[redacted]

ITU/IMPACT Country Readiness Assessment To Establish a National CIRT

Confidentiality

This document contains proprietary information that is confidential to IMPACT. Disclosure of this document, in full, or in part, may result in material damage to IMPACT. Written permission must be obtained from IMPACT prior to the disclosure of this document to any third party.

Jalan IMPACT, 63000 Cyberjaya, MALAYSIA.
www.impact-alliance.org

1. Introduction

Many countries and governments are using the dynamic and inter-connected environment of today's networked information systems to improve communications, provide control, protect information, and encourage competitiveness. Computers have become such an integral part of daily activities that computer-related risks cannot be separated from general business, health, and privacy risks. Valuable country assets and critical national infrastructures are now at risk over the Internet.

Overall reliance on the Internet continues to increase[1]. Unfortunately, in this dynamic, distributed, and interconnected environment cyber attacks occur rapidly and can spread across the globe in minutes without regard to borders, geography, or national jurisdiction. As a result, there is a growing need to be able to communicate, coordinate, analyze, and respond to cyber attacks across different business sectors and national borders. The Internet itself has become a critical infrastructure[2] to many nations, businesses and people that must also be protected.

It is important for governments to create or identify a national organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, and whose national mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between government entities, the private sector, academia, and the international community[3] when dealing with cybersecurity issues.

Therefore, 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.

[1] http://www.cert.org/archive/pdf/NationalCSIRTs.pdf
[2] http://www.itu.int/ITU-D/connect/flagship_initiatives/impact.html
[3] http://www.itu.int/md/D06-SG01-C-0249/en

Governments have the key role in ensuring coordination among these entities.

The establishment of a national CIRT is needed to help to ensure the protection of the nation's Critical Information Infrastructures, assist in drafting the overall plan on the country's approach to cybersecurity related issues, and thus can serve as a focal point for further building and implementing the National Culture of Cybersecurity.

2. Objectives:

The primary objectives of this project is to assist countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as discussed in this document. The National CIRT will provide a capability to identify, respond and manage cyber threats and at the same time will enhance the cybersecurity posture of the sovereign country. This project will introduce and propose a framework which can be used by government bodies to establish a CIRT at national level.

The final outcome and deliverable of this mission will be a report for each participating country which will contain key issues, key findings, analysis and recommendations and a phased implementation plan for setting up the National CIRTs. The report will be prepared and submitted to participating countries within four weeks after the experts have completed the on-site assessment and returned to base.

Collectively, with the integration of best practices and processes, experienced people and robust technology, it is believed that the National CIRTs can play the role of maintaining round-the-clock vigilance to defend critical national infrastructure/assets against cyber attacks, and also serve as a critical cyber-nerve centre in analysing threat information; which can extend towards alerting public and private sector agencies pre-emptively in enhancing their security awareness, assist in remediation of identified vulnerabilities, and improving overall security posture.

3. Current State Assessment

The current state assessment will be divided into two parts; i.e. on-site assessment and off-site assessment. The on-site assessment work will involve preliminary consulting work undertaken with a focal point from the participating country. The focal point will assist to organise and coordinate meetings, discussions and site visits as well as provide valuable information during the assessment stage. A questionnaire will be sent to the focal point before the on-site activity to better prepare the local team and stakeholders for the on-site assessment. The questionnaire will contain the questions that would be discussed during the on-site assessment interviews. Upon completing the on-site assessment, close contact with the focal point will still be maintained to collect more information and documents relevant to the on-site assessment for the completion and preparation of the recommendation report.

The on-site assessment involves activities such as conducting awareness for all stakeholders to impart the idea of establishing a National CIRT. These awareness sessions greatly helps the stakeholders to better understand what constitutes a National CIRT and the way forward. A detailed list of activities that will be carried out during the on-site assessment stage is as below:

- Interviews and discussions with local stakeholders, law enforcement representatives, private sector executives, government representatives and representatives from financial institutions and regulatory bodies.
- Conduct capacity building activities such as awareness sessions. The capacity building activities are critical to impart the ideas of establishing

and operating a National CIRT, the processes and the technologies involved, and the services that a National CIRT will render out to the constituency.

- Discussions with local ICT experts, particularly those performing cybersecurity roles and responsibilities and with regulators and law enforcement officers.
- A country survey in the form of an assessment questionnaire encompassing every aspect of cybersecurity with the stakeholders to collect their opinions and views.
- Online research to review key websites with information related to ICT and cybersecurity in the country.
- A review of relevant documents, past reports, policies, strategies and plans relating to cybersecurity that were provided by the stakeholders during the interviews and meetings.

