EU-LAC
DIGITAL ALLIANCE
POLICY DIALOGUES

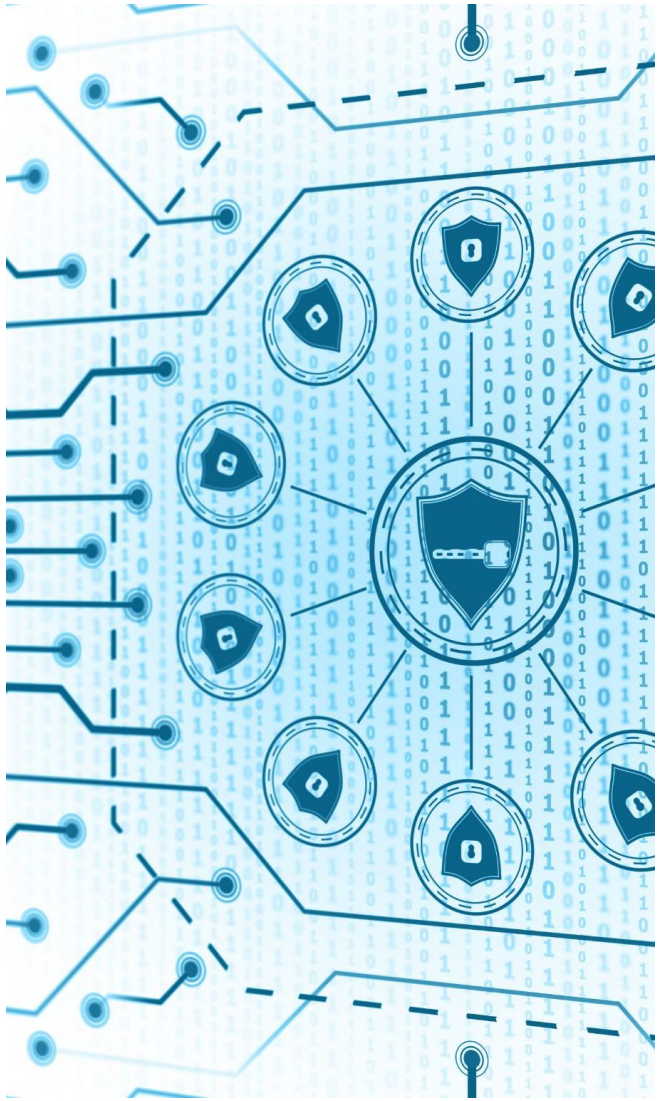
EL PACCTO 2.0
EU-LAC Partnership on justice and security

CARICOM CYBERSECURITY CYBERCRIME ACTION PLAN (CCSCAP) UPDATE

Caribbean Community (CARICOM)
Implementation Agency for Crime and Security (IMPACS)
Keate Street, Port of Spain
Tel#1-(868)-235-5511
Fax# 1(868)-627-3064

Introduction

- About CARICOM IMPACS
- Regional Threats and Trends
- CCSCAP Pillars
- Strategic Priorities
- Opportunities and Next Steps
- Call For Action



Antigua & Barbuda, Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Haiti, Jamaica, Montserrat, St Lucia, St Kitts & Nevis, St Vincent & The Grenadines, Suriname, Trinidad and Tobago

ASSOCIATE STATES

Anguilla, Bermuda, British Virgin Islands, Cayman Islands, Curaçao, Turks and Caicos Islands

Established by the Twenty Seventh (27th) Meeting of the Conference of Heads of Government in July 2006, in Bird Rock, St Kitts and Nevis

Headquarters

Regional Intelligence Fusion Center (RIFC)

Joint Regional Communication Center (JRCC)

Regional Cyber Threat Landscape

Diverse Cyber Threats

Ransomware, phishing, and data breaches target government, finance, healthcare, and education sectors.

Critical Infrastructure Risks

Energy and telecommunications face rising cyber attack concerns impacting regional stability.

Challenges in Cybersecurity

Limited resources, fragmented laws, and low awareness worsen the regional cyber threat landscape.

Strategic Mitigation Approach

CCSCAP enables coordinated efforts and planning to enhance cyber resilience in the Caribbean.

