ITU-IMPACT

Applied Learning for Emergency Response Teams (ALERT)

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

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 the 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 the Governments in addressing cyber security 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 capability, 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 cyber security 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 cyber security and reduction of the human capacity gap in cyber security

Preparedness:

- This training and exercise will improve the national preparedness of the partner countries on the identification, prevention, response, and resolution of cyber security 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 of governments together can fight against cyber threats/cybercrime.
- Enhance the cooperation on cyber security in response to the needs of developing countries, in close collaboration with the relevant partner.

ITU - IMPACT

Conducting cyber drills in different regions of the world where many partner countries can participate, will add value to ITU-IMPACT reputation as international cyber security/cyber crime experts. In addition, there many from least developed countries and developing countries that need our help to reduce the cyber threat and criminality.

One of the best ways to help the world communicate with each other against cyber threats is to bring countries together in as many regions as possible and demonstrate the power of international communication and cooperation.

Apart from achieving the mission of ITU "*....enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy...*" organizing **ITU-IMPACT ALERT** in at least four regions will give our partner countries a chance to exercise and experience some of the up to date cyber attacks' practices.

The significance of conducting **ITU-IMPACT ALERT:**

- *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.
- Establish organizational structures, such as computer incident response teams (CIRTs), to identify, manage and respond to cyber threats, and cooperation mechanisms at the regional and international level.
- Build advanced national capacity for each government, in order to facilitate further development within the area of national critical information infrastructure protection, such as establishing sector CIRTs, etc.

Furthermore**, the purpose of ITU-IMPACT ALERT is to emphasize at collaboration and readiness for potential cyber threats.**

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 of our partner countries have the 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 cyber security issues.

- Enhancing cooperation on cyber security 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 cyber crime challenges.
- This practice will add knowledge to ITU-IMPACT experts to quickly identify the problem and handle the cyber security incidents.
- This exercise will make ITU-IMPACT as 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 organization to have a fast and effective means of responding. The speed with which the organization can recognize an incident or attack and then successfully analyze it and respond will dramatically limit the damage done and lower the cost of recovery. This project focuses on assisting countries to organize and equip themselves to better respond to cyber-threats. It pays particular attention to improving cyber security 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.

_____