ITU-IMPACT ALERT - CYBER DRILL 2014 for Partner Countries

"Lack of effective international cooperation today is the main reason for the increasing presence of malicious activities in cyberspace, ranging from cybercrime to cyber espionage to large-scale cyber-attacks" (Jamie Shea – Deputy Assistant Secretary general, NATO, 2011).

ITU
150 NATIONS
HAVE JOINED THE COALITION.
ITU-IMPACT IS TODAY, THE LARGEST GLOBAL CYBERSECURITY ALLIANCE

The purpose of the ALERT, which can be seen as a simulation in a controlled environment, is to enhance the communication and participating teams' incident response capabilities.

This simulation aims to assist Member States to develop and Implement operational procedures in response to various cyber incidents, and to identify future planning and process improvements.

This exercise also aims at maintaining and strengthening the international cooperation between countries in ensuring continued collective effort against cyber threats.

One of the main goals of this activity is to assist Member States to draft the overall plan on the country's approach to cyber security related issues, to serve as a trusted, central coordination point of contact for cyber security, aimed at identifying, defending, responding and managing cyber threats.

ITU-IMPACT's role in this activity is to demonstrate to Member States the importance of standard operating procedures, communications and incident response policies to various cyber incidents and to identify future planning and process improvement

Problem Statement

Due to the increased expertise and number of attackers, the national CIRTs have a key role to play in supporting governments in addressing Cybersecurity related issues at the national level as this pertains to preparing for, detecting, managing, and responding to cyber incidents if and when they occur. However, implementing an incident management mechanism requires consideration for funding, human resources, training, technological capabilities, government and private sector relationships, and legal requirements. Taking the foregoing into consideration, countries with limited human, institutional and financial resources face particular challenges in elaborating and implementing national policies and frameworks for cybersecurity and critical information infrastructure protection.

Key Objectives

Capability:

- Build and develop the national capacity of the partner countries in order to facilitate further development within the area of national critical information infrastructure protection.
- Build capacity to protect against cyber threats/cybercrime, in collaboration with one another
- Enhance the national expertise on cybersecurity and reduction of the human capacity gap in cybersecurity

Preparedness:

- This training and exercise will improve the national preparedness of the partner countries on the identification, prevention, response, and resolution of cybersecurity incidents
- Train them how to quickly handle incidents via collaboration with others

Communication and Collaboration:

- The cyber drill project will emphasize on how communication and collaboration between governments can assist in the fight against cyber threats/cybercrime.

  Enhance the cooperation on cybersecurity in response to the needs of developing countries, in close collaboration with the relevant partners.

ITU - IMPACT

In order to assist partner countries and their national CIRTs in improving their capability to detect, identify and mitigate cybersecurity incidents, ITU-IMPACT has been conducting regional Applied Learning for Emergency Response Teams (ALERT) cyber drills. Cyber drills have proven to be a valuable tool to demonstrate the importance of standard operating procedures, adherence to international best practices and incident response policies as well as strengthen international cooperation between national CIRTs and the collective effort against cyber threats.

The significance of conducting ITU-IMPACT ALERT – AFRICA CYBER DRILL 2014 is to:

- Achieve efficient and effective international cooperation, which is a must to defend and deter against global cyber threats.

- Create opportunities for our partner countries to meet face to face and develop close relationships for future collaborations and enhance the communication and cooperation within and between the national CIRT teams;
- Deliver capacity building sessions and workshops on CIRT best practices, policies and procedures and current cybersecurity issues;
- Assist the national CIRT teams with improvements to current CIRT practices, processes and procedures;
- Assist the national CIRT teams in identifying areas for CIRT development and capacity building.

Collaboration and Communication

- Collaboration at the national and international level is necessary to effectively align capabilities and expertise to manage incidents and raise awareness of potential incidents and steps toward remediation. Governments have a key role in ensuring coordination among these entities.
- ITU-IMPACT will play an important role in facilitation of collaboration between government entities, the private sector, academia, and the international community when dealing with Cybersecurity issues.
- Enhancing cooperation on Cybersecurity in response to the needs of developing countries in close collaboration with the relevant partners

Preparedness

- This activity will practically enhance ITU-IMPACT experts to be prepared in the major cybercrime challenges.
- This practice will add knowledge to ITU-IMPACT experts to quickly identify the problem and handle Cybersecurity incidents.
- This exercise will make ITU-IMPACT the main contact point in most developing countries whenever any information security threats occur among our partner countries.

When computer security problems occur, it is critical for the affected organisation to have a fast and effective means of responding. The speed with which the organisation can recognise an incident or attack and then successfully analyse it and respond will dramatically limit the damage done and lower the cost of recovery. This project focuses on assisting countries to organise and equip themselves to better respond to cyber threats. It pays particular attention to improving cybersecurity to ensure better protection of a country's ICT infrastructure, including critical information infrastructure and the availability of dependent services provided to government agencies, citizens and businesses. Many of these services are part of daily life and have a direct impact on a country's economic well-being and progress.

ITU-IMPACT ALERT AFRICA CYBER DRILL

Name of Project	ITU - IMPACT ALERT Africa Cyber Drill for Partner Countries
Date	29th to the 1st October 2014 in Zambia

Project Details

Project Objectives & Purpose	The objective of the cyber drill is for participating teams to exercise communication, incident response policies, and operational procedures in response to various cyber incidents, and to identify future planning and process improvements. The teams will respond to the simulated incidents and share information to detect and analyse malware, to request taking systems pertaining to hosting of malware or the botnet offline, and to inform the critical infrastructure companies and the community of the security threats.
Project Scope	Under the direction of the ITU, in cooperation with the national counterparts and in close collaboration with the relevant security teams of partner countries, the experts will undertake the following activities onsite and offsite: Conduct a three day ALERT event designed to be a platform for cooperation, information sharing, and discussion on current cybersecurity issues as well as a hands-on exercise for the national CIRTs.
Project Deliverables & Milestones	Deliverables / Milestones
	Pre Workshop - Offsite work - five experts will undertake the offsite preparation work before the workshop and cyber drill
	Workshop - Onsite Work and cyber drill - six experts will be present for the entire duration of the workshop and cyber drill
	Post Assessment – Offsite Work - two experts will undertake the offsite preparation work after the workshop and cyber drill

Project Organization

Project Stakeholders	• International Telecommunication Union (ITU) – Project Owner • IMPACT – Project Implementer • Partner Countries: Six countries from the Africa Region • Minimum of six teams • Three or four participants per team • Three cyber drill players • One media/relations

Required List of Items by Participants (onsite): Each participant is required to bring a notebook computer.