Asia-Pacific
Economic Cooperation

2019/SOM1/TEL59/PLEN/020
Agenda Item: 11

Final APEC Framework for Securing the Digital Economy

Purpose: Information
Submitted by: Thailand

APEC
CHILE 2019

59th Telecommunications and Information Working Group Meeting
Santiago, Chile
4-7 March 2019

Asia-Pacific
Economic Cooperation

APEC FRAMEWORK
FOR SECURING THE DIGITAL ECONOMY

APEC TELECOMMUNICATIONS AND INFORMATION WORKING GROUP (TEL)
Security and Prosperity Steering Group

MARCH 2019

Contents

Foreword

Digital economy offers many possibilities for APEC member economies, including opportunities in electronic commerce and digital trade. The Internet and the digital economy enable greater economic integration, more innovation, as well as robust, sustainable, and inclusive economic growth for the Asia-Pacific region. To achieve these objectives, the 2016 APEC Leaders Declaration noted[1]:

> *We will collaborate to unleash the potential of the digital economy and strongly support an accessible, open, interoperable, reliable and secure ICT environment as an essential foundation for economic growth and prosperity. We will continue to promote policy and regulatory environment to ensure ICT security, data and privacy protection by developing interoperable and flexible frameworks. …*

and the 2017 APEC Ministerial Statement also noted[2]:

> *We welcome the implementation of the Telecommunications and Information Working Group (TEL) Strategic Action Plan 2016 - 2020. We support the continued development of information technology and communications, promoting a secure, resilient and trusted information and communications technologies (ICT) environment. We stress the importance of capacity building and the application of new technologies to promote innovative and inclusive growth. We commend TEL for its coordination with other fora to develop a safe and reliable information technology environment.*

Recognizing that APEC is an economic cooperation forum, the *APEC Framework for Securing the Digital Economy* ("the Framework") provides non-binding principles and strategic recommendation to inform member economies as they develop policy and regulatory frameworks to secure their digital economies, and their digital futures.

1) Preamble

1. The 10th Ministerial Meeting on Telecommunications and Information (APEC TELMIN10) endorsed the APEC TEL Strategic Action Plan 2016-2020 with 5 Priority Areas that include: Develop and support innovation; Promote a secure, resilient and trusted ICT environment; Promote regional economic integration; Enhance the digital economy and the Internet economy; and Strengthen cooperation. APEC member economies recognize the important role that digital security plays in protecting their economies and enabling socio-economic development.

2. To enable accelerated and sustained growth for the economy in the Asia-Pacific region, member economies should take steps to foster digital security in order for digital economy to support innovation[3].

[1] https://www.apec.org/Meeting-Papers/Leaders-C

[2] https://www.apec.org/Meeting-Papers/Annual-Ministerial-Meetings/2017/2017_amm

[3] 2016 APEC Leaders Declaration: "We recognize that innovation is a key driver of quality growth. In this regard, we encourage efforts to identify new growth engines, and will embrace the opportunities brought forth by sectors such as the Internet and Digital Economy."

3. Recalling that in 2002, APEC Leaders made specific commitments to establish legal and regulatory frameworks, including "the enactment of domestic cybersecurity laws, the development of domestic computer security incident response teams, and the promotion of international cooperation to strengthen cybersecurity and combat cybercrime."[4] Ministers also endorsed the *APEC Cybersecurity Strategy*, developed by the APEC Information Working Group, in 2002. The *APEC Cybersecurity Strategy* identified six areas: legal developments, information sharing and cooperation initiative, security and technical guidelines, public awareness, training and education, and wireless security to "serve as the basis of APEC's efforts on cybercrime and critical infrastructure protection."[5]

4. Also recalling in 2005, APEC Senior Officials endorsed the *APEC Strategy to Ensure a Trusted and Sustainable Online Environment.* The 2005 strategy encouraged APEC member economies to take actions in several areas, including security awareness for users, cohesive domestic strategies, cooperative efforts among economies, building partnerships among government, industry, academics and others, and ensuring that legal and policy frameworks address substantive, procedural, and mutual assistance arrangements.

5. Also recalling in 2013, the joint APEC-OECD Symposium on Security Risk Management in the Internet Economy[6] to exchange views on policy issues and trends related to managing security risk for economic and social prosperity in the digital economy.

6. Having regard to the 2004 *APEC Privacy Framework*[7] endorsed by APEC Leaders and updated in 2015[8] which aims to promote electronic commerce throughout the Asia-Pacific region and reaffirms the value of privacy to individuals and society. And, noting the security safeguards in the *APEC Privacy Framework* provide a foundation for the security of personal information.

