An Analysis of the Global Cybersecurity Index (GCI) 2024

Progress, Challenges and Opportunities for Cybersecurity in the Caribbean

Corlane Barclay, PhD, LLB, CLE, PMP

October 2024

DPO Caribbean

Privacy | Cybersecurity | Policy & Legislation

dpocaribbean.com

An Analysis of the Global Cybersecurity Index (GCI) 2024

Progress, Challenges and Opportunities for Cybersecurity in the Caribbean

ISBN

978 976 97440 0 4 (Electronic version)

Table of Contents

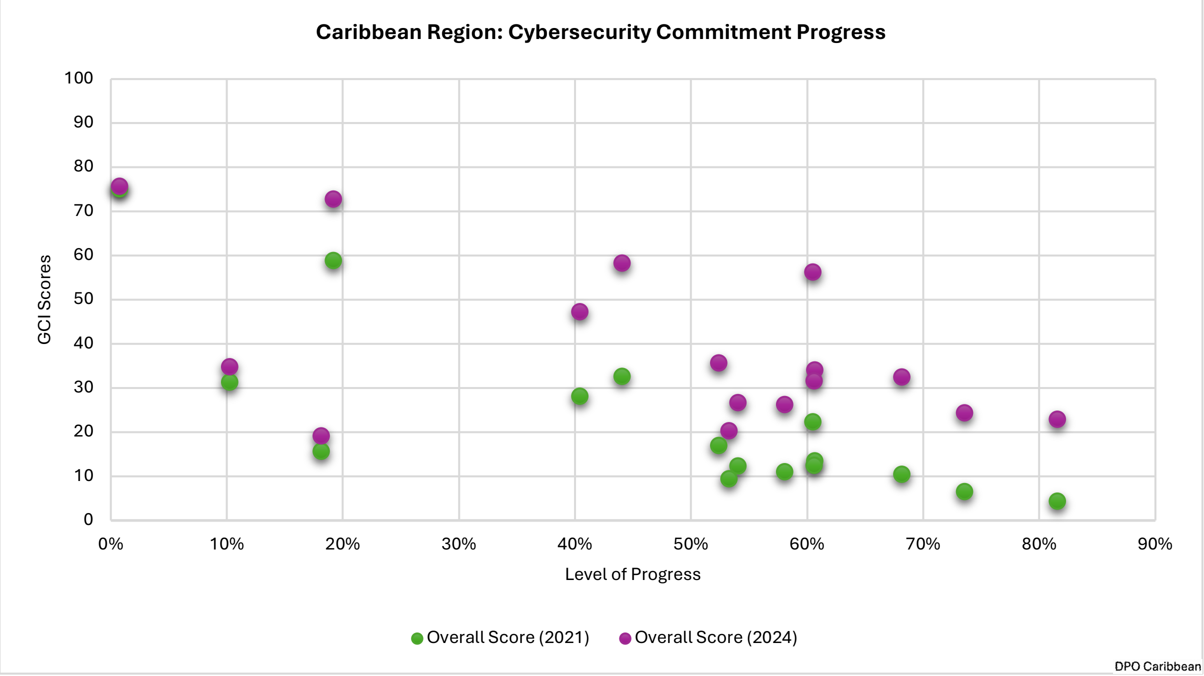
List of Figures

Report Synopsis

Two significant cybersecurity developments occurred in the last two months: the UN General Assembly's committee's agreement on a draft text of the convention on cybercrime[1]; and the release of the International Telecommunications Union (ITU) Global Cybersecurity Index (GCI) 2024 Report[2]. Both events underline the importance of a unified approach in tackling cyber threats and adopting robust cybersecurity practices and measures to foster national security and development.

The latest GCI edition reports that the global average country score has risen to 65.7/100[3], which means that many countries are demonstrating more government-led activities geared towards managing cybercrime and cybersecurity and thus are taking steps to improve their commitment to cybersecurity.

Figure 1: Caribbean Region: Progress in Cybersecurity Commitment (GCI 2021 & 2024)



The GCI 2024 edition assessed 16 countries in the Caribbean on actions and measures concerning each country's cybersecurity commitment. According to the analysis of the GCI data:

- The Caribbean region experienced substantial improvements in its overall GCI scores (Figure 1), with more than half of these countries experiencing over 50% increase over the previous GCI edition (2021). Despite this progress, the region still lags behind its counterparts in the rest of the Americas in all five cybersecurity pillars.

[1] https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html
[2] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
[3] Ibid

- Most countries are considered low to middle tier (i.e., Evolving and Establishing tiers) in their respective level of cybersecurity commitment, with Cuba and Dominica Republic leading the region. A single country, Antigua and Barbuda, is classified at the lowest (Building tier).
- Consistent with the global trend, the legal measures pillar remains a relatively strong area across the Americas. However, the Caribbean has a lower regional average score, signifying opportunities for revised and new cybercrime and cybersecurity-related laws and regulations aligned with global conventions, good practices and developments in the cybersecurity ecosystem.
- The technical measures pillar provides a strong opportunity for advancement in the region as it is shown to be one of the weakest areas. In addition to the development of national cybersecurity incident and reporting teams/operations (CIRTs) aligned with good practices, priority actions should also include the systematic identification and adoption of cybersecurity standards and frameworks for managing cybersecurity risks and building technical capabilities.
- Greater attention and investment in government incentive mechanisms, research and development, as well as other capacity development measures, must be prioritised if countries in the region are to level up to the next performance tiers.
- Organisation measures, including systematic monitoring and updates of National Cybersecurity Strategies/Plans (NCSs), identification of responsible agencies for cybersecurity and related activities, coupled with the provision of clear mandates for them, are essential in managing cybersecurity risks.
- All forms of cooperation measures must be effectively leveraged to fully experience the benefits of a collaborative stance in tackling cybersecurity risks. These measures include increased inter-agency coordination, information sharing schemes, partnerships among businesses and government agencies, and more active participation in regional and global treaties and conventions.

Background

The latest edition of the GCI[4] was released last month. It showed that countries have made progress in their cybersecurity-related actions and commitment to cybersecurity, resulting in an increase in the global average country score to 65.7/100. This is apparent in the increased cybersecurity-related actions such as the implementation of legal frameworks relating to cybercrime and cybersecurity, active incident response management processes, adoption of NCSs, policies and plans, increased partnerships and targeted awareness efforts. Despite this achievement, the gaps between countries such as Small Island Developing States (SIDS) and more developed nations continue to persist[5].

Notably, many countries in the Americas are ranked in the low to middle tiers, particularly in comparison to Europe, where numerous countries occupy the upper tiers. The current cybersecurity outlook is concerning, as Caribbean nations significantly affect the overall ranking of the Americas. The scores of several Caribbean countries in previous GCI editions have previously led the author to question the region's commitment to cybersecurity[6], a concern that remains relevant today. It therefore becomes apparent that more strategic interventions and leadership are needed to help countries in the Caribbean, and other developing economies, better understand the impact of cybersecurity risks on their economic development and to identify and adopt appropriate measures to combat these risks and build cybersecurity capabilities. Against this background, the GCI scores of Caribbean countries, which include several SIDS and other relatively lower-income economies, are examined within the context of the Americas.

An Overview of the GCI

The current edition of the GCI is the fifth in the series which started in 2015. This ITU cybersecurity-related composite index measures the commitment of countries to cybersecurity in the context of measures across five pillars[7], namely:

- **Legal**: Measures the laws and regulations on cybercrime and cybersecurity.
- **Technical**: Measures the implementation of technical capabilities through national and sector-specific agencies.
- **Organisational**: Measures national strategies, structures and institutions implementing cybersecurity.
- **Capacity Development**: Measures awareness campaigns, training, education and incentives for cybersecurity capacity development.
- **Cooperation**: Measures partnerships between agencies, firms and countries.

A tiered model for measuring the performance of countries was introduced in this edition of the GCI. Each country's performance is measured across five tiers, with Tier 1 being the highest and Tier 5 being the lowest. The model is summarised as follows:

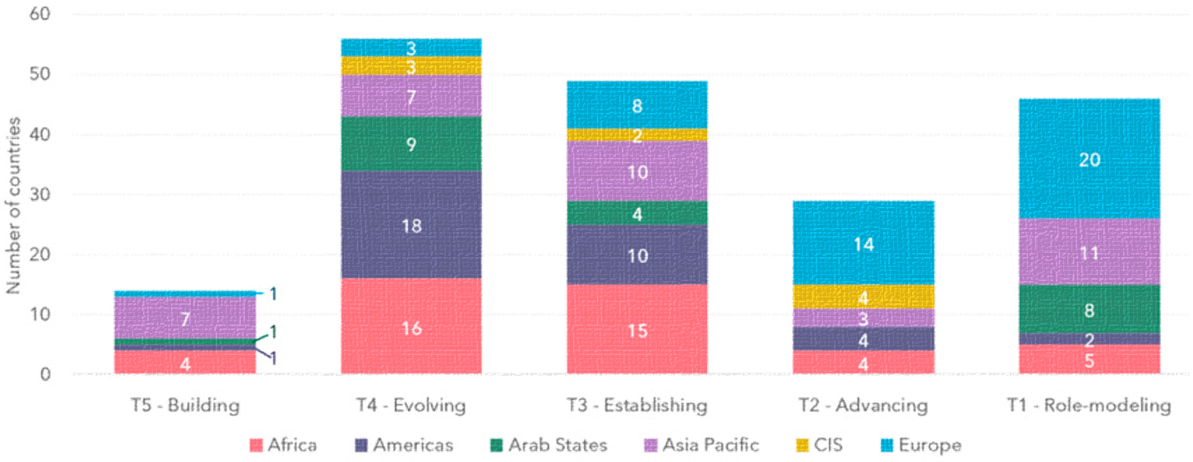
- Tier 1 (T1) – Role-modelling - a country with $95 \leq x \leq 100$ GCI score.

[4] Ibid
[5] Ibid
[6] https://dpocaribbean.com/dpo-updates/f/is-the-caribbean-community-committed-to-cybersecurity
[7] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

- Tier 2 (T2) – Advancing - a country with 85 ≤ x < 95 GCI score.
- Tier 3 (T3) – Establishing - a country with 55 ≤ x < 85 GCI score.
- Tier 4 (T4) – Evolving - a country with 20 ≤ x < 55 GCI score.
- Tier 5 (T5) – Building - a country with 0 ≤ x < 20 GCI score.

The tier performance across the six global regions (Figure 2), extracted from the GCI 2024 Report, highlights that the majority of global nations are at the Building, Evolving and Establishing stages of cybersecurity commitment while many countries in the Europe region are standouts in terms of relative commitment to cybersecurity. In contrast, the Americas has the lowest representation at the Role-modelling level.

Figure 2: Tier Performance by Region (GCI 2024)



Source: ITU

Cybersecurity Commitment Outlook in the Americas

The tier performance shows that the Americas features varying levels of cybersecurity commitment across the region, showcasing leaders and those with growth potential (see Figure 3):

- **T1 (Role-modelling)**: Brazil and the United States lead the region in demonstrating a strong cybersecurity commitment to coordinated and government-driven actions across all five pillars and the majority of the indicators.

