USAID
FROM THE AMERICAN PEOPLE

BEST PRACTICES IN ICT POLICY

INTERNATIONAL CYBER-SECURITY: BUILDING TRUST

Within the last decade, digital technology has evolved to dominate our business and our personal communication. Issues of security of information, confidentiality of transmission, sender authentication, authorization to access information, and integrity of transactions have reappeared in new forms as the technological progress has provided new methods of accomplishing tasks.

How do we "know" who we are dealing with, when we cannot see or hear them? How do we protect ourselves, when we cannot see or feel our attackers, or when what they attack cannot be touched or seen?

Computers and ICTs have increased our productivity and effectiveness enormously, but they have also increased the effectiveness and impact of malicious behavior — through automated attacks, global networks, integrated nature of software applications, and split-second completion of transactions.

With almost all countries connected to the Internet, **cyber-security** as well as critical infrastructure protection have become **global issues that require active cooperation among individuals, organizations, enterprises and government,** at all levels.

Trust in Cyber-Space is Crucial for:

- Data integrity and communications privacy.
- A secure e-commerce framework.
- Consumer protection mechanisms in cyberspace.
- Maintenance of Intellectual Property Rights.
- Effective application of conventional legal issues and laws in cyberspace, in conventional areas such as fraud and theft.
- System and network security and crime detection and prevention.

dot-GOV DOTCOM ALLIANCE

dot-GOV, funded by U.S Agency for International Development (USAID) and implemented by Internews Network, Inc. works with USAID Missions and Bureaus to promote competitive policy and regulatory reforms in telecommunications and e-commerce to enhance economic and social development, and to attain universal access to information and communications technologies (ICTs).

Information courtesy of: George Sadowsky, Senior Technical Adviser to dot-GOV, Internews Network. Additional information was obtained from selected documents listed on the back page of this publication.

KEY POLICY APPROACHES TO INTERNATIONAL CYBER-SECURITY

With any kind of security, the main concerns are prevention, detection, and prosecution.

All three concerns have faced serious challenges as technology stretches the traditional methods in which have been used to provide security in the past.

CONSUMER PROTECTION AS A METHOD FOR CYBER-SECURITY

USAID, through dot-GOV, is helping the Telecommunications Regulators Association of Southern Africa (TRASA) to work with member countries develop compatible definitions of consumer protection, including privacy rules for telecommunications operators.

Consumer empowerment, through the customers' knowledge of their rights and the operators' responsibilities, is key in preventing fraud and providing security to private citizens.

PREVENTION

- **Restrict both physical and network access**, using firewalls, proxy servers, encryption, virtual private networks, and multiple data repositories.
- **Authenticate users** strongly, through means such as electronic signatures, public key encryption, digital certificates, and biometric recognition.
- **Identify critical infrastructure** — financial institutions, transportation networks, protective services, government networks — and develop business continuity strategies and backup systems.
- **Increase public awareness** of cyber-security issues in all sectors and enlist active cooperation of everyone involved at all levels.
- **Strengthen international expertise and cooperation** among all countries, working toward a uniform minimum level of security throughout the world.
- Adopt a l**egislative and regulatory framework** that actively enables legitimate use of ICT resources but strongly discourages misuse.

DETECTION

- Implement best of breed **computer and network based security systems** and educate broadly regarding awareness of potential and possible security incidents
- Create a **24/7 security analysis** capability in each country, all linked in a worldwide network, for **rapid notification and action** to combat security breaches
- **Define data and communications privacy and data property rights,** standards and expectations so that in the case of an attack, information can be shared quickly without compromising privacy.
- Promote **effective sharing of security holes**, alerts, breaches, and solutions between companies and governments.
- Increase **international cooperation to help trace and locate cyber-criminals**, since the nature of the Internet virtually assures that most incidents will be international in scope.

PROSECUTION

- Clearly **define laws on what constitutes cyber crime**, especially intellectual property rights and copyright law. Ensure that existing law is sufficient to address adequately criminal activities in cyberspace.
- Ensure that **laws and regulations** have a form that **apply equally to non-electronic and electronic rights and crimes.**
- **Train investigators** internationally in **proper forensics procedure**, including establishing chains of electronic evidence in cyberspace, so that local and international criminal prosecutions can be effective.

LAW ENFORCEMENT METHODS OF TRACKING AND PROSECUTING CYBER-CRIME

USAID, through the dot-GOV program, provided an experienced consultant to join a US Department of Justice team to support the development of a cyber-security and cyber-crime response unit in Indonesia.

The consultant established a ground-breaking electronic forensics laboratory and trained officials in its use. As a direct result, a hacker who attempted to break into the Indonesian electoral system was caught and prosecuted.

- Create **international agreements on the sharing of evidence** and the prosecution of cyber crime across national borders.

IMPROVED REGIONAL RESPONSIVENESS AND COLLABORATION

USAID worked with the US State Department to help organize the South East Europe (SEE) Cyber-security Conference in Bulgaria, where representatives from 14 SEE countries met to discuss the need for a regional strategy addressing cyber-crime.

Participants worked on collaboration plans at national and regional levels to protect critical information infrastructures by creating a culture of cyber-security through education and awareness-building; information-sharing; and government-industry cooperation.

