Sector de Desarrollo de las Telecomunicaciones

Reunión Preparatoria Regional de la CMDT-10
para la Región de las Américas
Santa Marta, Colombia, 9 - 11 de septiembre de 2009

Document RPM-AMS09/48-S
10 de septiembre de 2009

Original: English

Para información

SOURCE **Telecommunication Development Bureau**

TITLE **Iniciativa ITU-IMPACT**

Contacto: Nombre/Organización/Entidad: M. Maniewicz, Jefe, BDT/POL
Teléfono: +41 22 730 5421
Correo-e: mario.maniewicz@itu.int

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

Oficina de Desarrollo
de las Telecomunicaciones

T E L E F A X

Place des Nations
CH-1211 Ginebra 20
Suiza

Teléfono +41 22 730 51 11
Telefax Gr3: +41 22 733 72 56
Gr4: +41 22 730 65 00

Fecha: **Hora:** **Página 1/8** **Ref.:** BDT/POL/CYB DM-136

To: **Fax:**

cc: Sr. Mohd Noor Amin, Presidente, Junta de Administración, IMPACT — mohd.amin@impact-alliance.org

Contacto: Marco Obiso, Asesor Aplicaciones TIC y ciberseguridad, BDT/POL

Para su respuesta:
Correo-e: cybmail@itu.int

Fax: +41 22 730 5484 **Tel.:** +41 22 730 6760

Asunto: Creación de capacidades de ciberseguridad – Centro de respuesta global IMPACT

«tpa_opening»

Tengo el gusto de comunicar a esa Administración que, durante la reunión de 2008 del Consejo de la Unión Internacional de Telecomunicaciones (UIT) y el Foro sobre la Gobernanza de Internet, hubo debates sobre la Iniciativa Alianza Internacional Multilateral contra el Ciberterrorismo (IMPACT).

La UIT e IMPACT concertaron oficialmente un Memorándum de Entendimiento con arreglo al cual la modernísima sede mundial de IMPACT en Cyberjaya (Malasia) será de hecho la sede física de la Agenda sobre Ciberseguridad Global de la UIT.

La Agenda sobre Ciberseguridad Global de la UIT (GCA), que el Dr. Hamadoun I. Touré, Secretario General de la UIT, lanzó en 2007, es un marco de cooperación internacional que tiene por objeto mejorar la confianza y seguridad en la sociedad de la información.

Dadas las estrechas sinergias entre los cinco ámbitos de trabajo de la Agenda sobre Ciberseguridad Global y los servicios e infraestructuras facilitados por IMPACT, una asociación mixta es una etapa lógica de la lucha mundial contra las ciberamenazas, la ciberdelincuencia y otros usos indebidos de las tecnologías de la información y la comunicación.

La UIT, a través de su Sector de Desarrollo de las Telecomunicaciones, ha acumulado una experiencia considerable en la facilitación del establecimiento de estrategias nacionales para la ciberseguridad y la protección de infraestructuras esenciales de la información, con inclusión del desarrollo de capacidades, y puede recurrir a una extensa red de grandes autoridades de la ciberseguridad.

A fin de tratar de manera apropiada los cinco ámbitos identificados por la GCA, y a fin de continuar los trabajos de la UIT encaminados a ayudar a los países a desarrollar capacidades de ciberseguridad, la UIT está colaborando con IMPACT para poner los recursos siguientes a la disposición de los Estados Miembros de la UIT:

- Centro de respuesta global.
- Capacitación y desarrollo de aptitudes.
- Centro de garantías de seguridad e investigación.
- Centro de políticas y cooperación internacional.

El primer servicio disponible será el Centro de Respuesta Global (GRC):

El GRC está concebido para ser el principal centro de recursos del mundo sobre ciberamenazas. En colaboración con, entre otros, instituciones docentes y gobiernos, el centro ofrecerá a la comunidad mundial un sistema total de alerta temprana en tiempo real. Este "sistema de alerta temprana en red" (NEWS, Network Early Warning System) ayudará a los países miembros a identificar rápidamente las ciberamenazas y les orientará sobre las medidas que pueden tomar para mitigar sus efectos.