Overview of CCSCAP

Strategic Framework Purpose

CCSCAP guides CARICOM members to enhance cybersecurity and strengthen regional resilience.

Objectives and Goals

The action plan aims to create a secure, resilient, and trusted cyberspace across Caribbean nations.

Collaborative Initiatives

CCSCAP promotes joint efforts to mitigate cyber threats and foster digital safety regionally.

Roadmap and Response

The plan offers a roadmap for policy, capacity building, and international cooperation.

CCSCAP Pillars
Action Plan

Public Awareness, Education and Advocacy ↔ Raising public awareness and promoting education are critical for creating a culture of cybersecurity and anti-crime.

Cyber Incident Management ↔ To create a security posture that can anticipate, withstand, and recover from a broad spectrum of cyber threats.

Capability Development and Capacity Building ↔ Strengthening organizational capabilities and human resources is essential for addressing the dynamic nature of cyber threats

Policy, Institutional and Regulatory Framework ↔ To create a robust and adaptable legal environment

Enhancing and Harmonizing Technical Standards and Infrastructure ↔ The Action Plan underscores the importance of unified technical standards and infrastructure improvements.

Regional and International Cooperation ↔ Recognizing the transnational nature of cyber threats, the Action Plan prioritizes collaboration at regional and global levels

CCSCAP Updated Action Plan

1. Public Awareness, Education and Advocacy

Public awareness campaign
- Planning as a component of the national strategy and execution

Targeted awareness initiatives
- Senior officials, parliamentarians and policy makers
- SMEs and vulnerable sectors

Awareness campaigns and educational initiatives in schools and for children
- School curricula initiatives

Regional coordination and inventory of initiatives
- Sharing of national best practice
- Coordination of media campaigns

Establishment of a Regional Cybersecurity Awareness Month
- Regional coordination of awareness initiatives

CCSCAP Updated Action Plan

2. Capability Development and Capacity Building

Develop Regional Expertise

- Build specialized competencies in cybercrime investigation and prosecution.
- Provide tailored training for sectors managing Critical Information Infrastructure (CII).

Promote Digital Forensic Training

- Establish agreements with institutions for structured curricula

Promote Operational Coordination

- Promote networks with other police organizations for joint operations.
- Improve coordination in cybercrime investigations..

Create Regional Expert Group

- Form a certified group of experts in legal, technical, and operational sector.
- Support on-demand deployments and mentorship schemes.

Additional Objectives: Standardize training and certification, facilitate knowledge exchange, strengthen academia–private sector partnerships, and develop a regional repository of initiatives.

CCSCAP Updated Action Plan

3. Enhancing and Harmonizing Technical Standards and Infrastructure:

Establish CARICOM-wide minimum cybersecurity technical standards

- Regional WG, alignment with ISO and others

Develop and implement national Critical Information Infrastructure (CII) protection frameworks

- Essential and important entities

Regional VA/PT Framework

Secure supply chain

- Cybersecurity requirements for procurement

Harmonized criminal justice statistics

- Template, models, methodology and centralized collection at national level

Regional framework for SOPs of digital forensics labs

- Uniform baseline for lab operations
- Chain of custody, digital storage protocols

Promote resource sharing

CCSCAP Updated Action Plan

4. Policy, Institutional and Regulatory Framework

Cybercrime Legislation Harmonization

- Standardize cybercrime laws across Member States.
- Align with international standards (Budapest Convention, UN Convention on Cybercrime).

Data Protection and Privacy Laws

- Promote national data protection laws aligned with global standards
- Establish independent, well-resourced Data Protection Authorities.

Cyber Risk Management Framework

- Implement a standardized methodology for cyber risk assessment and mitigation (aligned with ISO 31000, NIST).

E-Evidence and Digital Forensics Legal Framework

- Create common protocols for the collection, preservation, and admissibility of electronic evidence.
- Provide specialized training in digital forensics and chain of custody management.

Mutual Legal Assistance and Extradition

- Develop a standardized regional MLA and extradition framework for cybercrime.
- Designate national contact points and fast-track procedures.

