Critical Infrastructure Protection: Collaboration, Policy Drivers and the CIP Continuum

ITU Regional Cybersecurity Forum for Asia Pacific

Julie Inman Grant, Director of Internet Safety and Security Microsoft Asia Pacific

Vision

Critical Software and Services: trustworthy, resilient, and innovative

Mission

Advance the integrity and resiliency of critical software and services through trusted relationships, effective policies, and transparent practices.

- ## What are they?
  - *Critical infrastructures* are generally thought of *as the key systems, services, and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and/or national security*.

  - *These include, but are not limited to, communications, energy, banking, transportation, public health and safety, and essential government services.*

Government

"What's the goal"

Public-Private Partnership

"What's critical"

Infrastructure

"Prioritize Risks"

Operators

"Best control solutions"

Define Policy and Identify Roles

Determine Acceptable Risk Levels
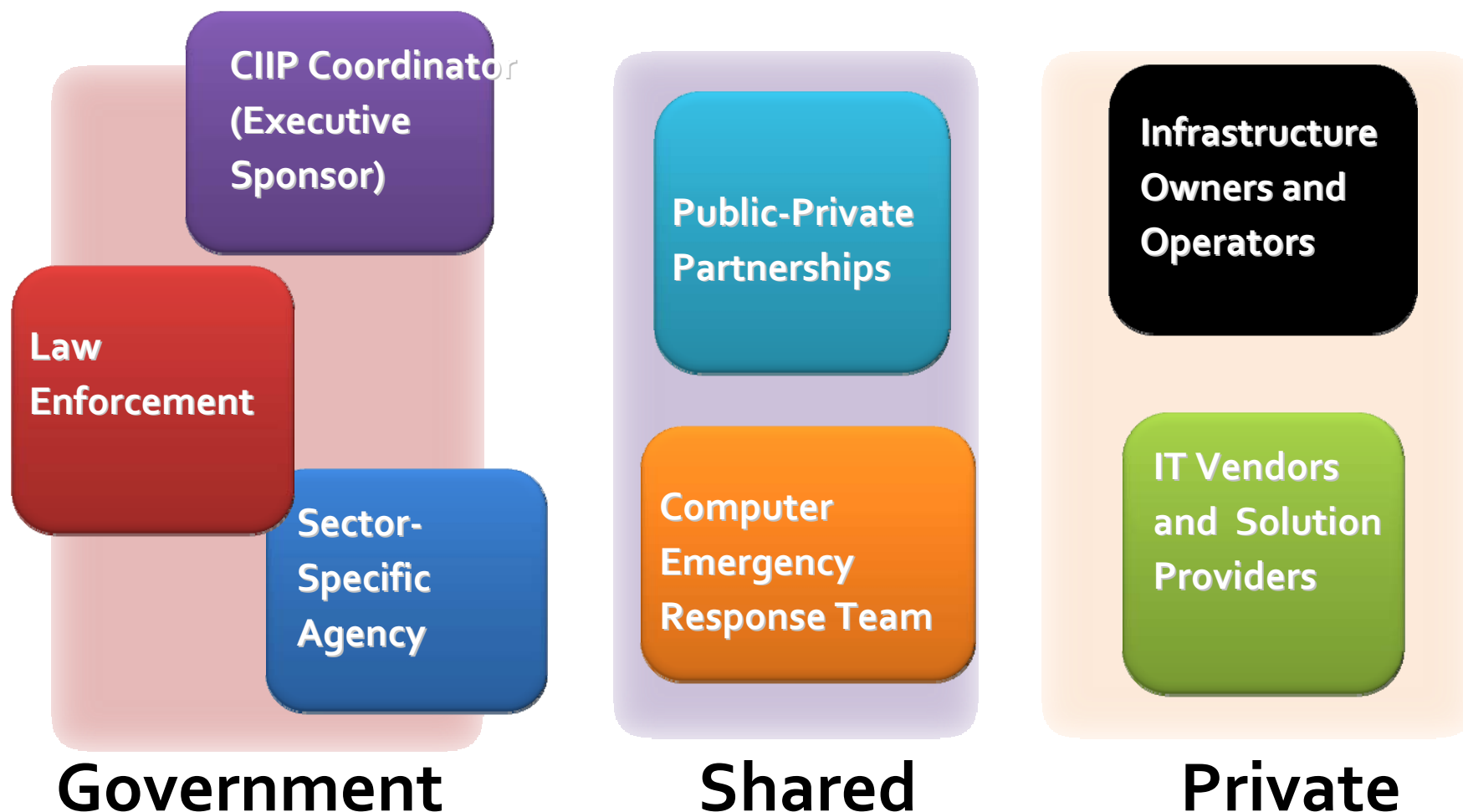
Measure Effectiveness

