International Telecommunication Union

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

ITU-IMPACT WORKSHOP FOR SIERRA LEONE ON

Enhancing Cybersecurity for Least Developed Countries (LDC)

JALAN IMPACT, 63000 CYBERJAYA, MALAYSIA
www.impact-alliance.org

Contents

Overview

This programme aim is to provide a highly intensive workshop programme on cybersecurity addressing the needs of ITU-IMPACT Partner Countries and stakeholders with significant roles in cybersecurity, tasked with identifying, mitigating and managing cyber threats focusing on critical and public sector organisations. The primary objective of this workshop programme is to assist ITU-IMPACT Partner Countries in the readiness to implement a National CIRT (Computer Incident Response Team) and get started with the process of establishing a National Cybersecurity Framework. The approaches and strategies will formulated be based on the findings and outcomes of the proposed workshop programme.

Scope

With careful consideration and under the direction of the ITU-IMPACT Partner Country, the workshop programme will be carried out in cooperation and collaboration with relevant Ministries and stakeholders which includes the following activities:

- Provide an overall understanding to the various sectors on the current cybersecurity status and needs.
- Provide high-level overview on the recommended cybersecurity posture for ITU-IMPACT Partner Country.
- Provide the participants with an understanding and overview of the benefits of establishing a National Level Cybersecurity Framework.
- Capacity building program for the various levels of stakeholders.
- Conduct parallel workshops focussed on the current job roles and responsibilities of the participants towards contributing to the National Cybersecurity Agenda.
- Provide awareness on the current threat landscape and mitigation strategies with a global perspective.
- Educate the individual agencies on their responsibilities of mitigating cyber threats.
- Provide an introduction to legal framework

Target Audience

This workshop is designed for Ministers, Private Sector CEOs, Banks CEOs/CFOs, Critical Sector/CNII Providers CEOs/CFOs**,** IT Companies, ISPs, Law Enforcement Agencies, Judiciary, Ministry Executives **,** Technical Team - (Network Administrators, Security Experts) and those with national responsibility in Cybersecurity development and capabilities.

ITU-IMPACT Experts

There will be four (4) ITU-IMPACT Experts assigned to carry out this workshop, whom are knowledgeable in the field of National Cybersecurity Framework, Incident Response, Cybersecurity Implementation and the use of the applicable International Standards and Best Practices. The ITU-IMPACT team will conduct on-site activities with meetings on planning and execution.

Workshop Approach and Details

The proposed workshop programme consist of 3 specialised tracks based on the job role, nature and responsibilities of various individuals attending this workshop. The workshop duration is 2 weeks/10 days.

WEEK 1 - CIRT READINESS ASSESSMENT			
	TRACK 1	**TRACK 2**	**TRACK 3**
Target Audience	Ministers, Private Sector CEOs, Banks CEOs/CFOs, Critical Sector/CNII Providers with National responsibility, CEOs/CFOs	IT companies, ISPs CEOs, Law Enforcement Agencies, Judiciary, and Ministry Executives	Technical Team - (Network Administrators, Security Experts, etc)
Schedule	**Topics**		
Day 1	• Introduction to ITU-IMPACT • Cybersecurity Landscape and Mitigation Strategy • National Cybersecurity Framework • Implementing Cybersecurity Capabilities • Implementation of National Awareness Programmes • Implementation of International Cooperation Model to curb Cyber crime • Panel Discussion on Cyber Threat Landscape • Introduction to Incident Handling • Categorisation of Incident • Prioritisation of Incident • Reporting Incidents		

Day 2 - 4		• Introduction to Cyber Crimes • Current Threat Landscape • Current Mitigation Strategies • National Cybersecurity Framework • Roles of Agencies mitigating cyber threats • Introduction to Legal Frameworks • Cybercrime Case Studies • Mock Incident Management Exercise • Summarisation of the scenarios	• Incident Analysis Methods • Introduction to Intrusion Detection System (IDS) • IDS Architecture and Deployment • IDS Technology (SNORT) • Installation and Configuration of IDS • IDS Analysis • IDS Fine Tuning
Day 5	• Implementation of National Cybersecurity Framework • Identification of key stakeholders and constituents for the implementation		

WEEK 2 - CYBERSECURITY CAPACITY BUILDING PROGRAMME		
Day 1-5	• Information Security Governance and Risk • Security Policies • Security Policies, Procedures and Guidelines • Security and Audit Frameworks • Risk Management Principles • Business Continuity and Disaster Recovery Planning • Physical and Environmental Security • Access Control • Operation Security • Legal, Regulatory, investigation and Compliance	• Security Testing / Penetration Testing • Operating System Vulnerabilities • Network Level Vulnerabilities • Application Layer Vulnerabilities • Penetration Testing Phases • Reconnaissance - Active and Passive • Vulnerability Assessment • Exploitation • Anti-Forensics • Web Application Security Testing / Penetration Testing • OWASP Top 10 Vulnerabilities • Cross-Site Scripting (XSS) • Broken Authentication and Session Management • Insecure Direct Object References

		• Cross-Site Request Forgery (CSRF) • Security Misconfiguration • Insecure Cryptographic Storage • Failure to Restrict URL Access • Insufficient Transport Layer Protection • Un-validated Redirects and Forwards

Workshop Financials

ITU-IMPACT will be contributing USD50,000 as a form of financial assistance for conducting this workshop programme. Sierra Leone is required to pay for flight, ground transport and hotel accommodation for all ITU-IMPACT Experts.

Participating Country

Sierra Leone

Workshop Schedule

The workshop schedule is to be determined and agreed by both ITU-IMPACT and Sierra Leone. The proposed month is December 2013 and the date is subjected to confirmation.

Toolkit (on-site)

Listed below are items that are required to be made available on-site to the experts to complete the workshop successfully. The organising team shall be responsible to make the items available. Should there be any issue in ensuring the availability of any of the items; the ITU/IMPACT experts must be notified at least five (5) days before the departure of the experts from Kuala Lumpur.

1. Participants are required to bring a notebook computer each
2. Conducive training / seminar room
3. Broadband Internet connection for all participants
4. LCD Projector
5. Projector screen
6. White board
7. Marker pens (multiple colours)
8. A4 papers for classroom exercises
9. Big-sized white papers for student presentations
10. Laser printer
11. Audio connectivity for laptops
12. Sufficient power for all participants.
13. 2 conference halls to run 2 tracks in parallel with internet connectivity.

For Track 3 the below requirements are necessary:

1. Each participant are expected to have a laptop or computer with good performance having at least 4Gb RAM and 20GB of free disk space
2. VMware Player/Workstation on the participant laptops/workstation

END OF DOCUMENT