I even report?

There is no obvious front door. Is this a matter for the police, the bank, or the national CERT she has vaguely heard of but assumes is “for big companies”? The one official form she finds asks for an “indicator of compromise” and is only in the national language, not the regional one she trades in.

Day 1 — The platform, and only the platform.

She does the one thing that feels concrete: she reports through the marketplace app’s in-product flow and resets her password. This is rational — the platform controls the account — but it routes the incident into a private support queue, not any public channel.

Weeks 1–3 — Waiting.

Recovery of the account takes weeks. There is no human to call, no case number that means anything outside the platform, and no advice on what else to secure or whether customer data was taken. Business limps along on a personal account in the meantime.

The CERT is never contacted.

By the time the account is restored, the incident is “over” from the owner’s point of view. It is never reported to a national authority, so the attack pattern — credential theft and payout redirection on that specific platform — never enters national or regional threat intelligence. The next twenty sellers hit by the same technique get no warning.

Every decision in this sequence is individually rational. The cumulative result is that a real, repeatable attack technique stays invisible to everyone positioned to warn other MSMEs — and the owner receives no faster recovery, technical help, or continuity support in return for the report she did make. That is the gap each recommendation in Section 5 is built to close.

Composite scenario, drawn from documented MSME reporting experiences across the region; illustrative, not a single real case.

The real quotes and cases below ground each of these friction points in evidence from across the region.

QUOTES FROM MSMEs IN THE PHILIPPINES

Women MSME: I don’t report [a] scam because I’m afraid to admit that I got scammed. This shows that I am vulnerable, and my customers might not buy from me anymore.

Young MSME: Scam reporting is confusing. I don’t know how and where to report. I only report to GCash app (Philippines-based E-Wallet), but sometimes it takes time to get feedback and my money back.

QUOTES FROM MSMEs IN SOUTH KOREA

Account takeover: I realized my business’s social media account had been hacked after a friend alerted me. The password and profile photo had been changed, and the account was being used to promote unrelated advertisements. I could not identify who was responsible or report the incident, but I eventually regained access through identity verification and now regularly check the account for signs of unauthorized access.

Instagram impersonation: I discovered that someone had created an Instagram account impersonating me and contacted me after acquaintances alerted me to it. I reported the account to Instagram, but my initial report was rejected. It was only removed about a month later after other users also reported it.



JAPAN: WHY MANY MSMEs SAY THEY ARE RELUCTANT TO REPORT CYBER INCIDENTS

Japanese MSMEs are often reluctant to report cyber incidents because they lack the resources, procedures, and recovery capacity needed to manage the consequences.

Many MSMEs do not have dedicated cybersecurity personnel or established incident-response processes. Limited experience can delay decisions on whether to involve external specialists and make it difficult to coordinate the initial response.

Business continuity is another major concern. Reporting and investigating an incident may disrupt essential systems such as ordering, accounting, and inventory management. Responsibilities may also be unclear across management, staff, and external providers, causing information to become fragmented or inconsistent.

Weak backup and recovery systems further increase the perceived risk. Backups may be incomplete, unavailable, or affected by the same malware or ransomware as the primary systems.

Cybersecurity investment also tends to be reactive. Some Japanese MSMEs only introduce stronger controls after experiencing an incident, rather than preparing in advance. Together, these factors can make reporting appear operationally burdensome and potentially damaging to the business.

Policy Takeaway:

The barriers to reporting are structural, not attitudinal. There is no clear front door; intake forms are technical and often available only in the dominant national language; there is no shared definition of what counts as a reportable event; and cross-border firms face several overlapping regimes at once. Each barrier points to a specific remedy — a single MSME-facing front door, localization into working languages, plain-language definitions, and confidential handling that lowers the risk of coming forward — which the recommendations in Section 5 take up directly.

Building a Culture of Transparency

Diagnosis is only useful to the extent that it shapes a more effective response. Accordingly, this section outlines the characteristics of a healthier MSME reporting ecosystem and highlights why its development serves broader economic interests, extending well beyond the concerns of regulators.