NEW REQUIREMENTS FOR CYBER-SECURITY

Cyber-security requires more effort and care from businesses, governments and citizens than traditional security – notably:

- Higher levels of **cooperation and interaction between the public and private sectors** and international actors.
- A new dimension of **technical training for** security experts and law enforcement officials.
- Different forms of i**nformation tracking and logging.**
- Development and dissemination of **best practices, guidelines, shared standards and protocols, and research results.**
- **Faster response times** – often within minutes of notification of an attack.
- A great deal of **information sharing, public awareness, and education.** This information needs to be treated cautiously because information about successful attacks can damage an organization's reputation and encourage repeat attacks.
- Commitment to **common standards of privacy and civil liberties**.

CIVIL LIBERTIES AND CYBER-SECURITY

Governments must balance the need to protect public security with the need to protect individual rights to privacy. This balance becomes especially challenging when criminals are using digital technologies to plan and commit crimes.

The current environment of terrorist threats makes it tempting to shift this balance towards national security and to encroach upon civil liberties beyond the previous balance point. Digital technologies can be used very effectively for information gathering and surveillance in many ways. In formulating laws and regulations with respect to cyberspace, cybercrime, and critical infrastructure protection, it is important to use the new powers of digital technologies to gather information and access in a manner that continues to respect individual rights.

Active and informed engagement of civil society with governments is essential to inform them of the impacts, positive and negative, of cyber-security decisions as well as to be part of a national debate weighing the balance of security and individual liberties. The more intrusive the investigative technology is, the more need for safeguards and checks and balances against its improper usage.

Suggested Reading:

The Context for Cyber-Security and International Development, Jonathan Metzger, USAID ANE Bureau, DOT-COM Presentation September 2004 http://www.dot-com-alliance.org/resourceptrdb/uploads/partnerfile/upload/85/Metzger.PDF

Council of Europe Convention on Cybercrime, November 2001 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Cyber-Security Issues in International Development, James Dempsey, Center for Democracy and Technology, September 2004 http://www.dot-com-alliance.org/resourceptrdb/uploads/partnerfile/upload/87/Dempsey-Security-PRINT.pdf

Cyber-Security Issues: Business & Economic Considerations, Jody R. Westby, American Bar Association, Privacy & Computer Crime Committee DOT-COM Presentation, September 16, 2004 http://www.dot-com-alliance.org/resourceptrdb/uploads/partnerfile/upload/83/Westby.PDF

Cyber-Security and the Need for Legal Infrastructures, Richard W. Downing, Computer Crime & Intellectual Property Section, U.S. Department of Justice, Criminal Division, DOT-COM Presentation, September 2004 http://www.dot-com-alliance.org/resourceptrdb/uploads/partnerfile/upload/84/R_Downing.pdf

Documents from the South East European Cyber-security Cooperation Conference http://www.cybersecuritycooperation.org/documents.html

Draft Model Law on Electronic Transactions for SADC Countries, Jayantha Fernando, SADC Model Laws on E-commerce Regional Workshop, November 2003

Information Technology Security Handbook, George Sadowsky, James Dempsey, Alan Greenberg, Barbara Mack, Alan Schwartz, World Bank infoDev Project http://www.infodev-security.net/handbook/

International Guide to Combating Cybercrime, American Bar Association http://www.abanet.org/abapubs/books/54500301/

Introduction to Legal Reforms On Electronic Transactions and Data Protection, Jayantha Fernando, SADC Model Laws on E-commerce Regional Workshop, November 2003

Project Overview, Indonesia National Police Cyber Crime Assistance Project, Michael L. Woodson, DATE 2004

Secrets and Lies: Digital Security in a Networked World, Bruce Schneier, Wiley; August 2000.

Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime. Global Internet Policy Initiative (GIPI), August 2002. http://www.internetpolicy.net/cybercrime/020800cybercrime.pdf

www.terror.net: How Modern Terrorism Uses the Internet: SPECIAL REPORT 116, Gabriel Weimann, United States Institute of Peace, March 2004 http://www.usip.org/pubs/specialreports/sr116.html

For more information, please contact:

USAID

Laura Samotshozo
dot-GOV Manager
EGAT/EIT/IT
202-712-4562
lsamotshozo@usaid.gov

Edward Malloy
Telecommunications Advisor
EGAT/EIT/IT
202-712-1579
emalloy@usaid.gov

dot-GOV

Sarah Tisch
Program Director
Internews Network
202-833-5740 x 203
stisch@internews.org

George Sadowsky
Sr. Technical Advisor
Internews Network
202 833-5740 x 200
george.sadowsky@internews.org

Alejandro Bermudez Del-Villar
Program Associate
Internews Network
202-833-5740 x 205
ahbermudez@internews.org

Funding for dot-GOV is provided by the U.S. Agency for International Development (USAID), Bureau for Economic Growth, Agriculture & Trade, Office of Energy and Information Technology (EGAT/EIT/IT) and Office of Women in Development (EGAT/WID), under the terms of Award number: GDG-A-00-01-00009-00. The views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

http://www.dot-com-alliance.org