Asia-Pacific Economic Cooperation

USAID FROM THE AMERICAN PEOPLE

STANDARDS AND PROCESS-BASED APPROACH TO ENHANCING CYBERSECURITY

June 2020

CONTENTS

ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Cooperation
BSSN	*Badan Siber Dan Sandi Negara*
CBPR	Cross Border Privacy Rules
CICTE	Inter-American Committee against Terrorism
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CNS	Computer & Network Solutions
COBIT	Control Objectives for Information and Related Technology
ECC	Elliptic Curve Cryptography
EGNC	E-Government National Centre
ICT	information and communications technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunication Union
LEA	Law Enforcement Agency
NCSP	National Cyber Security Policy
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OGCIO	Office of the Government Chief Information Officer
RMP	Risk Management Process
RSA	Rivest–Shamir–Adleman
SCSC	APEC Sub-Committee on Standards and Conformance
TDES	Triple Data Encryption Algorithm
TVRA	Threat, Vulnerability, Risk Analysis
UN	United Nations

UNIDIR	United Nations Institute for Disarmament Research
WTO	World Trade Organization

EXECUTIVE SUMMARY

Rapidly growing connectivity and digital transformation around the world have increased opportunities for innovation and economic growth. Digital connectivity, providing improved communications and increased market access, is benefiting businesses both large and small, as well as the common consumer. However, these opportunities likewise increase the exposure of economies around the world to the risk of cyber-attacks and cyber threats; the Asia-Pacific region is no exception.

Recognizing these increased risks, all Asia-Pacific Economic Cooperation (APEC) economies have developed cybersecurity approaches or are well on their way to develop them. However, the wide and diverging range of these approaches adopted in APEC creates a difficult landscape to maneuver for both policymakers and businesses alike. This also creates challenges for the alignment and coordination between domestic approaches and international arrangements/agreements. It is this diversity across economies and across regions that can pose a risk to the international trading system, especially as the digital economy matures.

International arrangements propose a standards and process-based approach towards cybersecurity, encouraging the use of globally-relevant standards developed through open, transparent and consensus-based processes and good cybersecurity practices to better harmonize economies' cybersecurity approaches and foster interoperability.[1] The ever-evolving risks that come with the expanding digital economy require an approach to regulatory responses that ensures any regulations or policy approaches are flexible, nimble and responsive. In particular, this paper recommends the adoption of a five-function framework to guide and supplement the use of globally-relevant cybersecurity standards and good practices. While there is no one-size-fits-all solution, the framework can be a foundational backbone that facilitates the formulation of a comprehensive cybersecurity approach. In adopting globally-relevant cybersecurity standards and good practices, it is integral that any cybersecurity approach addresses the framework's five critical functions: Identification, Protection, Detection, Response, and Recovery.

As a step to address this lack of harmonization, this paper aims to conduct an initial stock take of cybersecurity policies with a focus on standards in the APEC region. By identifying where differences have appeared in domestic cybersecurity approaches across APEC, this report seeks to inform the discussion on:

a) What trends on cybersecurity approaches are being developed in the APEC region;
b) Where differences in domestic approaches may be barriers and inadvertently restrict free and open trade;
c) How APEC economies can better align on cybersecurity risk management and adopt a standards and process-based approach to enhance regional trade.

This study was conducted under the auspices of the APEC Sub-Committee on Standards and Conformance (SCSC) as a part of a broader US-led APEC project to encourage facilitating trade through adherence to globally-recognized cybersecurity standards and best practices. This work builds on elements of the APEC Framework for Securing the Digital Economy, which was developed by the APEC Telecommunications and Information Working Group (TELWG) and encourages economies to

[1] These agreements are discussed in the section on "Globally-Relevant Standards and Good Practice Solutions."

"[develop] and/or [adopt] globally recognized standards and best practices," as well as the APEC Internet and Digital Economy Roadmap.

As APEC economies continue to refine their cybersecurity approaches, it remains ever-important that policymakers recognize the value of cross-border collaboration in enhancing cybersecurity and the merits of adopting globally-relevant standards and good practices premised on a process-based cybersecurity framework.

INTRODUCTION: INTERNATIONALLY-ALIGNED CYBERSECURITY IS FUNDAMENTAL TO VIBRANT DIGITAL TRADE

Digital technologies have transformed the way societies interact and trade. Organizations can instantaneously and more efficiently communicate with customers and vendors all over the world, small businesses can take advantage of the latest innovations and access new markets, and governments can procure from a global marketplace of vendors. Alongside the increased adoption of digital technologies is the increased impact these technologies have on the creation, processing, and transfer of data—activities that have now become key growth drivers of today's digital economy. The diffusion of technology has also promoted cross-border competition and improved efficiencies along increasingly interconnected supply chains.

Yet, as the increased use of digital technologies has enabled and enhanced global trade, it has been accompanied with the emergence of new risks. Cybersecurity plays an instrumental role in managing these risks and, in turn, fostering the trust needed to facilitate greater digital trade. Governments in APEC recognize the importance of cybersecurity – all 21 economies have developed or are well on their way to developing cybersecurity approaches.

Despite this recognition, the approaches to cybersecurity among APEC economies are wide ranging, and this variance creates challenges in the alignment and harmonization of approaches across economies and regions. Some have adopted a process-based approach, incorporating globally-relevant cybersecurity standards or actively participating in the development of such standards. Others have developed cybersecurity policies or legislation that take an economy-specific approach, adopting unique domestic requirements and localized approaches towards cybersecurity. This fragmented landscape risks hampering the region's ability to protect society and leverage the growth of its digital economy.

The international nature of cyber threats and the cross-jurisdictional nature of data flows will nevertheless require increased cooperation and coordination across economies to adequately address risk and support global trade. In reality, despite ongoing global and regional discussions on digital trade related aspects, such as digital taxation by the Organisation for Economic Co-operation and Development (OECD) and data governance at the G20 summit, multilateral coordination on cybersecurity are slow-moving.

Coupled with the constantly evolving cybersecurity environment and nature of technological innovation, economies are looking to international standards development organizations to provide a flexible and nimble response. By employing an open, transparent, and consensus-based process to developing standards, these standards are not only more responsive to the changing landscape of technology, but also reflect the state of technology and represent consensus of a broad section of stakeholders.

