APAC Cybersecurity Fund
The Asia Foundation

EXPOSURE TO EMPOWERMENT

Strengthening Micro, Small, and Medium Enterprises in the Age of AI

Overview:

Across the Asia-Pacific, Micro, Small, and Medium Enterprises (MSMEs) are rapidly adopting AI to enhance efficiency, reach new customers, and reduce operational costs. However, this adoption is often taking place without adequate safeguards, exposing MSMEs to unprecedented cyber, operational, and reputational risks. The dual impact of AI—empowering growth while amplifying threats—demands urgent action from policymakers, technology providers, and business networks.

AI Opportunities for MSMEs

AI is helping MSMEs close capability gaps with larger firms by enabling:

CUSTOMER ENGAGEMENT

- Chatbots and virtual assistants provide 24/7 support.
- **Example:** Vietnam logistics firms use GenAI assistants to manage communication surges during peak hours.

OPERATIONAL EFFICIENCY

- AI supports inventory management, predictive analytics, and demand forecasting.
- **Example:** Indian fashion brands use AI to reduce overstock and waste.

CONTENT CREATION & MARKETING

- Generative AI allows MSMEs to create low-cost marketing materials and real-time product creatives.
- **Example:** Early adopters in Indonesia report significant cost savings and reduced staff workloads

FINANCIAL MANAGEMENT

- AI tools detect fraud, flag anomalies, and automate financial reporting.

HR & INTERNAL OPERATIONS

- AI improves recruitment, employee engagement, and attrition prediction.

in partnership with CyberPeace Institute GLOBAL CYBER ALLIANCE with support from Google.org

AI Threats to MSMEs

EXTERNAL THREATS

- **Deepfake fraud & impersonation:** AI-generated voices/videos used to trick staff into transferring money or sharing data (sharp rises in India, Philippines, Vietnam).
- **Phishing-at-scale:** Generative AI produces highly realistic, localized phishing messages.
- **AI-powered reconnaissance:** Criminals map targets online presence to craft tailored attacks.
- **AI-generated malware:** Tools like WormGPT and DarkBard allow non-experts to generate malicious code.
- **Biometric exploitation:** Deepfake faces used to bypass authentication.

INTERNAL THREATS

- **Shadow AI:** Employees using unauthorized AI tools expose sensitive data.
- **Lack of AI governance:** No clear policies lead to inconsistent security practices.
- **Talent/knowledge gaps:** MSMEs lack staff with AI security expertise.
- **Reliance on inaccurate AI outputs:** Risks legal, financial, and reputational harm.

BRAND REPUTATION RISKS

- AI changes how businesses are discovered online.
- **Risks include:** brand sabotage, fake reviews, misinformation, and loss of control over how AI summarizes a business.

Recommendations

FOR MSMES WITH LOW DIGITAL MATURITY

- Share a simple AI-use policy internally.
- Provide micro-trainings during regular meetings.
- Conduct monthly online checks on brand presence.
- Implement the "Verify, Don't Trust" rule for payments or data requests.

FOR TECHNOLOGY PROVIDERS

- Offer secure, affordable AI tools for MSMEs.
- Participate in public-private threat-intelligence sharing.
- Provide AI-enabled tools for brand protection and fraud detection.

FOR MSMES WITH HIGHER DIGITAL MATURITY

- Develop a living AI governance policy.
- Offer structured AI/cybersecurity training.
- Use affordable tools to track brand reputation online.
- Establish formal verification controls (e.g., call-back systems, dual approval).

FOR GOVERNMENTS & POLICYMAKERS

- Fund training programs in AI and cybersecurity.
- Introduce AI "trust labels" indicating tool safety.
- Create AI regulatory sandboxes for safe experimentation.
- Develop ethical and regulatory frameworks to curb misuse.
- Promote regional cooperation to counter cross-border AI cybercrime.

Sources: Desk research and key informant interviews conducted by the CyberPeace Institute (CPI) and The Asia Foundation (TAF). Unpublished internal research, year not specified.

Call to Action

The rise of AI presents both a monumental opportunity and a significant threat to MSMEs. It is imperative that all stakeholders—governments, tech companies, and MSMEs—act now to build a secure, resilient, and inclusive digital ecosystem that allows these vital enterprises to thrive. The time to move from observation to action is now, ensuring that AI becomes a catalyst for growth rather than a vector for exploitation.