El GRC proporcionará a los Estados Miembros de la UIT acceso a herramientas y sistemas especializados, tales como la reciente "Plataforma de aplicación colaborativa y electrónicamente segura para expertos" (ESCAPE, Electronically Secure Collaborative Application Platform for Experts). ESCAPE es una herramienta electrónica con la cual ciberexpertos autorizados de varios países pueden aunar recursos y colaborar a distancia, en un entorno seguro y fiable. Al aunar en poco tiempo recursos y conocimientos de muchos países, ESCAPE permitirá que los países y la comunidad mundial respondan inmediatamente a ciberamenazas, especialmente en situaciones de crisis.

Además de lo que propone el GRC, IMPACT ofrecerá a los Estados Miembros en desarrollo que reúnan las condiciones, becas escolares para cursos de capacitación impartidos a través del Instituto SANS (Estados Unidos). La capacitación consistirá principalmente en crear un acervo de conocimientos que se puedan compartir posteriormente, para crear capacidades y conocimientos nacionales en materia de ciberseguridad.

En el marco de los preparativos de la Conferencia Mundial de Desarrollo de las Telecomunicaciones de 2010, en 2009 y 2010 se celebrarán reuniones preparatorias regionales (RPR) en todas las regiones de la UIT, que se espera contribuyan a determinar los objetivos y estrategias para un desarrollo regional equilibrado de las telecomunicaciones y las TIC. Durante esas reuniones se dedicarán sesiones especiales a la colaboración UIT-IMPACT, a fin de presentar la iniciativa y las actividades conexas a los Estados Miembros de la UIT.

Se adjunta información adicional sobre el GRC. También se puede consultar información adicional en línea en la dirección www.itu.int/osg/csd/cybersecurity/gca/impact/. Los servicios del GRC se pueden adaptar a las necesidades particulares de los Estados Miembros.

Para participar en las actividades mencionadas, responda a la presente carta, indicando el ámbito y los servicios específicos que interesan a su país.

Le recibiremos con gusto en la coalición y esperamos con impaciencia su valiosa contribución sobre cómo ayudar de manera apropiada a los Estados Miembros de la UIT.

Muchas gracias.

«tpa_closing»

[original firmado]

Sami Al Basheer Al Morshid
Director

Anexo: Nota técnica: Centro de Respuesta Global

Copia: SGO - CSD (A. Ntoko)
Jefes de las Oficinas Regionales

IMPACT Centro de respuesta global

Unión Internacional de Telecomunicaciones

Comprometida a conectar el mundo

Nota Técnica

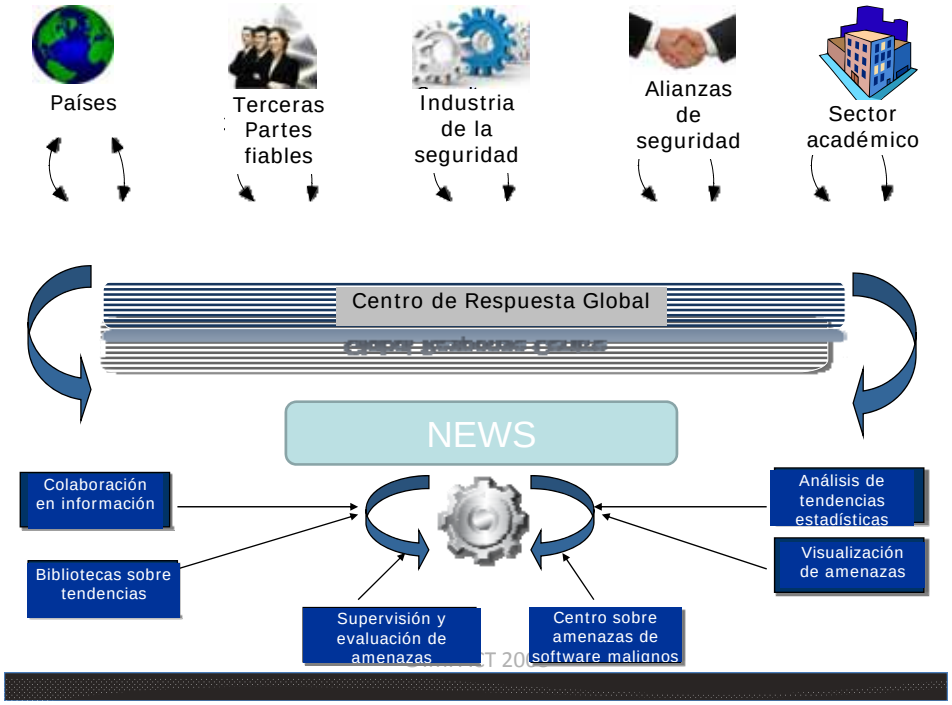
CENTRO DE RESPUESTA GLOBAL

INTRODUCCIÓN

El Centro de Respuesta Global (GRC) de IMPACT es el principal centro de recursos sobre ciberamenazas de que dispone la comunidad mundial. Proporciona respuestas de emergencia para facilitar la identificación de ciberamenazas y compartir recursos para ayudar a los miembros de IMPACT. Los dos elementos más destacados del GRC son NEWS (*Sistema de alerta temprana en red*) y ESCAPE (*Plataforma de aplicación colaborativa y electrónicamente segura para expertos*).

NEWS (Sistema de alerta temprana en red)

El GRC, en colaboración con grandes asociados del sector industrial, el sector docente y los gobiernos (Symantec Corporation, Kaspersky Labs, F-Secure, Trend Micro, SANS institute etc., son varios de los asociados actuales), proporcionará a la comunidad mundial un sistema de alerta temprana en tiempo real - NEWS.



Así pues, NEWS podría servir para compartir y divulgar información actualizada sobre las tendencias de la seguridad. NEWS ofrece, por ejemplo, lo siguiente:

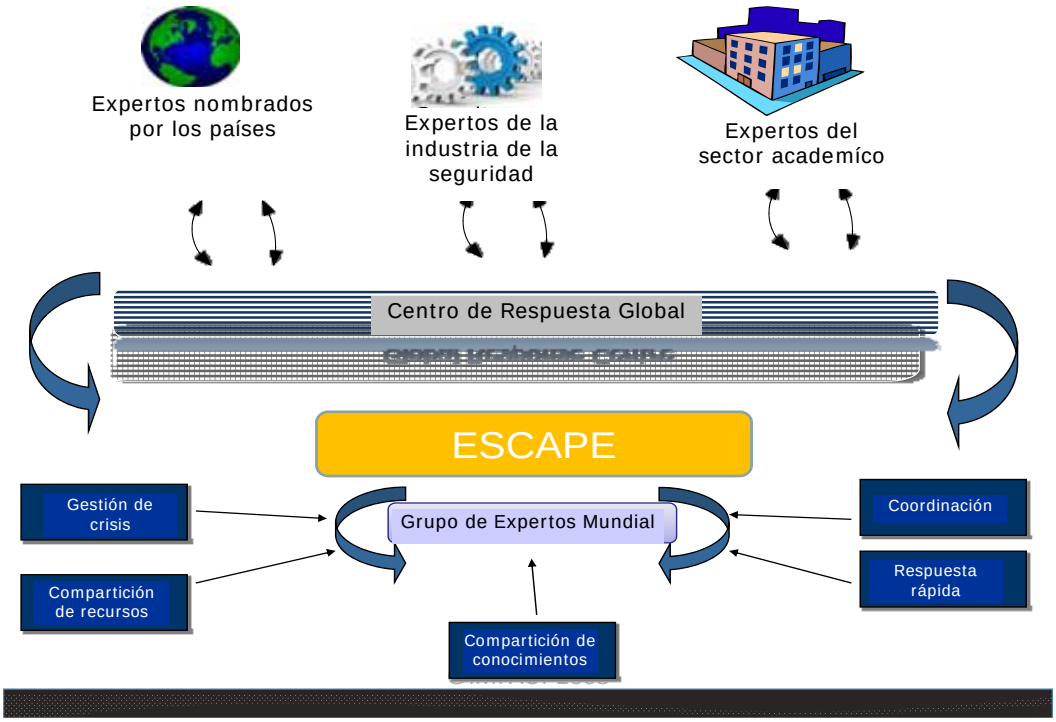
1) Supervisión y evaluación de amenazas en tiempo real: los países miembros pueden ver el nivel global de gravedad de una amenaza y las soluciones para mitigarla.