In addition to globally-relevant standards, this report makes the case for a process-based approach in developing cybersecurity approaches in the APEC region to enhance security, consistency and interoperability. A process-based approach relies on the conduct of processes, through the implementation of policies or guidelines, at different stages of an operation. This holistic approach considers various inputs to achieve specific objectives at different stages. For instance, the conduct of risk assessments to determine tailored and appropriate measures for protection, detection and response. This contrasts a more prescriptive, policy-based approach that depends on one-size-fits-all

requirements and has greater inertia in response to cybersecurity incidents. In addition to managing security risks and fostering trust in digital systems, a process-based approach further addresses technical risks and aligning organizational risk management. Where cybersecurity risks do not respect political borders and impacts global networks and supply-chains, alignment through the use of such an approach can ensure consistency across jurisdictions, and reliable, scalable implementation by digital services organizations across economies. A more detailed case will be made in the following sections.

This report is organized as follows. This first section lays out how a standards and process-based cybersecurity approach can promote cross-border digital trade to advance the growth of APEC's digital economy. The next section describes some emerging trends in cybersecurity approaches among APEC economies, particularly highlighting divergences that are posing as challenges for international harmonization. The final section provides the stock take of the different cybersecurity approaches adopted by APEC economies.

A STANDARDS AND PROCESS-BASED CYBERSECURITY FRAMEWORK

Governments play an important role in enhancing cybersecurity. In general, there are three areas of strategic focus related to cybersecurity: technology, processes, and people. While governments can promote and make available the use of technological solutions, as well as build awareness and develop human capacity on cybersecurity, crucially, they should also promote the development of the necessary process-based frameworks in collaboration with industry to enhance security and consistency. This task often falls under a dedicated cybersecurity agency or a department under the ministry of information and communications technology (ICT), which through the development and use of its own cybersecurity strategy or policy, has the ability to leverage and promote a standards and process-based cybersecurity framework—for use within the government, in the private sector and for society as a whole.

Governments can adopt a strategic approach to cybersecurity by promoting the use of processes that improve organizational risk management through transparency, inclusivity, and accountability. This holistic process-based approach developed together with the private sector can further foster collaboration, which increases the implementation of comprehensive risk assessments and agile safeguards against threats. Further, this approach would enable organizations to play a key role in enhancing interoperability, lowering implementation costs, and fostering trust.

For organizations with existing cybersecurity approaches, this can help guide the improvement or transformation of such existing approaches. A process-based framework evaluating different operational stages can aid enterprises in reassessing their current approach's sufficiency and appropriateness at each stage for the present cybersecurity landscape, as well as in identifying gaps which may need to be addressed going forward. For organizations that have yet to establish a cybersecurity approach, this can serve as a starting point, offering a process to manage their organizational risk.

GLOBALLY-RELEVANT STANDARDS AND GOOD PRACTICE SOLUTIONS

Digital trade increasingly transcends borders, as such greater international agreement and coordination on the management of cross-border risks is required. Multilateral organizations provide platforms for global and regional discussions to set the rules and guidelines that shape both global and regional trade environments in a consensus-based manner among member organizations and economies. However, this process can be time-consuming; especially when organizations often require immediate steps to address cyber threats and manage risks.

To address the rapidly evolving nature of cybersecurity threats, globally-relevant standards can and should form part of the foundation of economies' domestic cybersecurity framework. Such standards are developed by non-governmental international standards development organizations, not only in a transparent, inclusive and consensus-based process which involves global representation from industry, government, and academia, but also developed in response to market needs.

Many standards development organizations encourage global participation and, to maximize the benefits of a transparent model, government experts should proactively participate as subject matter experts in the development of standards, through opportunities like stakeholder working groups or topic-expert

technical committees. For instance, while all APEC economies are members of the ISO, not all are full members, or actively participating in the development of cybersecurity standards.[2]

Use of globally-relevant standards facilitates:

- **Agility:** High stakeholder participation in the development of international standards allows for the regular input and consideration of responses to changes in the very dynamic threat landscape. Among the responses that can be most wide-reaching are the modification or implementation of standards, and the development of new standards.
- **Consistency**: Using globally-relevant standards ensures a consistent approach and language among enterprises operating in different jurisdictions, improving compliance rates while lowering compliance cost.
- **Interoperability**: Having similar requirements, tools and procedures (and therefore compliance and enforcement) for cybersecurity to those in other jurisdictions not only allows economies to benefit more easily from globally-relevant cybersecurity solutions, but also supports cross-border data flows and digital trade.
- **Reliability**: Standards are frequently re-evaluated and updated by experts involved in the development of standards, increasing their reliability.
- **Scalability:** Adoption of these standards can spur a virtuous cycle of further promotion and adoption both within and across economies due to the various benefits.
- **Efficiency:** Conformity assessment mechanisms are scalable, efficient means to assure implementation, interoperability, compliance, etc.

Furthermore, good practices promote interoperability and understanding through common frameworks, concepts, terms and definitions. Good practices are generally proven, agreed behavior and working methods that provide positive benefits and results. Good practices are usually developed and published as guidelines by non-profit and non-government organizations through consensus-based, multi-stakeholder collaborations that are transparent and open. While standards may require mandatory compliance when incorporated into regulations or business contracts, good practices are voluntary and may be more cost-efficient and flexible to comply with as they do not require accreditation. For instance, the Center for Internet Security (CIS) is an example of a non-profit organization that has published 20 consensus-based Controls—guides curated by security practitioners and verified by an objective, volunteer community of cyber experts under a closed crowdsourcing model, to identify and refine effective security measures designed to protect organizations and data from cyber-attacks.[3]

The following provides additional resources to guide organizations on existing globally-relevant standards, good practices, and general resources on cybersecurity:

- ISO/IEC JTC 1 provides the standards approval environment for integrating diverse and complex ICT technologies. Its official mandate is to develop, maintain, promote and facilitate ICT standards required by global markets meeting business and user requirements.[4]

---

[2] ISO (n.d.), "About Us: Members," online., https://www.iso.org/members.html.
[3] Center for Internet Security (n.d.), "CIS Controls," (online). www.cisecurity.org/controls/
[4] ISO/IEC JTC 1 Information Technology, (online). https://www.iso.org/isoiec-jtc-1.html

- The American National Standards Institute (ANSI) Cybersecurity Portal provides information and resources from the contributions of ANSI and members of the ANSI Federation, as well as links to other selected public- and private-sector cybersecurity resources.[5]

- The National Institute of Standards and Technology (NIST) works with industry to create and maintain a catalogue of informative references of existing standards, guidelines and good practices that can be used as references in implementing its Cybersecurity Framework.[6] These references are illustrative and non-exhaustive, and regularly updated with new and revised standards based on industry collaboration.

