



22ND CARIBBEAN INTERNET GOVERNANCE FORUM

5TH CARIBBEAN YOUTH INTERNET GOVERNANCE FORUM

CARICOM Cyber Resilience Strategy 2030

Cybersecurity for Policy-makers

PRESENTED BY

Ms Utica Alves

Project Officer, ICT for Development (ICT4D), CARICOM Secretariat
Directorate of Economic Integration, Innovation and Development

24–26 August 2026 Radisson Grenada Beach Resort, St. George's



THE MANDATE

Ministerial Mandate and Rationale

In **2019** the Council for Trade and Economic Development – Information and Communications Technology (COTED-ICT) mandated a cyber-resilience strategy for the Caribbean Community (**CARICOM**)

Development was funded by the **United States Agency for International Development (USAID)** through its Digital Frontiers project, with Cambridge Global Advisors as Consultants on the project.

6

Strategic pillars

23 strategic objectives

220+

Stakeholders consulted

Member & Associate States

8

Steering Committee meetings

Dec 2023 – Apr 2025

US\$500k

USAID Digital Frontiers

Dec 2023 – Dec 2024

APPROVED

18 June 2026

The COTED-ICT approved the CARICOM Cyber Resilience Strategy 2030, and extended the Steering Committee to December 2027.



RATIONALE

Cybersecurity and Cyber Resilience

01

Cybersecurity

Identifying, preventing and mitigating threats to digital assets through controls, monitoring and patching.

02

Cyber resilience

Proactive risk management, the ability to operate during an incident and recover quickly afterwards, with response plans and business-continuity measures built in.

Key Objective of the Cyber Resilience Strategy: Establish unified and resilient cybersecurity capabilities across CARICOM Member States, empowering effective management of cyber risks through enhanced regional cooperation, resulting in a digitally secure community.

42%

of organisations in Latin America and the Caribbean lack confidence in their nation's cyber-incident preparedness

WEF Global Cybersecurity Outlook 2025

120%

increase in reported phishing incidents across the Region between 2021 and 2023

Caribbean Cyber Security Center

US\$20m+

lost to phishing scams across the Region in 2022 alone

Caribbean Financial Action Task Force

- | | |
|-----------|--|
| 01 | Mature governance across the CARICOM Region |
| 02 | Build capacity through human-capital management |
| 03 | Increase public awareness and cyber literacy |
| 04 | Defend critical information and infrastructure |
| 05 | Regional laws and regulations with cooperation and reciprocity |
| 06 | Regional information sharing and incident-response capability |



The pillars are designed to be complementary: regional cyber resilience depends on collaboration and mutual support across Member States.



PILLARS 01 AND 02

Governance and Human Capital

01

Mature governance across the Region

A single regional structure to set cyber policy, coordinate national cyber offices and commit Member States to help one another.

KEY ACTION 1

A regional cybersecurity authority

Establish a body to oversee cybersecurity policy, manage shared cyber resources and coordinate between national cyber offices, with sustainable funding for prevention, detection, response and recovery.

KEY ACTION 2

Mutual aid agreements

Commit Member States to assist one another during significant cyber incidents, with rapid information exchange, resource sharing and standardised protocols for triaging the most critical threats first.

02

Build capacity through human-capital management

A deliberate pipeline of cyber professionals, built with the Region's universities, training institutions and employers.

KEY ACTION 1

A regional cyber skills framework

Identify the critical skills the Region needs, drawing on established models such as the National Initiative for Cybersecurity Education and the European Cybersecurity Skills Framework, and map existing centres of excellence.

KEY ACTION 2

Partnerships with academia and industry

Work with universities, the private sector and Member States to tailor curricula to employer needs, upskill existing technical staff and create apprenticeship, mentorship and internship programmes.



PILLARS 03 AND 04

Awareness and Critical Infrastructure

03

Increase public awareness and cyber literacy

Citizens who can recognise social engineering, financial scams and misinformation are the Region's first line of defence.

KEY ACTION 1

Cybersecurity in the school curriculum

Work with Ministries of Education to develop and integrate age-appropriate cybersecurity content across all levels of education, supported by resources employers can use to train their own staff.

KEY ACTION 2

A regional public awareness campaign

Launch a multi-channel campaign of public service announcements, television, print, social media and educational video, anchored by regional cybersecurity weeks with workshops and competitions.

04

Defend critical information and infrastructure

A shared understanding of what is critical, and the monitoring and controls needed to keep it running.

KEY ACTION 1

Harmonised definitions and risk assessment

Agree common definitions of critical infrastructure across the Region so protection protocols are uniform, and conduct regular risk assessments prioritised by potential impact on public health and safety.