From Reactive to Proactive Reporting

The most useful conceptual reference comes from aviation safety. Modern aviation has been transformed by the principle of a "just culture," in which the reporting of near-misses, mistakes, and system failures is normalized, non-punitive, and structured to produce learning rather than blame (Reason, 1997; Dekker, 2007). The result is an industry that fails rarely and learns publicly when it does. Cybersecurity, by contrast, still treats incidents primarily as failures to be hidden.

Importing the just-culture principle, with appropriate confidentiality protections, would change the calculation for MSME owners considering whether to report (Ebert et al., 2025). ASEAN has already accepted the principle for one constituency: the ASEAN Cybersecurity Cooperation Strategy 2026–2030 proposes an ASEAN Guideline on Responsible ICT Vulnerability Reporting incorporating a standard operating procedure on confidentiality for disclosure (ASEAN, 2026). What is proposed for security researchers is precisely what MSMEs need and do not have. One case from the region shows how far current practice still sits from that posture, even at its best.

NIDEC CORPORATION, VIETNAM — MID-2024

A Vietnam-based Nidec Corporation subsidiary was breached via stolen virtual private network credentials; attackers exfiltrated more than 50,000 files, including invoices and supplier correspondence. Nidec went further than most breached firms in the region — it issued public notices and committed to warning affected partners. But the notice followed publication of the stolen files rather than detection of the breach, so the warning arrived after the exposure it was meant to pre-empt. Even the region's strongest disclosure practice is calibrated to reputational management rather than downstream defense.

Source: Nidec Corporation (2024); BleepingComputer (2024).

Trust-Building as Infrastructure

Trust is not an abstract aspiration. It is built or broken by specific design choices such as anonymity options, liability shields, confidentiality of trade-sensitive information, and clear limits on how reported data can be used. Above all, trust is built when reporting brings something tangible in return. A reporting system that responds to an MSME report with a phone call from a real person, free incident-response advice, and a confidential threat-intelligence update will, over time, be used. One that responds with a request for additional documentation and an audit notice will not. In turn, it provides better data to set up better preventive or responsive measures, both for MSMEs and the supply chain partners depending on them.

The Economic Case for Transparency

Public reporting of aggregated cyber incident data, without identifying individual victims, is a public good. It helps insurers assess and price cyber risk more accurately, enables supply-chain partners to make informed due diligence decisions, and gives investors greater confidence in the resilience and transparency of the digital economy. In contrast, when major cyber incidents occur in environments with limited transparency, they often trigger disproportionate concern because outsiders lack the broader context needed to understand the true level of risk. In this way, transparency is not merely a governance practice; it is an economic asset that supports trust, investment, and market stability.





Long-Term Competitiveness

A region that can credibly map and respond to MSME-level threats builds a more defensible digital single market. Two regional instruments now set the terms. The ASEAN Digital Economy Framework Agreement reached substantial conclusion of negotiations in October 2025 and is on track for finalization in 2026, which moves the opportunity from negotiation to implementation.

The ASEAN Cybersecurity Cooperation Strategy 2026–2030, published in April 2026, sets five dimensions and a slate of initiatives for the next five years — and does not mention MSMEs or SMEs once. The segment that comprises 99.8 percent of the region's enterprises is absent from the strategy governing its cybersecurity through 2030. Annual work-planning under the strategy, rather than a drafting window, is therefore where MSME-specific reporting commitments would now have to enter.

South Asia, while not subject to ASEAN, has parallel opportunities through the South Asian Association for Regional Cooperation's digital cooperation track, through bilateral arrangements between India and partner economies, and through the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation framework.

Policy Takeaway:

A just-culture posture, paired with a fast and tangible response, turns reporting from a risk into a service. Reporting then becomes the gateway to faster recovery, free technical assistance, restored business continuity, and threat intelligence that protects the next MSME — rather than an admission of failure that invites scrutiny. Reporting should not be framed as a duty businesses owe to the state. It should be a benefit that the state provides to businesses.