- The International Telecommunication Union (ITU) maintains a Security Standards Roadmap which provides a summary of existing, approved ICT security standards related to telecommunications.[7]

- InfoSec HK lists several internationally recognized information security standards, guidelines and effective security practices for reference. These include Government IT Security Policy and Guidelines, IT Governance Standards and Best Practices, Guidelines on Conducting Online Businesses and Activities, and Guidelines on Safeguarding Data Privacy.[8]

- The United Nations Institute for Disarmament Research (UNIDIR) Cyber Policy Portal is an online reference tool that provides an overview of the cybersecurity and cybersecurity-related policy landscape, as well as the cyber capacity of United Nations (UN) Member States and certain intergovernmental organizations.[9]

There is currently an extensive range of cybersecurity standards and good practice frameworks published[10], which may be confusing and complex to implement. When identifying which standards and good practices best suit an organization's risk management strategy, organizations can take reference from the recommended process-based approach described in the following section.

This recommended process identifies five-functions that inform organizations how to (i) implement cybersecurity standards and good practices, and (ii) achieve specific cybersecurity outcomes. These functions are meant, on an ongoing basis, to strengthen capacity, understanding, communications, and coordination, ultimately enhancing cybersecurity and risk management.

This suggested process does not need to follow a sequential path, nor should it lead to a static end-state. These functions should instead be performed in a cycle, continuously shaping the larger organizational and operational culture and capacity for managing cybersecurity. As both cybersecurity solutions and risks continue to evolve, this process should be consulted and updated regularly to ensure

---

[5] American National Standards Institute (n.d.), "Cybersecurity Portal," (online). www.ansi.org/cyber/
[6] National Institute of Standards and Technology (NIST) (n.d.), Cybersecurity Framework: Informative References," (online). https://www.nist.gov/cyberframework/informative-references
[7] ITU (n.d.), Searchable online cyber standards landscape. www.itu.int/net4/ITU-T/landscape#?topic=0.1.39&workgroup=1&searchValue=&page=1&sort=Revelance
[8] InfoSec (n.d.), "Technical References," (online). www.infosec.gov.hk/english/technical/standards.html
[9] United Nations Institute for Disarmament Research (n.d.) Cyber Policy Portal, (online). https://cyberpolicyportal.org/en/about
[10] A catalogue of suggested examples of informative references of existing standards, guidelines and good practices that can be used as references in implementing the five main processes can be found at www.nist.gov/cyberframework/reference-catalog.

that an organization's cybersecurity approach remains current and adequate in meeting the organization's evolving risk tolerance and management requirements.

FIVE-FUNCTION FRAMEWORK

When approaching cybersecurity, there are five main functions that an organization should address:[11]

1. **Identification**: Understanding the current state of potential risks, risk tolerance and cybersecurity readiness. This includes conducting a self-assessment on an organization's cybersecurity readiness, and a risk management exercise to identify security concerns and objectives.

> *Examples of globally-relevant cybersecurity risk management processes are ISO 31000:2009 on Risk Management[12], ISO/IEC 27005:2011 on Security Techniques for Information Technology[13], NIST Special Publication (SP) 800-39 on Managing Information Security Risk[14], ETSI TS 102 165-1 Methods and Protocols; Part 1: Method and Pro Forma for Threat, Vulnerability, Risk Analysis (TVRA), and the Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline.*[15]

2. **Protection**: Developing appropriate and sufficient means to protect critical operations and data given the risks and risk tolerance. These safeguards should limit and/or contain any potential cybersecurity risk event. These include safeguards for physical and virtual assets.

> *Examples include the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standard CIP-003-8 for Cyber Security—Security Management Controls[16], and the Center for Internet Security (CIS) Controls on Malware Defenses,[17] and CIS Control 12 on Boundary Defense.*[18]

Other activities at this phase include awareness and training for organizational personnel and partners, data security policies, information protection processes and procedures, maintenance and repair of industrial control and information system components, and the use of protective technology such as encryption.

> A good practice is to encrypt all data, in transit and at rest, by default with a minimum use of Advanced Encryption Standard (AES) (128 bits and higher), Triple Data Encryption Algorithm (TDES) (minimum double-length keys), RSA (1024 bits or higher (RSA=Rivest–Shamir–Adleman), ECC (160 bits or higher (ECC=Elliptic Curve Cryptography)), ElGamal (1024 bits or higher).

---

[11] Adapted and modified from the National Institute of Standards and Technology (NIST) Framework Core in its Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[12] ISO, ISO 310000:2009. www.iso.org/iso/home/standards/iso31000.htm.
[13] ISO, ISO 310000:2009. www.iso.org/iso/home/standards/iso31000.htm.
[14] ISO, ISO/IEC 27005:2011. www.iso.org/standard/56742.html.
[15] NIST, Managing Information Security Risk, NIST Special Publication 800-39. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
[16] NERC, CIP-003-8, https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20for%20Approval%20CIP-003-8.pdf#search=CIP%2D003%2D8; Balch, NERC Submits Proposed Reliability Standard CIP-003-8, https://www.balch.com/insights/publications/2019/05/nerc-submits-proposed-reliability
[17] NERC, CIP-003-8, https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20for%20Approval%20CIP-003-8.pdf#search=CIP%2D003%2D8; Balch, NERC Submits Proposed Reliability Standard CIP-003-8, https://www.balch.com/insights/publications/2019/05/nerc-submits-proposed-reliability
[18] CIS, CIS Control 8, https://www.cisecurity.org/controls/malware-defenses/

3. **Detection**: Establishing the means to detect cybersecurity risk events in a timely manner. Early detection (and response) can significantly reduce the harm associated with an event. Any anomaly or event may pose a cybersecurity risk, and all such activities on information systems and assets should be monitored continuously and logged against baseline activities. Detection processes should be tested regularly to ensure they remain functional, effective, and updated.

> *Examples include COBIT 5 APO13.02 on defining and managing an information security risk treatment plan, COBIT 5 DSS05.02 on managing network and connectivity security, which describes how to test detection processes, and COBIT 5 APO11.06 on maintaining continuous improvement.*[19]

4. **Response**: Taking action against a detected cybersecurity risk in an appropriate manner to address, mitigate, or contain the incident. A response planning procedure needs to be developed to ensure the responsible and relevant personnel know how to respond, while communications policies define how response activities are conducted between internal and external stakeholders.