- **T2 (Advancing)**: Countries from North America and Latin America, namely Canada, Ecuador, Mexico and Uruguay, are positioned at the Advancing level, demonstrating a strong cybersecurity commitment to coordinated and government-driven actions across the majority of pillars.

- **T3 (Establishing)**: Several Latin America and Caribbean countries, such as Peru, Dominican Republic, and Costa Rica are positioned at the Establishing level by demonstrating a basic cybersecurity commitment to government-driven actions across a moderate number of pillars or indicators.

- **T4 (Evolving)**: Most countries are placed at the Evolving level by demonstrating a basic cybersecurity commitment to government-driven actions across at least one pillar, or several indicators or sub-indicators. These countries include Argentina, Guyana, Bolivia, and Venezuela.

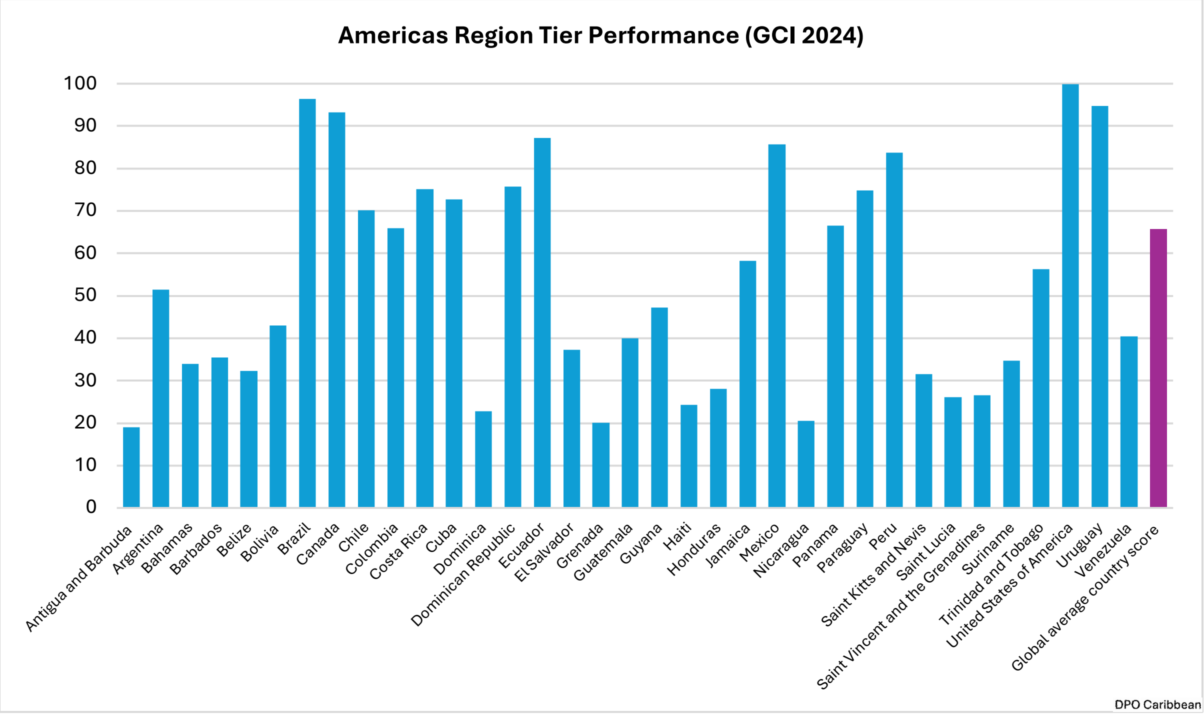
- **T5 (Building)**: Only Antigua and Barbuda is placed at the initial stage of building its cybersecurity commitment.

Figure 3: Americas Region Tier Performance and Ranking (GCI 2024)

Rank	Country	Americas Sub-Region	Tier Performance
1	United States of America	North America	T1, Role-modelling
2	Brazil	Latin America	T1, Role-modelling
3	Uruguay	Latin America	T2, Advancing
4	Canada	North America	T2, Advancing
5	Ecuador	Latin America	T2, Advancing
6	Mexico	Latin America	T2, Advancing
7	Peru	Latin America	T3, Establishing
8	Dominican Republic	Caribbean	T3, Establishing
9	Costa Rica	Latin America	T3, Establishing
10	Paraguay	Latin America	T3, Establishing
11	Cuba	Caribbean	T3, Establishing
12	Chile	Latin America	T3, Establishing
13	Panama	Latin America	T3, Establishing
14	Colombia	Latin America	T3, Establishing
15	Jamaica	Caribbean	T3, Establishing
16	Trinidad and Tobago	Caribbean	T3, Establishing
17	Argentina	Latin America	T4, Evolving
18	Guyana	Caribbean	T4, Evolving
19	Bolivia	Latin America	T4, Evolving
20	Venezuela	Latin America	T4, Evolving
21	Guatemala	Latin America	T4, Evolving
22	El Salvador	Latin America	T4, Evolving
23	Barbados	Caribbean	T4, Evolving
24	Suriname	Caribbean	T4, Evolving
25	Bahamas	Caribbean	T4, Evolving
26	Belize	Caribbean	T4, Evolving
27	Saint Kitts and Nevis	Caribbean	T4, Evolving
28	Honduras	Latin America	T4, Evolving
29	Saint Vincent and the Grenadines	Caribbean	T4, Evolving
30	Saint Lucia	Caribbean	T4, Evolving
31	Haiti	Caribbean	T4, Evolving
32	Dominica	Caribbean	T4, Evolving
33	Nicaragua	Latin America	T4, Evolving
34	Grenada	Caribbean	T4, Evolving

Rank	Country	Americas Sub-Region	Tier Performance
35	Antigua and Barbuda	Caribbean	T5, Building

Figure 4: Americas Region Overall Score (GCI 2024)



DPO Caribbean

The GCI overall scores highlight the varying levels of cybersecurity commitment across the Americas, with countries in North America leading, on average, followed by Latin America, and the Caribbean making steady progress (See Figures 3 and 4).

Regional Observations (Figure 4):

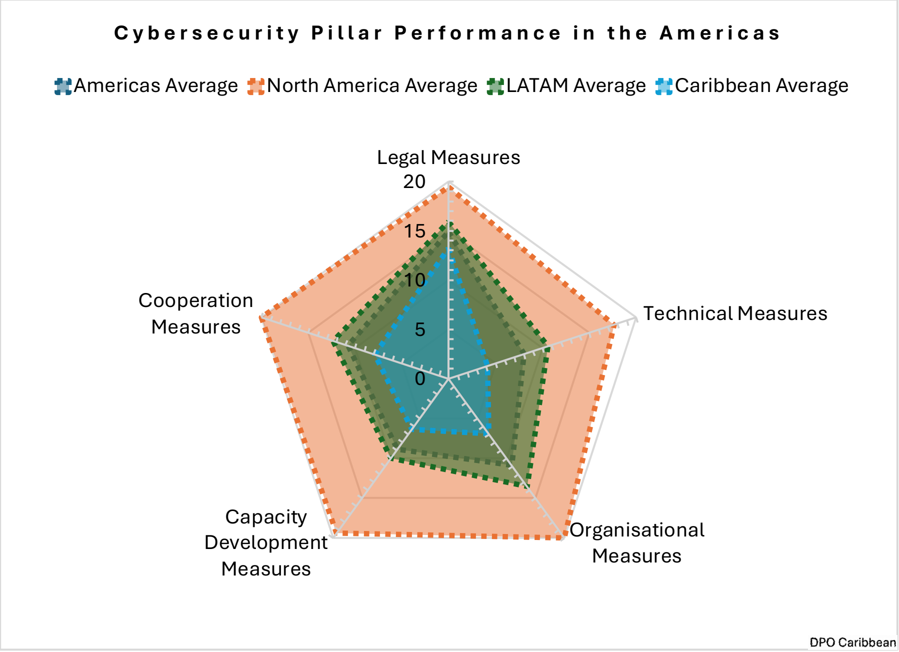
- Less than half of the countries in the Americas are positioned above the global country average score.
- The United States and Canada are consistently top performers, showcasing strong cybersecurity commitment measures across the five pillars.
- Brazil is identified as role-modelling while Ecuador, Mexico and Uruguay also lead the LATAM region with robust cybersecurity commitment measures.
- Dominica Republic and Cuba lead the Caribbean region in cybersecurity commitment measures.
- Jamaica and Trinidad are making notable progress in cybersecurity commitment measures, but significant gaps remain in each cybersecurity pillar.
- Antigua and Barbuda has the lowest GCI score, providing significant opportunities for progress in cybersecurity commitment.

Cybersecurity Pillar Observations (Figure 4):

- The Caribbean region lags behind North America and Latin America regions, as well as the Americas region average scores in all five cybersecurity pillars.
- The average score ranking among the pillars for the Caribbean in legal, cooperation, organisational, capacity development, and technical measures respectively, with only legal measures reaching the mid-point score, ≥ 10/20.
- On average, the legal measures pillar represents the strongest commitment across the region. This is consistent with the global trend, as the GCI 2024 Report highlighted *that most countries are strongest in the legal pillar*[8].
- Despite legal measures being the strongest, significant gaps exist in the Caribbean legislative and regulatory development landscape.
- The legal measures pillar also has less disparity among North America, Latin America and the Caribbean when compared with the other four pillars.
- Technical measures, on average, reflect the weakest position for the Caribbean. This is also consistent with global trends. Therefore, government-led initiatives to improve national capabilities concerning the management and governance of cybersecurity and its risks must be top priorities for national governments.

The findings underscore that the Caribbean region urgently needs to implement appropriate government-led initiatives to combat cybersecurity risks and improve all cybersecurity pillars (or capabilities).

Figure 5: Americas Performance across Cybersecurity Pillars (GCI 2024)



[8] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

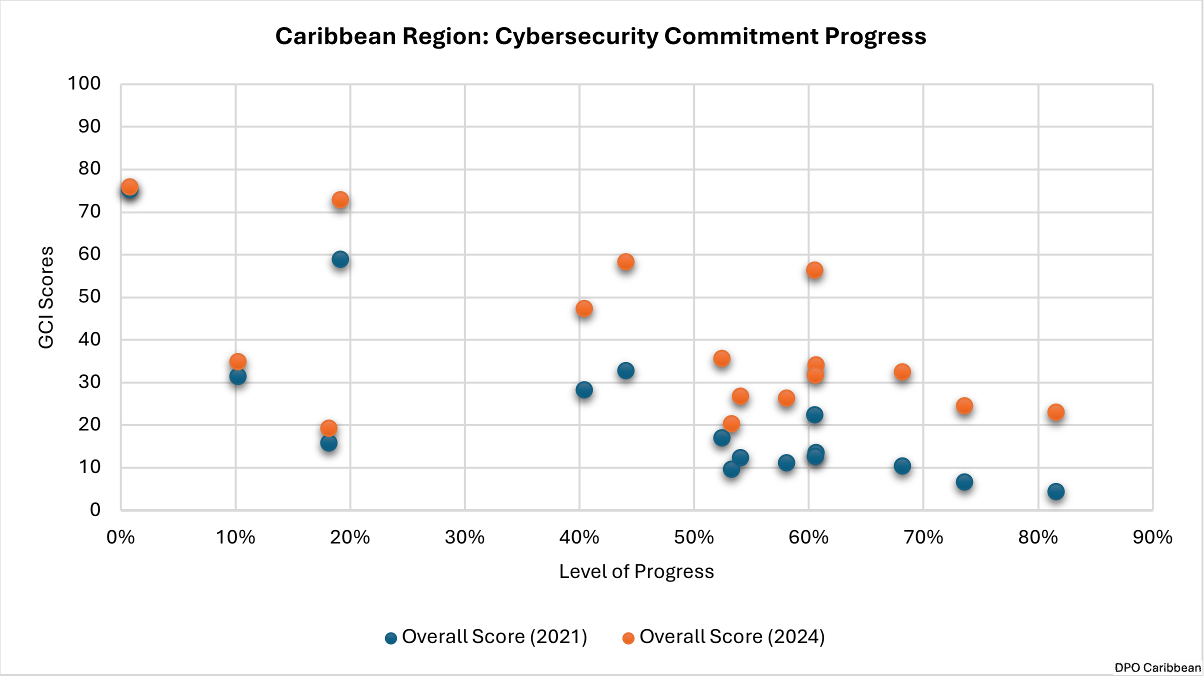
An Extended Analysis of Cybersecurity Commitment in the Caribbean

Countries in the Caribbean have shown substantial progress in cybersecurity commitment in 2024 compared to the previous GCI edition. The regional progress in adopting cybersecurity measures and government-led actions is noteworthy. However, the disparity among the countries is also evident.