When organizations report an incident, they should gain access to support, intelligence, and a clear path to recovery — not additional costs, scrutiny, or uncertainty. If reporting creates value, businesses will participate. If it creates a burden, they will remain silent. Every recommendation that follows is built on this simple principle: make reporting useful, and reporting will increase.

Recommendations

The recommendations below are organized by audience and prioritized for feasibility. Each is designed to be actionable in low-capacity settings and to map back to a specific barrier identified earlier in the brief.

FOR MSMEs



Adopt a one-page incident response plan and test it periodically.

Scaled to a business of fewer than 20 employees and written in the working language of the firm, the plan should answer four questions: who do we call first, what do we save, what do we change, and when do we tell customers. Templates already exist through the Global Cyber Alliance MSME Toolkit and the APAC Cybersecurity Fund's MSME curriculum (The Asia Foundation, 2024a). Test this plan annually to make sure it works in practice.

Use lightweight reporting channels where they exist.

WhatsApp, Line, and Zalo reporting channels operated by national authorities, where available, lower the threshold for first contact. Singapore's ScamShield and Japan's IPA SME consultation services offer useful reference models.

Designate a "first call" inside the business.

In firms without IT staff, this is usually the owner or a trusted relative. Naming the role in advance and saving the relevant numbers (bank fraud line, platform support, national CERT) in a single visible and offline (printed) place removes the friction of looking them up at 9 p.m. on a Friday.

Participate in peer networks.

MSME-to-MSME knowledge transfer is consistently the most trusted form of cybersecurity learning across APAC surveys. Business associations, sector chambers, and local industry groups are the most realistic vehicles.



Establish a simplified, MSME-specific reporting front door.

A single number or portal, in local languages, with a plain-language intake form and a guaranteed human response within a defined window. Singapore CSA's SG Cyber Safe initiative and Japan's IPA SME consultation channels offer useful starting points. The default should be confidential handling, with public reporting only of aggregated, anonymized data.

Introduce concrete incentives for reporting.

Legal safe harbors from punitive damages for firms that report in good faith (modeled on US state laws including Ohio in 2018, Connecticut in 2021, Iowa in 2023, and Texas in 2025), subsidized incident-response vouchers, and tax credits for MSMEs that adopt recognized frameworks such as Center for Internet Security Controls Implementation Group 1 or the US National Institute of Standards and Technology Cybersecurity Framework 2.0. The principle is simple: reporting should produce help, not paperwork.

Translate reporting infrastructure into working languages.

Bahasa Indonesia, Vietnamese, Thai, Tagalog, Hindi, Bangla, Urdu, Sinhala, Tamil, and the major regional languages of India and the Philippines should be supported as a baseline. This is a comparatively low-cost intervention with disproportionate impact.

Strengthen regional cooperation through the ASEAN Regional CERT and equivalents.

The ASEAN Regional CERT, established in October 2024 and based in Singapore, received a commitment of USD 10.1 million over ten years. Its Information Sharing Mechanism was introduced in 2025 (CSA Singapore, 2024; ASEAN, 2026). Extending that mechanism to receive anonymized MSME-segment telemetry from member-state CERTs is an incremental change to a live system, not a new build. Goal 1.3 of the ASEAN Cybersecurity Cooperation Strategy 2026–2030 already tasks the Regional CERT with developing links to business associations and private-sector partners.

For South Asia, parallel mechanisms, whether through the South Asian Association for Regional Cooperation, bilateral India-led arrangements, or the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation's digital cooperation track, should be actively explored.

Use procurement and licensing as a lever on large entities, not small ones.

Condition public procurement contracts, and digital platform licensing, on the supplier's or platform's participation in confidential incident reporting and on its obligation to pass warnings down to the small firms in its chain. Obligation should sit where capacity sits. Attaching reporting conditions to business registration renewal for micro-enterprises should be avoided: it converts reporting back into the compliance burden this brief argues against, for precisely the firms least able to absorb it.