7. Recalling that the *APEC Internet and Digital Economy Roadmap* which was endorsed in 2017 put "enhancing trust and security in the use of ICTs" into the key focus areas. It recommends that the public and private sectors, and other stakeholders, including academia, should work together to enhance trust and security in the use of ICTs, while taking advantage of the benefits of modern digital systems.

8. Recognizing that the underlying objective of this Framework is to foster economic and social prosperity within the region.

9. Building on past endorsements and commitments from the APEC Economic Leaders, the *APEC Framework for Securing the Digital Economy* provides agreed high-level principles and specific strategies to: enable greater economic integration in the region, promote innovation, and provide a solid foundation for a growing digital economy. Through the collaboration and collective effort of member economies and other participants in the digital economy, cybersecurity challenges can be effectively addressed.

10. Recognizing and building on the important work done by regional groupings in the Asia-Pacific region such as ASEAN, which among others include the ASEAN Cybersecurity Cooperation Strategy, which provides a roadmap to strengthen cybersecurity cooperation on cybersecurity

[4] APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment
[5] APEC Cybersecurity Strategy
[6] http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2014)1&doclanguage=en
[7] https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework
[8] https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

incident response, Computer Emergency Response Team (CERT) policy and coordination, and cybersecurity capacity building; the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of ICTs (ARF ISM-ICT) which focuses on the implementation of the 2015 ARF Work Plan on Security of and in the Use of ICTs; and the ASEAN Leaders' Statement on Cybersecurity Cooperation, which tasks relevant Ministers from all ASEAN Member States to recommend feasible options to better coordinate ASEAN's cybersecurity efforts among various platforms of the three pillars of ASEAN and to make progress on discussions relating to the adoption of practical, voluntary and non-binding norms of responsible State behaviour in cyberspace, taking reference from recommendations set out in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE).

2) Scope and Application

11. The purpose of Part 2 of the *APEC Framework for Securing the Digital Economy* is to make clear the extent of the coverage of the Principles and Strategies.

12. For the purpose of this Framework:
    - **Digital security** refers to the availability, integrity and confidentiality of digital infrastructure, software, communications, and data that supports economic and social activities and services.
    - **Digital security risk** refers to the likelihood of detrimental effects on economic and social activities resulting from threats and vulnerabilities in the digital environment. It is not possible to create an entirely safe and secure digital environment conducive to prosperity and growth. There is always some level of digital security risk. However, risk can be reduced to an acceptable level considering the economic and social activity at stake and the context. Digital security risk has great economic and social significance: it includes loss of business reputation, money, innovation, opportunities, and privacy, as well as disruption of operations, and destruction of physical assets and physical harm to people. Since there will always be residual security risk that has to be accepted, it is important to also be prepared to mitigate the effect of incidents. For example, encrypting stored personal information could prevent its misuse in the event of a data breach.
    - **Digital security risk management** refers to actions taken by organizations, individuals or economies to address digital security risks while maximizing opportunities. Digital security depends not only on how well digital security risks are managed by an individual, organization or economy, but also on how well these actors manage the digital security risks they may pose to others, whether through their action, or inaction.

13. As the social, cultural, economic, and legal backgrounds of each member economy may differ, there should be flexibility in implementing these Principles and Strategies.

    A common principles-based approach and a mutual interest in the management of digital security risks among APEC members will strengthen the resilience of APEC digital economies and greatly facilitate electronic commerce and explore opportunities for digital trade within, and beyond, the region.

14. This Framework addresses digital security as it relates to economic and social prosperity. The Principles and Strategies in the Framework focus on those aspects of digital security that are most important for safeguarding the digital economies.

15. Exceptions to the Principles and Strategies in the Framework should be:
    a. in accordance with the law; and
    b. made known to the public.

16. The Principles and Strategies in the Framework should be interpreted as a whole, rather than individually. The Principles and Strategies work closely together as parts of a holistic approach to digital security.

17. While recognizing the importance of protecting the digital economy and strengthening user trust, the Framework is not intended to impede governmental activities authorized by law when taken to protect security, public safety, or other public policy. At the same time, economies take into consideration, as appropriate, the possible economic and social impact of these activities on the digital economy, individuals and organizations' trust in digital technologies and the economic and social activities that rely on them, as well as the responsibilities and legitimate interests of individuals and organizations.

3) Principles

18. Member economies are encouraged to consider the following principles in developing policies to secure their digital economies:

Awareness:

Awareness is the first step towards better digital security.

19. Participants in the digital economy should have a sufficient understanding of digital security risk. They should also understand how to minimize the digital security risk their actions or inactions can create to others. Also, they should be empowered to assess and manage the risk they face.