2) Análisis estadístico de las tendencias en materia de ciberamenazas: los países miembros pueden consultar las cibertendencias y amenazas más recientes en todo el mundo, presentadas en gráficos, curvas, mapas y cuadros fáciles de consultar.

3) Centro sobre amenazas de software maliciosos: los miembros pueden enviar software maliciosos y recibir información sobre los detalles técnicos completos del análisis correspondiente.

ESCAPE (Plataforma de aplicación colaborativa y electrónicamente segura para expertos)

Además de NEWS, IMPACT propone ESCAPE a sus países miembros. Se trata de un instrumento electrónico exclusivo con el cual ciberexpertos autorizados de distintos países pueden aunar recursos y colaborar a distancia en un entorno seguro y fiable.



Este sistema dispone de una base de datos completa y evolutiva de los principales recursos en todo el mundo – incluidos expertos IT, personas autorizadas (funcionarios públicos), y otros organismos de confianza (EIII), a los cuales se puede pedir ayuda durante una crisis. Así pues, los miembros pueden crear rápidamente un equipo de respuesta para tratar prácticamente cualquier ciberamenaza que se presente. Con su avanzada plataforma de colaboración y la posibilidad de acceder a expertos de los gobiernos, el sector académico y la industria privada, IMPACT es una plataforma sin igual para la respuesta de emergencia global.

Paquete inicial

Todos los países miembros reciben, cuando se inscriben, el paquete inicial del GRC, que les permite acceder a NEWS y ESCAPE. El sistema global de alerta temprana en red (NEWS) de IMPACT ofrece a sus miembros noticias actualizadas de las ciberamenazas en todo el mundo. Esas amenazas se extraen de datos procedentes de docenas de noticias de seguridad públicas y privadas y se presentan en una serie de gráficos, curvas, mapas y cuadros fáciles de leer. Con NEWS, los miembros pueden buscar los orígenes de los ataques en todo el mundo, identificar las ciberamenazas y los ataques contra la ciberseguridad actuales.

El paquete inicial también ofrece a los países miembros la posibilidad de entablar contacto con otros profesionales de la ciberseguridad de toda la red IMPACT a través de ESCAPE. Al aplicar las técnicas de contacto social de las empresas a los países miembros, IMPACT les permite aprovechar todo el acervo de conocimientos de la comunidad de IMPACT. El paquete inicial permite establecer cinco conexiones a ESCAPE y añadir expertos locales en ciberseguridad a la comunidad de expertos de IMPACT. Con este paquete, los países miembros pueden elevar sus problemas de seguridad a los expertos globales de IMPACT, que ofrecen asistencia y proponen soluciones apropiadas. Además, ESCAPE proporciona noticias periódicas sobre seguridad, informes, y la posibilidad de enviar software maliciosos a los expertos de IMPACT para que los estudien y analicen.

Para el paquete inicial, los miembros señalarán un miembro del equipo de intervención en caso de incidente de seguridad informática para proporcionar asistencia cuando sea necesario.

Dado que todos los equipos y software de los miembros del paquete inicial son hospedados por el Centro de Respuesta Global de IMPACT en Malasia, este sistema es ideal para los países que desean un mayor nivel de presencia y reconocimiento sin invertir en infraestructuras locales.