Assess Risks

Implement Controls

Identify Controls and Mitigations

Define Roles

Understanding roles and objectives promotes trust and efficiency

CIIP Coordinator (Executive Sponsor)

Law Enforcement

Sector-Specific Agency

Public-Private Partnerships

Computer Emergency Response Team

Infrastructure Owners and Operators

**IT Vendors and Solution Providers**

Government

Shared

Private

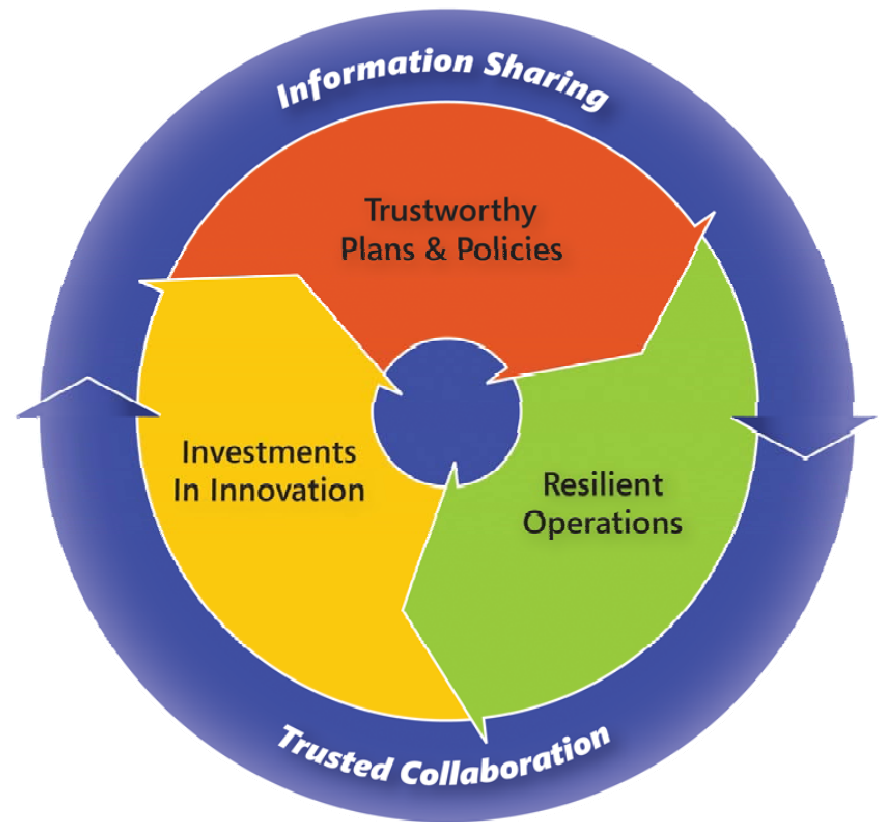# Defining Precise Industry Roles and Partnerships is Equally Critical

ICASI is a collaborative effort among the leading global IT vendors committed to:

• Increasing the speed and effectiveness of multi-vendor, cross-product, and cross-border security response