Fund and publicize the value of reporting.

A small share of national cyber budgets should be allocated to producing public, MSME-readable annual threat reports based on reported incident data. The objective is to make it tangible that reporting produces useful, sector-specific intelligence that other MSMEs can act on.

Adopt a "just culture" posture toward breached MSMEs, in official and media communications alike.

A firm that reports in good faith should be treated as a victim and early-warning sensor, not a culprit to be named — modeled on NASA's confidential, non-punitive Aviation Safety Reporting System (ASRS), run separately from the regulator to keep reporting safe. National cyber agencies should extend the same norm to the press, framing incidents around systemic causes rather than the "careless employee who clicked." As long as the problem is framed as sitting between the chair and the keyboard, reporting will be punished by reputation.



FOR INDUSTRY AND SERVICE PROVIDERS



Build one-click breach reporting into widely used MSME platforms.

Shopee, Tokopedia, Lazada, Flipkart, Rakuten, Grab, GoTo, Google Workspace, and Microsoft 365 together touch the majority of APAC MSMEs. An in-product button labeled “I think my account has been compromised” or “I suspect a cyberattack,” with optional onward reporting to a national CERT, would lower the reporting threshold.

Offer tiered, accessible security services.

Priced and scoped for the under-20-employee segment, with local-language onboarding and pre-configured defaults. Free baseline protection (multifactor authentication on by default, suspicious login alerts, automatic backups) should be the floor, not an upsell.

Share anonymized threat intelligence upstream.

Platform telemetry from MSME accounts is among the richest sources of attack-pattern data in the region. Structured, anonymized sharing with national CERTs and the ASEAN Regional CERT, under clear privacy protections, would help close the visibility gap directly.

Standardize post-incident support.

Account recovery, evidence preservation, and clear escalation paths should be uniform across platforms. Recovery processes that currently take weeks should be measured in hours for verified business accounts.

Engage business associations and chambers as distribution partners.

Reaching the most informal segment of the MSME economy requires intermediaries trusted by the firms themselves. Local chambers in Vietnam, Bangladesh, the Philippines, and Indonesia have been effective channels for prior digitalization programs and are the most realistic route for cybersecurity capacity-building at scale.

Call to Action

The reporting gap in APAC is not a technical problem. It is a design problem, and it can be fixed. MSMEs are not failing to report because they do not care. They are failing to report because the systems built to receive their reports were not built for them. The Filipina seller who stays silent because admitting she was scammed would cost her customers; the young entrepreneur who reports only to her e-wallet because she does not know where else to go; the Korean owner who could not identify who took over her account or where to report it; the Japanese firm that judges the investigation more disruptive than the breach — each is making a rational decision inside a poorly designed incentive structure.

Closing the gap requires meeting these firms where they are. That means reporting channels in working languages, in formats that fit the time, value, and attention of a small business owner, with confidentiality protections that are credible and concrete benefits that are visible. It means treating reporting as a service that the state and the platforms offer to MSMEs, not as a compliance burden the state imposes on them. And it means recognizing that aggregate, anonymized transparency is a regional public good — one that strengthens investor confidence, supply-chain resilience, and the credibility of APAC as a digital-economy partner.

The instruments are in place; what is missing is MSME-specific content inside them. The ASEAN Digital Economy Framework Agreement is moving to implementation and the ASEAN Cybersecurity Cooperation Strategy 2026–2030 is now in its first year — both are shaped from here by work-planning rather than drafting. South Asia's digital cooperation tracks, and the APEC digital economy agenda each offer parallel routes. Governments, platforms, business associations, and MSMEs themselves each have a role, and each must act on it. Reporting is not the end of an incident. It is the beginning of a defense that works for the businesses that make up most of the region's economy.

