Emancipating, Enriching, Equalising, Empowering through the use of ICTs

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

National Cybersecurity Development Barbados

18 November 2014

NATIONAL CYBERSECURITY STRATEGY DEVELOPMENT PROCESS

- Identify lead/responsible institution
- submit requests/proposals to relevant higher authority
- Identify experts in the field of Cybersecurity and set up committees to develop the policy content
- Hold stakeholder consultation workshops to review the policy
- Adopt and Implement Policy
- Review and update policy

National Cybersecurity Committee

- **OBJECTIVE**
  - Direct the development and implementation of the Cybersecurity strategy policy

- **ACTION/ACTIVITIES**
  - Carry out appropriate background research on use of Cyberspace and level of Cybersecurity taking existing policies and regulations into consideration;
  - Identify policy objectives/goals/principles
  - Set up subcommittees to develop relevant sections of the policy

Subcommittees

- **OBJECTIVE**
  - Identify activities that needs to be carried out in order to achieve the strategic objectives
- **ACTION/ACTIVITIES**
  - Define practical actions that should be undertaken to meet strategy objectives
- **POTENTIAL SUBCOMMITTEES**
  - Institutional/technical framework
  - Legal/regulatory framework
  - Capacity building
  - Awareness campaign

Institutional/technical framework subcommittee

- **OBJECTIVE**
  - establish institutional mechanisms to implement national Cybersecurity initiatives

- **ACTION/ACTIVITIES**
  - Set up appropriate governance and institutional structures to facilitate policy development and implementation
  - Identify and establish institutions required to implement strategy
  - Build the capabilities of institutions responsible for implementing Cybersecurity initiatives. i.e.
  - Adopt measures to foster institutional and technical collaboration
  - Establish centres of excellence in cyber security (e.g. R&D centre of excellence)
-

Legal/regulatory framework Subcommittee

- **OBJECTIVE**
  - Ensure that appropriate policies and legislations are put in place to support Cybersecurity initiatives

- **ACTION/ACTIVITIES**
  - Review the legislative landscape of existing Cybersecurity policies and legislations
  - Design measures to review the policies and legislations to identify gaps for improvement
  - Make recommendations for the development of new policies and legislations where necessary
  - Identify relevant stakeholders and form public-private-partnerships at the national, regional and international level to foster collaboration and benchmark legislative frameworks
  - Design R&D mechanisms to bring the country up to date with regional and international Cybersecurity legislative trends

Capacity Building

- **OBJECTIVE**
  - Ensure the availability of the right skills set needed to secure cyberspace
- **ACTION/ACTIVITIES**
  - Conduct a baseline study to ascertain the current Cybersecurity knowledge status of the country
  - Carry out a training needs assessment of all relevant institutions
  - Design capacity building programs with special attention on critical sectors. i.e. standardization, legal and regulatory
  - Recommend training modules for inclusion in training curricula
  - Provide modalities for integrating Cybersecurity into national education curricula to train Cybersecurity experts and build cyber skills into the country's national workforce
  - Propose the adoption of recruitment and retention strategies to attract the right skills set into public institutions;
  - Encourage collaboration with training providers at the national, regional and international level in designing training curricula.
  - Put measures in place to promote collaboration among relevant training and research institutions and industry at the national, regional and international level.
  - Identify incentive mechanisms to encourage careers in Cybersecurity

Awareness Raising

- **OBJECTIVE**
  - Develop a framework to increase Cybersecurity awareness within the private and public sector
- **ACTION/ACTIVITIES**
  - Lunch public awareness schemes to increase awareness among the citizens taking into consideration the needs of vulnerable groups
  - Develop special awareness initiatives for the protection of children online
  - Design educational communication tools (i.e. online information dissemination portal, Cybersecurity information center and social-networks) to promote cyber safety
  - Design appropriate mechanisms to integrate public awareness into the agenda of all national institutions
  - Developing and implementing awareness creation programs to create a culture of cyber awareness and responsibility and discourage the use of counterfeit ICT equipment;
  - Encourage service providers to establish consumer alert systems and ensure implementation
  - Identify relevant stakeholders and form public-private-partnerships at the national, regional and international level to increase Cybersecurity awareness

Let’s work together to make the Cyberspace a safe place

www.cto.int

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION