Document: DIWG 39-013
Draft: **FIRST**
Date: 15 April 2019
Source: ABAC Chile
Meeting: Jakarta, Indonesia

Meeting Document Summary Sheet

Document Title:

Workshop: Enhancing cybersecurity in APEC

Purpose:

For consideration

Issue:

Single out best practices and make some recommendations as to how improve fight against cybercrime in APEC economies

Background:

Over the past few years, cybersecurity has become one of the most relevant and concerning issues in the digital agenda. The ability of institutions to effectively confront cyber threats and data breaches greatly depends on displaying appropriate service providers that enhance cyber resilience without inhibiting the digital economy's dynamism.

The development of local Computer Emergency Response Teams (CERTs) has proved to be one of the effective ways to fight cybercrime and could be one of the approaches to be followed by APEC economies.

Following this path, ABAC Chile held a high-level workshop where specialists on cybersecurity exchanged views and best practices that stand out in this matter, such as the Israel's financial CERT FC3, which has been proved to be able to steadily improve the overall ecosystem to fight against cybercrime based on voluntary information sharing. It was also highlighted the importance of "trust" as a key element for creating the necessary collaborative environment.

Proposal /Recommendations:

- Open a discussion about the relevance of developing a set of best practices based in APEC economies experience on this matter.
- Recommend Leaders to develop and adopt a set of best practices that could lead to the creation of an APEC strategy to tackle cybercrime.

Workshop: Enhancing cybersecurity in APEC

Rosario Navarro
ABAC Chile

Workshop on cybersecurity

- A high-level workshop on cybersecurity was held in Santiago in April

- The workshop goals were to single out best practices and make some recommendations as to how to improve fight against cybercrime in APEC economies

- Experts from highly qualified companies and business organizations such as Microsoft, CLERT and ACTI (Chilean Association of IT Companies) attended

- The workshop was based on expert presentations by Lavy Shtokhamer, Head of Israel’s National Computer Emergency Response Team (CERT) at Israel National Cyber Directorate of the Prime Minister’s Office, and Mr. Richard Wu, executive board director PwC - Asia

Three fundamentals

- **1. Trust:**
  - Basic principle in order make possible any collaborative environment conducting to strategies aiming to fight against cybercrime (e.g. Israel's Computer Emergency Response Team, CERT)
  - Facilitates and encourages knowledge sharing
  - Evidence from cases like Israel's CERT shows that when institutions share information:
    - Develop and perform good practices
    - Steadily improve the overall ecosystem to fight against cybercrime

Three fundamentals

- **2. Voluntary basis:**
  - Participation should be voluntary, so as to naturally socialize the importance of setting and consolidating plans to fight cybercrime among critical industries

- **3. Added Value:**
  - If added value from participating in cybersecurity schemes is well explained to relevant stakeholders, it will encourage them to share information and set cybersecurity programs. Give and take mechanism. Regular round tables could contribute to consolidate a win-win relationship

Some best practices

- Based on existing models, most notably Israel’s CERT, some best practices stand out in order to set strategies on cybersecurity:
  - Establishing clear protocols as to:
    - Which companies and how they can participate
    - What type of information they can share and
    - With whom they can share it
  - For any economy to put in place effective schemes against cybercrime:
    - A clear understanding of which industries are crucial. E.g., Water, Telecommunications, Financial Services, Robotics, Transport, etc.
    - Those crucial industries should be fully engaged

Some best practices

- Focussing on developing schemes for every critical industry at the local level, so as to:
  - Scalating from a more basic scheme up to a more sophisticated system

  (CERT → System and controls for Cybersecurity, for instance)

  - Providing an anonymous space of information sharing, so to overcome natural resistance from businesses to share information
- Knowledge sharing process should be independent from what has to be reported to regulators
- Permanent reporting to regulators to trigger more public/private collaboration

Some recomendations

- To bring about a collaborative network: involved entities need to appreciate and understand the added value coming from information sharing. Trust
- Take into account the entire chain of service providers or related industries to critical sectors
- Private/public collaboration to develop and implement cybersecurity schemes
- Robust and clear legal frames
- Take cybersecurity beyond reactive practices and move it into more proactive policies from both public and private sectors