> *Examples include NIST SP 800-53 Rev. 4 CP-3 (contingency training)*[20]*, IR-4 (incident handling)*[21]*, IR-6 (incident reporting)*[22]*, and PM-15 (contacts with security groups and associations).*[23]

5. **Recovery**: Recovery activities are used to restore services and operations in the least disruptive manner, as well as to suggest improvements that strengthen the resilience of an organization's cybersecurity framework. A recovery plan should be executed immediately after or even during a cybersecurity incident, to restore systems and assets as soon as possible. Further, any lessons learnt shall be used at this stage to institute improvements to the existing implementation. Restoration activities will also require communication and coordination processes between internal and external stakeholders.

> *Examples include CIS Control 10 on data recovery capability, which describes the processes and tools used to properly back up critical information with a proven methodology for timely recovery,*[24] *COBIT 5 BAI05.07 on sustaining changes, and BAI07.08 on performing post-implementation reviews.*[25]

There is no one-size-fits-all approach to cybersecurity, with different enterprises facing different risks and employing different solutions and tools. However, there are commonalities which all enterprises must address, and processes and standards are structural elements that can aid this process. This process-based approach is fundamental in ensuring agility and the benefits of having consistent approaches across organizations and jurisdictions. Hence, there is a significantly greater need for the development of domestic and regional cybersecurity approaches through a transparent, process, than for economies to adopt a prescriptive regulatory approach towards cybersecurity.

---

[19] Glenfis, COBIT 5, (online). https://www.glenfis.ch/application/files/7614/3040/2296/COBIT5_Glenfis-Laminate-20.pdf.
[20] NIST, SP 800-53 Rev. 4 CP-3, https://nvd.nist.gov/800-53/Rev4/control/CP-3.
[21] NIST, SP 800-53 Rev. 4 CP-3, https://nvd.nist.gov/800-53/Rev4/control/CP-3.
[22] NIST, SP 800-53 Rev. 4 CP-3, https://nvd.nist.gov/800-53/Rev4/control/CP-3.
[23] NIST, SP 800-53 Rev. 4 CP-3, https://nvd.nist.gov/800-53/Rev4/control/CP-3.
[24] CIS, CIS Control 10, https://www.cisecurity.org/controls/data-recovery-capability/.
[25] CIS, CIS Control 10, https://www.cisecurity.org/controls/data-recovery-capability/.

TRENDS IN CYBERSECURITY POLICIES IN THE APEC REGION

Several APEC economies are already leveraging the use of globally-relevant cybersecurity standards and a process-based approach in developing their cybersecurity approaches. These include an open, transparent, and multi-stakeholder process to develop domestic cybersecurity strategies and laws with high levels of collaboration with industry. Some domestic standards bodies like in Japan and Thailand also actively participate in the activities of international standards development organizations in discussing, updating, and developing relevant global cybersecurity standards. Furthermore, APEC economies like Japan, Korea and Singapore are participants under the Common Criteria Recognition Arrangement (CCRA), which recognizes ISO/IEC 15408 for computer security, cooperating to ensure high levels and consistent standards for IT Products and Protection Profiles.[26] In other APEC economies, globally-relevant cybersecurity standards are referenced in the development of domestic cybersecurity standards that may be translated into domestic languages for domestic use.

Despite these trends, APEC economies have a diverse use of cybersecurity standards in APEC, and not all align with international good practices. This variety is illustrated in Figure 1.

Figure 1: Variety of Cybersecurity Standards in APEC

As mentioned above, a fragmented approach risks increased threats and vulnerabilities for economies in the region, more broadly, in the international cybersecurity landscape. Without the benefit of consulting a broad range of stakeholders, a localized approach will be by nature more vulnerable and less capable in both recognizing threats and responding to minimize harm. This can lead to economies or regions becoming a target of cyber-attacks or a home from which cybercriminals launch attacks on other economies. Furthermore, by taking a differentiated approach, an economy may compound the compliance measures obligated by enterprises to comply with both globally-relevant standards and the unique local standards. Harmonized standards allow economies to achieve greater efficiency, consistency, scalability, reliability, and agility through globally-relevant standards (and the participation in international cybersecurity fora) than through economy-specific standards.

The following paragraphs highlight four general trends where divergences from international good practices are prominent within APEC economies, providing a perspective of different economies' priorities regarding cybersecurity regulation.

---

[26] Common Criteria, Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf

[27] Non-comprehensive examples include: CIS Controls, COBIT Standards, ISO/IEC 27000 Standards, ITU Security Standards, NIST SP-800 Standards, NERC CIP Standards

IMPOSITION OF DATA LOCALIZATION REQUIREMENTS

In recent years, APEC has seen a rise in digital protectionism, particularly with increased restrictions on cross-border data flows. Governments are increasingly employing measures that prohibit data from traveling across borders. These policies vary in objectives, scopes and enforcements, but can be categorized into three broad groups. The strictest policies demand forced local data storage, requiring data to be stored in facilities physically located within a geographic border. In these economies, government organizations and businesses are unable to take advantage of globally-located servers, restricting businesses from using global cloud computing services that can lower hardware and ownership costs and can enable the use of innovative services such as big data analysis and artificial intelligence. These local data storage requirements may apply to data about foreigners or overseas businesses. The second group includes policies that require sector-specific data storage requirements. These commonly include sectors such as health, finance, and government data. Lastly, some economies necessitate consent requirements or regulatory approvals on data transfers. This model does not specifically mandate local data storage, but could adversely impact the ability to transfer data across borders. For instance, one economy's data protection law features mandatory consent for any private sector data sharing; data sharing agreements with transferees; and appointed data protection officers to ensure the protection of data privacy and security across border.

