GSMA

Cybersecurity in Small Island Developing States (SIDS)

Caribbean-Specific Risks and Strategic Imperatives

Whitepaper

August
2026

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

Contents

1. Executive Summary

The Caribbean region is undergoing rapid digital transformation driven by expanding mobile broadband coverage, increasing smartphone adoption, digital government initiatives, and the growing centrality of digital platforms to economic activity. Mobile networks now underpin essential services across government, finance, energy, health, transport, and tourism. At the same time, this transformation has materially increased exposure to cyber threats.

For Small Island Developing States (SIDS), these risks are amplified by structural constraints, including small market size, limited fiscal and human capital resources, geographic fragmentation, and high exposure to natural disasters. For example, ransomware attacks have affected telecommunications providers, government agencies, and major retailers, including the Caribbean's largest recorded data breach in 2022, which exposed over 700,000 customer and employee records.

Within this context, digital transformation has become not only a development imperative but a defining element of national resilience for SIDS, including many Caribbean nations that are increasingly pursuing digitalization as a central pillar of resilience and development. This digital expansion, while promising significant social and economic benefits, has elevated cybersecurity to a strategic priority, yet many states lack comprehensive national cybersecurity frameworks. Embedding security into digital infrastructure is critical to safeguarding public services, data, and trust.

According to the World Economic Forum, cybersecurity is "quickly becoming a top priority" for SIDS as digital ecosystems expand, with international collaboration highlighted as key to building secure and resilient digital environments. However, the majority (60%) of Least Developed Country SIDS have yet to establish national cybersecurity strategies, underscoring urgent policy gaps.

Initiatives such as the Caribbean Digital Support Facility and joint UNDP–ITU cybersecurity programs illustrate emerging multilevel approaches to strengthening cyber resilience across SIDS. Regional cooperation plays a critical role in pooling technical expertise, optimizing limited resources, and advancing greater alignment of cybersecurity standards and practices.

This GSMA white paper examines cybersecurity in Caribbean SIDS through an operator-centric and evidence-based lens. It argues that cybersecurity is no longer a discrete technical concern, but a foundational requirement for digital resilience, economic stability, and public trust. Drawing on Caribbean-specific evidence, regional policy frameworks, and global best practice, the paper highlights why conventional cybersecurity models designed for large economies are insufficient for SIDS contexts.

Instead, cybersecurity in the Caribbean must be treated as a regional public good, supported by collective action, policy harmonization, shared infrastructure, and sustained investment in human capital.

Mobile Network Operators (MNOs) occupy a dual role in this ecosystem. They are both critical national infrastructure operators responsible for network security and continuity, and key enablers of digital inclusion, disaster response, and economic development. Strengthening cybersecurity across mobile networks, therefore, delivers system-wide benefits that extend well beyond the telecommunications sector.

The paper reviews the regional cyber threat environment, assesses current governance and capacity gaps, analyses the economic and infrastructure dimensions of cyber risk, and outlines strategic imperatives for Caribbean SIDS. It situates existing regional initiatives, including the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP), within a broader resilience framework and identifies priority actions for governments, regulators, operators, and regional institutions.

2. Introduction

Digital connectivity has become a central driver of economic and social development across the Caribbean. Mobile networks provide the primary means of internet access for most of the population, with mobile penetration exceeding 100 per cent in most Caribbean markets according to GSMA Intelligence, reflecting widespread multiple-SIM ownership, and mobile broadband accounting for more than two-thirds of internet connections in several SIDS. Governments increasingly rely on digital platforms for public service delivery, including digital identity systems, tax administration, customs processing, and social protection services, many of which are accessed primarily via mobile devices. In Jamaica, national digital government initiatives and online public services depend on secure mobile connectivity to reach citizens at scale, while Barbados has expanded the use of digital platforms across licensing, regulatory, and public administration functions.

Private sector growth across the region is similarly dependent on secure and reliable connectivity. In tourism-dependent economies such as the Bahamas and Saint Lucia, where tourism can account for more than half of total economic activity when direct and indirect effects are combined, digital systems underpin reservations, payments, border management, port operations, and logistics coordination. Financial services, energy, transport, and small and medium-sized enterprises increasingly rely on mobile-enabled applications and cloud-based platforms to support daily operations, reinforcing the importance of cybersecurity as a foundation for economic continuity and consumer trust.

