CYBERSECURITY STANDARDS AND CONFORMANCE TO SUPPORT DIGITAL TRADE IN ASEAN

2022 | US-ASEAN BUSINESS COUNCIL

FOR THE 54TH ASEAN ECONOMIC MINISTERS' (AEM) MEETING

Executive Summary

Digitalization has been benefitting organizations with data-driven insights and increased productivity, including in the trade sector. However, the increasing reliance on technology and data-driven innovation in business and consumer activities has significantly increased the risks and costs brought by cyber threats. These risks are often perceived as an Information Technology (IT) issues rather than a business problem – linked to the lack of strategic mindset, policy preparedness, and institutional oversight on cybersecurity.

The US-ASEAN Business Council (US-ABC) is grateful for the opportunity to work with the ASEAN Consultative Committee on Standards and Quality (ACCSQ) and Digital Trade Standards and Conformance Working Group (DTSCWG) over the past year, to lay out the principles of digital trust as an imperative component to buttress the ASEAN's digital trade ecosystem. We commended the important work of the ACCSQ and DTSCWG in streamlining trade processes through standards harmonization and reduction of technical barriers to advance ASEAN's regional integration.

Cybersecurity is fundamental to digital trade; just as cyber threats undermine confidence in digital services. ASEAN needs to build digital trust and confidence in the digital ecosystem to facilitate several aspects of trade, including data use and electronic payments, among others. According to a two-year study conducted by the U.S. Department of Veteran Affairs and UL Solutions, *standards*, *testing* and *certification* enhance cybersecurity threat management and provide greater user confidence.[1] This could be achieved through a common approach by developing international standards that build on collaborative processes among relevant stakeholders.

Fragmented or bespoke regulations in specific jurisdictions limit the ability of digital trade participants to protect global enterprises and may serve as technical barriers to trade (TBT). From an industry perspective, varying standards and separate certifications in the name of cybersecurity without clear improvement to cyber space can be more costly than tariffs.[2] Moreover, the divergence in standards can collectively weaken cybersecurity and become barriers to domestic companies, including ASEAN micro, small and medium enterprises (MSMEs) – which online presence is rising – from seeking to serve regional and global markets.

Below are some common cybersecurity-related TBTs that have been affecting businesses in digital trade and require attention by AMS:

1. Technical regulations and standards that are not based on existing internationally-recognized standards. Restrictions on the ability for an organization to use an encryption product that is already based on internationally-recognized standards can force them to use multiple incompatible products across their networks, increasing complexity and potential

[1] https://www.ul.com/sites/g/files/qbfpbp251/files/2021-12/LHS-UL-VA-Research-Report-StrengtheningMedicalDeviceCybersecurityAcrosstheHealthcareEcosystem.pdf
[2] https://unctad.org/news/trade-costs-non-tariff-measures-now-more-double-tariffs

vulnerabilities.[3] Consequently, in May 2021, the U.S. proposed that the World Trade Organization (WTO) TBT Committee begin to explore the "landscape of views on cybersecurity regulation"[4] to identify and promote the application of regulatory approaches that are aligned with the WTO principles such as the use of internationally-recognized standards and best practices to maximize security, trade, and innovation outcomes.[5]

2. In-country testing, inspection and certification requirements and/or non-acceptance of recognized overseas certificates that certify to the same level of compliance or later editions. The non-acceptance of lab results from accredited or globally recognized labs or the requirement for duplicative in-country testing is a common market access barrier. This often applies to telecommunication equipment. The unclear requirements, limited lab capacity and undefined timelines result in significant delays to getting products into market.

3. Ambiguous/unclear or overlapping/duplicative technical regulations. This consumes unnecessary time and resources for both the regulators and companies. Moreover, with the current global supply chain challenges, producing samples for testing is itself an issue due to component shortages. This is currently apparent in ASEAN, in the case of importation procedures of telecommunication equipment which often have both radio transmission capabilities and civil cryptographic functions, but subject to several certification processes. The duplicative and inconsistent requirements lead to unnecessary delays, increased costs and create uncertainty for business compliance.