Data localization refers to government requirements to use servers located within an economy's borders to collect, process, and/or store data. In some cases, these data can be transferred across jurisdiction, subject to prior approval or the maintenance of a copy domestically. The five common objectives of governments in imposing data localization requirements are (i) cybersecurity, (ii) data privacy, (iii) law enforcement and regulatory oversight access, (iv) protectionism, and (v) "leveling the playing field.[28]" With regards to cybersecurity, governments often assume that data stored locally are more secure. However, the security of data is in reality dependent on several other factors, including the technical, organizational, and financial capacity of the data controller and data center operator.[29]

These measures are often justified on the grounds of protecting personal privacy, ensuring domestic security, improving economic competitiveness and/or leveling the regulatory playing field, often based on the assumption that data transferred and stored overseas is less secure. However, economies are experiencing that security is not necessarily strengthened when data is kept locally. In fact, it may well be weakened by the risk of common physical vulnerabilities like natural disasters, power supply inconsistencies, etc. Globally-located servers can in fact provide higher degrees of resilience and better redundancy than geographically-concentrated servers. Further, multinational cloud service providers are likely to have greater resources and expertise compared to domestic providers.

Notably, the APEC Privacy Framework, endorsed in 2005 by Ministers and updated in 2015, recognizes the "importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region."[30] Specifically, the Framework originally called for the creation of a mechanism to ensure cross-border data flows when implementing

[28] J. Meltzer and P, Lovelock (2018), *Regulating For A Digital Economy: Understanding The Importance Of Cross-Border Data Flows In Asia*, Global Economy & Development Working Paper 113, March 2018, Washington, DC: Brookings Institution. https://trpc.biz/wp-content/uploads/digital-economy_meltzer_lovelock_web.pdf.
[29] Meltzer and Lovelock (2018).
[30] APEC, APEC Privacy Framework, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

privacy laws. APEC realized this goal through the creation of the APEC Cross-Border Privacy Rules (CBPR) System to both ensure privacy protections and data flowed across borders. The Privacy Framework, originally modeled on the OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, is an international good practice recognizing the importance and impact of data flows in driving the global digital economy.

The use of data classification frameworks can also help balance regulatory requirements and reservations on localizing all forms of data by only requiring highly-classified or sensitive data to be hosted domestically. This allows for the use of global servers for the hosting of non-classified and less-sensitive data, which tends to form the bulk of data, thus allowing organizations to take advantage of the use of global servers and cloud services by saving costs and efficiencies.

CREATION OF DOMESTIC CYBERSECURITY STANDARDS

In some APEC economies, domestic cybersecurity standards have been developed based on global standards with amendments or additions of distinct requirements. The use of domestic standards partially adapted from international standards, as opposed to incorporating complete international standards, could result in distinct and duplicative requirements for the domestic market. In other cases, economies base their domestic standards on a few or limited standards developing organizations, where it may be more useful to adopt a process-based approach to develop and implement domestic standards based on their domestic needs and requirements. Taking reference from globally-relevant standards, rather than from the standards developing organizations, would greatly expand and enhance the risk management capabilities.

The bigger challenge is the emergence of domestic cybersecurity standards that have been developed in silo without making any references to globally-relevant standards. Apart from including unique requirements, these domestic standards are often developed without an open consultative process with stakeholders.

BANNING OF FOREIGN CONTENT AND PROVIDERS/VENDORS

Where the internet and digital technologies have enhanced the ability of organizations to communicate, some economies have chosen to ban foreign content, as well as connectivity and content providers, citing security concerns. While security concerns may be a legitimate justification for banning foreign vendors and providers, especially for critical infrastructure services, there are scenarios where a lack of evidence or substantiation on such bans could be perceived as protectionist measures. For instance, some economies continue to adopt stringent internet censorship policies, including blocking information from foreign sources and platforms as well as virtual private networks (VPNs). Consequently, this approach can limit innovation and artificially restrict competition within markets.

While some bans include restrictions from foreign service providers operating within a market or certain sectors, others may include requirements for foreign content providers, such as content or social media providers, to remove illegitimate or abhorrent violent material promptly. However, the nebulous nature of these circumstances means that authorities are left to make discernments depending on the circumstance, without clear or definitive guidance on when this is acceptable. The intermediary liability in these cases can be far more burdensome than the more commonly accepted notice-and-takedown regimes.

FRAGMENTED PRIVACY RULES AND LACK OF HARM-BASED DATA BREACH REQUIREMENTS

Privacy and cybersecurity are closely related in a digital environment, where the alignment and protection of personal data and strong privacy rules are instrumental in promoting cross-border data flows. Taken together, the concepts are generally referred to as "data protection." However, while APEC economies have been making progress in enacting and aligning cybersecurity approaches with international good practice, there is growing fragmentation between economies on privacy. While the APEC Privacy Framework was meant to guide common approaches to privacy laws and the CBPR System was meant to bridge those differences, domestic implementation of privacy, cybersecurity, data localization, and other data governance regulations risk fragmenting the internet and the digital economy in APEC. Other examples of guides and standards to common approaches include ISO/IEC 19592, ISO/IEC 18033 and NIST Privacy-Enhancing Cryptography (PEC) project. Some economies have enacted comprehensive privacy regulations, while others have enacted regulations lacking key characteristics of a comprehensive privacy law such as the absence of a personal data protection regulator or lack of clear definitions and distinctions between data controllers and data processors, which are key actors of the digital economy. The fragmentation of privacy laws creates an environment of uncertainties and challenges. Across APEC, privacy laws are being revised or adopted and should account for the digital economy, balancing privacy and prosperity, while ensuring economies take into consideration the principles and guidelines of the APEC Privacy Framework which reaffirms the importance of privacy to individuals and to today's information society, while noting the necessity of cross-border data flows.[31] This would also accelerate an economy's ability to participate in the APEC CBPR System, a government-backed data privacy certification developed and endorsed by APEC economies to support digital trade by certifying companies that have demonstrated compliance with internationally-recognized data privacy protections.[32]

Another point of deviation is on data breach requirements, which range from a lack of mandatory data breach requirements to another extreme form of stringent notification requirements that requires service providers to inform victims without delay upon discovery of the loss, theft, or leak of personal information. For instance, one economy requires data subjects to be notified even by the prospect of a leak, loss or distortion of personal data. Stringent requirements to inform victims and potential victims may unnecessarily alarm users who may upon further investigation be found to be minimally or unaffected. The more commonly used good practice is to conduct an initial risk analysis to determine the level of 'harm' to those affected, and if notification would have any benefit, such as enabling the affected to take defensive actions. Nevertheless, data breach notifications continue to be challenging due to the need to balance being timely, ensuring transparency, while managing over-notifications. While there is ongoing work in APEC to discuss common good practices for data breach notification laws, there is no uniform standard to facilitate compliance and consumer awareness.

