Public-Private Cooperation to Support Cybersecurity for Development

Cybersecurity supports development

The Tunis Agenda sets a goal of “building confidence and security in the use of information and communication technologies” (ICT)\(^1\). A culture of cybersecurity helps to build trust in the digital environment, enabling economic growth, social inclusion, and innovation. In fact, a recent OECD report recommended that cybersecurity be treated as an economic issue, rather than solely a technical one, given the critical role it plays in the achievement of social and economic goals.\(^2\) As ICT increasingly becomes essential to everyday life, its security has undeniably become a development issue.

Trust in ICTs is vital to achieving the United Nations Sustainable Development Goals

Looking at cybersecurity through the lens of the Sustainable Development Goals (SDGs) demonstrates the socio-economic importance of trust in and security of the digital environment. Effective use of innovative technologies is critical to the realization of many of the SDGs, and the path to those goals would be substantially undermined in the absence of appropriate cybersecurity practices – either by reducing trust and therefore ICT adoption, or simply through the financial and personal costs of cyber-attacks. Following are some examples of how select SDG goals can be furthered by the trusted use of ICTs:

- **Develop industry, innovation, and infrastructure (SDG 9):** ICT can enable better management of infrastructure roll-out and maintenance, increase agricultural productivity, and provide additional business opportunities and market intelligence through online services.

- **Achieve gender equality and empower all women and girls (SDG 5):** ICT can enable access to information and services that empower women to participate and succeed in academia and business. Capacity building and user education on staying safe online can boost technology use to this end.

- **Make cities inclusive, safe, resilient and sustainable (SDG 11):** ICT can enable sensing and communication technologies to more efficiently use resources, detect and mitigate natural disasters.

- **Revitalize the global partnership for sustainable development (SDG 17):** ICT can connect people and institutions, enable sharing of information, and ultimately further the cross-pollination of ideas and innovation across industries.

Industry and government have important roles to play in cybersecurity

Cybersecurity is a true common cause, as industry shares many risks and objectives with governments, users, and other stakeholders. The breadth of cybersecurity threats is vast; from cyber terrorism to online safety and conventional cybercrimes. For this reason, and because cyber threats transcend borders, discussion and action on the topic are distributed across many venues, using national, regional, multilateral, and multistakeholder models, examples of which can be seen in Figure 1.

While the United Nations (UN) Group of Government Experts (GGE) coordinates among Members States on norms for cybersecurity\(^3\) and the Council of Europe’s Budapest Convention on Cybercrime created the foundation for trust relationships among signatories and coordinates technical cooperation programs,\(^4\) the Internet Society

---

shares tools and industry partnerships to combat spam, and the 50+ organizations and states of the Global Forum on Cyber Expertise (GFCE) scale practical initiatives on cybercrime and e-governance to the global level.

To support the SDGs, industry contributes through technology development, sharing of best practices, capacity building, and coordination on online safety. Governments have a role to play on issues such as cyberterrorism and state-sponsored attacks. Governments also play a critical role in raising awareness, promoting the use of globally recognized cybersecurity standards and tools, and educating users about cybersecurity practices.

Industry also often collaborates with governments and other organizations to address cybersecurity issues. While the models for cooperation vary, all benefit from drawing on diverse expertise and perspectives. Recognizing this value, the Tunis Agenda reaffirms “the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity.” Industry is committed to this goal.

---

### How can the private sector help?

Industry is well positioned not only to build and maintain the security of its own technologies but to share best practices and to join with others in securing the digital ecosystem. One example is the Microsoft Active Protections Program, in which Microsoft shares vulnerability information with security software providers, enabling them to provide faster protection to customers. Collaborative approaches such as this one enable a greater number of stakeholders to benefit from expertise and lessons learned, and in turn contribute to managing cybersecurity risk.

The role of the private sector can generally be divided into two categories: (1) capacity building through training and awareness raising with policy-makers and other stakeholders; and (2) operational collaboration, through developing highly secure technology, sharing best practices, and facilitating a multistakeholder response to assist in preventing, identifying, and responding to cyber threats.

Specific activities by the private sector that contribute to confidence in the use of ICTs include:

- development and sharing of global best practice in prevention, mitigation, and resilience; and presentation of risk trends;
- provision of technology, including highly secure communications, automated solutions for information sharing, and response management; and
- unified development of threat analysis methodology and mechanisms.

---

5 [http://www.internetsociety.org/spamtoolkit](http://www.internetsociety.org/spamtoolkit)
6 [http://www.thegfce.com/about](http://www.thegfce.com/about)
7 Tunis Agenda for the Information Society, paragraph 39, [http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html](http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html)
Effective cooperation: case studies

Capacity Building: Access to Cybersecurity Expertise for OAS Member States

The GFCE, the Organization of American States (OAS), and the governments of Argentina, Chile, and Estonia have launched an ongoing initiative called “Cyber Security in OAS Member States.” The project aims to build an integrated approach to cyber threats, and includes seven workstreams, covering topics such as adoption of technical standards, crisis management exercises, and best practice in e-government.9

One of the workstreams looks at “Access to Cybersecurity Expertise” and provides assistance in the formulation, implementation, and technical review of national cybersecurity policies. While the initial participants were government entities, the program has since expanded to include additional partners: private-sector companies, including Microsoft, Trend Micro and Symantec; academia via the Global Cyber Security Capacity Centre; and non-profit organizations, such as the World Economic Forum, the Latin American and Caribbean Network Information Center, and the Internet Corporation for Assigned Names and Numbers (ICANN).