4. Unnecessary labelling requirements. Cybersecurity is a particularly challenging use case for labelling given the dynamic, context-specific and hard to measure nature of it. Furthermore, it often subject to expensive certification process and the absence of agreed upon parameters to define the objectives, metrics and design of the label would add risks and costs.

The World Economic Forum's Centre for Cybersecurity has identified three key priorities to minimize the gap between cybersecurity experts and policymakers towards reinforcing cybersecurity[6]:

1. ***Building cyber resilience.*** Develop and scale forward-looking solutions that promote best practices across digital platforms.

---

[3] Congressional Research Service, "Digital Trade and U.S. Trade Policy", December 9, 2021, p, 23, https://sgp.fas.org/crs/misc/R44565.pdf

[4] "The United States suggested the Committee hold a thematic discussion that would explore the current landscape of Member and stakeholder views on cybersecurity regulation with a view to: identifying relevant nexuses for the TBT Committee; and promoting the application of regulatory approaches in accordance with core TBT principles to maximize security, trade, and innovation outcomes."

[5] World Trade Organization, "Committee on Technical Barriers to Trade", May 17, 2021, p. 1, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/TBT/W747.pdf&Open=True

[6] Davis, Jonathan and English, Erin. Demystifying cyber supply chain security and zero trust architecture. Visa Economic Empowerment Institute (VEEI). http://usa.visa.com/content/dam/VCOM/regional/na/us/sites/documents/veei-demystifying-cyber-supply-chain-security.pdf

2. ***Strengthening global cooperation.*** Enhance public and private sector collaborations in developing collective response towards cyber threats.
3. ***Understanding future networks and technology.*** Cultivate further research on the challenges and opportunities of the emerging technologies.

We encourage ASEAN Member States to adopt internationally-recognized standards and best practices to support greater policy alignment among them and with the external trade partners. This will facilitate cross-border collaboration and drive economic growth and mutual understanding by allowing for interoperability in approaches to address common threats in cyber space. There are several internationally-recognized cybersecurity frameworks that ASEAN could reference e.g. the U.S. National Institute Standards and Technology (NIST) Cyber Security Framework (CSF) that entails cybersecurity standards, guidelines, best practices and other resources to meet the needs of U.S. industry and public in general.[7] The CSF covers specific information that can be put into practice immediately as well as longer-term research that anticipates advances in technologies and future challenges. It seeks to cultivate trust in information, systems, and technologies and to help organizations measure and manage risk. The Framework also considers the evolving cyber-threat landscape and the needs of public and private sectors in areas such as digital supply chains, ransomware and industry-specific requirements like the Financial Sector Cybersecurity Profile.

In general, cybersecurity standards and best practices vary in terms of focus and scope and can overlap in certain areas. Broadly speaking, the leading standards and practices can be clustered into one of the following three categories of focus and scoped as addressing broad, enterprise-wide requirements or more narrow industry and application-specific needs:

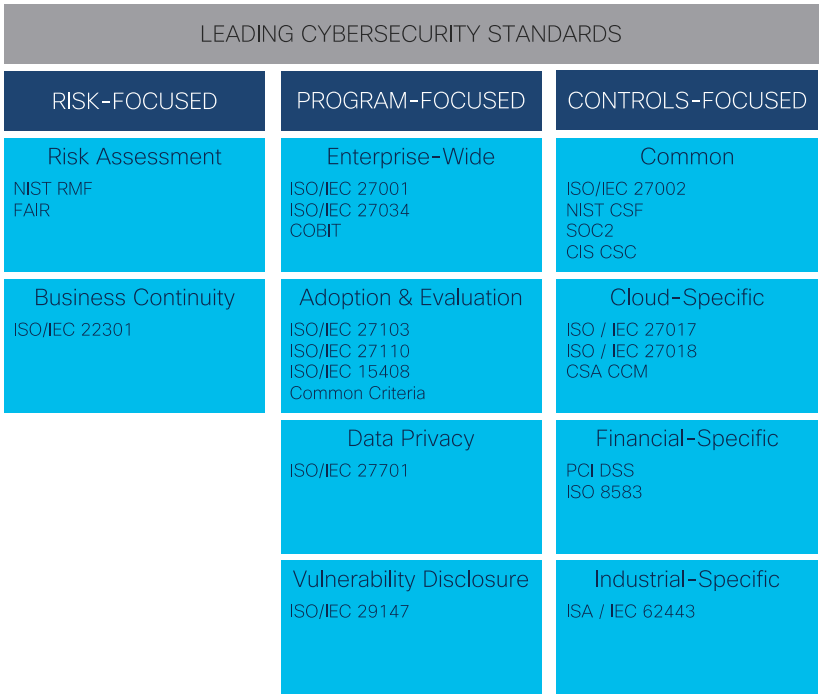

Figure 1. Leading Cybersecurity Standards

1. ***Risk-focused***: provide guidance on processes and techniques for evaluating and managing risk
2. ***Program-focused***: provide guidance on implementing and managing security programs and operations
3. ***Controls-focused***: provide guidance on selecting and implementing security controls

[7] NIST, "*Framework for Improving Critical Infrastructure Cybersecurity*", April 16, 2018, (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)

AMS also need to work on a more coordinated approach to set a higher, common cybersecurity baseline. The adoption of a common Cybersecurity Maturity model could help assess readiness and guide AMS towards a path forward in strengthening regional cybersecurity. This Cybersecurity Maturity Model and Assessment would help both the individual countries and the region to move towards cyber resiliency by measuring the level of maturity of each country's cybersecurity capabilities and recommending actionable steps to close gaps and improve overall security readiness. To this end, the Council and key members are driving the examination of ASEAN Cybersecurity Maturity Model and Assessment procedures that may assist AMS in agreeing on a suitable process that the region can commonly adopt.

Promoting cybersecurity is also imperative as ASEAN looks to define digital trade agreements. The upcoming negotiations on an ASEAN Digital Economy Framework Agreement (DEFA) should also consider risk-based approaches to cybersecurity regulations to mitigate threats and vulnerabilities. The DEFA may want to incorporate actions on vulnerability disclosure principles on known and public vulnerabilities and cryptography, such as transparency, timeliness and responsible reporting.

We hope ASEAN governments would work closely with the private sector in developing such regional frameworks to ensure inclusivity and transparency of policymaking and to improve trust in the digital space. In addition, ASEAN may consider establishing a user-friendly repository of cyber scams and threats to facilitate information sharing among stakeholders and vulnerable internet users and raising awareness of common cyber-attacks and risks, including the ways to avoid or counter them.

The Council is currently consolidating a more detailed recommendation paper on Cybersecurity Standards and Conformance to Support Digital Trade in ASEAN, to be submitted for further deliberation with the ACCSQ and DTSCWG. We recognize that this cooperation fulfils Strategic Thrusts II, IV and VI of the ASEAN Standards and Conformance Strategic Plan 2015-2025[8], a subsidiary to the ASEAN Economic Community Blueprint 2025. We look forward to continue supporting the ACCSQ and DTSCWG in scoping out the relevant digital standards to harmonize across AMS. We would also be pleased to organize expert workshops to discuss the recommended standards that require further clarification, as part of our continued efforts in supporting cybersecurity capacity building and resiliency in ASEAN.

[8] ASEAN Standards and Conformance Strategic Plan 2015-2025, "*Forging Ahead Together: Ensuring Quality & Building Confidence*" p. 5., https://asean.org/wp-content/uploads/2021/01/ASEAN-Standards-and-Conformance-Strategic-Plan-2016-2025.pdf

ABOUT THE US-ASEAN BUSINESS COUNCIL

US-ASEAN
BUSINESS COUNCIL, INC.

For more than 35 years, the US-ASEAN Business Council has been the premier advocacy organization for U.S. corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN), serving as the leading voice of the U.S. private sector in promoting mutually beneficial trade and investment relationships between the United States and Southeast Asia. We believe opening and investing in the sustainability of efficient, resilient and competitive markets are critical to the continued growth of our member companies and innovation and job creation in the United States and Southeast Asia. ASEAN now represents more than 650 million people and a combined GDP of US $2.8 trillion across Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. The Council's members include many of the world's largest American multinational corporations in numerous industries and range from those that have been working in Southeast Asia for more than a century to newcomers entering Asia's most dynamic regional economic community.

The Council has offices in Washington, DC; New York, NY; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.