• Developing a common operational response protocol

• Sharing knowledge of current and future threats
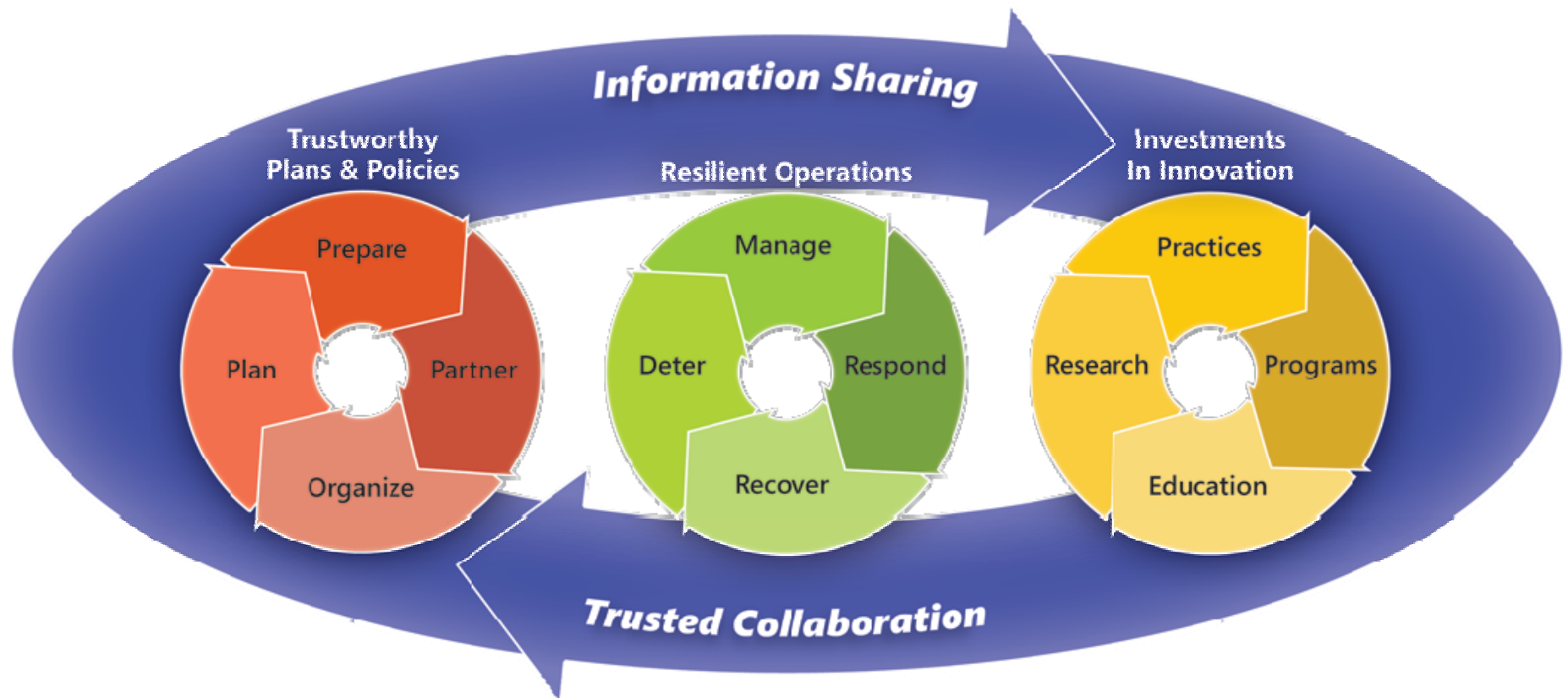
• Providing industry expertise on
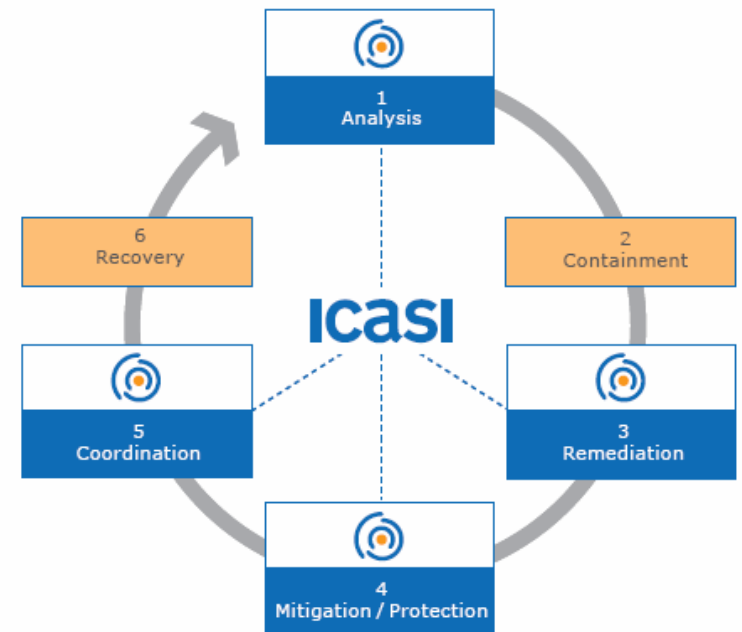
CIP and Microsoft

- In 2002, Microsoft established Trustworthy Computing as a top company priority.

