GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

COE Judicial Training
A Trainers Perspective

Integrating the issues of Cybercrime and Electronic Evidence into Judicial Training Curricula

Johannesburg, South Africa, 11-13 April 2016

Nigel Jones
Council of Europe Consultant

and
Director of the Centre for Cyberforensics
Canterbury Christ Church University
United Kingdom
Tel +44 1227 782089
Mobile: +44 7786 317995
Email: nigel.jones@canterbury.ac.uk

Challenges

The Changing Nature of the Requirement

Common Law vs Civil Law Systems

Strategic Support vs Practitioner Enthusiasm

Commitment of Judicial Players

Resources – Trainers – Developers – Materials

Building a Sustainable Programme

Maintaining the Impetus – Post Project

International Workshop under Cybercrime@EAP and GLACY Projects
Bucharest
2nd – 3rd June 2014

Elements of a Judicial Training Strategy

- Justification
- Objectives
- Training Requirements (Needs Analysis)
- Training Capabilities and Resources
- Other Considerations

Justification

This part should explain why a training strategy is necessary and why resources should be allocated.

For example:

- Societies rely on ICT and are vulnerable to risks:
  - Economic, social, political, security, human rights
  - = Actual and potential risks and impact justify investment in training and
  - institution building
- Types of offences:
  - Attacks against computer data and systems (cia offences)
  - Offences by means of computer systems (forgery, fraud, child pornography, IPR- offences etc)
  - Electronic evidence related to any offence
  - = All Judicial Officers need to be trained at different levels
- Technological developments:
  - Mobile devices, cloud computing, social platforms, etc.
  - = Judicial Officers need to keep up to date, update training programmes/materials

Objectives

The objective of a training strategy could typically be formulated as follows:

- To ensure that Judicial officers have the skills/ competencies necessary for their respective functions to
    - investigate cybercrime,
    - secure electronic evidence,
    - Consider the admissibility of electronic evidence in trials
    - assist other agencies

Considerations: Sustainability, standardisation, certification, institutionalisation, efficiency, scalable, linked to other institution building measures, skills of prosecutors and judges, establish system

Training Requirements
(Needs Analysis)

- A training strategy should realise and cater for the different levels of knowledge and skills needed by individual Judicial staff tasked with investigating, prosecuting or adjudicating crimes involving technology.

- There are no generic names for roles within different organisations, however by describing the functions of the roles, it is anticipated that it will be possible to translate the descriptors into local and regional roles.

Training Capabilities and Resources

Training capabilities and resources required will differ between regions of the country and even between courses within programmes. There are generic requirements; however each course training pack that is developed should contain a detailed list of all the resources required for each event. This will include details of classrooms, technology, trainers as well as specifics for each course delivery. These requirements should be identified during the course development phase.

Potential Lead Training Organisations

Mauritius	Institute for Judicial and Legal Studies (IJLS)
Morocco	Moroccan Higher Institute of the Judiciary
Philippines	Philippine Judicial Academy (PHILJA)
Senegal	Judicial Training Centre (JTC)
South Africa	South African Judicial Education Institute (SAJEI)
Sri Lanka	Judges Training Institute
Tonga	Attorney General's Office & Ministry of Justice