Responsibility:

Digital security is a shared responsibility.

20. Participants in the digital economy should act responsibly and be accountable, based on their roles, the context, and their ability to act, for the management of digital security risk to ensure trust, and economic and social prosperity.

Cooperation:

Cooperation is essential to effectively manage digital security risk.

21. Regional and global interconnectedness means that the security of the digital economy is dependent on the actions of everyone involved. Successfully managing digital security risk will require cooperation. Cooperation should include all relevant stakeholders and extend across borders. International cooperation is vital for effective cyber-resilience as cyber security threats and challenges are multi-jurisdictional with no adherence to or recognition of economy boundaries.

Privacy

Privacy protection and digital security should reinforce each other.

22. Privacy and security are one of the central considerations for building trust and confidence in the Internet and digital economy. Economies should adopt or strengthen measures for privacy protection. Digital security measures should be consistent with the principles in the *APEC Privacy Framework*. Where possible, they should strengthen privacy protection.

4) Strategies

I. Digital security risk management

23. A risk management approach should be taken to strengthen digital security. In organizations, digital security risk management should be an integral part of economic and social decision-making processes that includes an overall policy framework to manage all risks related to economic and social activities. Digital security risk management relies on a holistic, systematic and flexible set of cyclical and iterative processes that are as transparent and explicit as possible. This set of processes helps to ensure that digital security risk management measures ("security measures") are appropriate to, and commensurate with, the risk, and the economic and social objectives at stake.

24. To manage digital security risk, stakeholders should conduct regular risk assessments for each of their activities that uses digital technologies. On the basis of each risk assessment, they should decide how to treat the digital security risk related to this activity. Risk treatment is generally a mix of four possibilities: taking the risk and facing the negative consequences in case of an incident; reducing the risk by adopting security and preparedness measures; transferring the risk for example through insurance contracts; or avoiding the risk by not using digital technologies.

25. Digital security risk assessment should guide the selection, operation and improvement of security measures to reduce the digital security risk to an acceptable level determined by the risk assessment and treatment. The selection of security measures should take into account their potential negative and positive impact on the economic and social activities they aim to protect and on the legitimate interests of others. All types of measures should be considered, whether they are physical, digital, or related to people, processes or technologies involved in the activities. Organizations in APEC economies should seek out and appropriately address vulnerabilities as soon as possible.

26. Preparedness measures are based on the recognition that incidents will happen. These measures are essential to ensure the resilience of the economic and social activities that rely on digital technologies. Based on digital security risk assessment, a preparedness and continuity plan including response should be developed, adopted and tested to reduce the adverse effects of digital security incidents, and support the continuity and resilience of economic and social activities. The plan should identify measures to protect, detect, respond and recover from digital security incidents. It should provide mechanisms to ascribe clear levels of escalation based on the magnitude and severity of the effects of digital security incidents, as well as their potential to extend to others in the digital environment.
27. Innovation should be considered integral to reducing digital security risk to an acceptable level determined by the risk assessment and treatment. It should be fostered both in the design and operation of the economic and social activities that rely on the digital environment as well as in the design and development of security measures.

28. APEC member economies are encouraged to:
    - Promote best practices and procedures for digital security risk management that are publicly available.
    - Support an economy digital security risk management approach strategy, including the protection of Critical Information Infrastructure (CII).
    - Promote a digital security risk management approach among all stakeholders by engaging in capacity building activities, including the development and/or adoption of globally recognized standards and best practices.
    - Lead by example by using a digital security risk management approach in the public sector.
    - Promote information sharing around current risks and risk management practices among stakeholders and member economies through economy-level Computer Security Incident Response Teams (CSIRTs) and other networks.
    - Promote cooperation, analysis and research into the coexistence of diverse laws on the cross-border digital economies.

II. Develop economy strategies

29. In view of the interest of economies in maximizing the economic and social benefits of digital technologies, economy strategies for digital security should foster trust in digital technologies and the activities that rely on them and create the conditions for participants in the digital economy to manage their digital security risk.

30. Economy strategies for digital security:

    a. Should be supported at the highest level of government. They should articulate a clear and transparent "whole of government" approach that is flexible, technology-neutral and coherent with other strategies that foster economic and social prosperity;
    b. Should be developed through a coordinated, open intra-governmental approach as well as a transparent process involving all stakeholders. They should be reviewed regularly and updated based on experience and best practices;
    c. Should take into account the variety of participants in the digital economy, including the large number of micro, small and medium-sized enterprises (MSMEs) who may not have the same abilities and resources to manage digital security risk as governments or large corporations;
    d. Should promote an approach to digital security risk management that does not increase the risk to other economies.
    e. Should work in complement with technical cybersecurity methodologies and guidelines.
    f. Should enable customization to address specific sectors and industries
    g. Should allow for evolution and be flexible to keep pace with law, regulation, policy, technology, and risk, as well as encourage the adoption of lessons learned, best practices, and innovative new technologies; and
    h. Should encourage the utilization of broadly accepted and globally recognized standards.