The State of Cybersecurity Progress

Almost all countries experienced significant progress in cybersecurity commitment over the previous GCI edition. Figure 6 underlines that all countries experienced progress, however, most of the countries experienced over 50% increase in their GCI overall score over the previous edition.

Figure 6: Caribbean Region: Progress in Cybersecurity Commitment (GCI 2021 & 2024)



The change in GCI methodology may account for some aspects of the demonstrable progress, however, several countries have implemented notable cybersecurity initiatives during the reporting period (2021-2024), such as:

- **The development of cybercrime and cybersecurity laws**: Bermuda has revised its cybercrime law while Barbados' law is undergoing revision[9].

- **Party to Budapest Convention**: Grenada acceded to the Budapest Convention earlier this year (2024), the first from the English-speaking Caribbean, and follows the Dominican Republic that acceded in 2013. Since 2021, Trinidad and Tobago has been invited to accede[10].

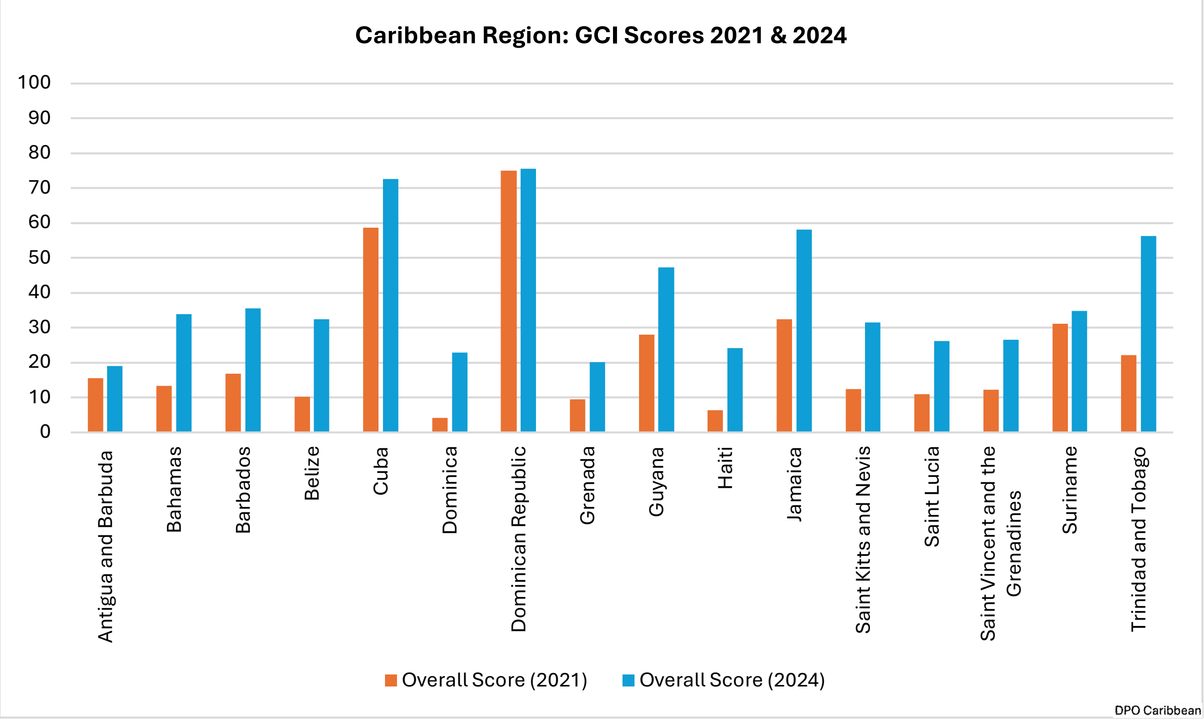
[9] A Report on Cybercrime Laws in the Caribbean, 2024, http://dx.doi.org/10.13140/RG.2.2.13491.85285

[10] https://www.coe.int/en/web/cybercrime/parties-observers

- **The development of data protection and privacy laws**: Several countries such as Barbados, Belize, Guyana and Jamaica have enacted modern data privacy laws that are largely modelled after the General Data Protection Regulation (GDPR)[11].

- **The establishment of national cybersecurity teams**: Bermuda is setting up its dedicated cybersecurity unit and incident response team[12].

Figure 7: Caribbean Region Overall Score (GCI 2021 & 2024)



Legal Measures

The legal pillar measures the adoption of certain legal frameworks concerning cybercrime and cybersecurity. These frameworks encompass conventional cybercrime legislative measures, including offences like illegal access, illegal interception, and online harassment. The legal measures also cover data protection and privacy laws, legal mechanisms for child online protection, and cybersecurity-related regulations

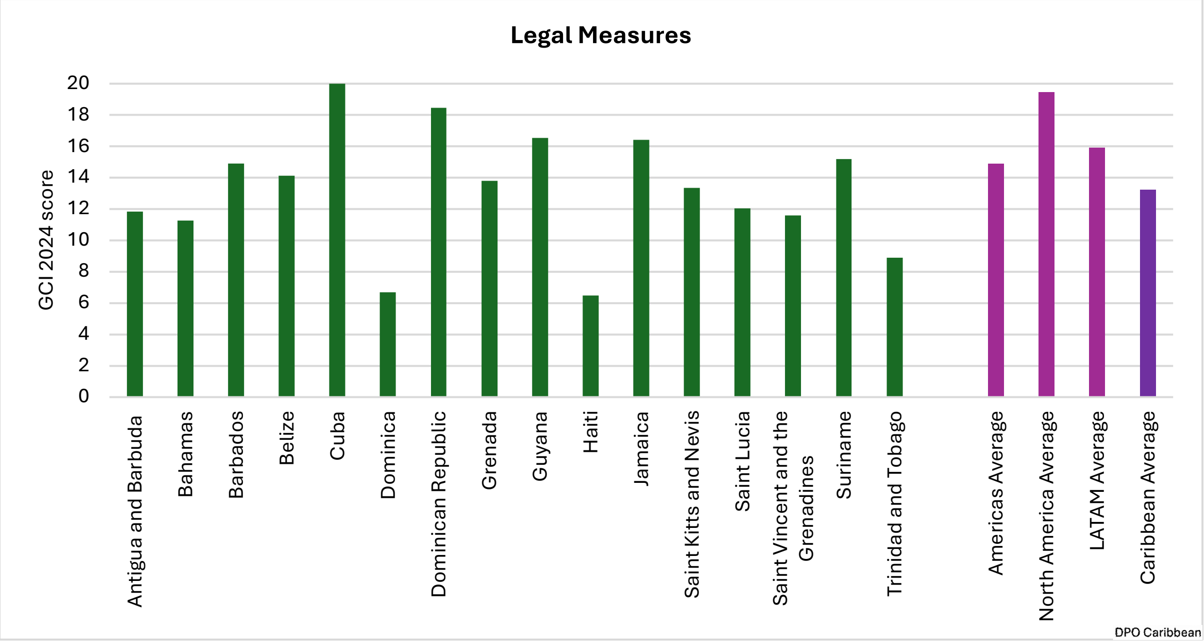
Several countries are above the regional averages concerning legal measures, namely Cuba and, the Dominican Republic.

Haiti, Dominica and Trinidad and Tobago on the other hand are positioned at the lowest levels. Factors attributing to this are that Dominica and Haiti do not appear to have any dedicated laws

[11] The State of Data Protection and Privacy Laws in the Caribbean, 2024, http://dx.doi.org/10.13140/RG.2.2.33510.19527/1
[12] https://www.gov.bm/articles/cybersecurity-0

that create offences relating to cybercrime while Trinidad and Tobago has only partially operationalised its data protection law while working to update its framework[13].

Figure 8: Legal Measures



Technical Measures

The technical pillar measures the existence of institutions, standards and frameworks addressing cybercrime and cybersecurity. This includes national capabilities for the management and governance of cybersecurity risks.

Significant opportunities exist to strengthen technical measures in the region. Many countries were unable to obtain a score in this pillar: Antigua and Barbuda, Belize, Dominica, Grenada, Haiti, Saint Lucia, and Saint Vincent and the Grenadines. This means nearly half of the countries in the region are unable to demonstrate any suitable technical measures for addressing cybercrime and cybersecurity, such as the presence of a national CIRT or national frameworks for the implementation of cybersecurity standards.

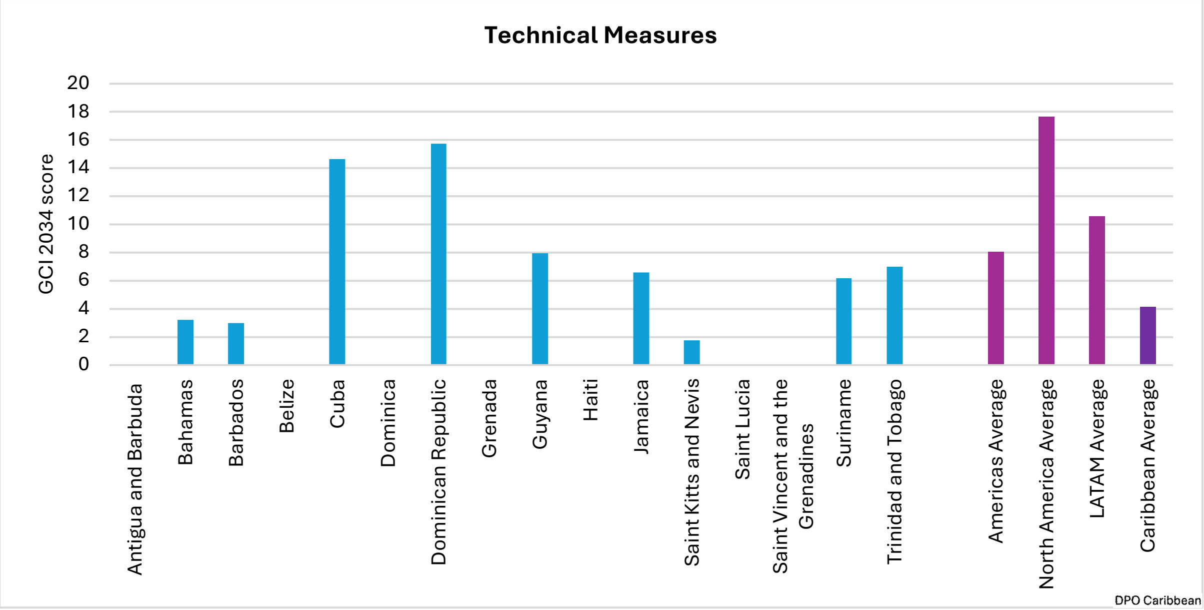
Countries with operational CIRTs, such as Dominican Republic (CSIRT-RD), Guyana (CSIRT.GY), Jamaica (Ja-CIRT), Suriname (SurCSIRT) and Trinidad and Tobago (TTCSIRT); many are still at the formative level, due to issues such as the cybersecurity skills gap, human resource availability and retention rates, and access to funding[14].