[31] APEC, APEC Privacy Framework, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)
[32] APEC, What is the Cross-Border Privacy Rules System?, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

STOCK-TAKE OF APEC ECONOMIES' CYBERSECURITY APPROACHES

The majority of APEC economies have released their cybersecurity strategies or approaches in the last several years. These domestic approaches take numerous forms ranging from incorporating cybersecurity standards to drafting and implementing cybersecurity legislation to drafting domestic level strategies. This stock take attempts to record both ongoing and finalized discussions in APEC economies related to cybersecurity approaches.

The objective of this stock take is to demonstrate the range of cybersecurity approaches in the APEC region, as well as provide a starting point to discuss how to create more alignment and coordination between economies.

TABLE 1: APEC ECONOMIES CYBERSECURITY APPROACHES

APEC ECONOMY	CYBERSECURITY APPROACH
Australia	The Australian Government is developing its **2020 Cyber Security Strategy** as part of its commitment to protecting Australians from cyber threats. The 2020 Cyber Security Strategy will set out the Australian Government's philosophy and program for meeting the challenges of the digital age. The new Cyber Security Strategy will be a successor to Australia's landmark **2016 Cyber Security Strategy**, which set out the Government's four year plan to advance and protect Australian interests online. Australia has also opened the **Australian Cyber Security Centre** (ACSC), which acts as the single point of cyber expertise for the Australian Government. The ACSC provides cyber security guidance, advice, assistance and support across the economy. The Australian Government has created **Joint Cyber Security Centres** to work more closely with Australian businesses, and a **24/7 Global Watch** to respond to critical cyber incidents.
Brunei Darussalam	The E-Government National Centre (EGNC) is developing the Brunei National Cyber Security Framework to support the **Digital Government Strategy 2015-2020**, driven by the Wasawan 2035 vision statement.[33]
Canada	Canada's officially recognized domestic and sector-specific strategy for cybersecurity is the **National Cyber Security Strategy (2018).**[34] **The National Cyber Security Action Plan (2019-2024)** is Canada's domestic roadmap for governance of cybersecurity. The purpose of this Action Plan is to provide specific initiatives under the Strategy for the government, private sector and personal use.
Chile	Chile has officially recognized **National Cybersecurity Policy 2017–2022** as its domestic strategy. Chile's National Cybersecurity Policy 2017–2022 includes a

[33] Brunei Darussalam Government, Digital Government Strategy 2015–2020. www.digitalstrategy.gov.bn/Themed/index.aspx
[34] Government of Canada. National Cyber Security Strategy. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

	roadmap developed through a multi-stakeholder process focused on the protection of users and promoting a free, open, safe, and resilient cyberspace.[35]
China	China's **National Cyberspace Security Strategy (2016)** aims to build China into a cyber power while promoting an orderly, secure, and open cyberspace and safeguarding domestic sovereignty by streamlining cyber control.[36] **Cybersecurity Law of the People's Republic of China (2017)** defines and strengthens the protection of Critical Information Infrastructure (CII), including obligations and security requirements for Internet products and services providers, standardizing how personal information is collected and used.[37]
Hong Kong, China	Hong Kong, China's **Information and Communication Security Management Act (2019)** aims to implement a domestic information security policy and to build a secure information environment to protect domestic seucirty and public welfare focusing on critical infrastructure providers. **The Legislative Council Panel on Information Technology and Broadcasting: Information Security** is the cybersecurity roadmap in Hong Kong, China.[38]
Indonesia	Indonesia's **National Cyber Security Strategy** is the official domestic strategy on cybersecurity. It is based on the five principles of sovereignty, independence, security, togetherness, and adaptive.[39] Based on the principles, the Indonesian State Cyber and Crypto Agency (*Badan Siber Dan Sandi Negara* (BSSN)) is meant to further develop policies on cyber resilience, public service security, cyber law enforcement, cyber security culture, and cyber security in the digital economy.[40] Related aspects of cybersecurity including data protection and information security are governed by multiple laws such as **Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (GR82)**.[41]
Japan	The officially recognized domestic strategy for cybersecurity is Japan's **Cybersecurity Strategy,** which was revised in 2018 to take into account potential new threats related to the 2020 Olympic Games and the Internet of Things (IoT),[42] In 2017, the Ministry of Economy, Trade and Industry (METI) and the Independent Administrative Agency Information-Technology Promotion Agency (IPA) revised their **Cybersecurity Management Guidelines**.[43] The revised guidelines are very much aligned with the recommendations herein and the NIST

[35] Gobierno de Chile, National Cybersecurity Policy, www.ciberseguridad.gob.cl/media/2017/05/NCSP-ENG.pdf.
[36] Cyberspace Administration of China, "National Cyberspace Security Strategy," (online). http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
[37] Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). New America, www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
[38] Legislative Council Panel on Information Technology and Broadcasting. Information Security. https://www.legco.gov.hk/yr09-10/english/panels/itb/papers/itb0712cb1-2465-3-e.pdf
[39] National Standardization Body (BSSN), "Profil: Indonesian Cyber Security Strategy," (online). https://bssn.go.id/strategi-keamanan-siber-nasional/.
[40] National Standardization Body (BSSN), "Profil: Indonesian Cyber Security Strategy," (online). https://bssn.go.id/strategi-keamanan-siber-nasional/.
[41] Regulation of the Government of the Republic of Indonesia. Number 82 of 2012. http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html
[42] National center of Incident readiness and Strategy for Cybersecurity. Cybersecurity Strategy. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf
[43] Ministry of Economy, Trade and Industry, Cybersecurity Management Guidelines Revised, https://www.meti.go.jp/english/press/2017/1116_001.html

