ITU Workshop on ICT Security Standardization Challenges for Developing Countries

Geneva, Switzerland, 15-16 September 2014

The main objective of the workshop is to present and discuss ICT security challenges, in particular for Developing Countries. The objective is to provide concrete advice and best practices of international ICT security standards such that standardization competence can be enhanced. The workshop also aims to improve and yield better collaboration with other standards-setting organizations.

The workshop will bring together leading specialists in the field, from ITU members, regulatory agencies, policy makers, service providers, telecommunication operators, manufacturers, solution providers, academia, standardization organizations, forums and consortia.

Participation is open to ITU members and to any individual from a country which is a member of ITU who wishes to contribute to the work. This includes individuals who are also members of international, regional and national organizations. The workshop is free of charge but no fellowships will be granted.

The workshop will open at 1400 hours on 15 September 2014. Registration will begin at 1300 hours.

Draft Programme

Day 1: 15 September 2014

14:00 – 14:30

Opening Session
Chairman: George Lin

Session Objectives
The objective of the workshop is to present activities and achievements of standardization on cybersecurity, data protection, trust services and cloud computing, focus in methodology of securing ICT within critical infrastructure, hear a reaction from security industry, address the interests and needs of users, and encourage collaboration between SDOs in security standardization for the special needs of developing countries.

14:30 – 16:30

Session 1 – ICT infrastructure development, new security threats and counter-measures
Chairman: Patrick Mwesigwa

Session Objectives
Today the critical role of ICT in virtually all socio-economic activities cannot be over-emphasized. Disruption of the ICT infrastructure can therefore result in disastrous consequences for governments as well as citizens' social wellbeing. The need to ensure ICT robustness against cyber-attacks remains a key challenge at national as well as global level.

This session will address the current situation of ICT infrastructure development and the challenges such as new security threats and countermeasures including new trends in ICT. The session will highlight best practices in formulation of national strategies, government and industrial collaboration, sound legal formulation to fight cybercrime, national incident capabilities, and importance of rising national awareness on cybersecurity, among other things.

16:45 – 18:30

Session 2 – End user security round table from both public and private sectors
Chairman: Koji Nakao

Session Objectives
After a set of presentations that highlight "end user security" in terms of identified security issues and requirements from each presenter's perspective, a roundtable discussion will explore and identify security requirements/security capabilities required from the end user's view points and how to utilize security technologies/standards.

Members of the roundtable discussion will cover both public and private sectors such as critical information infrastructure sectors, medical sector, educational sector (university) and telecom/mobile sectors etc.

Day 2: 16 September 2014

09:00 – 10:45 **Session 3 – Cybersecurity and data protection**
Chairman: Sacid Sarikaya

Session Objectives
Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment. Widespread use of internet technologies and increasing number of cyber threats make cyber security more important. In this session, representatives from Kenya will share their cyber security experiences and challenges. Also, ITU-T cyber security standards, information exchange techniques, and ITU-D cyber security studies will be presented by the experts.

11:00 – 12:45 **Session 4 – ICT role in critical infrastructure protection**
Chairman: Antonio Guimaraes

Session Objectives
Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society, such as energy, transportation, telecommunication, water supply, agriculture, public health, financial services, etc. Most critical infrastructures rely on Information and Communication Technologies (ICTs), including industrial control systems (ICS), to perform essential functions. This dependency represents potential vulnerabilities and risks to operations. This section will focus in existing ICT security standards, guidelines, methodologies, and practices to enable critical infrastructure providers to achieve the resilience required.

14:00 – 15:45 **Session 5 – Trust services and cloud security**
Chairman: Heung Youl Youm

Session Objectives
Cloud computing is a model for enabling service user's ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. Identity management (IdM) is the management of the life cycle and use of identity information. This session will focus on presenting existing ICT security standards, guidelines, and best practices in the area of cloud computing security and identity management to ensure trust services and cloud computing security.

16:00 – 17:45 **Session 6 – Security standardization challenges**
Chairman: Herb Bertine

Session Objectives
After a set of presentations that highlight ICT security standardization efforts in international and regional bodies, a roundtable discussion will explore security standardization challenges. Topics will include insights on the benefits and challenges associated with collaboration and cooperation and on challenges associated with ensuring standards will meet the needs of users, especially those in developing countries.

17:45 – 18:30 **Closing panel**
Chairman: Mohammed Elhaj

Session Objectives
Summary and conclusions, final discussion, and closing remarks.

Workshop webpage: **www.itu.int/en/ITU-T/Workshops-and-Seminars/ict-sec-chaldc/**
Contact: **Martin Euchner, TSB, martin.euchner@itu.int**