Another widespread challenge is the limited adoption of regulatory frameworks for the implementation of cybersecurity standards by government agencies and other entities, such as NIST Cybersecurity Framework (CSF), ISO 27001/2 or SOC 2 (Service Organisation Control 2).

[13] A Report on Cybercrime Laws in the Caribbean,2024, http://dx.doi.org/10.13140/RG.2.2.13491.85285
[14] https://dpocaribbean.com/dpo-updates/f/is-the-caribbean-community-committed-to-cybersecurity

These and other cybersecurity standards address diverse ranges and issues and have been shown to help demonstrate maturity and expertise in managing cybersecurity risks.

Figure 9: Technical Measures



Organisational Measures

The organisational pillar measures the adoption and implementation of lead agencies, as well as policies and strategies for cybercrime management and cybersecurity development at the national level. This includes the adoption of current good practices concerning the crafting and implementation of national policies and strategies development and the establishment of responsible agencies for cybersecurity as well as the development and adoption of appropriate cybersecurity metrics and child online protection initiatives.

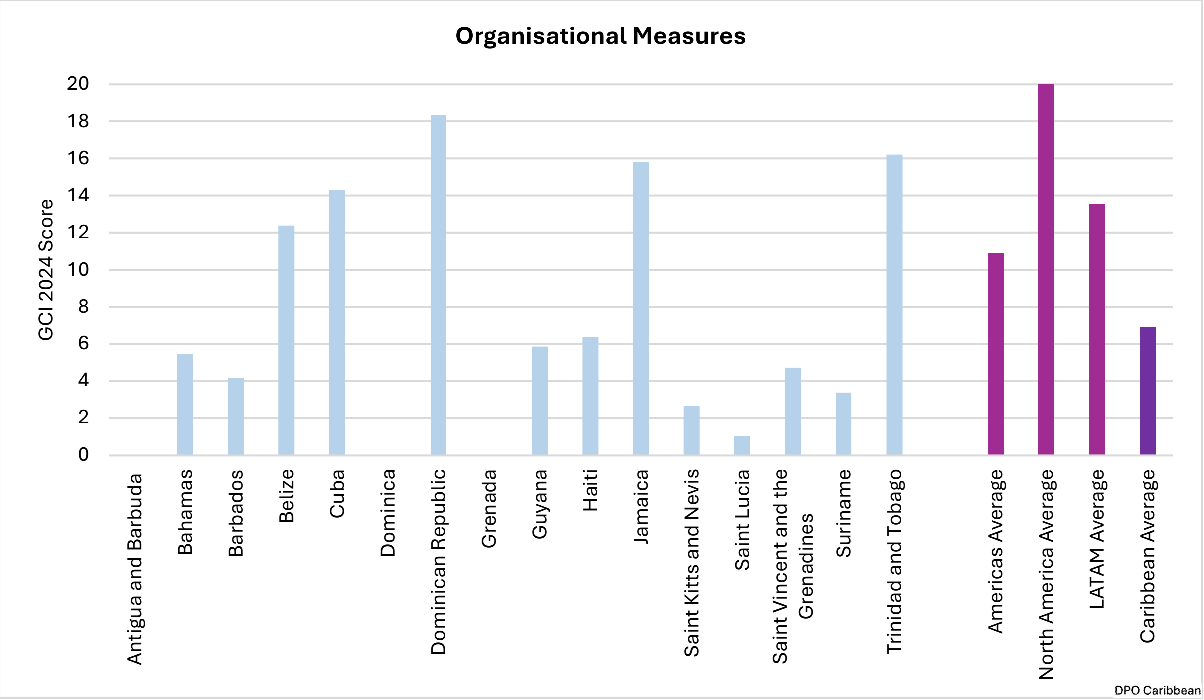
There is a wide disparity in countries' implementation of organisational measures. Top performers include the Dominican Republic, Jamaica, and Trinidad and Tobago. On the other hand, Antigua and Barbuda, Dominica, Grenada, Saint Lucia, and Suriname have demonstrated little or no formal mechanisms to support cybersecurity development.

The average score of the Caribbean is less than 8/20, which calls for stronger governance and formal mechanisms necessary to address cybersecurity in the region, which should include current and active NCSs that identify national cyber priorities and address how countries will respond to and manage the changing cyber threat landscape[15], among other relevant matters. Illustratively, key indicators from North America include systematic updates and revisions of national strategies relating to cybersecurity and the government empowering agencies with responsibility for cybersecurity through modern regulatory or legislative instruments. This

[15] Ibid

approach promotes improved transparency, as well as clear responsibilities and accountabilities among government agencies with distinct but related mandates.

Figure 10: Organisational Measures



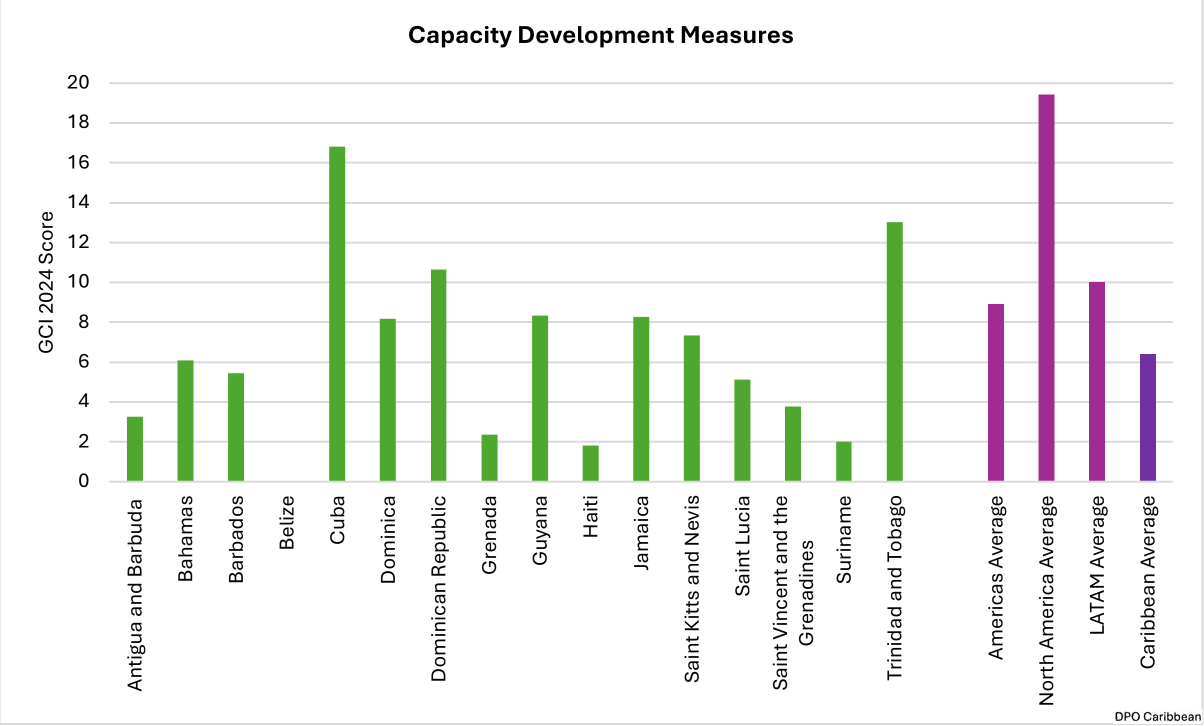
Capacity Development Measures

The capacity development pillar measures government-led actions relating to awareness, training, education and other forms of developing national capabilities in cybersecurity. These measures include specifically targeted campaigns for all segments of the population, including the vulnerable, marginalised, neurodiverse, and differently-abled citizens, as well as active support for training and education for diverse categories of professionals dealing with cybersecurity matters, active research and development, and strong government incentive mechanisms to foster growth and development in the cybersecurity ecosystem.

Cuba stands apart from the rest of the region regarding measures relating to capacity development, followed by Trinidad and Tobago. Several countries were unable to demonstrate any substantial capacity development measures, particularly Belize, Grenada, Haiti, and Suriname. The disparity among countries is also evident and suggests an urgency for more government-led actions and regional interventions to encourage good cyber hygiene practices and a vibrant cybersecurity industry.

Examples of measures adopted in North America include multiple forms of incentive programs to reduce cybersecurity risks and help foster strong national cybersecurity ecosystems such as the USA's State and Local Cybersecurity Grant Program (SLCGP)[16] and Canada's Cyber Security Innovation Network[17].

Figure 11: Capacity Development Measures



Cooperation Measures

The Cooperation pillar measures the existence of active partnerships, cooperation frameworks and information-sharing networks at the national, regional and global levels. This includes international agreements addressing cybersecurity, mutual legal assistance treaties and agreements, and collaborative partnerships between different entities.

Examples of active multilateral cooperation measures include the INTERPOL Cybercrime Capacity Building Project in the Americas[18] and the Council of Europe's Global Action on Cybercrime Project[19] which provides training, awareness initiatives and other forms of capacity development to countries in the Caribbean and Latin America.

