|  |  |
| --- | --- |
| **ITU-IMPACT - CYBER DRILL 2012**  **The purpose of this simulation is to enhance the communication and participating teams’ incident response capabilities.**  **This simulation aims to assist Partner Countries 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.** | C:\Users\Agron.Hoxha\Desktop\popup.jpg |
|  | |
| ***Brief Description:***  **The main goal of this activity is to assist the Partner Countries 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 Partner Countries the importance of standard operating procedures, communications and incident response policies to various cyber incidents and to identify future planning and process improvement.** | |

**ITU-IMPACT ALERT - CYBER DRILL 2012 for Partner Countries**

**" 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, 2011).**

**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 - Cyber Drill**

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 partners.

**The significance of conducting** **ITU-IMPACT ALERT - CYBER DRILL 2012 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.
* 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 - CYBER DRILL 2012 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.

**ALERT ITU-IMPACT CYBERDRILL**

|  |  |
| --- | --- |
| Name of Project | ITU - IMPACT ALERT Cyber Drill for Partner Countries |
| Date | 15th to the 17th July 2012 in Jordan |

**Project Details**

|  |  |
| --- | --- |
| Project Objectives & Purpose | The objective of the cyber drill for participating teams is 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 analyze the malware, to request knocking down systems pertaining to hosting of malware or the botnet, 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 on-site and off-site:  Conduct cyber drill for human capacity building to impart knowledge and skills for coordination of CIRTs with relevant agencies, both local and international. |
| 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 & 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 Arab Region * Minimum of six teams * Four participants per team * Three cyber drill players * One media/relations |

**Required List of Items by Participants (on-site):** Each participant is required to bring a notebook computer.