	Cybersecurity Framework. In 2019, METI also introduced its **Cyber/Physical Security Framework (CPSF)**.[44]
Malaysia	The first **National Cyber Security Policy (NCSP)** was developed in 2005 to support Malaysia's Vision 2020, and a new comprehensive NCSP is currently being developed by the National Cyber Security Agency.
Mexico	Mexico recognized the **National Cybersecurity Strategy (2017)** as its domestic strategy on cybersecurity.[45] This was developed in collaboration with the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) to build a resilient economy by strengthening cybersecurity across social, economic and political spheres and using ICTs in a responsible and sustainable manner.[46]
New Zealand	The **Cyber Security Strategy** (revised July 2019) is New Zealand's domestic strategy for cybersecurity. It identifies priority areas for the government to work together with individuals, businesses, and communities to enhance cybersecurity.[47]
Papua New Guinea	In Papua New Guinea, a new **National Cybersecurity Policy and Strategy** has been under development since 2017.[48] **The Cybercrime Code Act** (2016) criminalizes harmful cyber activities, including cyber-attacks on critical infrastructure.[49]
Peru	Peru's **National Cybersecurity Strategy**[50] is currently in development with assistance from the OAS.[51]
The Philippines	The Philippines issued the **National Cybersecurity Plan 2022** in 2017, which aims to assure continuous operation of CII, public and military networks; to enhance resiliency and ability to respond to cyber threats; to allow effective coordination with law enforcement; and to improve cybersecurity education in society.[52] The National Cybersecurity Plan 2022 adopts the NIST Cybersecurity Framework, the ISO/IEC 27000 family of standards, and other relevant international standards. The Philippines' **National Cybersecurity Plan 2022** includes a roadmap identifying key stakeholders and key program areas.[53]

[44] Ministry of Economy, Trade and Industry, The Cyber/Physical Security Framework, https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf
[45] https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf
[46] OAS, Press Release, https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-082/17; Gobierno Mexicano (2017), National Cybersecurity Strategy. www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf .
[47] Government of New Zealand: Department of the Prime Minister and Cabinet (2019), New Zealand's Cyber Security Strategy 2019. July 2. https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019.
[48] UNIDIR, Cyber Policy Portal Papua New Guinea, (online). https://cyberpolicyportal.org/en/states/papuanewguinea.
[49] Parliament of Papua New Guinea (2016) Cybercrime Code Act, December 13. http://www.parliament.gov.pg/uploads/acts/16A_35.pdf.
[50] European Union Agency for Cybersecurity. Peru Cyber Security Strategy. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/peru-cyber-security-strategy
[51] UNIDIR, Cyber Policy Portal, Peru, https://cyberpolicyportal.org/en/states/peru
[52] Republic of the Philippines: Department of Information and Communications Technology, National Cybersecurity Plan 2022. https://dict.gov.ph/national-cybersecurity-plan-2022/
[53] Republic of the Philippines: Department of Information and Communications Technology, National Cybersecurity Plan 2022. https://dict.gov.ph/national-cybersecurity-plan-2022/

Republic of Korea	Korea's **National Cybersecurity Strategy (2019)** focuses on enhancing cyber defenses to protect the state and critical infrastructure, as well as on enhancing domestic competitiveness and research and development capabilities.[54]
Russia	**Federal Law No. 187-FZ (2017)** "On the Security of Critical Information Infrastructure of the Russian Federation" includes basic principles for ensuring the security of CII, including the related powers of state bodies, as well as obligations and responsibilities of CII providers.[55] Cybersecurity is recognized under the National Security Strategy, while a **Cyber Security Strategy** has been mooted since 2014.[56]
Singapore	**Singapore's Cybersecurity Strategy (2016)** sets out the economy's vision, goals and priorities and is underpinned by four pillars: a resilient infrastructure, creating a safer cyberspace, developing a vibrant cybersecurity ecosystem, and strengthening international partnerships.[57] In 2018, the **Cybersecurity Act of Singapore** was enacted to establish a legal framework for the oversight and maintenance of national cybersecurity in Singapore, with an emphasis on the proactive protection of critical information infrastructure against cyber-attacks.[58] In 2019, Singapore achieved Common Criteria certificate-issuing status as part of its adoption of international best practice and standards. To better secure Singapore's cyberspace and protect consumers against cyber threats, the Cyber Security Agency of Singapore will be introducing the Cybersecurity Labelling Scheme (CLS) for network-connected smart devices moving forward.
Chinese Taipei	Chinese Taipei's **Information and Communication Security Management Act (2019)** aims to implement a domestic information security policy and to build a secure information environment to protect domestic security and public welfare focusing on critical infrastructure providers.[59] Chinese Taipei's **National Cyber Security Program of Taiwan (2017-2020)** includes a blueprint to improve the nation's overall cyber security defensive capabilities' energy through prospective policies and nationally integrated resource investment.[60]
Thailand	The domestic cybersecurity strategy of Thailand is the **National Cybersecurity Strategy (2017–2021)**, which focuses on strengthening the security and defenses of the State, including supporting research and development in cybersecurity and human capacity building.[61]

[54] Republic of Korea: National Security Office (2019), National Cybersecurity Strategy, April. www.msit.go.kr/cms/www/work/ict/__icsFiles/afieldfile/2019/04/03/%EA%B5%AD%EA%B0%80%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EB%B3%B4%EC%A0%84%EB%9E%B5(%EC%98%81%EB%AC%B8)_0403.pdf.

[55] Vyacheslav Khayryuzov (2018), "Privacy and Cybersecurity in Russia" Mondaq, October 31. www.mondaq.com/russianfederation/x/750216/Data+Protection+Privacy/Privacy+And+Cybersecurity+In+Russia

[56] CCDCOE, https://ccdcoe.org/library/strategy-and-governance/

[57] Cyber Security Agency of Singapore (2016). Singapore's Cybersecurity Strategy. https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

[58] Cyber Security Agency, Cybersecurity Act, https://www.csa.gov.sg/legislation/cybersecurity-act

[59] Library of Congress, "Taiwan: New Cybersecurity Law Takes Effect," (online article). www.loc.gov/law/foreign-news/article/taiwan-new-cybersecurity-law-takes-effect/.