References

- ASEAN (2026). ASEAN Cybersecurity Cooperation Strategy 2026–2030. Jakarta: ASEAN Secretariat, April 2026. Author: ASEAN Network Security Action Council.
- The Asia Foundation (2024a). APAC Cybersecurity Fund Overview. The Asia Foundation, CyberPeace Institute, Global Cyber Alliance, and Google.org.
- The Asia Foundation (2024b). From Vulnerability to Resilience: Cybersecurity Challenges for MSMEs in the APAC Region.
- Asian Development Bank (2025). Asia Small and Medium-Sized Enterprise Monitor 2025.
- BleepingComputer (2024). Tech giant Nidec confirms data breach following ransomware attack.
- BSSN — Badan Siber dan Sandi Negara (2024). Statements on the PDNS 2 ransomware incident, Surabaya.
- CERT-In (2022). Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents.
- Cloudflare (2024). Navigating the New Security Landscape: Asia Pacific Cybersecurity Readiness Survey. Survey of 3,844 cybersecurity leaders across 14 APAC markets, June 2024.
- CSA Singapore (2024). Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region (9th AMCC press release, October 16, 2024); Establishment of ASEAN Regional CERT (background materials).
- The Cyber Express (2023). Mercedes' Battery Manufacturer in Thailand Targeted by Qilin Ransomware Group.
- CYFIRMA (2024). Weekly Intelligence Report — 01 Nov 2024.
- Dekker, S. (2007). Just Culture: Balancing Safety and Accountability. Ashgate.
- DSCI & Seqrite (2025). India Cyber Threat Report 2025. Data Security Council of India and Seqrite (Quick Heal).
- Ebert, N., et al. (2025). Learning from safety science: designing incident reporting systems in cybersecurity. *Journal of Cybersecurity*, 11(1).
- Information-technology Promotion Agency (IPA), Japan (2023). Survey of Information Security Measures Among Security Action Declaring Enterprises.

Lydon, L. (2022). Corporate under-reporting of cybercrime: Why does reporting to authorities matter? Royal Holloway Information Security Thesis Series (published via Computer Weekly).

Ministry of Electronics & Information Technology (MeitY), Government of India (2022). Year-wise cyber security incidents tracked by CERT-In, 2018–2021.

Ministry of MSME, Government of India (2024). MSME Trade Enablement and Marketing (MSME-TEAM) Initiative announcement.

NASSCOM & DSCI (2022). Representation to CERT-In on the Cyber Security Directions.

Nidec Corporation (2024). Security Incident at a Nidec Group Company (Report No. 2). Official notice.

Ooi, K.-B. & Teong-Lian, A. (2023). Cybersecurity incident reporting laws in the Asia-Pacific. *International Cybersecurity Law Review*, Springer.

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate.

Reuters (2022). Toyota suspends domestic factory operations after suspected cyber attack.

Sangari et al. (2022). Modeling Under-Reporting in Cyber Incidents. *Risks*, vol. 10, issue 11.

Security Affairs (2024). A cyberattack halted operations at Varta production plants.

SecurityWeek (2024). Cyberattack Disrupts Production at Varta Battery Factories.

Teikoku Databank (2022). Survey on Cyberattacks at Japanese Firms (online survey, March 11–14, 2022; 1,547 respondents).

Teikoku Databank (2025). Cyberattack Survey (online survey, May 2025; 10,645 valid responses).

UK Government (2020). *Cyber Security Breaches Survey 2020*. Department for Digital, Culture, Media & Sport.

UNODC (2013). *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.

UNODC. Education 4 Justice University Module Series: Cybercrime, Module 5 — Cybercrime Investigation.

Verizon Business (2025). *2025 Data Breach Investigations Report: Small- and Medium-Sized Business Snapshot*.

