Caribbean Community (CARICOM)

Last Updated: September 2020

Member States

POLICY

Strategy Documents

CARICOM Cyber Security and Cybercrime Action Plan

CARICOM Implementation Agency for Crime and Security (IMPACS), the Caribbean Telecommunications Union (CTU), the Organisation of American States (OAS), Commonwealth Secretariat

- Seeks to:
  - address the Cyber Security vulnerabilities in each participating Caribbean country
  - establish a practical, harmonised standard of practices, systems and expertise for Cyber Security, to which each Caribbean country could aspire in the short and medium terms
  - build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of Cybercrime and possible linkages to other forms of criminal activity
- Identifies 5 key areas:
  1. Public awareness
  2. Building sustainable capacity
  3. Technical standards and Infrastructure
  4. Legal Environment; and
  5. Regional and International Cooperation Collaboration - Incident response, cybercrime investigation and capacity building
- Addresses:
  - i. The establishment of a proper governance framework, including a Regional Cyber Committee
  - ii. The identification of minimum standards for Cyber Security for each country
  - iii. An updated (desk) status review of each countr
  - iv. Identification of mechanisms for implementation of the relevant action items - Common Needs, Solutions and agencies/partners with interest (present or potential); and
  - v. Monitoring and evaluation of activities to ensure that objectives are being achieved

Source Source 2

February 2017

Vision and Roadmap for a CARICOM Single ICT Space

CARICOM ICT Cluster, including: Caribbean Telecommunications Union (CTU), Caribbean Broadcasting Union (CBU), Caribbean Centre for Development Administration (CARICAD), Caribbean Knowledge and Learning Network (CKLNA), CARICOM Implementing Agency for Crime and Security (IMPACS), CARICOM Secretariat

- Approved at the Twenty-Eighth (28th) Inter-Sessional Meeting of the Conference of Heads of Government of the CARICOM
- Collates the views of Heads of Government and other stakeholders on the importance of a CARICOM Single ICT Space, elaborates a vision for an ICT-enabled borderless space and outlines a Roadmap for its establishment
- The objective: to provide the ICT-enabled foundation for enhancing both CARICOM's functional cooperation and fulfilling the social, cultural and economic imperatives of the region
- Identifies key characteristics of the CARICOM Single ICT Space:
  1. Regionally harmonised ICT policy, legal and regulatory regimes
  2. Robust national and regional broadband infrastructure
  3. Common frameworks for Governments, ICT service providers and consumers; and
  4. Effective, secure technology and management systems
- Components of the "Effective, secure technology and management systems" Characteristics include:
  - Regionally harmonised Cyber Security policy framework
  - Regionally agreed standards and best practices for Cyber Security at the national level to engender consumer trust
  - National Computer Security Incident Response Teams (CSIRTs) and a regional protocol for their co-operation

Source

16 February 2017 (approved)

Other Documents

Caribbean Community (CARICOM)

Last Updated: September 2020

CARICOM Crime and Security Strategy 2013: Securing the Region

CARICOM Implementation Agency for Crime and Security (IMPACS)

- Goal: to significantly improve citizen security by creating a safe, just and free Community, while simultaneously improving the economic viability of the Region
- Identifies the risks and threats prioritised into four (4) Tiers:
  - Tier 1 - Immediate Significant Threats: high-probability, high-impact events, current and present dangers - including Cyber-Crime
  - Tier 2 - Substantial Threats: both likely and high-impact, but are not as severe as Tier 1 Threats
  - Tier 3 - Significant Potential Risks: high-impact, but low-probability
  - Tier 4 - Future Risks: threats where the probability and impact cannot be assessed at this stage
- Identifies 14 Strategic Goals, including Strategic Goal 8: Strengthen CARICOM's Resilience to Cyber-Crimes
- Strategic Goal 8 Action Items include:
  1. Education and awareness of internet users
  2. Raising the standards of specialisation of the police, judges, prosecutors and forensic staff
  3. Exploring ways to establish a CARICOM Cyber Crime Centre
  4. Pursuing the establishment of a network of CARICOM Cyber Security Points of Contact (PoC)
  5. Pursuing the establishment of a CARICOM Computer Emergency Response Team (CERT)
  6. Recognizing the importance of each Member State establishing its own National Cyber Security Unit
  7. Seeking functional and active partnership with the private sector, in particular internet service providers, internet security organisations and financial services

