BSA The Software Alliance

STUMBLING BLOCKS IN THE PATH TO TRUE SECURITY

Some governments today are invoking cybersecurity as a justification for a variety of policies that go beyond what is needed to address legitimate security concerns. In fact, such policies often undermine cybersecurity rather than improve it. They also impose unfair market access barriers on global producers and service providers, whether intended or not.

Avoid Unnecessary or Unreasonable Requirements

A proper cybersecurity policy enables organizations to develop and adopt the widest possible choice of cutting-edge cybersecurity solutions. It also allows entities to implement the security measures that are most effective at mitigating the specific risks they face.

Some governments instead impose various requirements that restrict choice, increase costs and reduce the ability of their own firms to use the most appropriate cybersecurity tools available. These include, but are not limited to, country-unique certification conditions or local testing requirements; mandates for local content; requirements to disclose sensitive information, such as source codes and encryption keys; and, restrictions on foreign ownership of intellectual property.

Refrain from Manipulating Standards

Technology standards play a vital role in enabling and enhancing cybersecurity. By supporting internationally recognized technical standards that are developed with industry participation and accepted across markets, companies can more quickly develop and distribute newer and more secure products.

Even so, some governments have imposed country-specific standards with the argument that requiring market-specific rules will lead to improved cybersecurity. The real effect, however, is the opposite. Government-imposed standards, rather than bolstering security, tend to freeze innovation and force consumers and businesses into using products that might not suit their needs.

Avoid Data Localization Rules

With the rise of global cloud computing services, companies of all sizes around the world can leverage powerful resources that were once available only to the largest firms. The cloud model, though, is based on networks that allow the storage and processing of data in multiple locations and even in multiple countries. By allowing data to flow freely among multiple markets, cloud providers can deliver numerous advantages, including reliability, resiliency, and 24-hour service support.

Based on the mistaken assumption that data is safer in a specific location, some countries are imposing rules that prohibit or significantly impede data transfers across borders. Policies that unnecessarily restrict the free flow of data undermine the very benefits of cloud computing by increasing costs and threatening to prevent access to emerging cloud-enabled services.

Avoid Preferences for Indigenous Technologies

Cutting-edge products and services are developed through global collaboration in research and design centers in many different countries. Countries should create incentives for cross-border collaboration to facilitate voluntary technology transfer and the rapid development and deployment of enhanced products and services.

However, some countries take the opposite approach, assuming that by preventing foreign competition they can protect domestic champions, develop an indigenous technology industry, and enhance cybersecurity. By definition, indigenous technologies are a subset of global innovation. Preventing foreign competition reduces cybersecurity by denying firms and agencies from buying world-class products and services. Furthermore, such policies deprive domestic technology firms of valuable opportunities to collaborate with global leaders and make them less competitive internationally, harming global innovation.