31. APEC member economies are encouraged to:
    - Provide incentives to stakeholders to manage digital security risk, and to increase market transparency and efficiency.
    - Foster innovation in digital security risk management.
    - Promote collaboration among all stakeholders, including MSMEs, to help protect the digital economy.

- Promote security measures based on a risk-based approach.
- Promote awareness of digital security risk among their citizens, with an emphasis on vulnerable groups.

III. Resilient critical information infrastructure (CII)

32. The resilience of critical information infrastructure is essential to the sustained growth of the digital economy and the provision of essential services such as e-government.

33. APEC member economies are encouraged to:
    - Develop and apply a set of criteria for identifying CII.
    - Apply a digital security risk management approach to protect CII and encourage stakeholders to do so as well.

IV. Strengthen collaboration

34. Given the cross-cutting and multi-disciplinary nature of digital security, collaboration and coordinated actions among sets of stakeholders are necessary to manage digital security risks, especially across borders. Actions should be taken to promote greater collaboration and understanding among stakeholders, APEC member economies and beyond.

35. CSIRTs play an important role in helping economies and organizations manage digital security risk by identifying and raising awareness of digital security vulnerabilities, threats and incidents, helping organizations recover from attacks and identifying the steps stakeholders can take to respond to digital security incidents. CSIRTs also cultivate a community of security professionals where information on digital security risk and risk management practices can be shared and exchanged.

36. APEC member economies are encouraged to:
    - Participate in relevant regional and international fora and establish relationships to share experience and best practices, as appropriate.
    - Develop or strengthen existing economy computer security incident response teams (CSIRTs).
    - Provide assistance, on a voluntary basis, to other member economies in addressing common digital security challenges with the participation of other stakeholders.
    - Establish CSIRT points of contact for addressing cross-border requests relating to digital security risk management issues in a timely manner.
    - Work together to improve responses to domestic and cross-border threats, including through CSIRTs co-operations, coordinated exercises and other tools for collaboration.
    - Encourage responsible vulnerability research and reporting mechanisms.
    - Promote co-ordination and active participation among stakeholders in addressing identified vulnerabilities.

V. Digital user empowerment

37. Participants in the digital economy should be empowered with the education and skills necessary to understand digital security risk, how to help manage it, to evaluate the potential impact of their digital security risk management decisions on their security and the security of the digital economy.

38. Recognition of the impacts that their own action, or inaction, could have on the security of themselves and others is core to strengthening the security of stakeholders and the wider digital economy.

39. APEC member economies are encouraged to:
    - Support and develop a skilled digital security workforce, including through providing resources for security education and certification programs.
    - Introduce digital literacy into educational curriculums.
    - Promote the use of security best practices and globally recognized standards.
    - Foster information sharing among stakeholders.
    - Coordinate capacity building activities to avoid duplicate effort.

VI. Digital security technologies for trust

40. APEC member economies should support the innovation, development and use of technologies to protect data confidentiality, support authentication and authorization, data integrity, and tamper-detection and resistance to strengthen the digital economy against digital security threats.

41. APEC member economies are encouraged to:
    - Train individuals and organizations to raise awareness to reduce digital security risks. Foster the open development of and access to "easy-to-use" tools that enable users to secure their data and transactions.
    - Encourage online service providers to protect the security of their customers' data and communications by adopting best practices and/or globally recognized standards.

VII. Personal data security

42. Digital security is essential to protect privacy. Digital security risk management provides a robust foundation to implement the Security Safeguards principle of the *APEC Privacy Framework*. More generally, the *APEC Privacy Framework* and this Framework mutually reinforce each other.

43. APEC member economies are encouraged to:
    - Approach cybersecurity and privacy holistically.

- this page is intentionally left blank-

APEC Project: [insert project number]

Produced by

Electronic Transactions Development Agency
Ministry of Digital Economy and Society
The 9th Tower Grand Rama 9 (B)
33/4 Rama 9 Road
Bangkok, Thailand 10310
Tel +66 2 123 1234
Email info@etda.or.th

For

Asia Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

[Insert APEC Publication number]
[Insert ISBN/ISSN – only if applicable]