- Our commitment to TWC extends beyond the desktop to the broad cyber ecosystem.

- Drawing upon its work with global partners, coupled with more than three decades of its own experiences, Microsoft has learned that effective critical infrastructure protection efforts share three central areas of focus.
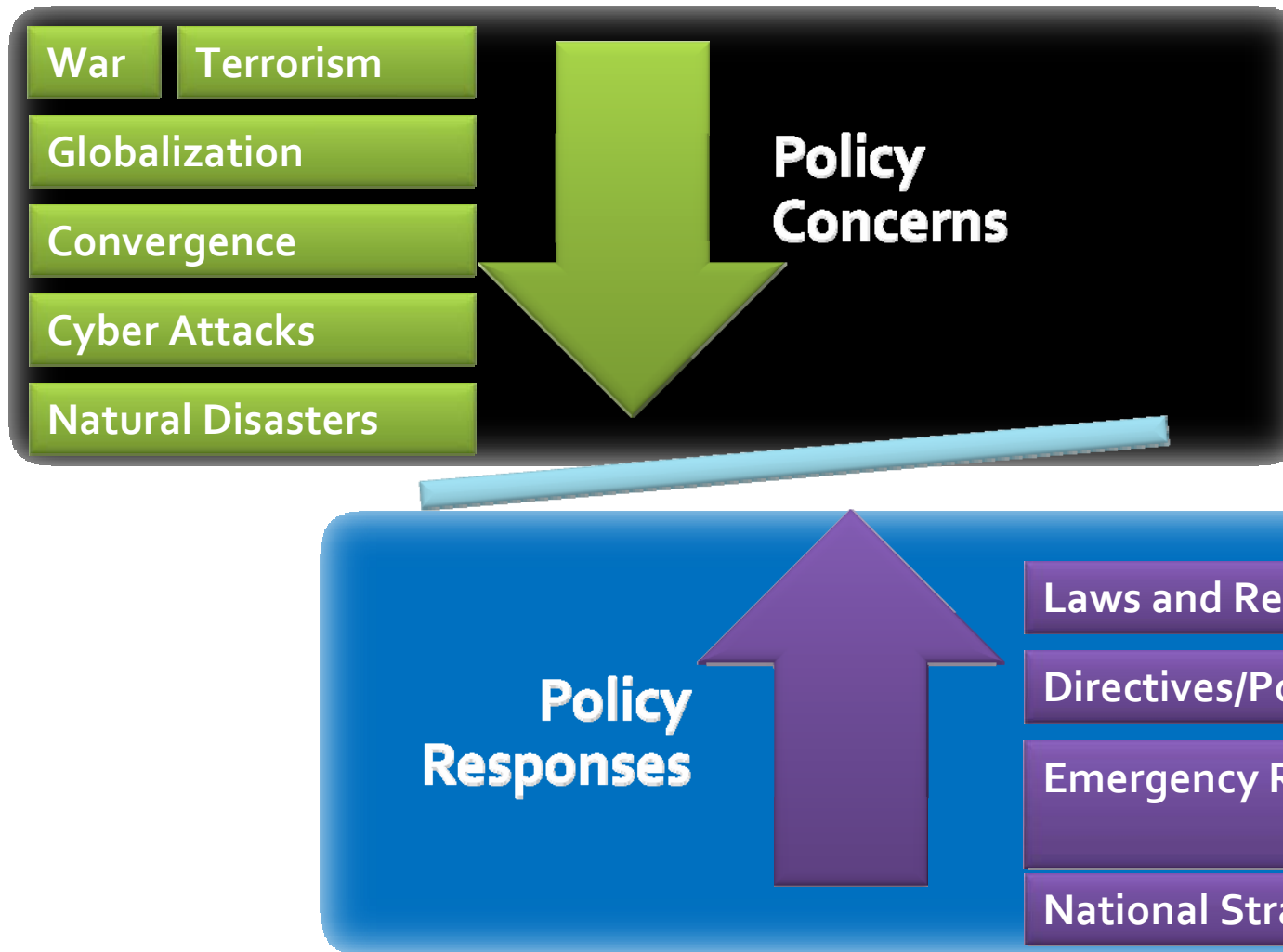
CIP Continuum Overview