KEY ACTION 2

Continuous monitoring and data protection

Build systems that monitor threats and vulnerabilities continuously against clear remediation targets, with controls protecting national security, financial, health and personal data.



PILLARS 05 AND 06

Legislation and Incident Response

05

Regional laws and regulations with cooperation and reciprocity

A common legal footing so that cybercrime can be investigated, prosecuted and reported consistently across borders.

KEY ACTION 1

Standardised offences and penalties

Adopt common definitions of cybercrimes and consistent region-wide sentencing so that no safe havens remain, with data retention requirements that support investigation across borders.

KEY ACTION 2

Data protection and incident reporting

Introduce comprehensive data protection regulation, require organisations handling sensitive data to meet recognised cyber hygiene standards, and make certain cyber incidents reportable.

06

Regional information sharing and incident response

One place for the Region to see threats early, respond together and recover faster.

KEY ACTION 1

A regional Information Sharing and Analysis Centre

Establish a centre servicing all Member and Associate States, providing cyber threat intelligence sharing, an incident response capability and technical advice on cyber defence, with centralised monitoring over time.

KEY ACTION 2

Connected national response teams

Build national computer incident response teams and connect them to the regional centre and to international counterparts, so that warnings and assistance move quickly in both directions.



STEERING COMMITTEE

Composition of the Steering Committee

MEMBERSHIP

Established in 2023 to guide development of the Strategy, the Committee was extended by Ministers in **June 2026**

Co-Chairs

Jamaica and Trinidad and Tobago, supported by the Secretariat's ICT4D Technical Lead.

Member States

Focal points from Belize, Grenada, Guyana, Jamaica, St. Vincent and the Grenadines, and Trinidad and Tobago. Remaining Member States to be invited to nominate.

Organs and Bodies

CARICOM Secretariat · CARICOM IMPACS · CDEMA · CARICOM Private Sector Organisation

Mandate period

From the First Meeting to December 2027, reporting to the Council for Trade and Economic Development, the Council for National Security and Law Enforcement and other relevant Councils.



Integration of the Two Action Plans

- 01 Strategic alignment.** The six CCSCAP priorities (IMPACS Action Plan) defined in 2024 correspond to the six Strategy 2030 pillars.
- 02 Steering Committee ownership.** The Committee leads the drafting, supported by the Secretariat and CARICOM IMPACS.
- 03 CDEMA cooperative model.** The model informs the Action Plan and is not a third document for consolidation.
- 04 Drafting and review schedule.** Drafting concludes in late October; the Second Meeting reviews the draft on 5 November.

CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) 6 Priorities Updated in 2024

CARICOM Cyber Resilience 2030 Strategic Pillars



CCSCAP priorities (2024) mapped to the Strategy 2030 pillars



WHAT HAPPENS NEXT

From Decision to Implementation

On 18 June 2026 Ministers approved the Strategy and extended the Steering Committee to December 2027. **One integrated Action Plan is due by 15 November 2026.** The work below carries the Strategy into implementation.

01 One Action Plan STEERING COMMITTEE · 15 NOV 2026 The Committee brings the Cyber Security and Cybercrime Action Plan and the Strategy together in one instrument, taking account of the CDEMA cooperative model.	02 Member State focal points MEMBER STATES · NOMINATIONS OPEN Remaining Member States are invited to nominate focal points to support the Committee, champion the Strategy and develop national response teams.	03 National consultations FOCAL POINTS · Q4 2026 – 2027 Consultations open in Q4 2026 and Q1 2027 to guide implementation in each Member State and to refine the Strategy further.
04 Resource mobilisation CARICOM SECRETARIAT · ONGOING The Secretariat and CARICOM IMPACS continue to mobilise resources for implementation of the Strategy and the Action Plan.	05 Lead Agency reporting LEAD AGENCIES · TO DEC 2027 Lead organisations report to the Secretariat. Reports go on to the Council for Trade and Economic Development and the Council for National Security and Law Enforcement.	06 Private sector and youth CARICOM SECRETARIAT · SEP 2026 Ministers invited the CARICOM Private Sector Organisation to nominate a representative. The Forum is invited to agree that a youth representative also serve on the Committee.



CONTACT INFORMATION

Contacts

ICT for Development Programme · Directorate of Economic Integration, Innovation and Development

PROGRAMME MANAGEMENT

Jennifer Britton

Programme Manager

PRESENTER

Utica Alves

Project Officer, ICT for Development (ICT4D)

CONTACT

ict4dstaff@caricom.org

ONLINE

www.caricom.org

LinkedIn · CARICOM ICT for Development