IMPACT – Funcionalidades ofrecidas por el paquete inicial

Descripción	Introducción
Centro de Respuesta Global	
• **Acceso a ESCAPE**	**Desde una dirección IP pública**
• **Capacidad de acceder a datos e imágenes de NEWS**	√
• **Número máximo de cuentas en el portal ESCAPE**	**5**
• **Capacidad de invitar expertos locales a la comunidad de expertos de IMPACT**	√
• **Capacidad de elevar incidentes a la comunidad de expertos de IMPACT**	√
• **Capacidad de enviar software maliciosos para que IMPACT los analice**	√
• **Capacidad de recibir noticias periódicas sobre seguridad**	√
• **Capacidad de recibir informes periódicos sobre seguridad (Genéricos)**	√
• **Capacidad de suscribir a contenido de ESCAPE**	√
• **Número mínimo de miembros del equipo de intervención en caso de incidente de seguridad informática nombrados**	**1**
Capacitación y desarrollo de capacidades	
• **Capacitación sobre ESCAPE**	√
• **Capacitación sobre NEWS**	√

Paquete estándar

Los países miembros que deciden desempeñar un papel más importante en IMPACT pueden optar por el paquete de miembro estándar. El paquete estándar ofrece muchos más servicios y posibilidades del GRC que el paquete inicial.

El paquete estándar ofrece, por ejemplo, cien conexiones simultáneas a ESCAPE, acceso a la base de conocimientos en línea de IMPACT, y acceso total a detalles técnicos de los software maliciosos enviados. El miembro estándar puede recibir informes de seguridad periódicos adaptados a sus propias necesidades (específicos de una región o de un sector de actividad industrial como petróleo y gas, finanzas, etc.).

Los miembros estándar de IMPACT reciben correos electrónicos, notificaciones por teléfono de emergencias de seguridad y, además, asistencia a través de los analistas y consultores de GRC. Los miembros estándar también pueden enviar solicitudes de servicio, acceder a reuniones en línea, patrocinar grupos privados, crear y consultar foros de discusión privados, crear y gestionar equipos de acceso limitado, etc.

Para proporcionar asistencia, en su caso, el país miembro dedica hasta cinco miembros del equipo de intervención en caso de incidente de seguridad informática en el paquete estándar. Los miembros estándar pueden optar por el alojamiento local o utilizar el Centro de Respuesta Global de IMPACT en las instalaciones de Malasia.

IMPACT – Funcionalidades estándar ofrecidas

Descripción	Estándar
Centro de Respuesta Global	
• **Acceso a ESCAPE**	**A partir de una dirección IP pública**
• **Capacidad de crear múltiples conexiones para acceder a ESCAPE**	√
• **Capacidad de acceder a datos e imágenes de NEWS**	√
• **Número máximo de cuentas en el portal ESCAPE**	**100**
• **Capacidad de invitar expertos locales a la comunidad de expertos de IMPACT**	√
• **Capacidad de elevar incidentes a la comunidad de expertos de IMPACT**	√
• **Capacidad de enviar software maliciosos para que IMPACT los analice**	√
• **Capacidad de recibir detalles técnicos completos del análisis de software malicioso**	√
• **Capacidad de recibir noticias periódicas sobre seguridad**	√
• **Capacidad de recibir informes periódicos sobre seguridad (Genéricos)**	√
• **Capacidad de recibir informes periódicos sobre seguridad (Personalizado)**	√
• **Notificación por correo electrónico de emergencia de seguridad**	√
• **Notificación por teléfono de emergencias de seguridad**	√
• **Acceso a analistas y consultores de GRC**	√
• **Acceso a la biblioteca en línea y base de conocimientos de IMPACT**	√
• **Acceso a reuniones en línea**	√
• **Posibilidad de abonarse a contenido de ESCAPE**	√
• **Posibilidad de elevar solicitudes de servicio**	√
• **Capacidad de crear un equipo localizado (Gestión de equipos)**	√
• **Número mínimo de miembros del equipo de intervención en caso de incidente de seguridad informática nombrados**	**5**
Capacitación y desarrollo de capacidades	
• **Capacitación sobre ESCAPE**	√
• **Capacitación sobre NEWS**	√

Sr. Sami Al Basheer Al Morshid
Director
Oficina de Desarrollo de las Telecomunicaciones
Unión Internacional de Telecomunicaciones
Place des Nations
CH-1211Geneva 20
Suiza

Ref : BDT/POL/CYB DM-136

Asunto: Creación de capacidades de ciberseguridad – Centro de respuesta global IMPACT

Estimado Sr. Director,

En referencia a su carta relativa al asunto antes mencionado, nos gustaría darle las gracias por la oportunidad que se ha brindado a _____ para participar en la Iniciativa UIT-IMPACT.