The scores highlight significant opportunities to develop, strengthen and formalise regional partnerships. Public-private partnerships and bilateral agreements among countries in the

[16] https://www.cisa.gov/resources-tools/resources/state-and-local-cybersecurity-grant-program-fact-sheet#:~:text=In%20Fiscal%20Year%20(FY)%202024,%2C%20local%2C%20and%20territorial%20governments

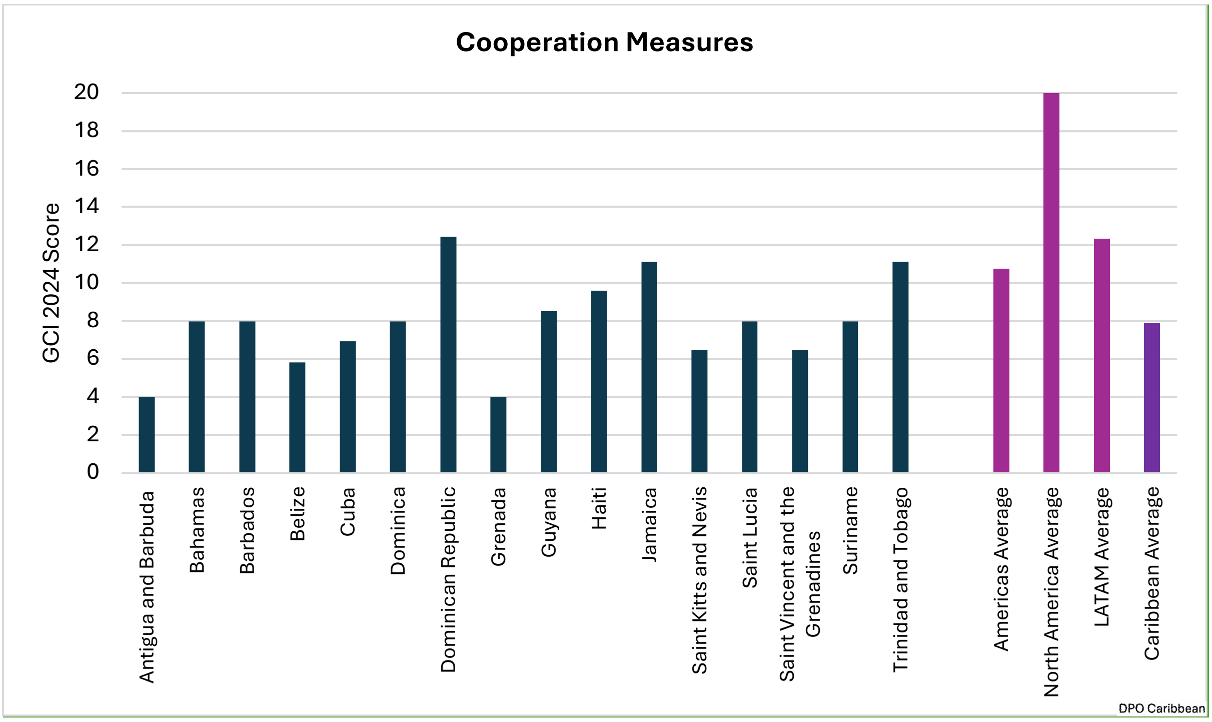
[17] https://ised-isde.canada.ca/site/cyber-security-innovation-network/en

[18] https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Cybercrime-Capacity-Building-in-the-Americas

[19] https://www.coe.int/en/web/cybercrime/-/glacy-interpol-heads-of-police-cybercrime-units-and-prosecutors-from-24-countries-in-latin-americas-and-the-caribbean-met-in-santo-domingo-to-discuss-strategies-for-tackling-the-rising-challenge-of-cybercrime

region are potential avenues for countries to better leverage and support real-time intelligence sharing, development initiatives, and good practices. In addition, the opportunity exists for regional agencies, such as the Caribbean Community (CARICOM) to enrich its cybersecurity leadership in the region.

Figure 12: Cooperation Measures



Role-Modelling Cybersecurity Commitment

The perspective of *role-modelling* is adapted to consider not only countries within that tier but also the identification of specific measures adopted by other countries and regions to help reduce cybersecurity risks and better manage cybersecurity. This perspective can provide relatable measures and may serve as a model for countries in the Caribbean.

Some key role-modelling activities include:

- **Workforce development**: Developing and adopting cybersecurity curricula at the primary, secondary and tertiary levels.

- **Cyber governance and accountability**: Increased systematic and transparent monitoring and updates of NCSs and action plans to improve governance and accountability while taking into account the changing cybersecurity risks, national circumstances and responses.

- **Digital identity protection**: Establishing and adopting digital identity legal frameworks that address the verification of the identity of individuals and businesses as well as the authenticity of electronic documents.

- **Cyber legislative framework**: Keeping pace with the evolving cybersecurity legislative framework through the implementation of diverse laws and regulations to include not only cybercrimes or digital evidence but also matters relating to critical infrastructure protection, national resilience, standards development, and responsible artificial intelligence (AI) deployment and use, other innovations, among other related issues, etc.

- **Child online protection**: Creating and managing 24/7 helplines to support child protection issues, including online safety.

- **Cybersecurity drills and training**: Leading and actively participating in cybersecurity drills, on a regular basis, that address countries and organisations' ability to effectively manage cybersecurity issues, assess resilience, and develop capabilities.

- **Inclusive cybersecurity awareness**: Utilising modern tools and services to ensure that the vulnerable, neurodiverse or differently abled citizens are granted access to cybersecurity, continuously educated on cybersecurity threats, and are represented in targeted campaign strategies.

- **Incident response**: Developing and participating in the cybersecurity incident response and management ecosystem through diverse institutional frameworks such as regional CIRT networks, sectoral CIRTs, security operation centres (SOCs) and information sharing and analysis centres (ISACs).

- **Public-private partnerships**: Developing and implementing regulatory frameworks for Public-Private Partnerships (PPPs).

- **Research and development**: Creating and adopting legal and policy frameworks to support or incentivise research and development in cybersecurity.

- **Standards and frameworks**: Developing and implementing cybersecurity standards and frameworks concerning the cybersecurity body of knowledge and processes of cybersecurity management.

- **International cooperation**: Signing and acceding to diverse international conventions and treaties relating to topics such as cybercrime, child protection, transnational crime and mutual legal assistance.

- **Strategic policy design and implementation**: Applying the GCI country findings to inform domestic strategic policy directives concerning cybersecurity.

Policy Directions for the Caribbean Region

Over the last five years, the region has experienced a surge in cyberattacks and cybercrime. It is estimated that ransomware attacks account for nearly 30% of reported cyber incidents in the region[20]. Other top regional cybercrimes and threats comprise phishing attacks, malware, insider threats, card frauds, online scams, and business email compromises[21]. A whole-of-society approach is therefore needed to systematically and sustainably address these evolving risks, protect digital infrastructure and data, safeguard citizens, and improve national security and resilience. To achieve these cybersecurity imperatives, countries in the region must actively demonstrate leadership in cybersecurity and not view cybersecurity as a secondary concern or merely a buzz topic discussed during Cybersecurity Awareness Month.

Based on earlier recommendations[22], several policy directions are proposed:

Theme 1: Inclusive Public Awareness and Education

- **Design Inclusive Campaigns**: Develop public awareness and education campaigns that reach all segments of society, including vulnerable, marginalised, and gender-based groups. Responsible agencies should also use accessible language, tools, techniques, and culturally relevant examples to educate citizens about cybersecurity risks and good practices.

Theme 2: Comprehensive Capacity Building, Innovation and Research

- **Integrate Cybersecurity into Education Systems**: Governments must invest in cybersecurity education at all levels. It is also essential to integrate cybersecurity curricula into primary, secondary, and tertiary education, provide training and support for educators, and develop specialised programs to create a skilled workforce capable of addressing cyber threats.

- **Foster Cybersecurity Research and Innovation**: Prioritise cybersecurity research and development investments by establishing dedicated research centres and funding academic research programs and projects addressing domestic and regional issues.

Theme 3: Adaptive Policy and Legislation

- **Modernise Legal and Regulatory Frameworks**: Continuously update policies, laws and regulations to address evolving cybersecurity and digital risks and promote trust and security. This includes cybercrime legislation and other laws, standards and frameworks concerning cybersecurity, data protection, privacy, AI, digital identity, and emerging technologies.

- **Develop Comprehensive Strategies**: Develop, monitor, and update national cybersecurity strategies regularly. These should reflect the country's experiences, vision, and goals, with clear accountability, sound governance structures, and a sustaining budget.

[20] https://www.coe.int/en/web/cybercrime/-/glacy-interpol-heads-of-police-cybercrime-units-and-prosecutors-from-24-countries-in-latin-americas-and-the-caribbean-met-in-santo-domingo-to-discuss-strategies-for-tackling-the-rising-challenge-of-cybercrime

[21] https://dpocaribbean.com/dpo-updates/f/top-cybersecurity-threats-in-the-caribbean

[22] https://dpocaribbean.com/dpo-updates/f/is-the-caribbean-community-committed-to-cybersecurity

- **Strengthen Enforcement**: Rigorously enforce laws to build confidence in national legal and investigative frameworks.

- **Foster Good Governance and Accountability**: Establish mechanisms and institutional arrangements for regular review, monitoring, and updating of cybersecurity practices, policies, and frameworks. Mandates should include conducting audits and vulnerability assessments, research and development, and ensuring transparent reporting on cybersecurity efforts.

Theme 4: Holistic Risk and Capabilities Management

- **Develop Threat Management Capabilities:** Improve incident response and management capabilities by establishing and developing national and sector-specific CIRTs, SOCs, and information sharing platforms, plus designing and leading cybersecurity drills addressing top global and domestic issues, threats and risks.

- **Enhance Critical Infrastructure Protection**: Invest in technologies and practices that bolster the resilience of critical infrastructure, including financial systems, healthcare, utilities, government services, and telecommunications. This should include conducting regular risk assessments and implementing comprehensive incident response and continuity plans.

Theme 5: Active Networks and Partnerships

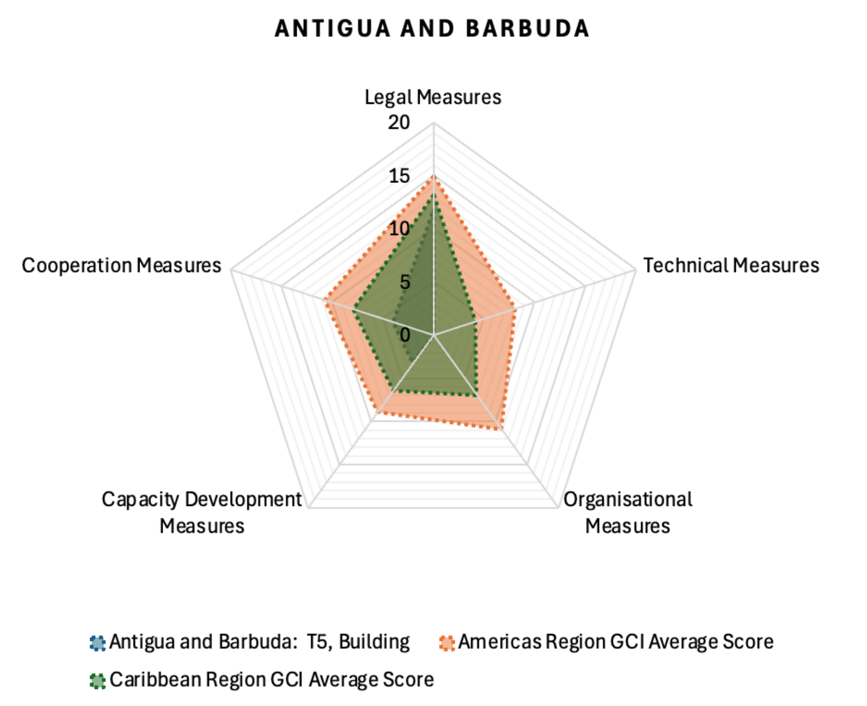
- **Encourage Local and Regional Collaboration**: Build local and regional networks for information sharing, capacity building, and collaboration. Encourage partnerships between the public and private sectors and with regional countries to facilitate the exchange of threat intelligence, scientific data, and best practices.

- **Leverage Private Sector Expertise**: Create frameworks that encourage collaboration between government agencies and private companies. This may be manifested through joint initiatives for cybersecurity training, threat intelligence sharing, and developing innovative cybersecurity solutions that drive development and enhance national capabilities.