This diverse partnership has enabled the 35 governments of the Americas to access relevant expertise through formal reports, and on-demand joint initiatives such as training activities, workshops, and roundtables. Through these activities, governments gain access to practical training in implementing the best practice presented.

Policy-making: NIST Framework for Improving Critical Infrastructure Cybersecurity

Effective risk management depends on many stakeholders – government, private sector, technical community, and end users – working together, sharing experience and best practice. Governments can therefore develop most effective policies by collaborating and obtaining buy-in from these same stakeholders during the policy development process. One example of this principle in action is the US Framework for Improving Critical Infrastructure Cybersecurity, which was developed by the National Institute for Standards and Technology (NIST).

The voluntary framework assists entities in determining their level of risk, and the corresponding maturity of their current cybersecurity practices. It is focused first and foremost on the most critical infrastructures for a country, therefore reflecting the need to prioritize cybersecurity resources effectively. Furthermore, the framework provides flexibility for organizations of different sizes and risk levels, and helps them prioritize the use of their resources for further mitigation of that risk.

The final voluntary guidance was issued in February 2014, based on existing standards and practices that have proved successful, and designed for adoption by critical infrastructure organizations.10 During its 12-month development of the Framework, NIST ensured that there were many opportunities for industry to provide input. In addition to accepting comments on an initial draft, which was published in July 2013, NIST hosted numerous regional workshops around the United States, inviting global stakeholders to participate in public conversations about what security guidelines the Framework should promote. Following the initial release, the framework created an ongoing partnership between stakeholders and the government, as NIST has committed to improving the document on an ongoing basis based on stakeholder comments.

As a result of NIST’s open and coordinated process, U.S. industry understands and is seeking to implement the voluntary Framework. For instance, Microsoft, Intel, and various banks, health care providers, and gas and electric companies have all proactively committed to implementing and benefitting from the Framework.

Standards development: The Information Security Forum

At the Information Security Forum (ISF), members participate in a trusted and confidential environment which focuses on sharing information and developing tools and best practices across a variety of sectors, including government and industry. The ISF has constructed evaluation tools, written best practices, and set standards for information security that are adopted on a voluntary basis by its members. In addition, it manages a secure

9 https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-security-oas-member-states
The ISF has dedicated chapters in 16 countries and a further four regional networks providing global coverage, and counts on more than 10,000 information security professionals to help its member organizations secure their critical information and infrastructure.

Since its founding in 1989, the ISF has grown to include some of the world’s largest brands—including IBM, Huawei, Nokia, and Tech Mahindra—as well as government agencies and academia. It has also opened its doors to Small and Midsize Enterprises, helping to create a culture of cybersecurity among SMEs.

The ISF Standard of Good Practice for Information Security is a comprehensive, voluntary, risk-based information security standard, covering more topics than the ISO standards on information security. It helps ensure compliance with the NIST Cyber Security Framework, UK Cyber Essentials, COBIT 5 and ISO 27002:2013 standards. In 2014, the Standard was updated to include topics such as Cyber Resilience, Supply Chain Security, Mobile Device Security, Cloud Privacy, and Critical Infrastructure Protection.11

Resources for governments

<table>
<thead>
<tr>
<th>ORGANIZATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Global Forum on Cyber Expertise – <a href="http://www.thegfce.com">www.thegfce.com</a></td>
</tr>
<tr>
<td>• Global Cyber Security Capacity Centre – <a href="http://www.oxfordmartin.ox.ac.uk/cybersecurity">www.oxfordmartin.ox.ac.uk/cybersecurity</a></td>
</tr>
<tr>
<td>• The Forum of Incident Response and Security Teams (FIRST) – <a href="http://www.first.org">www.first.org</a></td>
</tr>
<tr>
<td>• The Cybersecurity Capacity Portal – <a href="http://www.sbs.ox.ac.uk/cybersecurity-capacity">www.sbs.ox.ac.uk/cybersecurity-capacity</a></td>
</tr>
<tr>
<td>• United States Telecommunications Training Institute – <a href="http://www.ustti.org">www.ustti.org</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DOCUMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Moving Forward Together: Recommended Industry and Government Approaches for the Continued Growth and Security of Cyberspace – <a href="http://tinyurl.com/jeitamovingforward">tinyurl.com/jeitamovingforward</a></td>
</tr>
<tr>
<td>• Digital Security Risk Management, 2015 (OECD) – <a href="http://tinyurl.com/oecdsecurity">tinyurl.com/oecdsecurity</a></td>
</tr>
<tr>
<td>• The Budapest Convention on Cybercrime – <a href="http://tinyurl.com/budapestconvention">tinyurl.com/budapestconvention</a></td>
</tr>
<tr>
<td>• UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 – <a href="http://tinyurl.com/UNGGGE">tinyurl.com/UNGGGE</a></td>
</tr>
<tr>
<td>• Global Cyber Security Capability Maturity Model – <a href="http://tinyurl.com/cybercapability">tinyurl.com/cybercapability</a></td>
</tr>
</tbody>
</table>