Al respecto, nos complace confirmar nuestro interés en unirnos a la coalición y tener la oportunidad de recibir servicios concretos en el marco de la Agenda sobre Cigerseguridad Global de la UIT y apoyar al Sector de Desarrollo de la UIT en sus esfuerzos para lograr Ciberseguridad.

En consideración a_____ asociarse y obtener acceso a los servicios del CRG y las instalaciones de IMPACT, _____ está interesado en las siguientes áreas:

- Centro de respuesta global (NEWS, ESCAPE)
- Capacitación y desarrollo de aptitudes
- Centro de garantías de seguridad e investigación
- Centro de políticas y cooperación internacional

Agradeciéndole de antemano y en la espera de nuestra futura fructífera colaboración y cooperación,

Le saluda atentamente,

_____

Fecha

_____

Confidence and Security in the Information Society: ITU-IMPACT Alliance

Information for the participants to the RPM for Americas 9-11 September 2009

English only

International Telecommunication Union

Committed to connecting the world

ITU-IMPACT Alliance: Background Information

- As facilitator of WSIS Action Line C5 on "Building Confidence and Security in the use of ICTs", ITU launched the Global Cybersecurity Agenda (GCA) as framework for international cooperation aimed at enhancing confidence and security in the information society
- Within GCA, ITU and the International Multilateral Partnership Against Cyber-Threats (IMPACT) are pioneering the deployment of solutions and services to address cyber-threats at a global scale
- On September 3 2008, ITU and IMPACT formally entered into a Memorandum of Understanding (MoU) in which IMPACT's new state-of-the-art global headquarters in Cyberjaya, Malaysia, will effectively become the physical home of the GCA
- On March 20 2009, the global headquarters of IMPACT was inaugurated by Malaysia's Prime Minister Dato' Seri Abdullah Haji Ahmad Badawi and ITU Secretary-General Dr Hamadoun Touré

International Telecommunication Union
Committed to connecting the world

ITU-IMPACT Alliance:
Partners

- Support of key intergovernmental organizations
  - United Nations
  - International Police Organization INTERPOL
- Industry and academia
  - Symantec Corporation, Kaspersky Lab, F-Secure Corporation, Trend Micro Inc., Microsoft Corporation, Cisco Systems Inc. and Dell Inc.
- Leading cybersecurity training institutions
  - The SANS™ Institute
  - The International Council of E-Commerce Consultants (EC-Council)
  - The Honeynet Project
  - (ISC)² Inc.

ITU-IMPACT Alliance:
Goals

In accordance with the signed MoU, the five pillars of the GCA were mapped with the tracks identified by IMPACT

- **Legal Measures** - Elaborate strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures;
- **Technical and Procedural Measures** - Develop strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives;
- **Organizational Structures** - Elaborate global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime;
- **Capacity Building** - Develop a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above-mentioned areas;
- **International Cooperation** - Propose a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

ITU-IMPACT Alliance:
Activities

- BDT is facilitating the implementation process, managing communication and needs assessment with Member States and coordinating with IMPACT, which is currently providing all the necessary technical support, expertise and resources in order to facilitate the deployment operations and capacity building programs

- Global Response Centre
  - NEWS
  - ESCAPE
- Establishing National CIRTs
  - CIRT Lite
- Capacity building
  - Training and skills development

ITU-IMPACT Alliance:
Global Response Centre (GRC)

GRC acts as the foremost cyber threat resource centre for the global community. It provides emergency response to facilitate identification of cyber threats and sharing of resources to assist IMPACT members

NEWS
Information collaboration platform providing:
- Real time threat monitoring and assessment
- Statistical cyber threat trend analysis
- Malware threat centre

ESCAPE
- A collaborative platform that enables authorized cyber experts across the different countries to pool resources and remotely collaborate with each other in a secure and trusted environment
- A comprehensive and growing database of key resources around the world – including IT experts, empowered persons (government regularity officials), and other trusted bodies (CERTS), who can be called in to assist during a crisis.