National Cybersecurity Strategies

- Ensure each Member State develops, updates, and implements a national cybersecurity strategy.
- Promote periodic review and alignment with regional priorities

Additional Initiatives to be Developed: Virtual Assets and VASP regulation; Cybercrime Victim Support and Restitution Systems; AI readiness Assessment and Model AI Legislation

CCSCAP Updated Action Plan

5. Cyber Incident Management

Establish national CSIRTs and foster incident handling capabilities

Regional coordination of incident reporting and operational handling

- RCFC acting as the regional hub for coordination and infromation exchange, assuming the role of a Regional CSIRT

Standard Incident Reporting Protocol

- Unified Incident Reporting Framework
- Cyber Incident Reporting and Escalation Playbook

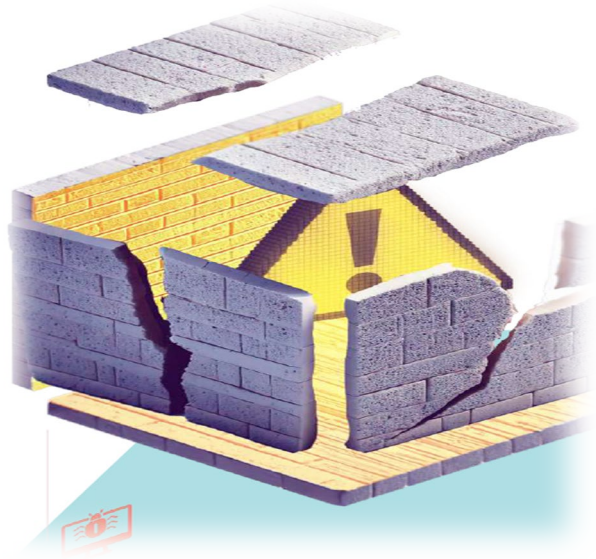
Test and evaluate incident response capacity through simulation exercises

- Sustainable and continuous training (foundational and advanced) for technical units
- Annual simulation exercise at regional level

Threat intelligence sharing and coordination mechanism

Work towards the establishment of a regional incident response support fund

Annual simulation exercise at regional level



CCSCAP Updated Action Plan

6. Regional and International Cooperation

Strengthen Cross-Border Cooperation

- Promote international agreements and partnerships (e.g. Budapest Convention UN Treaty).
- Align cybersecurity policies with international standards

Regional Cyber Fusion Centre (RCFC)

- Serve as the operational hub for regional coordination.
- Coordinate with CSIRTs, law enforcement, and critical infrastructure.
- Host annual CARICOM cybersecurity policy meeting.

Operational Networks and Threat Intelligence

- Develop informal networks for law enforcement and cybercrime investigations.
- Launch protocols for real-time threat intelligence sharing.
- Connect with global platforms (e.g. INTERPOL, FIRST, ITU)

Public-Private Sector Collaboration

Establish regional ISACs for joint threat analysis and response.

Create working groups with private sector stakeholders.

Share tools, practices, and technology access.

Cyber Diplomacy & Global Engagement

- Train diplomats on cyber policy, AI, and international law.
- Ensure Member State participation in global cyber governance (UN, ITU, GFCE).
- Represent regional positions in international forums.

Governance Structure

Strategic Objective

The Governance Structure is design a comprehensive framework for decision making, coordination, and accountability within

the CCSCAP, supporting an integrated approach to cybersecurity across the region.

The governance framework is designed to:

Establish independent monitoring and evaluation (M&E) mechanisms that guarantee transparency, objective performance assessment, and continuous improvement.

Ensure operational delivery through a dedicated technical center responsible for daily coordination.

Provide strategic leadership and oversight through a regional body that sets direction and priorities.

Opportunities and Next Steps

Regional Collaboration

Foster collaboration through regional cyber – related hubs to unify efforts and share knowledge.

Workforce Development

Invest in cyber training and certifications to build a skilled and knowledgeable workforce.

