

Agenda

- UCC Mandate
- Online Safety in East Africa
- Incident Management
- National Computer Incident Response Team (CIRT)
- Building East Africa's Incident Management Capacity
- Need for an Incident Management Framework
- Conclusions



UCC Mandate



- UCC regulates and promotes the development of Uganda's communications industry.
- **Our Vision:-** A Uganda in which development is facilitated through universal access to communications services largely delivered through the private sector
- **Our Mission:-** Regulate communications sector in order to facilitate growth of communications services for **sustainable development**;
- Our role is vital because the Telecommunication Sector is Uganda's leading tax contributor

Rural Communications Development



Under the new RCD Policy, UCC aims to:

- To expand coverage so as to increase access to ICT services;
- Provide broadband connectivity especially to educational institutions and health centres; and
- Support content development;
- Mandate of UCC in line with IGF which also aims to promote the secure and sustainable development of the Internet particularly in developing countries

IGF Mandate – Tunis Agenda



The mandate of the Forum is to:

- Help foster the sustainability, robustness, security, stability and development of the Internet;
- Facilitate exchange of information/best practices;
- Contribute to capacity building for Internet governance in developing countries;
- Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users such as **online safety**

Online safety in East Africa



Online Safety

- Like other regions, online safety is a major issue in East Africa due to increasing threats to the reliable functioning of Critical Internet Resources (CIRs) and the integrity of the information therein;
- Cyber incidents have included:
 - Defacement of major government websites;
 - Disruption or destruction of ICTs such fibre cables;
 - Spread of malicious software e.g. viruses, spam etc
 - Identity Theft
- The media and communities such as i-Network discuss cyber threats/incidents extensively

Improving Online Safety



UCC is keen to improve online safety because:

- **Customers/subscribers need confidence in the network and the services offered, including availability of services (especially emergency services) in case of major catastrophes such as recent Kampala bombings and natural disasters;**
- **The Government of Uganda demands security by directives and legislation** such as through the recently passed “Regulation of Interception of Communications Bill”, “Computer Misuse Bill” and Electronic Transactions Bill”

Need for Online Safety ...



- **Network operators/service providers themselves need security to safeguard their operation and business interests, and to meet their obligations to customers and the public, at the national and international level;**
- UCC is aware that cyber threats are transnational and demand coordinated regional/global action
- Due to shared infrastructure such as undersea cables TEAMS, EASSy and SEACOM, East Africa requires collective action on cyber threats
- Coordinated response boosts regional security

Incident Management



Definitions

- **ISO/IEC 27002:2005** defines a security incident as a “**security breach, threat, weakness and malfunction that might have an impact on the security of organisational assets.**”
- **Recommendation ITU-T E.409** regards a security incident as “**any real or suspected adverse event in relation to the security**” of an ICT including:
 - Intrusion into a computer system via the network;
 - Computer viruses;
 - Probes for vulnerabilities via the networks; and
 - Any other unauthorised internal or external actions.

Incident Management Purpose



- To **ISO/IEC 27002:2005** incident management focuses on ensuring that security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken;
- Thus, organisations should have formal event reporting and escalation procedures; and
- All users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organisational assets.

National Computer Incident Response Team (CIRT)



Incident Management Capacity



- World Telecommunication Standardisation Assembly, October 2008 (WTSA-08) **Resolution 58** encourages the creation of national CIRTs particularly in developing countries;
- **Resolution 58** invites Member States:
 - To consider the creation of a national CIRT as a high priority;
 - To collaborate with other Member States and with Sector Members,
- Resolution invites States and Sector Members:
 - To cooperate with the ITU-T and ITU-D in this aspect

Purpose of a National CIRT



- Acts as a single point of contact for cyber incident reporting and coordination in a sovereign country;
- Establishes trusted communication mechanisms among incident management stakeholders;
- Develops mitigation and response strategies;
- Shares data and information about incidents and corresponding responses;
- Publicises incident management best practice;
- Coordinates global cooperation on cyber incidents;
- Builds capacity in all the above areas.

Building East Africa's Incident Management Capacity



Regional initiatives under EACO



- The East African Communications Organisation (EACO) brings together communications operators and regulators in East Africa
- EACO aims to define and harmonise cybersecurity policies and legislation in East Africa;
- considering ways to improve effective implementation of the **WTSA-08** Recommendations and Resolutions;
- EACO resolved to form CIRTs to fight cybercrime
- EACO agreed to form a collaboration framework for the national CIRTs at regional and global levels

Global Cybersecurity Agenda



- The EACO activities are in line with the ITU Global Cybersecurity Agenda (GCA);
- GCA Goal 4: “Development of strategies for the creation of a global framework for **watch, warning and incident response** to ensure cross-border coordination between new and existing initiatives.”
- EACO also adopted a proposal for telecom operators to form and run sectoral CIRTs and nominate representatives to sit on national CIRTs.

