World Summit on the Information Society
Turning targets into action

WSIS+10
HIGH-LEVEL EVENT

Document Number: WSIS+10/4/2

Note: This Executive Summary captures the main achievements, challenges and recommendations of the Action Line during the 10-year period of WSIS Implementation; this has been submitted by the Action Line Facilitator in response to the request by the participants of the Third WSIS+10 MPP meeting. The complete report on the 10-Year Implementation of the Action line was submitted to the Third WSIS+10 MPP meeting held on 17-18 February 2014 and is available at the following url: www.itu.int/wsis/review/reports/#actionline

10-Year WSIS Action Line Facilitator's Reports on the Implementation of WSIS Outcomes
WSIS Action Line – C5: Building confidence and security in the use of ICTs
Lead Facilitator: ITU

Executive Summary

1. Introduction

This document presents a brief summary of the progress made in the implementation of Action Line C5 since WSIS (2005), and highlights some emerging trends and related post-2015 potential challenges.

2. Achievements

2.1. Some of the areas of Action Line C5 that saw good progress are:

a) **Education/Awareness** as part of most national cybersecurity strategies.
b) **Fight against SPAM** resulting in decreasing numbers of spam and phishing attacks.
c) Worldwide growth in the **use of electronic documents and transactions.**
d) **Sharing of best practices** at national and international level.
e) Increase of the **incident response** capabilities of many organizations and governments
f) Growing focus on the **security of Online Transactions**.

2.2. Some of the areas that, despite current efforts, may not have been sufficiently addressed are:

a) **Cooperation between governments:** Some initiatives exist but appear fragmented.

b) **Response to Cybercrime (Public Private Partnership):** A close cooperation between both public and private actors is needed to reach a shared situational awareness that can help organizations to understand the real risk and the correct action to be taken to counter cybercrime.

c) **Strengthening the Trust Framework:** Increasing the level of trust in digital services, in cybersecurity and creating a trusted environment between public and private

organizations are key challenges. The level of citizen trust in digital services and the Internet must be improved.

d) **Encouraging further development of secure and reliable applications:** Application security breach and related incidents due to the exploitation of application-level vulnerabilities are common. Many organizations still struggle with the most basic security flaws.

e) **Developing a nation-wide approach to cybersecurity - integrated within the overall national ICT policy and strategy:** Many countries are addressing cybersecurity as a separate element and not as an integral part of the national ICT strategy.

3. Challenges

Challenge #1: The ubiquitous nature of the Internet has facilitated the cross-border emancipation of digital activity, both legitimate and illegal. The lack of adequate international cooperative efforts aimed at tackling the issue has been a real boon for cybercrime. Despite some regional efforts, **international cooperation** is still quite fragmented.

Challenge #2: Malware is becoming **increasingly complex**, using a variety of tools and techniques to mount high-level cyber attacks that can thwart even the most comprehensive cybersecurity defences.

Challenge #3: **The nature of the Internet and Digital services is evolving** at an incredible pace, changing the role of the actors involved.

Challenge #4: Lack of strong authentication mechanisms for verifying identities and granting access to online resources are challenges in combating fraud and forgery. Most of the online services rely on **digital identities** that are protected by a password. Such security features have been proved to be weak.

Challenge #5: The emergence of connected **smart devices** other than smartphones and tablets is increasingly being made possible by the growth of machine to machine (M2M) communications. However, the technology's continued success will depend on its ability to respond to a number of pressing challenges. Currently, the M2M landscape lacks basic security requirements.

***Challenge #6*:** High-profile enterprises, such as multi-national organizations, and those in critical sectors, such as finance, energy, and pharmaceutical, for example, will be preferred targets across all threat actor groups. For this reason, **intelligence and effective incident response mechanisms** are key needs for organizations.

Challenge #7: The lack of public awareness of new threats, such as APTs and mobile threats and vulnerabilities is hampering the full development of a global culture of cybersecurity. End-users and individual consumers have not yet realised the full implications of not securing their devices and personal data and current efforts in **awareness-raising are not sufficient**.

Challenge #8: Many governments and organisations have developed **best practices** that could reduce vulnerabilities and could help better manage cybersecurity incidents. Unfortunately these best practices are not always shared and are underused.

Challenge #9: **Standards** could help both governments and the private sector increase their security, identify better solutions and also make international cooperation easier. There are different types of standards such as technical, functional, mandatory, optional and sector-specific. Each of these is the

result of knowledge and wisdom acquired on specific cybersecurity aspects that, when shared, can enhance the capabilities of all users.

Challenge #10**:** Few **measures/metrics** are available for cybersecurity. In technology, what cannot be measured cannot be protected and this is also valid for cybersecurity. There is a need for better metrics and performance indicators to be developed and shared.

Challenge #11**: Cloud computing** is a big opportunity and will continue to play a major role in the ICT environment. At the same time, cloud computing presents cybersecurity issues at different levels - technical, organizational, procedural and legal – that have to be addressed.

Challenge #12**: Protecting children and teenagers** in cyber space is a growing concern. The number of digital platforms from which they can access the Internet is constantly increasing. Understanding the dangers and the motivations behind threat actors, as well as the effects of new technologies on children can help determine suitable solutions.

Challenge #13**:** Despite many countries having launched their **National CERTs**, several CERTs worldwide do not yet have the capability to address the increasing complexity of cyber-related threats. This is in large part because most countries do not have a comprehensive **National Cyber Security Strategy**. Unfortunately, cybersecurity is not yet at the core of many national and industrial technology strategies.

4. Recommendations

4.1 Continue to strengthen international cooperation mechanisms, including through:

- Country to country relations through discussion forums and information sharing.
- Public-private partnerships

4.2 Support the development of national capabilities by nation states, such as the assessments for national CIRTs/CERTs / CSIRTs and the elaboration of national cybersecurity strategies.

4.3 Enable better understanding of cybersecurity demands and requirements by working on indices and metrics for measuring cybersecurity development and implementation levels.

4.4 Underpin cooperation and support efforts for the elaboration of cybersecurity standards and other technical specifications

4.5 Support cybersecurity development as applied to different sectors and technologies: critical infrastructure, mobile, cloud services, etc.

4.6 Understand and further cooperate for the protection of vulnerable groups: children, newly connected people, etc.

4.7 Provide a repository and database for multi-national efforts, information sharing, standardization work, events, best practices, guidelines, legal practices of bodies working on cybersecurity development and cybercrime prevention.