CIP Policy Drivers

Understanding the policy context is key to success

War

Terrorism

Globalization

Convergence

Cyber Attacks

Natural Disasters

Policy Concerns

Policy Responses

Laws and Regulations

Directives/Policies

Emergency Response Plans

National Strategies

Cybercrime legislation

- Cybercrime legislation is essential to building trustworthy plans and policies and ultimately enabling resilient operations
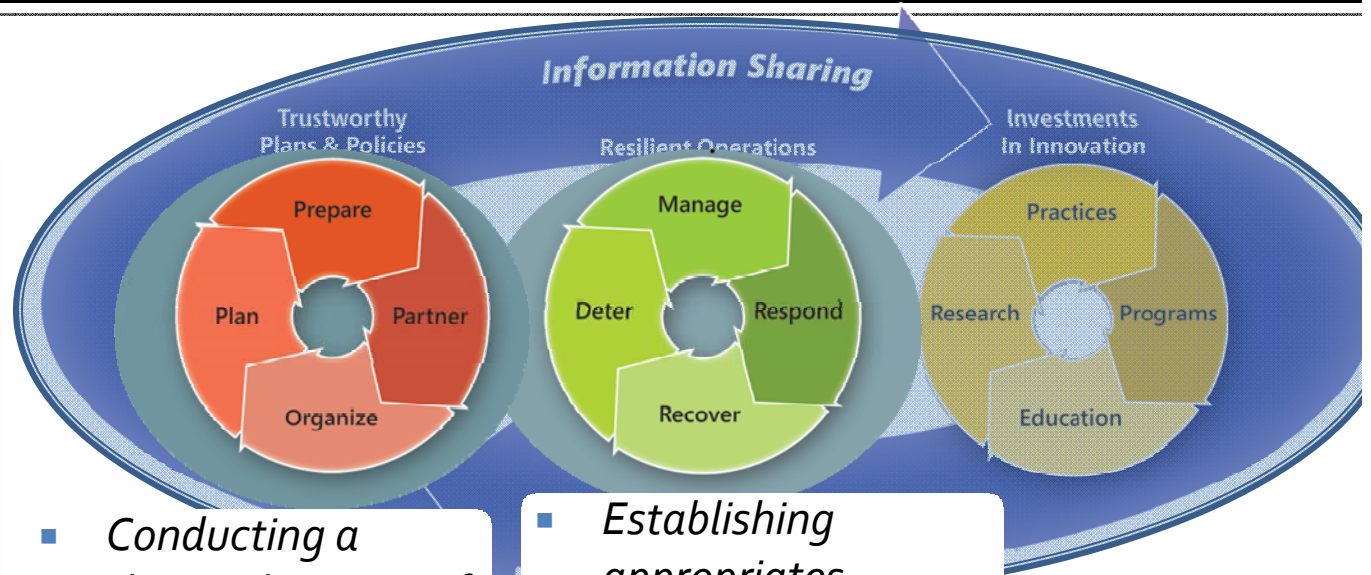
- *Conducting a thorough review of existing cybercrime laws is an important part of preparing for developing national CIP strategies/plans.*

- *Establishing appropriates statutes and developing LE capabilities increase national capabilities for risk management, incident response and long-term deterrence of crime.*

Cybercrime: An Analysis of Current and Pending Laws in Asia Pacific

- Regional study of computer security, privacy, spam and online child safety laws
- Updated in October 2007
- Covers fourteen countries in the Asia Pacific region

Australia	Japan	South Korea
China	Malaysia	Taiwan
Hong Kong	New Zealand	Thailand
India	The Philippines	Vietnam
Indonesia	Singapore	

- Domestic laws compared against benchmark legislation

Computer security benchmark legislation

Council of Europe Convention on Cybercrime (2001)

⇒ **Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems**

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices

⇒ **Title 2 of the Convention on Cybercrime – Computer-related offences**

- Computer-related forgery
- Computer-related fraud

⇒ **Title 5 of the Convention on Cybercrime – Ancillary liability and sanctions**

- Attempt and aiding or abetting
- Corporate liability

Alignment of enacted computer security laws with benchmark legislation

Favourable Alignment	Moderate Alignment	Weak Alignment
Australia	China	India
New Zealand	Hong Kong	Indonesia*
Singapore	Japan	
Taiwan	Malaysia	
Thailand	The Philippines	
	South Korea	
	Vietnam	

Thank You

www.microsoft.com/asia