ITU-IMPACT Alliance:
Establishing National CIRTs

ITU and IMPACT have elaborated a strategy for the establishment of CIRT (Computer Incident Response Team).

CIRT Lite Project is an initiative to set up National CIRTs, providing:

- Incident Management
- Advisories
- Mailing List

plus:

- IMPACT ESCAPE and NEWS Integration
- IMPACT Local Honeypot Deployment

ITU will support countries in the implementation of the National CIRT through the establishment of the overarching policy framework to support this technical solution and related watch, warning and incident response capabilities as part of a national strategy.

ITU-IMPACT Alliance:
Capacity Building

- ITU/BDT is coordinating with IMPACT to roll out the tools available through projects, training programs and specific applications to be integrated in the GRC
- Training and services that will be offered include:
  - SANS Scholarships for developing countries;
  - EC-Council Scholarships;
  - Other possible providers of scholarships in the future in addition to IMPACT run training courses that are currently being developed.
- CIRT staff training
  - Staffs that have been identified will be provided with the necessary basic skill training in order for them to be able to perform the basic incident response and handling functions;
  - These training will be sponsored for the countries and for a specific number of staffs that will be determined accordingly;
  - Training of the staffs will be done for both management and technical to ensure that relevant skill sets are adequately present in the team.

ITU-IMPACT Alliance:
Status of Collaboration

- 30 countries have formally joined the ITU-IMPACT collaboration: Afghanistan, Andorra, Brazil, Bulgaria, Burkina Faso, Costa Rica, Cote D'Ivoire, Democratic Republic of Congo, Egypt, Gabon, Ghana, India, Indonesia, Iraq, Israel, Kenya, Malaysia, Mauritius, Montenegro, Morocco, Nepal, Nigeria, Philippines, Saudi Arabia, Serbia, Seychelles, Tunisia, Uganda, United Arab Emirates, Zambia;
- In terms of access to the GRC, 5 countries have now access to the platform -UAE, Ghana, Zambia, Uganda, and Kenya-. Within the next few days, IMPACT will send the full package (including the logins, and the training materials to all countries formally joining);
- Concerning the establishment of National CIRT, several countries asked for assistance from ITU including Ghana, Zambia, Kenya, Uganda, Cote D'Ivoire, Burkina Faso, Afghanistan, Nigeria, among the others. ITU-IMPACT will deploy CIRT Lite solution, fully compliant with the GRC before the end of the year;
- GRC expected to be deployed in 50 countries by the end of 2009.

ITU's Upcoming Events

- ITU Regional Cybersecurity Forum for the Americas 2009
  - Aims to identify some of the main challenges faced by countries in enhancing cybersecurity and securing critical information infrastructures
  - Initiatives on the regional and international levels to increase cooperation and coordination amongst the different stakeholders
  - Capacity building activities concerning:
    - Development of legal frameworks
    - Development of watch, warning and incident management capabilities including the establishment of a national computer incident response team (CIRT)
    - Actions to be considered when developing a national cybersecurity strategy and harmonization within the key principles of international cooperation
  - More information soon available at: www.itu.int/ITU-D/cyb/

Links to More Information

- ITU-IMPACT Resources
  - www.itu.int/ITU-D/cyb/cybersecurity/impact.html
- An Overview of ITU Activities in Cybersecurity
  - www.itu.int/cybersecurity/
- ITU Global Cybersecurity Agenda
  - www.itu.int/cybersecurity/gca/
- ITU-D ICT Applications and Cybersecurity Division
  - www.itu.int/ITU-D/cyb/
- ITU Cybercrime Legislation Resources
  - www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- Regional Cybersecurity Forums and Conferences
  - www.itu.int/ITU-D/cyb/events/
- ITU Child Online Protection (COP)
  - www.itu.int/cop/

Thank You!

For more information on
ITU's Cybersecurity Activities
visit the website at:
www.itu.int/cybersecurity/

or contact cybmail@itu.int