Source

18-19 February 2013

Strategic Plan for the Caribbean Community 2015 – 2019: Repositioning CARICOM

CARICOM Secretariat

- Outlines the strategic repositioning of the Community, and captures a development agenda going forward that encompasses:
  1. a review of development needs
  2. a Resilience Model for socio-economic progress
  3. strategies to renew the commitment to and strengthen actions for enhancing regional unity; and
  4. an agenda for the reform of governance mechanisms to achieve these two major forward thrusts
- Proposes the set of 6 integrated Strategic Priorities within the context of a resilience model including:
  - Strategic Priority 2: Building Social Resilience – Equitable Human and Social Development (SOC)
  - Strategic Priority 4: Building Technological Resilience (TEC)
- Strategic Priority 2 (SOC) involves Strategy SOC 4 - Enhance Citizen Security and Justice, with part c) dedicated to Strengthening CARICOM's Resilience to Cyber Crime
- Strategic Priority 4 (TEC) involves Strategy TEC 3: Strengthening Cyber Security with focus on initiatives to fully secure the single ICT space

Source Source 2

3 July 2014

STRUCTURE

Specialized Agencies

(proposed) Regional Cyber Committee

CARICOM Implementing Agency for Crime and Security (IMPACS)

- Outlined in Cyber Security and Cybercrime Action Plan, and proposed to be established to expand the role of CARICOM IMPACS' Regional Intelligence Fusion Centre (RIFC) by improving its capacity to monitor Cyber Security and Cybercrime
- To be chaired by CARICOM IMPACS representative, with membership comprised of National Cyber Points of Contact
- Envisioned responsibilities:
  1. Serve as the mechanism for the sharing of information as it relates to cybercrime activities (with possibly links to other criminal activities) nationally and/or regionally
  2. Serve as a mechanism for the exchange of lessons learnt, resources and expertise as they relate to cyber security and cybercrime from a regional perspective
  3. Be an effective mechanism that will aid in the coordination of projects aimed at sustainable capacity building initiatives
  4. Disseminate information, through the NCPOCs, ensuring that each member of the Committee is responsible for the communication and coordination within the jurisdiction which they represent as it relates to the activities of the Committee. This will also entail

Caribbean Community (CARICOM)

Last Updated: September 2020

working along with other stakeholders and other points of contact personnel within their jurisdiction (e.g. OAS/CICTE – National Points of Contact)

5. Provide relevant reports to the various stakeholders including the Steering Committee, IMPACS Standing Committees, CONSLE, etc.

Source

February 2017 (outlined)

(proposed) Regional Capacity Centre for Cyber Security and Incident Response

CARICOM IMPACS

- Outlined in CARICOM Cyber Security and Cybercrime Action Plan as part of proposed actions items on Regional and International Cooperation Collaboration - Incident response, cybercrime investigation and capacity building
- Envisioned objectives and solutions for its establishment include:
  - Identifying the skill set required
  - Identifying the Human Resources within the Caribbean Region
  - Providing the relevant Training
  - Developing mechanism/SOP for operations
- CARICOM agencies and current and potential interested partners include:
  - CARICOM IMPACS
  - Commonwealth Secretariat
  - International Telecommunication Union (ITU)
  - Organization of American States/Inter-American Committee against Terrorism (OAS/CICTE)

Source

February 2017 (outlined)

Key Positions

Cybercrime Policy Specialist, IMPACS 11th EDF Project

CARICOM Implementation Agency for Crime and Security (IMPACS)

- Position established for the Eleventh European Development Fund (11th EDF) Project – CARIFORUM Crime and Security Cooperation Programme: Capacity Building for CARIFORUM Member States on Asset Recovery and Cybercrime
- Expected to lead all project related activities under the Cybercrime and Cybersecurity components of the IMPACS CARIFORUM Crime and Security Cooperation Programme
- Major functions and responsibilities include:
  - Provide anti-cybercrime and cybersecurity policy and legislative expertise for the establishment of a regional guidance framework
  - Provide support to the desk review of existing cyber legislative and policy frameworks in view of regional and international standards
  - Basing on the review, support the development of a regional cybercrime policy and legislative guidance document to direct the establishment of harmonised policy and legislation within Member States in keeping with the objectives of the CARICOM Cybersecurity and Cybercrime Strategy
  - Basing on the review, participate in consultations with regional stakeholders in order to finalise the frameworks
  - Report to the IMPACS Programme Coordinator, on the day to day operations of the project, and liaise with the ICT Manager and other IMPACS staff members
  - Work with external stakeholders such as Ministries responsible for national security, law enforcement, cyber security and cybercrime, as well as with civil society organisations and the private sector