Caribbean Country Performance

The analysis assesses each country's GCI score with the average scores in the Americas and the Caribbean. The country performance analysis is designed to help inform government policies by identifying the relative advantage of each country and recommending priority actions across cybersecurity pillars to enhance commitments to cybersecurity.

Antigua and Barbuda



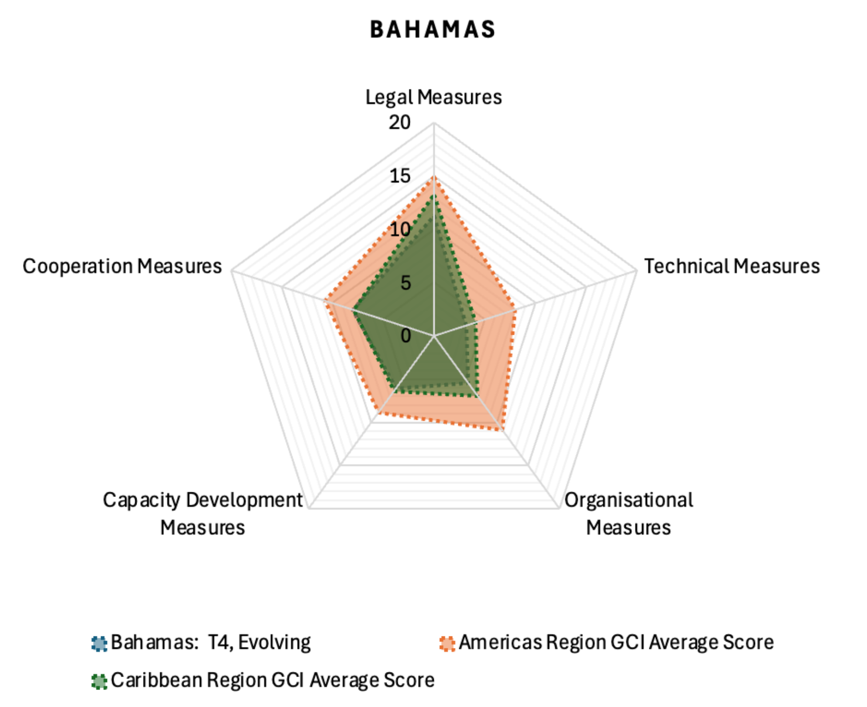
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Bahamas



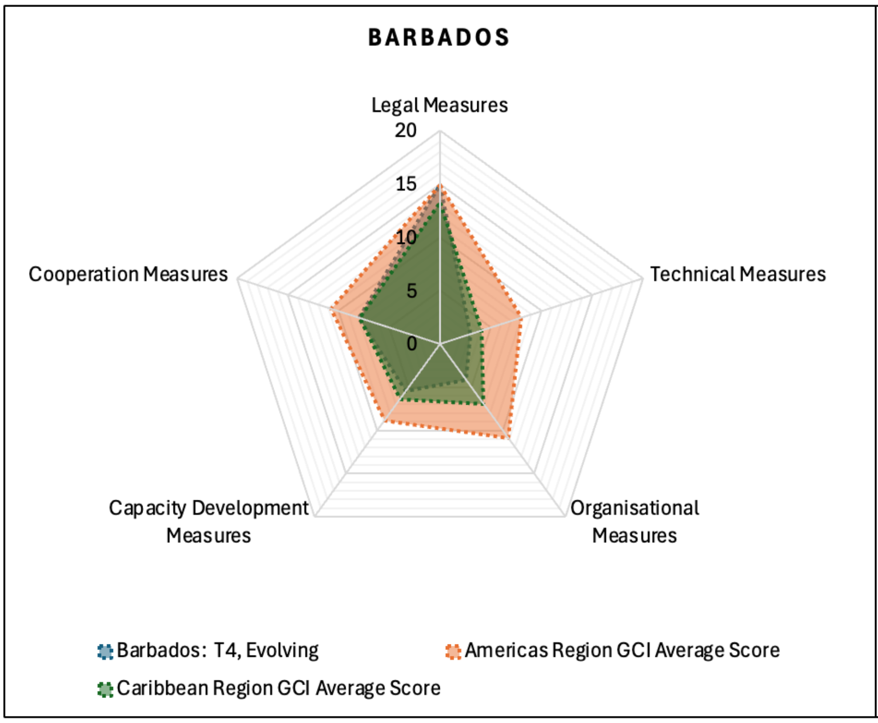
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Barbados



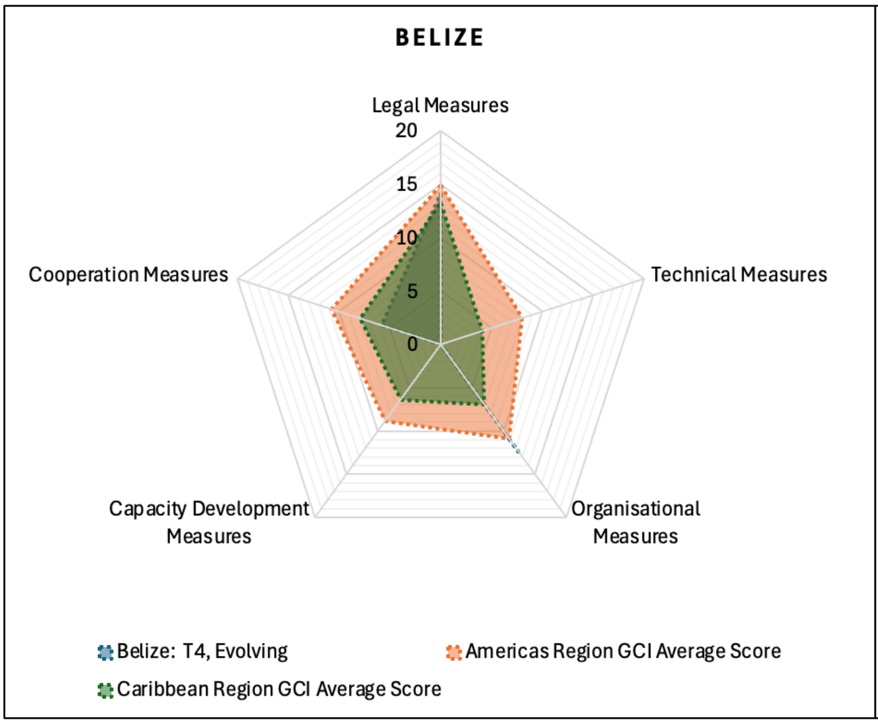
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Belize



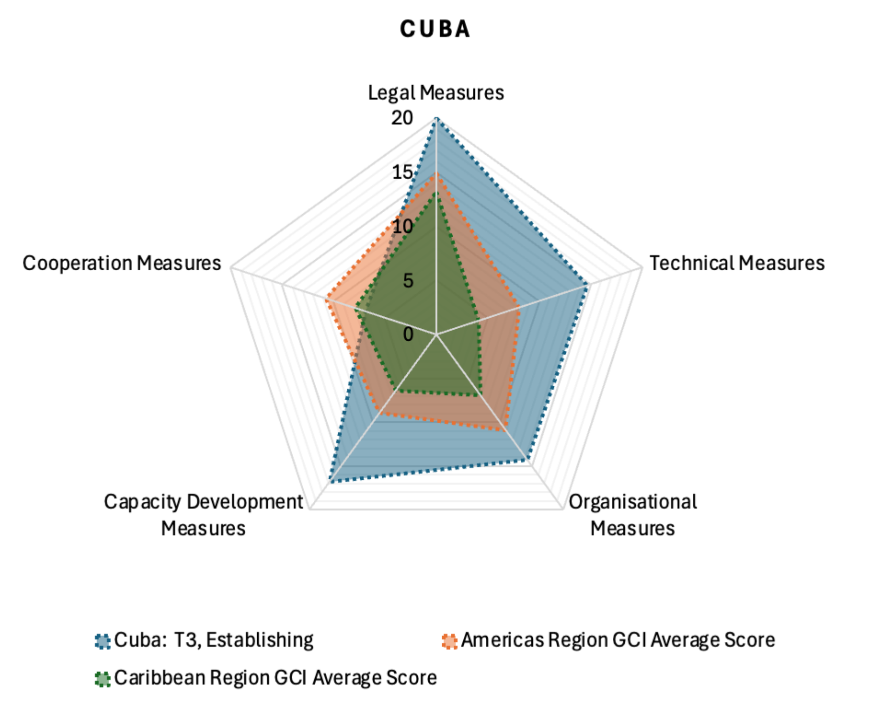
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Cuba



GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas

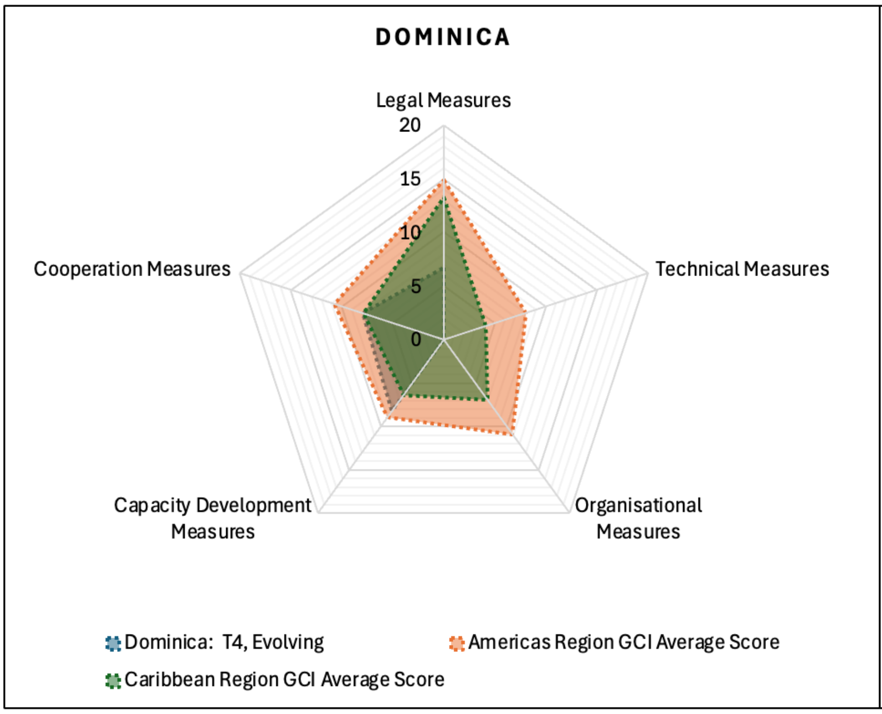
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures

Area(s) for Priority Actions

Cooperation Measures

DPO Caribbean

Dominica



GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas

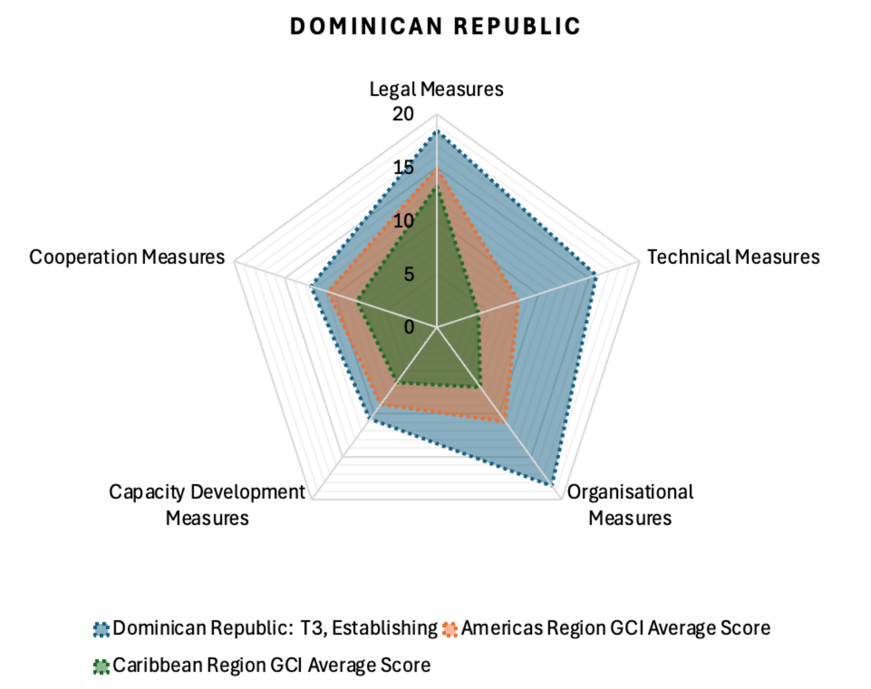
None

Area(s) for Priority Actions

Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Dominica Republic



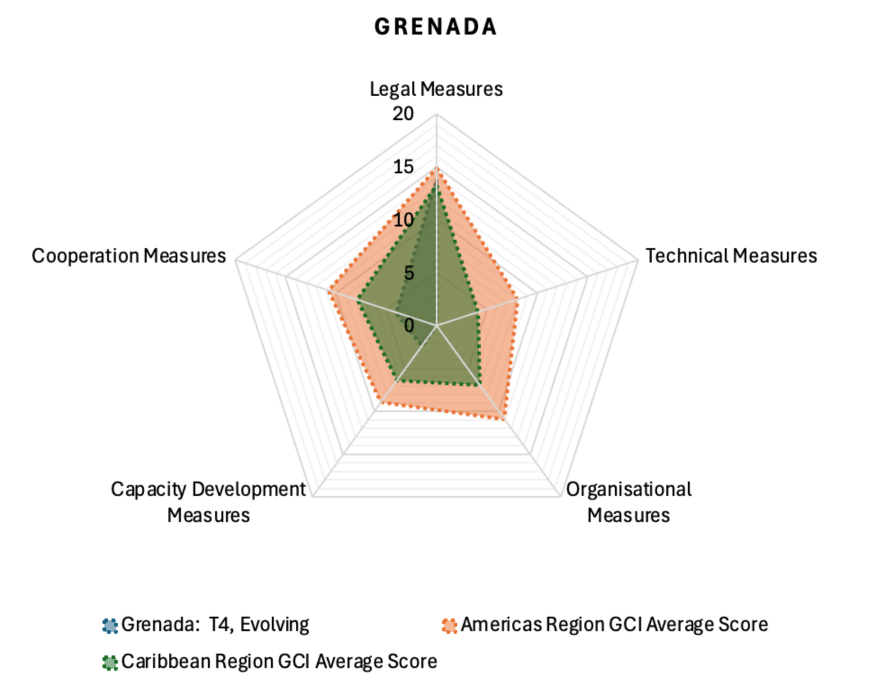
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Actions
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Grenada



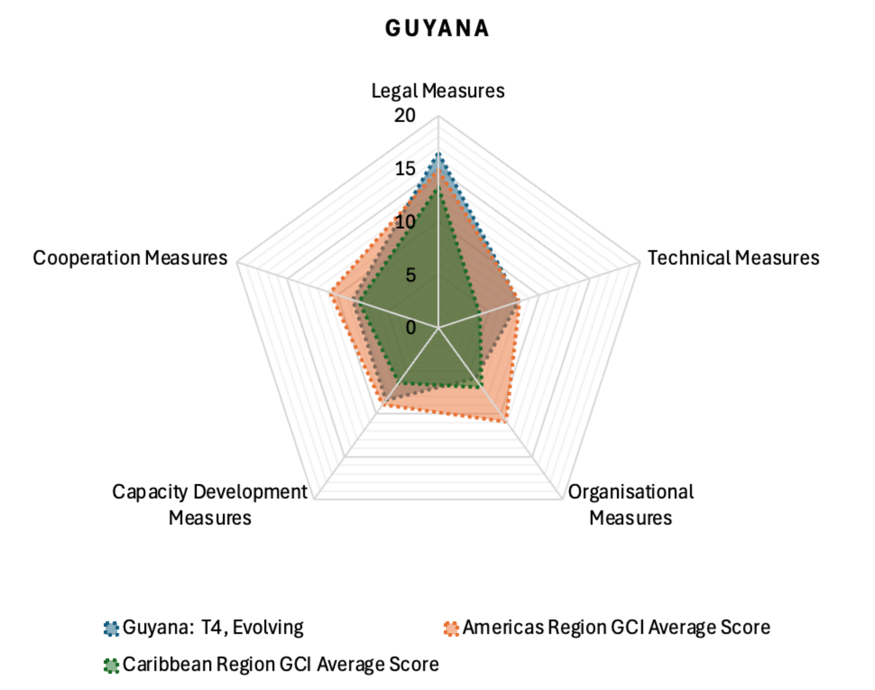
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Guyana



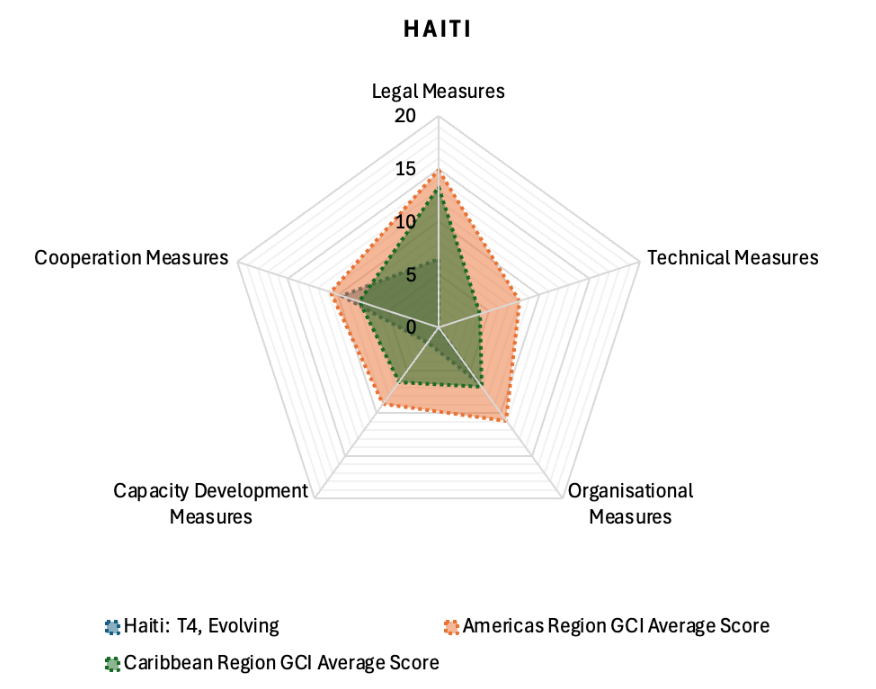
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
Legal Measures

Area(s) for Priority Actions
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Haiti



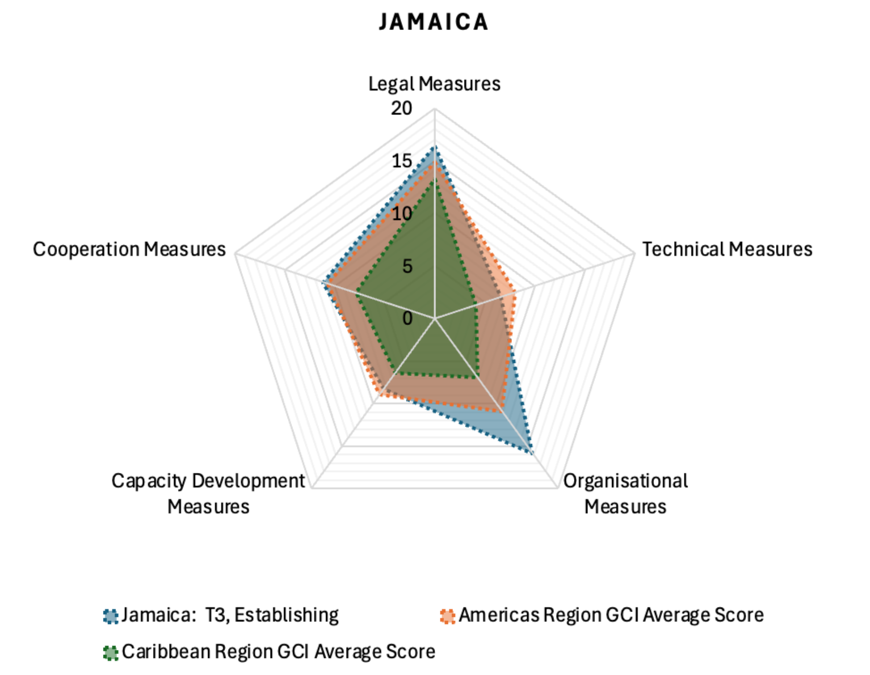
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Jamaica



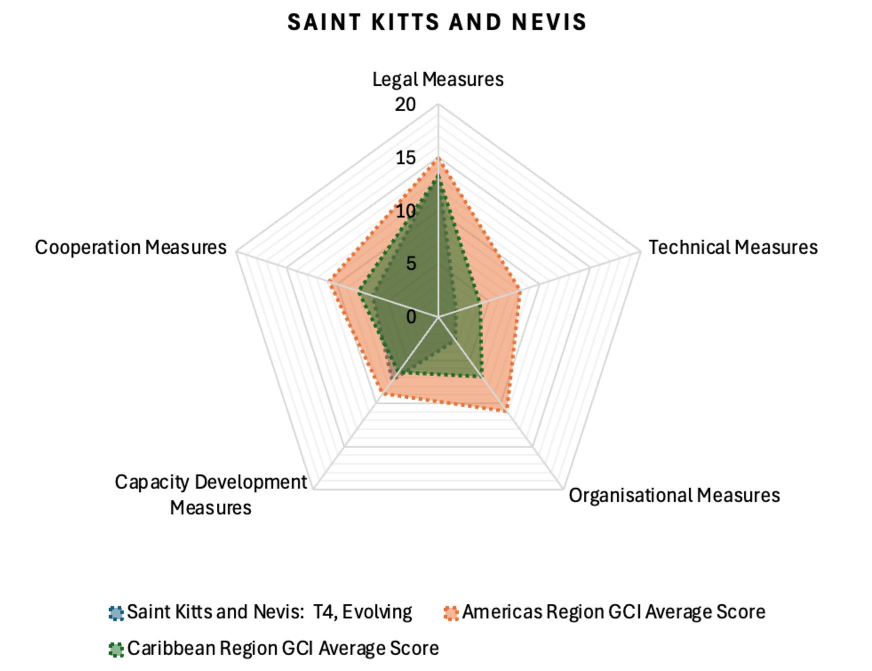
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
Legal Measures
Organisational Measures