Some of the key information that will be gathered during the assessment stage is as below:

- What cybersecurity needs does the constituency have?
- What are the critical assets that must be protected?
- What types of cyber incidents are frequently reported?
- What is the desired response and notification strategy?
- What is the current technology infrastructure and skill set?
- What processes are required?
- What assistance and expertise is needed?
- Who will perform the identified roles?
- Which organisation(s) takes the lead for cybersecurity related activities?
- Is funding available for the sustenance and operation of a CIRT?

The assessment will clearly identify what the current gaps are. This will be valuable information towards the successful establishment of the National CIRT.

4. Management Support and buy-in

Creating an effective incident response capability can be extremely difficult without management approval and support to the assigned person, a group of people or an agency that will act as the project team for implementing the CIRT. This support must be shown in numerous ways, including the provision of resources and funding. This includes executive and business or department managers and their staffs committing time to participate in this planning process. Their input would be extremely essential during the design effort.

The first step towards introducing a CIRT is to make people understand why they need a CIRT and what the benefits of establishing a CIRT are. Keeping the information assets secure requires a multi-layered approach. Creating a CIRT is one layer, along with implementing secure configurations, security awareness training, and internal and external defences. The exercise creates awareness about a CIRT amongst the various constituencies. It also gives the implementation team the necessary knowledge for implementation at a later stage.

Awareness can be done through various methods:

- In class lecture style training
- Workshop instructor-led sessions to get participants involvement

5. Recommendation Report

The readiness assessment report is divided into key areas and points out the issues, details the findings and analysis conducted, as well as recommends solutions to address the issues. The key areas include

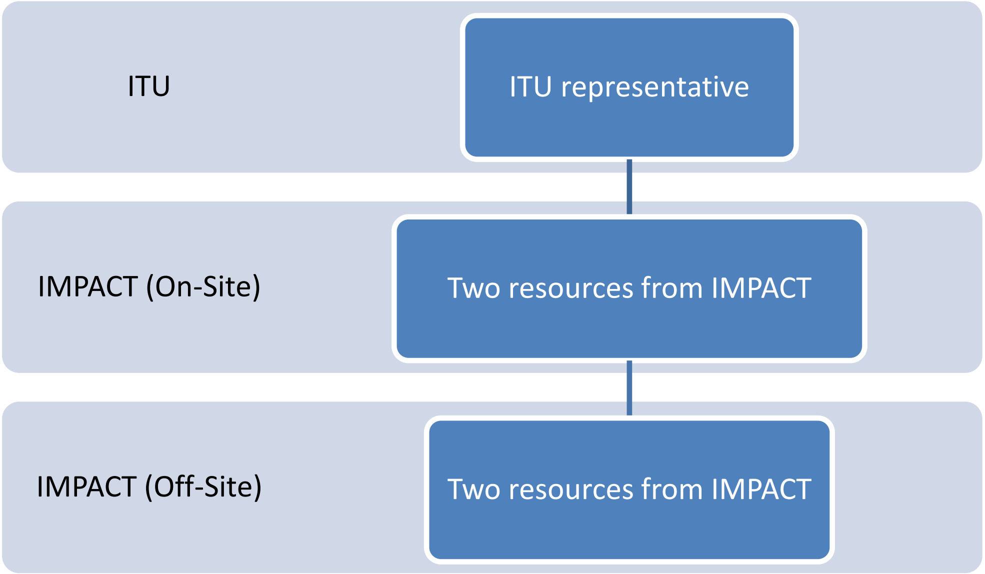
- the ICT readiness of the country against Cyber threats,
- Cybersecurity/ICT legislation,
- Common Standards/Regulatory framework,
- Constituency/Stakeholder participation,
- Cybersecurity training and education,
- Current physical infrastructure and its operational aspects, and
- the financial model to be adopted.

6. ITU/IMPACT Experts:

There will be two (2) experts assigned to carry out this assessment exercise. Both of them will be knowledgeable in the field of cybersecurity and CIRT, and also in the use of the applicable international standards and best practices involved.

7. Mission Organisation:

Mission Stakeholders	• International Telecommunication Union (ITU) – Mission owner • IMPACT – Project Implementer • Participating Countries – Client / Customer
Organisational involvement – Functional units	• IMPACT – Global Response Centre (GRC), Operations, HR and Finance • IMPACT – Security Assurance Division • ITU – Telecommunication Development Bureau, HR and Finance

Mission Team Organisation	 ITU ITU representative IMPACT (On-Site) Two resources from IMPACT IMPACT (Off-Site) Two resources from IMPACT

8. Who Should Attend?

The team will record all findings based on the current posture of cybersecurity situation in the country and try to gather all key issues, recommendations and propose a phased implementation plan for setting up the National CIRT. The assessment methods will be mainly questionnaires, meetings, and training sessions.

