Increasing the Global Availability and Use of Secure Information and Communication Technology (ICT) Products and Services

An EastWest Institute Breakthrough Group

Executive Summary

For more than three decades, the EastWest Institute (EWI) has been an independent and trusted institution, providing thought leadership and mobilizing resources to address some of the most critical security issues facing the world. It brings together key leaders, policy makers, and groundbreaking innovators to develop new solutions to today's daunting challenges.

In 2009, EWI established the Global Cooperation in Cyberspace Initiative to formalize its work on cyberspace issues. As part of that initiative, EWI established seven Breakthrough Groups, each devoted to a specific focus area. This document pertains to the Breakthrough Group (BG) entitled: "Increasing the Global Availability and Use of Secure Information and Communication Technology (ICT) Products and Services."

This BG's objective is to enhance cybersecurity for governments and enterprises globally by enabling the availability and use of more secure ICT products and services. For stakeholders in the ICT supply chain, the BG will promote the use of recognized and proven international standards and best practices that improve product and service integrity. For buyers of ICT, the BG will work to foster the use of procurement practices that are founded on recognized and proven standards and best practices for secure ICT. We will also work to prevent, and where necessary, break down trade barriers so that buyers can identify and utilize trusted providers regardless of their locale.

The purpose of this document is to inform interested parties of this group's efforts, facilitate dialogue and engagement and build momentum towards our objectives. A key indicator of progress will be when guidance or requirements for governments' and critical infrastructure enterprises' procurements integrate recognized standards and practices for integrity and assurance, ultimately helping to enhance the cybersecurity of their systems and operations.

The Challenge

While governments and enterprises around the globe depend on ICT products and services, they are increasingly aware of and concerned about cyber risks. The challenges associated with improving cybersecurity and providing ICT products and services that have sufficient integrity to support these users' critical operations are enormous. One challenge derives from the nature of the ICT marketplace, which thrives in part because technological innovation and development leverages resources—cyber, physical and human—from all over the world.

This global approach provides economies of scale and efficiencies, driving down costs and enabling people and organizations around the world to use and realize the benefits of ICT products and services. However, the sheer number and diversity of individuals, entities, services, and components involved in the technology lifecycle—that includes design, development, deployment, configuration, and operation of ICT—also introduces risks. In the face of more and more serious and dynamic cyber threats, governments and enterprises are increasingly uncertain about whether the global ICT market is driving enough meaningful progress on security and assurance of ICT products and services and their underlying supply chains.

This environment of uncertainty and mistrust has contributed to a growing number of countries proposing or implementing protectionist initiatives as they seek to manage security concerns related to their government and critical infrastructure operations. Unfortunately, initiatives that focus on promoting local solutions, such as country-specific regulations and bans on foreign products, inevitably raise costs. They are also likely to increase security risks by limiting access to secure ICT and innovations that develop in the global marketplace. Finally, these initiatives may create trade barriers that have problematic economic effects beyond the ICT security market.

Countries should instead foster and maintain an environment that promotes innovation and healthy competition, enabling the development of and access to the most secure technology, now and for years to come. To do so, they should use risk-informed, fact-based procurement practices founded on widely recognized international standards and best practices and objective conformance regimes, which countries can agree to follow and implement transparently. With such a regime in place, ICT providers, component suppliers, integrators, and resellers that adhere to established global standards or certification programs could be recognized as trusted sources—regardless of the country in which they're incorporated or in which they develop, buy, assemble, or operate their products and services. This approach would not only level the playing field for ICT providers globally but also enable more effective cyber risk management and better security.

Buyers of ICT products and services should also be made more aware of and informed about what they should consider consistently asking of, or requiring from, their suppliers. To date, the demand side of the global ICT marketplace has not adequately incentivized ICT providers to integrate increased security. Too often, ICT buyers in both governments and industry do not know what to request or require from providers to improve the security of the products and services that they use. As a result, while some ICT providers are using standards and best practices to improve security and integrity, many do not. Instead, ICT buyers need to consistently demand and incentivize increased security, understanding the risks facing their organizations and defining requirements that are proportionate to the risks that they choose to manage. By asking informed questions and making commercially reasonable demands of ICT providers, buyers can significantly reduce the risk of a range of cyber threats.

The Problem Space & the Stakeholders

Key issues in this problem space include the availability of and access to secure ICT products and services and buyers' ability to procure and use those products and services:

ICT buyers' use of secure ICT products and services:

- Misinformed political and regulatory forces can skew security purchases that would otherwise be risk-informed and market-driven. For instance, restricting ICT purchases based on country of origin inhibits ICT buyers' ability to acquire the most innovative, affordable, and secure products and services.
- Governments have numerous, often conflicting roles as users, protectors, and exploiters of technology, complicating the exchange needed to align market supply and demand.

