ABTA Supports an Effective Cybersecurity Framework in Asia

The Asia Business Trade Association (ABTA) recognizes that a sensible cybersecurity framework is needed to help ensure that global trade flows can continue to flourish in the 21st century. As the digital economy has grown rapidly around the world, so has the importance of digital trade.

The movement, use and exchange of information not only drives global economic growth, but allows companies—especially small businesses—to incorporate into global value chains and sell goods and services directly to companies and customers around the world. Nevertheless, reliance on information networks has made businesses and governments vulnerable to complex and diverse array of cyber security threats.

Growing in volume, intensity and sophistication, cyber threats are global in nature and can pose serious risks to the global IT ecosystem on which economic growth and global trade depend. As a result, the need to protect information and identify the sources and nature of cyber threats have become a legitimate responsibility of governments seeking to foster trust in the IT ecosystem that underpins the growth of their digital economy.

Moreover, the implementation of cybersecurity policy regimes does not only concern critical economic and national security infrastructure, but the growth of IT and trade ecosystems. Cybersecurity laws and regulations can affect trade facilitation measures, the structure and efficiency of global supply chains, and the exchange of digital products across markets. Thus, while it is important that policymakers take risks seriously, it is instrumental that they ensure that measures that improve security and yet do not threaten trade and economic growth. Trade officials must be part of the solution.

In consideration of: (i) the need for policies that protect government and businesses against cyber threats and (ii) the importance of guaranteeing that those policies do not inhibit the exchange of ICT products and services, the Asia Business Trade Association has developed the following Cybersecurity Framework. The framework offers a series of best practices that governments in the region can follow to regulate their cybersecurity space and ensure they can take full advantage of the opportunities from trade and the digital economy.

1 **Adopt a Comprehensive and Inclusive National Cybersecurity Strategy**

A national cybersecurity strategy sets out a nation’s overall approach to cybersecurity and allows it to situate national cybersecurity activities in the context of international cyber activities and of other activities affected by cybersecurity efforts. The strategy should be inclusive by allowing collaboration and coordination among key stakeholders, which include government agencies including trade ministries, industry, and academia and citizen groups. It should be comprehensive by incorporating critical infrastructure cybersecurity strategy and ensuring a functional interagency process. An inclusive and comprehensive strategy will ensure that trade and economic growth is not unduly compromised by an overly strong security focus.
Ensure the Free Flow of Information Across Borders

Technologies that allow the storage, processing and transfer of information across international borders drive global economic growth and are essential for trade in the digital age. Laws that restrict the cross-border transfer of data or impose data localization requirements make data more vulnerable to cyber attacks, forgo many of the security benefits of cloud computing technologies, and undermine the benefits of information technology that underpin the modern economy.

The future of global trade increasingly will depend on smart and sensible regulation of information.