INTERNATIONAL TELECOMMUNICATION
UNION Telecommunication Development Bureau
and
Makerere University
School of Computing & Informatics Technology

ITU Centres of Excellence Training Workshop on

Cyber Security :Technologies ,Standards and Operations

For English Speaking countries in Africa Region

18 - 22 April 2011, Kampala, Uganda

Agenda

Brief Description

The workshop aims to provide an in-depth technical foundation to the development of sound organizational or national cyber security strategies. In particular, it will provide participants with the knowledge and resources required to meet the needs of the “Technical Measures” within the ITU’s Global Cyber-security Agenda (GCA).

The specific objectives include to:

1. Introduce participants to fundamental of digital security like threat analysis, modeling and common attack patterns
2. Introduce participants to standards, best practices and technologies of building secure systems
3. Introduce participants to best practices of cyber risk management plan fo organizations and Nations
4. Introduce participants in cyber security audits and IT security formulations

Target Audience

This workshop is suitable for stakeholders with technical background and job responsibilities – Chief Information Office (CIO), Chief Technology Officer (CTO) and IT Operations (such as systems, webserver, and network administrators). Also the workshop is ideal for person who are at the begining of their career in IT security and digital forensics

Monday , 18 April 2011	
08:30- 09:00	**Registration**
09:00- 10:30	1- Issues and Challenges • Introduction to Cyber security and Challenges • Cybercrime Trends and Drivers – What? How? Why? Where to? Whom? Who? Where from? • Cyber Attacks – Types (Network both wired and wireless + Application + Social Engineering) • Cyber Attacks on CII of a Country (Private Sector – provide Critical Infrastructures to the country) and its protection importance

10:30-11:00	**Coffee break**
11:00-12:30	2- Threats – Understanding • Threats to the CII of the Country • Threats to the Private Sector
13:00-14:00	**Lunch**
14:00-15:30	2- Threats – Understanding • Threats to the Citizens and Public Sector • Types of threats o to wired networks o to wireless networks o to application infrastructure
15:30-16:00	**Coffee/Tea Break**
16:00 – 17:20	3- The Information Security Main Pillar – GRC (Governance, Risk and Compliance) • Identity and Access Management o Logical o Physical o Risk Based Access Control and Fine Grain Access Policy Management o Entitlements Management • SOD – Segregation of Duties • Compliance Requirements – Local, Industry and International
17:20-17:30	**Day synthesis**

Tuesday , 19 April 2011

09:00 – 10:30	Information Assurance Foundations o Risk Models o Authentication vs. Authorization o Data Classification o Vulnerabilities o Defense In-Depth Information Security Policies o How Policies Serve as Insurance o Roles and Responsibilities
10:30 - 11.00	**Coffee/Tea Break**
11:00 – 12:30	Contingency and Continuity Planning o Legal and Regulatory Requirements o Disaster Recovery Strategy and Plan Business Impact Analysis o Emergency Assessment o Business Success Factors o Critical Business Functions
13:00 – 14:00	**Lunch**

14:00 − 15:30	Password Management o Alternate Forms of Authentication (Tokens, Biometrics) o Single Sign On and RADIUS o Privileged Password Management Incident Response and Handling o Preparation, Identification and Containment o Eradication , Recovery and Lessons Learned o Investigation Techniques and Computer Crime
15:30 − 16:00	**Coffee/Tea Break**
16:00 − 17:20	Incident Response and Handling o Ethics o Offensive and Defensive Information Warfare Web Services Security o Web Communication o Web Security Protocols o Active Content o Attacking Web Applications o Web Application Defense Mechanisms
17:20 − 17:30	***Day synthesis***
Wednesday , 20 April 2011	
09:00 − 10:30	Host-based Intrusion Detection and Prevention Network-based Intrusion Detection and Prevention o NIPS – Network IPS o WIPS – Wireless IPS
10:30 - 11.00	**Coffee/Tea Break**
11:00 − 12:30	Honeypots Network and Computer Forensics Effect of Firewalls on IDS/IPS Sensors
13:00 – 14:00	**Lunch**
14:00 − 15:30	Methods of Attacks Firewalls and Other Perimeter Security Devices o Types of Firewalls o Secure Architecture o Network Admission Control (NAC) o Content Security AV Gateways
15:30 − 16:00	**Coffee/Tea Break**
16:00 − 17:20	Risk Assessment and Auditing o Risk assessment methodology o Risk approaches o Calculating risk
17:20 − 17:30	***Day synthesis***
Thursday , 21 April 2011	

09:00 – 10:30	Cryptography o Intro o Encrypting Networks (VPN or Link Encryption) o Encrypting Messages (PKI) o Encrypting Data in Transit or Storage o Crypto Attacks o Application and Applied Cryptography o Types of Encryption Devices (Network, Email, Link, Phone, Video and Fax Encryption)
10:30 - 11.00	**Coffee/Tea Break**
11:00 – 12:30	Email Security o PGP o S/MIME – X.509 Operations Security o Awareness Creation and Refreshing o Social Engineering Attacks Intro o Social Engineering Defense Techniques
13:00 – 14:00	**Lunch**
14:00 – 15:30	Wireless Security o Encryption (WPA types) o Wireless Access Control
15:30 – 16:00	**Coffee/Tea Break**
16:00 – 17:20	o Digital Rights Management and Document Control
17:20 – 17:30	***Day synthesis***
Friday , 22 April 2011	
09:00 – 10:30	Information Security Infrastructure o OS Security o Directory Services o PIM – Privileged ID Management (Admins
10:30 - 11.00	**Coffee/Tea Break**
11:00 – 12:30	User Access Rights – Groups, Users, etc Technical Security Policies (Technology Enforced) Patch Management Securing Network Services – VPNs, Wireless, IPsec, etc
13:00 – 14:00	**Lunch**
14:00 – 15:30	Access and Application Auditing User ID Attestation Virtual Machines Security Desktop Security – Endpoint Security
15:30 – 16:00	**Coffee/Tea Break**
16:00 – 16:30	o Evaluation o AOB
16:00 – 17:00	***Closing ceremonial***