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 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

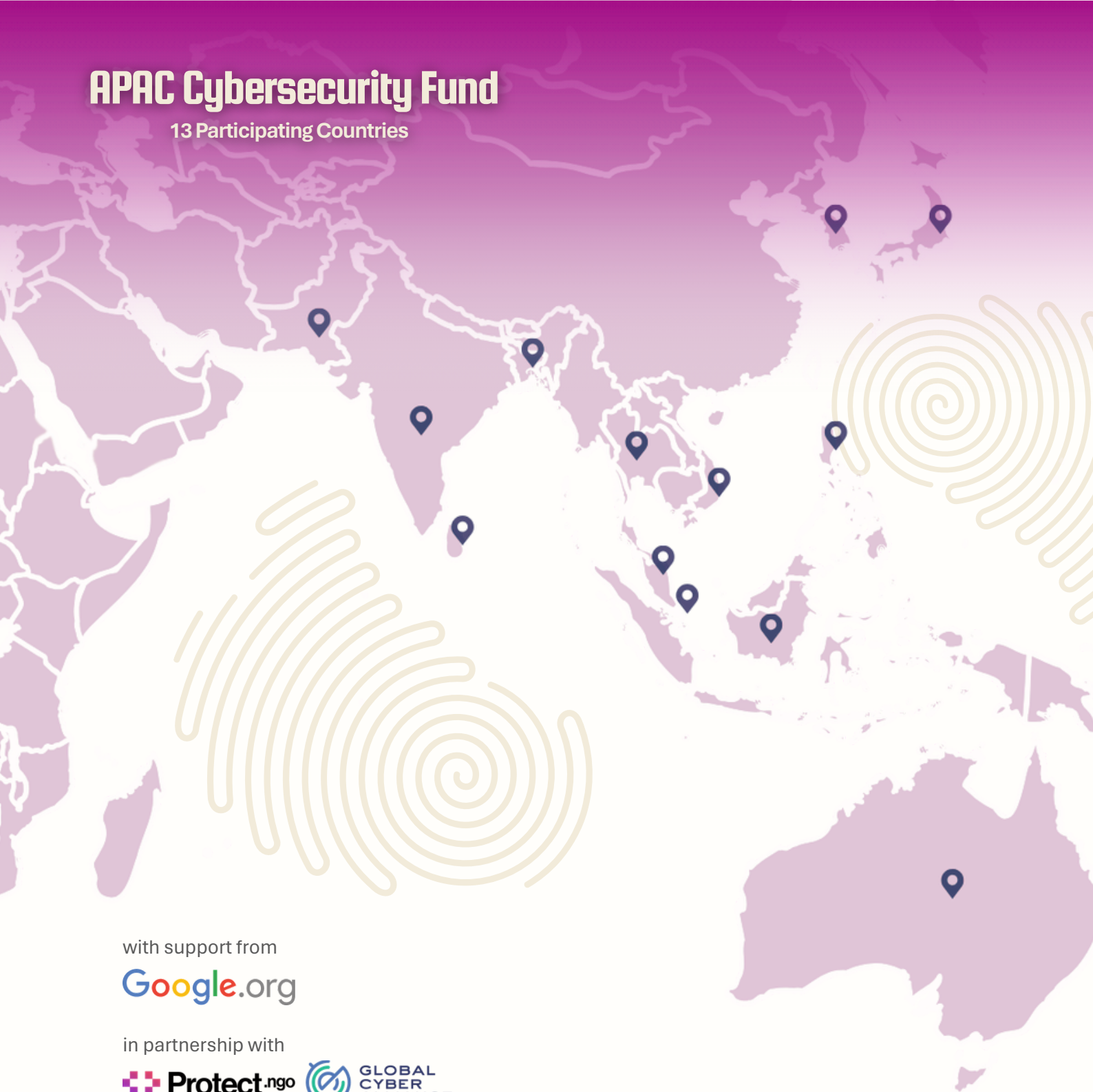
The Asia Foundation is an international nonprofit organization working to solve the toughest social and economic challenges in Asia and the Pacific. Informed by more than 70 years of experience and deep local knowledge, we work with partners across more than 20 countries to improve lives and expand opportunities.

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



The Asia Foundation
www.asiafoundation.org

© The Asia Foundation 2026