Area(s) for Priority Actions
Technical Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Saint Kitts and Nevis



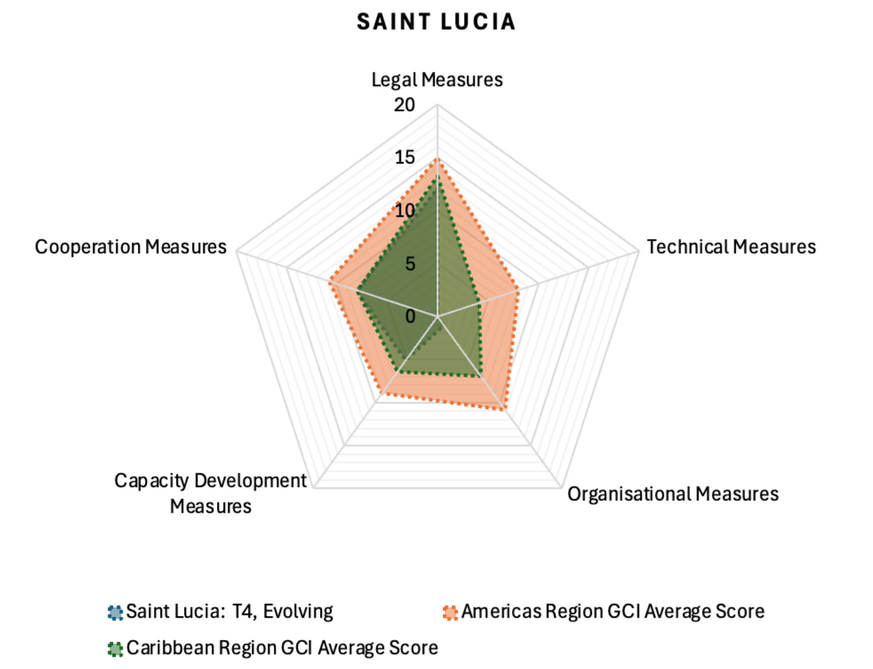
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Saint Lucia



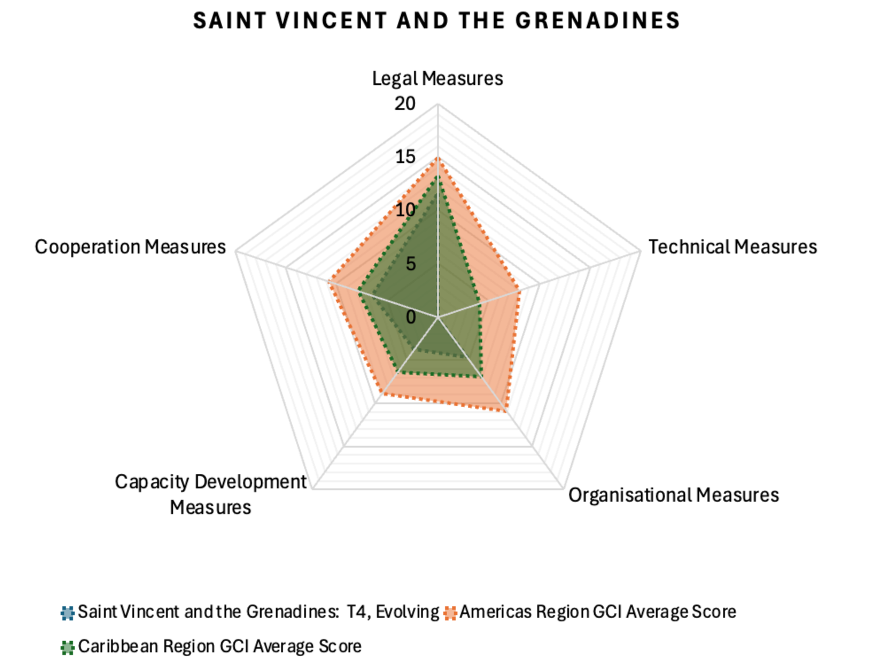
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Saint Vincent and the Grenadines



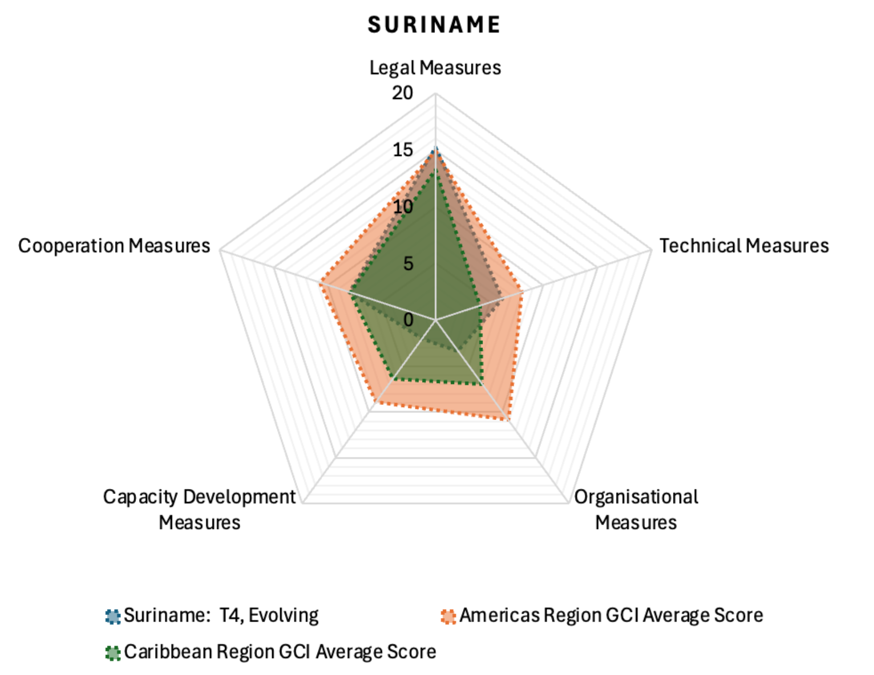
GCI 2024
CARIBBEAN REGIONAL
CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas
None

Area(s) for Priority Actions
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Suriname



GCI 2024

CARIBBEAN REGIONAL

CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas

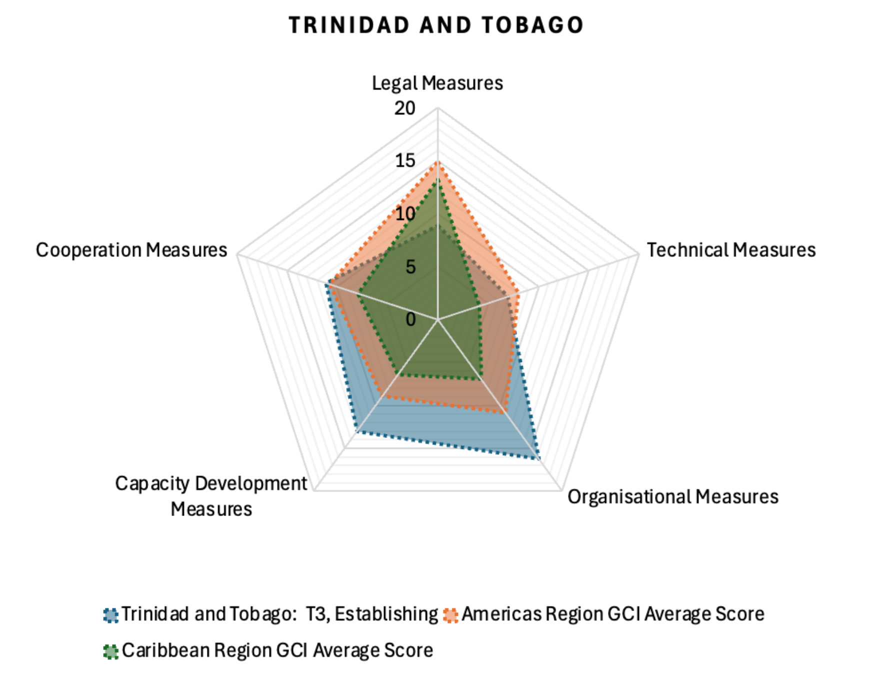
None

Area(s) for Priority Actions

Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DPO Caribbean

Trinidad and Tobago



GCI 2024

CARIBBEAN REGIONAL

CYBERSECURITY COMMITMENT OUTLOOK

Pillar(s) of Relative Strength in the Americas

Organisational Measures
Capacity Development Measures

Area(s) for Priority Actions

Legal Measures
Technical Measures
Cooperation Measures

DPO Caribbean

Conclusion

The Report focuses on the GCI performance of the Americas region, with particular emphasis on the Caribbean. It delves into the GCI 2024 data to provide a comprehensive analysis and insights into the following areas:

- **GCI Tier Performance and Ranking**: It presents the tier performance and rankings of 35 countries in the Americas, segmented into sub-regions of North America, Latin America, and the Caribbean.
- **Cybersecurity Commitment Analysis**: It provides an extended analysis of the GCI performance of Caribbean countries, highlighting growth between the current and previous editions.
- **Cybersecurity Pillar Assessment**: It examines the GCI performance of countries in the Americas across the five cybersecurity pillars supported by sub-regional observations.
- **Good Cybersecurity Practices**: It identifies global practices that the Caribbean and other regions can model to enhance the effectiveness of their cybersecurity measures.
- **Country Performance Benchmarking**: It outlines country performance in relation to the Americas and Caribbean regional levels and recommends priority actions.
- **Policy Directions for the Caribbean**: It devises strategic policy directives tailored for the Caribbean region to manage risks and bolster the cybersecurity commitment of countries.

The analysis highlights that while Caribbean countries have made strides in their cybersecurity efforts, notable gaps remain. The smaller islands, in particular, have the largest gaps and are even more vulnerable to economic, climatic and cybersecurity risks. This situation presents a crucial opportunity for enhanced intervention by regional agencies and increased government-led initiatives across all cybersecurity pillars. The Report therefore provides regional and national policymakers and stakeholders with actionable insights, which, when combined with the GCI 2024 Report, can guide the determining of priority actions for managing and governing both national and regional cybersecurity and its associated risks. The Report particularly emphasises areas for priority action within Caribbean countries, considering the broader context of the Americas region. While countries need to recognise their national cybersecurity advantages, it is even more beneficial to benchmark against other countries, especially those within the same region or those with similar economic, social, or political contexts. The comparative analysis undertaken in this Report can aid Caribbean nations in refining their national cybersecurity plans and strategies. While resource access and availability undeniably influence the prioritisation of cybersecurity measures, especially in the Caribbean, governments should be able to learn from others and adopt creative and frugal innovative approaches, when necessary, to address systemic cybersecurity risks while carefully considering how they can improve their commitment to cybersecurity and elevate their capacities and capabilities to the next level.

DPO Caribbean
20 West Kings House Road
Kingston 10
Jamaica WI

ISBN 978-976-97440-0-4

9 789769 744004