Source

1 July 2019 (position active)

LEGISLATION

Regulations and Directives

Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts (HIPCAR Project)

CARICOM Secretariat, European Union, International Telecommunication Union (ITU), Caribbean Telecommunication Union (CTU)

Caribbean Community (CARICOM)

Last Updated: September 2020

- Developed as a part of the ITU-EC-ACP Project "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" (HIPCAR Project) with funding from European Union
- Objective: to assist CARIFORUM countries to harmonize their information and communication technology (ICT) policies, legislation and regulatory procedures so as to create an enabling environment for ICT development and connectivity, thus facilitating market integration, fostering investment in improved ICT capabilities and services, and enhancing the protection of ICT consumers' interests across the region
- Six (6) inter-related model legislative frameworks developed over the course of the Project:
    1. Access to Public Information (Freedom of Information)
    2. Privacy and Data Protection
    3. Electronic Commerce (Transactions)
    4. Electronic Commerce (Evidence)
    5. Cybercrime:
        - defines offences, investigation instruments and the criminal liability of key actors
    6. Interception of Electronic Communications:
        - establishes an appropriate framework that prohibits the illegal interception of communication;
        - defines a narrow window that enables law enforcement to lawfully intercept of communication if certain clearly defined conditions are fulfilled

Source Source 2

2012 (published)

COOPERATION

External Cooperation

Capacity Development for CARIFORUM Member States on Financial Compliance, Asset Recovery and Cybercrime Project

European Commission, Caribbean Forum of ACP States (CARIFORUM), CARICOM IMPACS

- Conducted within the framework of the Caribbean Regional Indicative Programme for the period 2014-2020 based on the agreement between CARIFORUM and the European Commission on behalf of the European Union
- Approved by the European Commission Decision of 11.12.2017 on the Annual Action Programme 2017 - part II - in favour of the Caribbean Region to be financed from the 11th European Development Fund (11th EDF)
- Aims at increasing compliance in the CARIFORUM region with international norms on money laundering, countering the financing of terrorism and other financial crimes while also improving the capacity of CARIFORUM Member States to deal with the issues of asset recovery and cybercrime
- Comprises three components:
    - Component A: Implementation of the Mutual Evaluation Programme
    - Component B: National Risk Assessments and National Action Plans
    - Component C: Asset Recovery and Cybercrime
- Component C shall be implemented via direct management through a direct award to the CARICOM Implementation Agency for Crime and Security (IMPACS); it has 4 main scopes of engagement:
    1. Legislation review and update to meet international standards
    2. Capacity building/training of law enforcement, judiciary and legislators including through incorporation of cybercrime/cybersecurity modules in selected national and regional educational institutions
    3. Engagement and awareness raising of decision makers, parliamentarians, public sector ICT professionals and private sector representatives;
    4. Strengthened regional capacity to coordinate efforts to counter cybercrime through support to the RIFC and IMPACS

Source Source 2

11 December 2017 (adopted)

Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR Project)

CARICOM Secretariat, European Union, International Telecommunication Union (ITU), Caribbean Telecommunication Union (CTU)

- Launched by the International Telecommunication Union (ITU) and the European Union in December 2008, in close collaboration with the CARICOM Secretariat and the CTU
- Two work areas were covered by the Project Working Groups:
    1. ICT Policy and Legislative Framework on Information Society Issues, dealing with six subareas: e-commerce (transactions and evidence), privacy & data protection, interception of communications, cybercrime, and access to public information (freedom of information)
    2. ICT Policy and Legislative Framework on Telecommunications, dealing with three sub-areas: universal access/service, interconnection,

Caribbean Community (CARICOM)

Last Updated: September 2020

and licensing in a convergent environment

- On Cybercrime, the WG on the ICT Policy and Legislative Framework on Information Society Issues produced Report cointaining Model Policy Guidelines and a Model Legislative Text including Explanatory Notes
- The 5 Model Policy Guidelines on Cybercrime provide that the CARICOM States shall:
    1. Aim to Establish Necessary Common Interpretations for Key Terms Associated with Cybercrime
    2. Develop Substantive Criminal Law Dealing with Cybercrime
    3. Develop Effective but Balanced Procedural Instruments That Enable Competent Authorities to Investigate Cybercrime but Protect the Rights of the Suspect
    4. Develop Instruments for Transnational Cooperation in Cybercrime Investigations
    5. Develop a Framework Regulating the Responsibility of Internet Service Providers

Source Source 2

2008 (launched)