



Mr. Malcolm Johnson
Director,
ITU Telecommunication Standardization Bureau

ITU Open Forum on Cybersecurity

Opening Remarks (Extract Hyderabad, India. 06 December 2008

Ladies and Gentlemen,

Good morning ladies and gentlemen and welcome to this ITU Open Forum on Cybersecurity.

This Open Forum is an opportunity to continue the dialogue started last year in Rio to discuss with other stakeholders how to win the war against cyber-threats.

According to a new study by a well known internet security company (Symantec) the underground economy is booming... even as the rest of the global economy heads towards recession.

The company reports that the cybercrime economy has grown into an efficient, global marketplace to handle the trade in stolen goods and fraud-related services.

It estimates the combined value of goods in underground forums at \$276m for the 12 months prior to the end of June 2008.

The international community has in its power the ability to show these people that crime does not pay.

It has never been more important for those that seek to defend the safety, security and integrity of the world's ICT networks to step up their efforts.

A fundamental role of ITU, following the World Summit on the Information Society (WSIS) is to build confidence and security in the use of information and communication technologies (ICTs). Heads of states and government and other global leaders participating in WSIS entrusted ITU to take concrete steps towards curbing the threats and insecurities related to the information society.

As a consequence ITU launched the Global Cybersecurity Agenda (GCA) in March 2007, and more recently its Child Online Protection initiative.

A High-Level Experts Group (HLEG) provided expert advice and guidance to the ITU Secretary-General on strategies to promote cybersecurity.

This expert panel attracted top specialists from the likes of AT&T, Intel, Microsoft, Interpol, Verisign, as well as high-level government, academic and industry representatives from across the world

These people have contributed their insights and thought leadership on how best to tackle the growing challenges to the security of the online world.

An important part of this process is standardization work, to ensure that common standards for network security are adopted as widely as possible.

Not only will harmonization of standards increase the level of security, it will also reduce the costs of building secure systems.

ITU-T Study Group 17 has the lead responsibility for security.

I am happy to welcome the recently appointed chairman of this group, Mr Arkadiy Kremer here today.

There are now literally hundreds of ITU-T Recommendations on security, or which have security implications. All these standards are now available for downloading free of charge from the ITU website.

We also provide on our website an ICT Security Standards Roadmap to assist in the development of security standards by bringing together information about existing standards and current standards work in ITU and other key standards development organizations.

The recently concluded World Telecommunication Standards Assembly mandated ITU-T to identify best practices to establish Computer Incident Response Teams and to collaborate with international experts and bodies to realize their establishment in particular in developing countries.

Ongoing ITU-T work on security includes architecture and frameworks; cybersecurity; risk management; incident handling; traceback; countering spam; identity management; security for NGN, IPTV, home networks, mobiles etc.

The work on traceback has garnered much publicity as you may have seen.

Traceback enables the determination of the origin of electronic communications that will mitigate denial of service (DoS) attacks and short message service (SMS) spam.

Work on traceback will also better enable settlements for carrying traffic over IP networks, and provide consumer protection from cyber crimes such as stalking and child pornography.

One particularly urgent area of work is in combatting identity theft, which was identified in an ITU survey as the biggest fear preventing users from placing more trust in online networks.

The survey by Symantec that I referred to reports that login details for online accounts are the second most commonly offered commodity by cyber criminals.

An ITU-T Focus Group on this topic completed its work in September 2007.

Its work is now being processed by Mr Kremer's Study Group 17.

The adoption of multiple – proprietary – approaches is, experts agree, an inherently more vulnerable approach.

ITU-T is in a unique position given its international scope and the fact that it brings together the private sector and governments to coordinate work on standards and influence the harmonization of security practices worldwide.

The ITU's Development sector also does some significant work in the field.

ITU-D provides expertise through its work programme with initiatives and projects designed to respond to the needs of the Member States for assuring safer ICTs.

This work programme includes the organization of regional forums and workshops, with recent events held in Bulgaria, Zambia, Australia, Qatar, Cape Verde, Argentina, and Vietnam, to name a few, to build the necessary capacity for countries to tackle cyber-threats effectively. As with all ITU workshops these are open to anyone to attend free of charge.

ITU-D is also responsible for the production of various guides and manuals, such as the national cybersecurity self-assessment tool, the botnet mitigation toolkit, a study on the economic aspects of network security, cybersecurity best practice documents, road maps and action plans.

ITU-D is also very active in the development watch, warning and incident response capabilities, and concrete activities related to enhancing Child Online Protection, to face the emerging risks to cyberspace.

In terms of the work of ITU's Radiocommunication sector – ITU-R I can report that many of ITU's Radio Recommendations on generic requirements and the protection of radiocommunications against interference are relevant to security.

ITU-R has also published Recommendations on security principles for next generation mobile.

Ladies and Gentlemen, in the real – non-virtual – world, risk management is well understood and so the infrastructure has been developed to protect against theft, fraud and other kinds of attack.

The virtual world should be no different. ITU's work can provide the backbone for this risk-management infrastructure.

As we will explain during this Forum ITU can give businesses and countries the systematic approach to information security that they need to keep network assets safe. I hope you find it interesting and look forward to your contribution to our work.