The constituencies that should attend the assessment are stipulated in the table as below;

A. Communication 1) Telco's 2) Cellular operators 3) ISP's	B. Cybersecurity 1) Regulatory agencies 2) CIRT's 3) ICT Ministry/Bodies 4) National Security Agency
C. Financial Sector 1) Banks 2) Central monetary agency 3) Financial companies	D. Research 1) Academia 2) National research bodies 3) Cybersecurity research organizations

E. Others bodies 1) NGO's 2) Law enforcement 3) Policy makers 4) Local private organisations involved in Security initiatives	

9. Financials

The mission will be funded by ITU.

10. Programme Schedule:

Day 1	
9.00am – 10.00am	- Ice Breaking & Program Overview Sessions - IMPACT Presentation - ITU-IMPACT Collaboration Presentation - Video presentation
10.00am – 10.30am	- CIRT Introductory Training
10.30am – 10.45am	- Break
10.45am – 12.30pm	- CIRT Introductory Training (continued)
12.30pm – 2.00pm	- Lunch
2.00pm – 3.30pm	- Fundamentals of Computer Incident Handling Training
3.30pm – 3.45pm	- Break
3.45pm – 5.00pm	- Exercise 1 (Triage, Prioritization & Basic Incident Handling)

Day 2	
9.00am – 10.30am	- Video presentation - Steps of Incident Handling Training
10.30am – 10.45am	- Break
10.45am – 12.30pm	- Exercise 2 (Incident Handling Procedure) - Exercise 3 (CIRT Infrastructure) - Exercise 4 (Recruitment)
12.30pm – 2.00pm	- Lunch
2.00pm – 2.45pm	- Video presentation - Breakout Assessment Session with Country 1
2.45pm – 3.30pm	- Breakout Assessment Session with Country 2
3.30pm – 3.45pm	- Break
3.45pm – 4.30pm	- Breakout Assessment Session with Country 3
4.30pm – 5.15pm	- Breakout Assessment Session with Country 4

Day 3	
9.00am – 10.30am	- IMPACT GRC Portal Training & CIRT-Lite Walkthrough
10.30am – 10.45am	- Break
10.45am – 12.30pm	- Exercise 5 (Vulnerability Handling)
12.30pm – 2.00pm	- Lunch
2.00pm – 2.45pm	- Breakout Assessment Session with Country 1
2.45pm – 3.30pm	- Breakout Assessment Session with Country 2
3.30pm – 3.45pm	- Break
3.45pm – 4.30pm	- Breakout Assessment Session with Country 3
4.30pm – 5.15pm	- Breakout Assessment Session with Country 4

Day 4	
9.00am – 10.30am	- Exercise 6 (Writing Security Advisories)
10.30am – 10.45am	- Break
10.45am – 11.30am	- Breakout Assessment Session with Country 1
11.30am – 12.15pm	- Breakout Assessment Session with Country 2
12.15pm – 1.30pm	- Lunch
1.30pm – 2.15pm	- Breakout Assessment Session with Country 3
2.15pm – 3.00pm	- Breakout Assessment Session with Country 4
3.30pm – 3.15pm	- Break
3.15pm – 4.30pm	- Video presentation - Exercise 7 (Incident Handling & Role Playing)
4.30pm – 5.15pm	- Wrap-up session

Day 5	
9.00am – 10.30am	- Exercise 8 (Establishing External Contact)
10.30am – 10.45am	- Break
10.45am – 12.00pm	- Exercise 9 (Cooperation with Law Enforcement Agencies)
12.00pm – 1.30pm	- Lunch
1.30pm – 3.00pm	- Breakout Assessment Session with Country 1 - Breakout Assessment Session with Country 2
3.00pm – 3.15pm	- Break
3.15pm – 4.45pm	- Breakout Assessment Session with Country 3 - Breakout Assessment Session with Country 4
4.45pm – 5.30pm	- Wrap-up session (All countries)

a) **Details of the Breakout Assessment Sessions**:

1. ***Day 2 Breakout Assessment Session:***
    a. *ICT readiness of the country*
    b. *Identifying stakeholders*
    c. *Vision, mission and goals*
    d. *Cybersecurity initiatives within the country*

2. ***Day 3 Breakout Assessment Session:***
    a. *Identifying constituencies*
    b. *Place in organisation or reporting structure*
    c. *Relationships with other CIRTs*
    d. *Financial model*

3. ***Day 4 Breakout Assessment Session:***
    a. *Identifying CIRT services*
    b. *Manpower planning*
    c. *Physical infrastructure*
    d. *Hardware and software*

4. ***Day 5 Breakout Assessment Session:***
    a. *Child Online Protection (COP)*
    b. *Cybersecurity research initiatives*
    c. *Training needs assessment*
    d. *Cybersecurity legislative framework and policy*