CIRT Capacity: Need for incident Management Framework



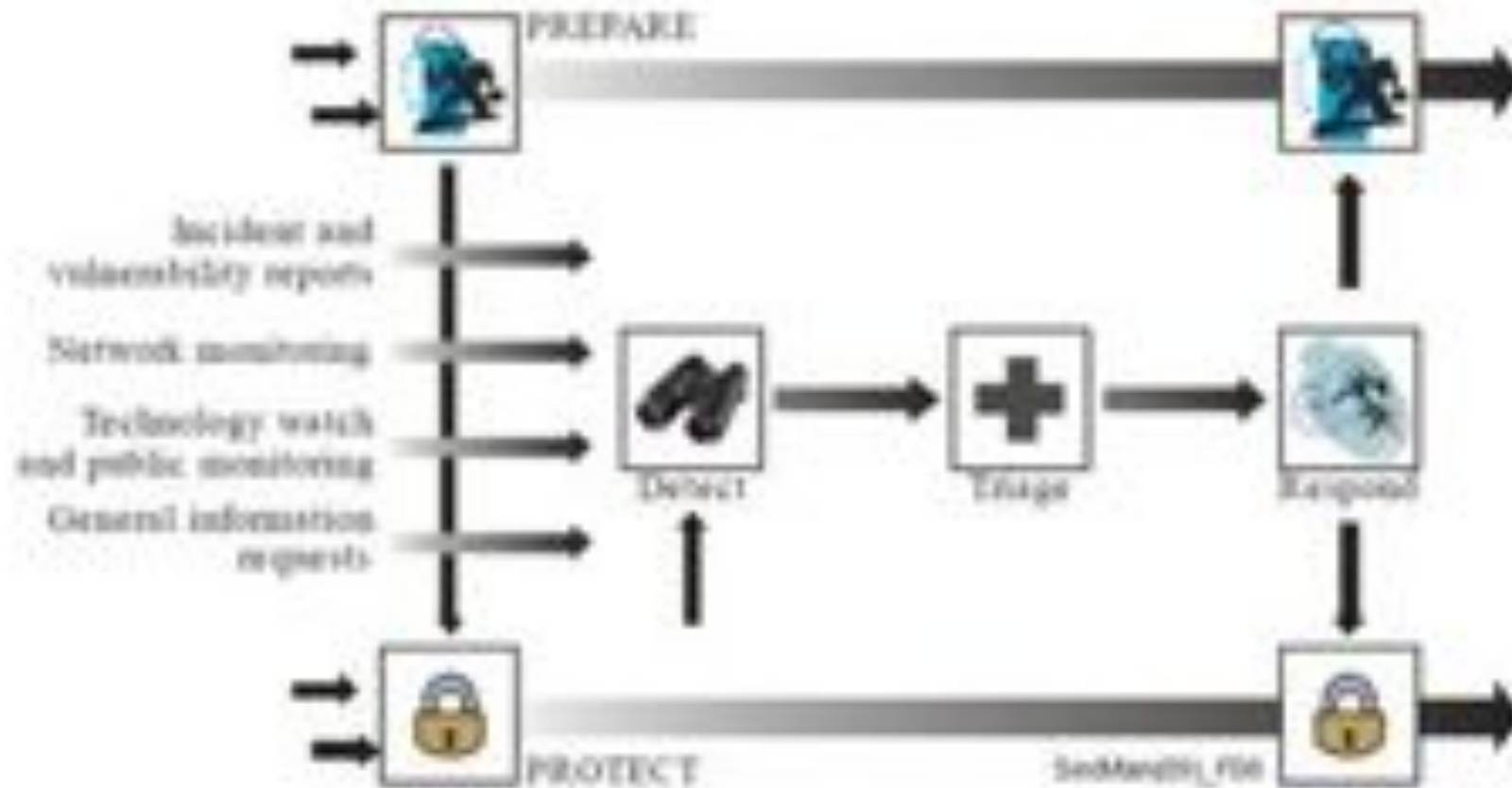
Purpose of Incident Framework



Countries/companies require a framework because:

- It helps in the planning and implementation of a security incident management capability;
- Helps organisations secure and harden Internet infrastructure to prevent security incidents from occurring or to mitigate ongoing incidents;
- Helps detect, triage, and respond to security incidents and events when they occur
- Next slide presents this ITU developed framework

Incident Management Processes



Source – Recommendation ITU-T X.1056

Processes

- **Prepare**

- This phase covers the planning and implementation of an initial CIRT capability; sustaining it and improving it;

- **Protect**

- The phase covers efforts to change an infrastructure to stop or mitigate an ongoing incident;
- It also covers tasks such as proactive scanning and network monitoring and security and risk evaluations;
- It transfers to the Detect process data about incidents and vulnerabilities uncovered during the evaluation.

Processes ...

- **Detect**

- Identifies and reports on security events;
- Analyses logs for malicious behaviour or threats; and
- Close any events not promoted to the Triage process

- **Triage**

- Categorises, correlate and prioritises events;
- Close events not forwarded to the Respond process or reassigned to other areas.

- **Respond**

- Coordinates and provides technical, management, and legal response to contain, resolve or mitigate incidents

Conclusions



Highlights of Presentation



- ICTs are vital to East Africa's development – in Uganda, the sector is a leading tax contributor;
- However, the region will not fully benefit from the infrastructure if online safety is not assured;
- The borderless nature of the Internet makes cyber threats a global issue that no single country, company and sector can address alone;
- Thus, it is vital to establish national and globally compatible incident management processes to spur cooperation, dialogue and coordination

Thank you for your Attention!



© Uganda Communications Commission
Plot 42-44 Spring Road Bugolobi
P. O. Box 7376, Kampala
Phone: +256 41 4339000
Fax +256 41 4348832
Email: mwesigwa@ucc.co.ug