[60] National Information and Communication Security Taskforce. Cyber Security Development Program. https://nicst.ey.gov.tw/en/807491F2A43DF876

[61] UNIDIR, Cyber Policy Portal, Thailand, https://cyberpolicyportal.org/en/states/thailand; Government of Thailand: Office of the National Security Council (2017), National Cybersecurity Strategy 2017–2021. www.nsc.go.th/Download1/%E0%B8%A2%E0%B8%B8%E0%B8%97%E0%B8%98%E0%B8%A8%E0%B8%B2%E0%B8%AA%E0%B8%95%E0%B8%A3%E0%B9%8C%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A3%E0%B8%B1%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%A1%E0%B8%B1%E0%B9%88%E0%B8%99%E0%B8%84%E0%B8%87%E0%B8%9B%E0%B8%A5%E0%B8%AD%E0%B8%94%E0%B8%A0%E0%B8%B1%E0%B8%A2%E0%B9%84%E0%B8%8B%E0%B9%80%E0%B8%9A%E0%B8%AD%E0%B8%A3%E0%B9%8C%E0%B9

	Cybersecurity Law (May 2019) strengthens the government's ability to safeguard critical information infrastructure, including private entities.[62]
United States	The United States recognized the **National Cyber Strategy (2018)** as the official domestic cybersecurity strategy. It focuses on deterrence, through the strengthening of agencies and law enforcement partners to respond to cybercrime and attacks, and promoting a vibrant and resilient digital economy in line with domestic priorities.[63] The Department of Homeland Security's **Cybersecurity Strategy (2018)** describes how the department to execute its responsibilities in building resilience and keeping pace with the evolving cyber risk landscape.[64] The **National Institute of Standards and Technology (NIST) Cybersecurity Framework (2018)** is a guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. It focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management process.[65] This Framework is mandatory for U.S. government and voluntary for industry.
Viet Nam	Viet Nam's **Cybersecurity Law (Jan 2019)** focuses on protecting domestic defenses and social order, including strengthening the government's control of Internet content.[66]

%81%E0%B8%AB%E0%B9%88%E0%B8%87%E0%B8%8A%E0%B8%B2%E0%B8%95%E0%B8%B4%20%E0%B8%9E.%E0%B8%A8.%E0%B9%92%E0%B9%95%E0%B9%96%E0%B9%90-%E0%B9%92%E0%B9%95%E0%B9%96%E0%B9%94.pdf

[62] Ministry of Digital Economy and Society. Cybersecurity Act B.E. 2562. https://www.mdes.go.th/law

[63] The White House (2018), National Cyber Strategy of the United States of America, September. www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[64] U.S. Department of Homeland Security (2018), Department of Homeland Security Cybersecurity Strategy, May, www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

[65] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[66] Ministry of Public Security, Draft Decree of Network Security Law, http://bocongan.gov.vn/van-ban/van-ban-moi/du-thao-nghi-dinh-quy-dinh-chi-tiet-mot-so-dieu-cua-luat-an-ninh-mang-314.html; Business Times, US Tech Giants Face Stricter Censorship under New Viet Law, https://www.businesstimes.com.sg/technology/us-tech-giants-face-stricter-censorship-under-new-viet-law

CONCLUSION AND NEXT STEPS

As cybersecurity risks continue to evolve, a robust cybersecurity framework is foundational to the sustainable development and continued growth of the digital economy. International cooperation is essential to enable and sustain cross-border trade, as well as to achieve socioeconomic growth within economies, and regionally. As APEC economies continue to implement and refine their domestic cybersecurity strategies, there still remains a gap between some governments' approaches and global good practices. Some governments fail to recognize the value of collaboration across borders in enhancing cybersecurity and the merits of adopting process-based cybersecurity frameworks that are premised on globally-relevant standards and good practices that have been developed through a transparent and multi-stakeholder process. In emphasizing a process-based approach towards cybersecurity, it is prudent that the principles that undergird this approach and promote collaboration are not overlooked. Principles like inclusivity, international cooperation and transparency are key factors that make globally-relevant standards valuable and sustainable.

This document characterizes some of the different approaches taken by APEC economies toward addressing cybersecurity. As APEC economies continue to revise and reposition their cybersecurity frameworks in support of their digital economy, it is vital that they continue to align with globally-relevant standards and adopt a process-based approach to enhance cybersecurity.

On the margins of the Third Senior Officials' Meeting (SOM 3) 2019 in Puerto Varas, Chile, the APEC Workshop on Facilitating Trade through Adherence to Globally-Recognized Cybersecurity Standards and Best Practices[67] gathered a wide variety of speakers and experts to kick-off the APEC SCSC's first discussion on cybersecurity standards. In the context of Chile's focus on Digital Society, the workshop aimed to promote information-sharing of cybersecurity standards, provide examples of how industries have applied cybersecurity standards, and open the discussion to what APEC could do to further alignment. The workshop was also an opportunity to solicit inputs to the initial findings and trends of this report. The culmination of the workshop sessions, inputs from experts as well as attendees, and discussions during the interactive sessions reinforced the significance of this issue and the importance of leveraging APEC as a multilateral platform to confront these challenges.

During the workshop's interactive sessions, attendees were tasked to identify the current challenges/constraints and capacity gaps experienced by economies, as well as potential solutions that can be implemented through APEC to address these challenges. In small group discussions, key challenges that were raised included:

- difficulty of changing behavior through education and consistent messaging by providing the right tools and incentives;
- difficulty responding to the fast-evolving technologies;
- determining which standard your economy should use (i.e., Canada determined that doing a lite version of ISO/IEC 27000 would suffice);
- getting the right expertise and resources for training and implementation of standards, both from government and relevant stakeholders;

[67] Summary Notes of the APEC Workshop on Facilitating Trade through Adherence to Globally-Recognized Cybersecurity Standards and Best Practices were endorsed by the APEC Sub-Committee on Standards and Conformance (SCSC) on September 25, 2019

- one dimensional standards that do not consider size of businesses and/or development stage of economies;
- difficulty of prioritizing progress over time to address security issues;
- lack of consensus on definition of cybersecurity;
- lack of a developed workforce leads to a lack of adoption of voluntary frameworks;
- municipalities/localities creating standards;
- competing/conflicting standards;
- and lack of resources and guidelines to implement standards.

In response, some ideas from the small groups to address these challenges included:

- creating an online hub/international knowledge sharing platform to share experience and raise awareness with stakeholders;
- providing a business case for why cybersecurity standards are important to industry leadership and management;
- providing a cost-benefit analysis of implementing cybersecurity standards on a sector by sector basis;
- identifying building blocks and/or starter kits for economy-level cybersecurity frameworks;
- creating a maturity model for implementing cybersecurity standards that incorporates a baseline and have the model mature of its development;
- increasing understanding of best practices by policymakers by using a train-the-trainer model;
- a workshop on how to implement standards with experts from ISO, IEC, and other international standards organizations;
- creating an APEC toolkit to create awareness and provide guidance on implementation and audits;
- developing guidance on how to implement ISO/IEC 27000-lite;
- convening an intra-APEC meeting with representatives from all working groups to discuss cybersecurity.

Among these ideas, the APEC toolkit, maturity model for implementing cybersecurity standards, and the intra-APEC meeting were the three most favored ideas from the audience.