Availability and access to secure ICT products and services:

- Existing ICT product and services assurance standards and best practices do not scale to accommodate varying levels of risk tolerance and objectives.
- Market demand has not adequately informed and incentivized ICT providers to build security and integrity into their products and services. In addition, inconsistent demands from ICT buyers leave providers facing multiple, disparate, and inadequate signals about which standards might be considered appropriate.

Numerous stakeholders should cooperate to align supply of and demand for secure ICT products and services. A few of the major stakeholders and their potential risks are listed below:

- ICT providers, including original equipment manufacturers (OEMs), hardware and software component suppliers, integrators and resellers.
- ICT buyers, including government, industry and individuals.
- ICT policy influencers, including nonprofits, researchers and standards organizations.

Principles and Approach

This BG is initially taking a two-pronged approach to this problem, focusing on both ICT providers and buyers. Two sets of complementary principles underpin this approach:

1: Supply Side Principles – providers of ICT need:

- An open market that fosters innovation and competition.
- A level playing field for ICT providers, regardless of locale.
- Broader use of a set of scalable and proportionate standards and best practices for security and integrity.
- Buyers of ICT to use procurement processes that utilize fact-driven, risk-informed and transparent requirements.
- Streamlined, agile, and scalable international standards and approaches to conformance.
- A commitment by governments and ICT providers to avoid requirements or behavior that undermines trust in ICT (e.g., by installing back doors).

2: Demand Side Principles – buyers of ICT need:

- Tools and approaches to assess risk.
- A comprehensive understanding of lifecycle costs for ICT to inform decisions not only based on lowest initial costs but also on best overall value.
- Methods to develop and implement consistent procurement requirements appropriate to assessed risks.
- A set of providers recognized as conforming to international standards and best practices for product and service integrity.

Based on these principles, the BG's approach includes providing guidance to:

- ICT providers—regarding how their products, services, and development lifecycles can demonstrate security and integrity by utilizing appropriate and applicable standards, best practices and conformance approaches.
- ICT buyers—regarding what they should be asking for, or requiring from, their providers to align ICT product and service security and integrity to risk tolerance.

Plan

To provide guidance according to the above-described approach, five activities are planned:

1) Collect

From ICT providers, this BG will collect information regarding the standards, best practices, and technologies they use or don't use and their reasoning for doing so. From ICT buyers, this BG will collect input regarding how they assess risks, including ICT supplier risk, and the methods they use (e.g., standards and best practices, contractual requirements and conformance) to manage those risks. Throughout this phase, existing and emerging international standards and best practices for assurance and integrity (e.g., ISO 27036 and 27034, The Open Group's Open Trusted Technology Provider Standards (O-TTPS) also known as ISO DIS20243, Common Criteria and FIDO) will be inventoried, and any supply side gaps will be identified. Likewise, emerging risk management approaches (e.g., NIST Cybersecurity Framework and Huawei's Cybersecurity Perspectives—Top 100 Requirements white paper) will be inventoried, and any demand side gaps will be identified. This phase is planned to be completed by Q3 2015.

2) Aggregate

The BG will aggregate and, whenever feasible, align supply side standards and best practices with risk management approaches collected from the demand side. This list of aggregated standards, best practices, approaches, and mechanisms is intended to help facilitate alignment of ICT providers in developing and ICT buyers in procuring products and services consistent with their levels of risk tolerance. This phase is planned to be completed by Q4 2015.

3) Customize

The BG will customize the aggregated list of standards, practices, and risk management approaches to enable communities of ICT buyers with similar but unique needs to articulate sector-specific implementations. Published as separate and customizable references or guidance documents, the aggregated lists of supply side standards and best practices and demand side approaches and mechanisms will be applicable to the needs of entities that face similar risks, such as the banking and public sectors. This adaptability will ease implementation with the goal of increasing usability. This phase is planned to be initiated by Q1 2016.

4) Formalize

The BG will integrate customized guidance into the methods of evaluation that key ICT buyers use to determine from which providers they will procure secure ICT products and services. In addition, in contracting with providers, ICT buyers may reference this BG's guidance documents, and existing or emerging standards documents may reference this BG's sector-specific guidance.

5) Mobilize

The BG will mobilize support for the guidance documents, utilizing our extensive networks in capitals and corporate headquarters around the world, to seek global utilization of this work.

Upcoming Meetings and Events

The below-described events and meetings are planned to facilitate dialogue around this BG's work and to broaden support for its initiatives:

- Conference calls and meetings with the BG, interested parties and recognized experts
- Interactive webinars
- The Global Cyberspace Cooperation Initiative's annual EWI Summit, at which this BG will report back to the plenary.

Get involved

If you are interested in participating in this BG, would like more information, or would like to be informed of upcoming webinars or other EWI events, please contact Ashley Dennee at adennee@ewi.info.