Five Ways to Increase the Security of Cyber Products and Services

A Progress Report of the EastWest Institute Breakthrough Group on **Increasing the Global Availability and Use of Secure Information and Communication Technology (ICT) Products and Services**

December 2015

Governments and enterprises around the globe depend on ICT products and services. They are becoming 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 – which 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 from 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 EastWest Institute's international Breakthrough Group on Increasing the Global Availability and Use of Secure ICT Products and Services is working to create a reference guide to assist buyers in asking those questions and making those demands. During 2015, the group developed a set of principles that are driving additional work. In addition, it conducted an industry survey which produced insights into how buyers, and suppliers, think about the security of the ICT products and services.[1]

Government and industry act in multiple roles in the ICT marketplace. The government acts as a policy maker; industry provides ICT products and services. And both parties buy ICT products and services. Accordingly, each sector has different responsibilities when it comes to increasing the security of ICT products and services. These roles and responsibilities are summarized in Figure 1, below.

Actor →	Government		Industry
Role →	Policy-Maker	ICT Buyer	ICT Provider
The Five Ways			
1. Maintain an **open market** that fosters innovation and competition and creates a **level playing field** for ICT providers	✓		
2. Create procurement practices that utilize **fact-driven, risk informed, and transparent requirements** based on international standards and approaches		✓	
3. **Avoid** requirements or behavior that **undermines trust** in ICT (e.g., by installing back doors)	✓		✓
4. **Evaluate the practices** of ICT providers in terms of creating product and service integrity.		✓	
5. Create and use tools and approaches to **assess risk** and assign long-term **value** to cybersecurity investments	✓	✓	✓

Figure 1: Roles and Responsibilities in the Global Effort to Increase the Security of ICT Products and Services

In 2016, group will formalize recommended methods of evaluation that ICT buyers should consider using to determine from which providers they will procure secure ICT products and services.

[1] The principles are detailed in the group's scoping document which, together with the preliminary survey results can be found at http://www.eastwest.ngo/info/increasing-global-availability-and-use-secure-ict-products-and-services.
The breakthrough group's work is led by a team of representatives from Microsoft Corporation, Huawei Technologies, and Palo Alto Networks.

EastWest Institute

Global Cooperation in Cyberspace Initiative

SUPPORTERS

Microsoft
Huawei Technologies
Palo Alto Networks
NXP Semiconductors
Qihoo 360
Unisys
CenturyLink
The William and Flora Hewlett Foundation

PARTNERS

IEEE Communications Society
Internet & Jurisdiction Project
Munich Security Conference
The Open Group
The University of New South Wales

Building Trust
Delivering Solutions

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow, Washington, D.C. and San Francisco. Learn more at **www.eastwest.ngo**.