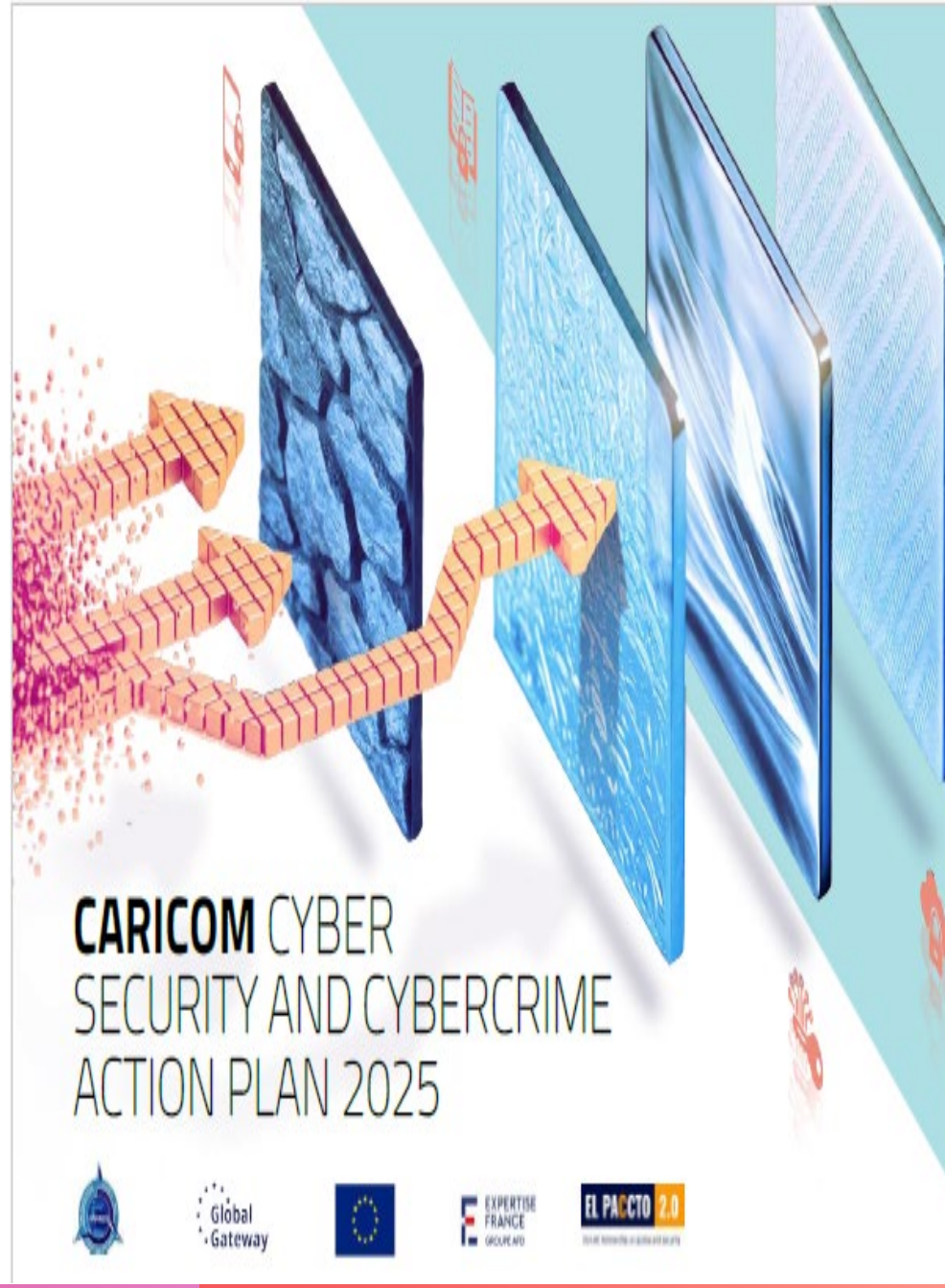
Public-Private Partnerships

Form partnerships between public and private sectors to pool resources and expertise.

Legal and Policy Strengthening

Enhance legal frameworks to ensure robust enforcement of cybersecurity measures.

CCSCAP Action Plan Updated



THANK YOU

Caribbean Community (**CARICOM**)
Implementation Agency for Crime and Security **(IMPACS)**
Website: www.caricomimpacs.org

Email: **secretariat@caricomimpacs.org**
cyberfusionunit@carimpacs.org

Telephone: **(868)-235-5511**