Asia-Pacific
Economic Cooperation

APEC Considerations for Communicating Cybersecurity Practices

Communicating Cybersecurity Risk

APEC economies recognize the importance of cybersecurity to the digital economy. Cybersecurity risk has only grown since the start of the COVID-19 pandemic, and APEC economies understand the urgency of building capacity around cybersecurity to support economic growth and facilitate trade.

Increasingly, economies around the globe are implementing confidence mechanisms to communicate cybersecurity risk to stakeholders. Confidence mechanisms provide an established process by which the user can rely on someone or something, drive improvement, and strengthen a sustainable and scalable business case. Cybersecurity confidence mechanisms can include traditional conformity assessment procedures in the form of certification, labeling, and other policies. While economies can build cybersecurity confidence mechanisms within their economies, diverging policies within the APEC region would create a fragmented regulatory landscape and barriers to trade. In the spirit of APEC's underlying approach of economic integration in the region, by aligning approaches, APEC economies can improve market access and enhance cybersecurity.

Considerations for Policy Development

During the March 2021 APEC Sub-Committee on Standards and Conformance (SCSC) workshop on “Communicating Cybersecurity Practices”, APEC economies discussed best practices for communicating cybersecurity risk to stakeholders. The cybersecurity landscape is constantly shifting, which creates challenges to communicate risk to stakeholders. Workshop participants encouraged economies to consider existing resources and practices when developing policies for communicating cybersecurity risks, as well as promoting information and experience sharing amongst economies. APEC economies noted the importance of utilizing existing globally recognized standards to communicate cybersecurity practices and encouraged global trading partners not to advocate for regional, domestic, or unique standards as a tool to limit competition or reduce market access. Where there are gaps not met by existing standards, APEC economies should work to develop them through consensus-based processes.

Based on mutual sharing of economy insights and experiences, APEC members recognize the following suggestions policymakers should consider before creating a new policy for communicating cybersecurity practices:

1. Build and increase awareness on the importance of cybersecurity to the digital economy. APEC economies noted the importance of building trust with stakeholders through cybersecurity education, awareness building, demonstrating the real-world impact of cyber-attacks, and other engagement tools.

2. Recognize voluntary partnerships and joint efforts with device manufacturers and service providers to encourage them to share cybersecurity information with consumers.

3. Consider the differences in cybersecurity risk management versus traditional physical risk management. Signaling cybersecurity risk to stakeholders may involve new processes for economies.

4. Understand the landscape: Examine existing policies and approaches to understand what globally recognized standards, conformity assessment procedures, and other confidence mechanisms already exist or are in the process of being developed. Consider whether these existing conformity assessment procedures may meet the needs of the stated objective of the policy under development and can be mutually recognized or implemented in a neutral and non-discriminatory manner.

5. Avoid creating an economy-specific policy when regional or global approaches exist and meet the defined objectives. Global approaches reduce fragmentation, facilitate trade, and can effectively address cybersecurity risks.

6. If a new policy is determined to be necessary, ensure it is risk-based and founded on voluntary, consensus-based, globally recognized standards. APEC economies recognized the importance of globally recognized standards to facilitate interoperability, build trust, and improve market access, especially for small and medium sized enterprises (SMEs).

7. Create a clear and narrowly defined scope and definition of success for what the policy is trying to accomplish.

8. Implement an inclusive consultation process that includes all relevant stakeholders, both domestic and international. Consider post-implementation outreach to these stakeholders to explain how the policy was developed and plans for alignment with other approaches.

9. Maintain transparency in the policy-making process. If an economy is developing a technical regulation or conformity assessment procedure, notify the WTO Technical Barriers to Trade Committee and allow for at least a 60-day comment period.

10. Allow for flexibility in the policy to accommodate for vulnerability disclosures and lifecycle considerations. In the ever-changing cybersecurity landscape, threats are constantly evolving. APEC economies recognize that devices may still be hacked or compromised even if confidence mechanisms are in place.

11. Work towards policy alignment in the APEC region to build a robust digital economy in the Asia-Pacific and beyond. APEC economies recognized the need for additional cybersecurity tools and capacity building, especially for developing economies, and recognized the value of continuing to regularly discuss cybersecurity topics within APEC.

This consensus document includes input from all participating APEC economies. The SCSC aims to complement ongoing and future cybersecurity work across all fora including the Telecommunications Working Group, Digital Economy Steering Group, and Small and Medium Sized Enterprise Working Group. Economies recognize that the above APEC actions can strengthen the region's cybersecurity practices and will endeavor to take them collectively according to each economies' unique needs, challenges, and circumstances.