At the same time, the Caribbean faces a rapidly evolving cyber threat landscape. Cyber incidents affecting government systems, financial institutions, utilities, and telecommunications providers have increased in frequency and sophistication, mirroring global trends. Ransomware, phishing, and social engineering attacks now account for a significant share of reported cyber incidents worldwide, and Caribbean public sector institutions and financial services providers reflect this exposure. Despite growing digital reliance, an estimated 60 per cent of Least Developed Country SIDS have yet to adopt a formal national cybersecurity strategy, and regional assessments consistently place Caribbean states below the global average in cybersecurity maturity. In small island contexts, where essential services are tightly interconnected and institutional redundancy is limited, cyber incidents can have systemic effects, disrupting service delivery, economic activity, and public confidence.

Caribbean states operate under structural conditions that differ fundamentally from those of larger economies. Small population size limits economies of scale in cybersecurity investment and constrains access to specialized technical expertise.

In many Caribbean SIDS, national cybersecurity functions are delivered by small teams, often fewer than 10 specialized staff, limiting the capacity to sustain continuous monitoring, incident response, and skills development. Heavy reliance on externally owned digital infrastructure, including cloud services, submarine cables, and satellite connectivity, further complicates governance, oversight, and cross-border incident response.

These challenges are compounded by high exposure to natural hazards. The Caribbean experiences multiple major hurricanes each year, and climate change is increasing the frequency and severity of extreme weather events. Hurricanes affecting states such as Dominica and Antigua and Barbuda have demonstrated how physical damage to power and telecommunications infrastructure can coincide with periods of heightened cyber vulnerability during emergency response and recovery. As mobile networks often serve as the primary communications backbone during disasters, disruptions to digital infrastructure, whether physical or cyber, can have cascading national and regional impacts. In this context, cybersecurity and physical resilience are deeply interconnected and central to the Caribbean's digital future.

3. Structural Cyber Vulnerabilities in Caribbean SIDS

Scale, Capacity, and Resource Constraints

Caribbean SIDS operate under persistent scale and capacity constraints that shape both public-sector cybersecurity governance and private-sector investment decisions. Public budgets are limited, and competition for specialized technical personnel is acute. Globally, demand for cybersecurity professionals outstrips supply by an estimated 3 million unfilled positions, and this gap is often more pronounced in smaller states. National cybersecurity functions in many Caribbean states are delivered by small units, typically fewer than 10 dedicated staff, embedded within ministries responsible for ICT, national security, or public administration.

These teams are often responsible for simultaneously developing strategy, coordinating incidents, managing Cybersecurity Awareness Programs, and managing international partnerships, while operating with annual cybersecurity budget shares well below 1% of total ICT expenditure. This concentration of responsibility increases systemic risk and constrains the ability to maintain continuous monitoring, conduct regular risk assessments, or respond rapidly to incidents outside normal working hours.

Even in larger markets such as Jamaica and Trinidad and Tobago, where institutional capacity is stronger, retaining specialized staff remains challenging because demand for cybersecurity talent in financial services and international markets often offers higher compensation. Operators face similar pressures: in Caribbean mobile markets with average revenue per user (ARPU) below the global average, justifying advanced investments in security operations centers or dedicated threat intelligence functions on a country-by-country basis can be challenging.

These realities underscore the importance of regulatory clarity, pooled capacity building, and regional shared services, such as coordinated threat intelligence hubs or joint training programs, to enable both public authorities and operators to invest in resilience without undermining cost competitiveness.

Dependence on External Digital Infrastructure

Caribbean digital ecosystems rely heavily on externally owned and operated infrastructure. According to GSMA data, over 80% of enterprise application workloads used by Caribbean public agencies and SMEs are hosted on global cloud platforms, and key services such as identity registries, customs clearance systems, and social service portals are often deployed on infrastructure physically located outside national jurisdictions. While these services enable rapid deployment and scalability, the World Bank reports that cloud adoption in the SIDS region has grown at a compound annual growth rate exceeding 25%. They also introduce dependencies that complicate cybersecurity governance and incident response.

Submarine cable infrastructure further illustrates this dynamic. Caribbean connectivity depends on a limited number of fiber optic systems shared across multiple markets; an outage on a major cable can affect connectivity for hundreds of thousands of users simultaneously. Smaller island economies typically do not hold equity stakes in these assets, which are operated by international consortia, constraining their ability to influence security practices or prioritization during outages. In island states such as the Bahamas, operators also rely on satellite and microwave backhaul to connect remote islands, so approximately 15–25% of total traffic in some areas traverses non-terrestrial links at any given time.

Mobile networks sit at the intersection of these dependencies, integrating terrestrial fiber, submarine cables, satellite backhaul, data centers, and cloud-native network functions into a single ecosystem.

As a result, cyber risks affecting one layer, whether in software supply chains or undersea systems, can cascade across sectors and services, amplifying impacts on everything from emergency communications to financial transactions.

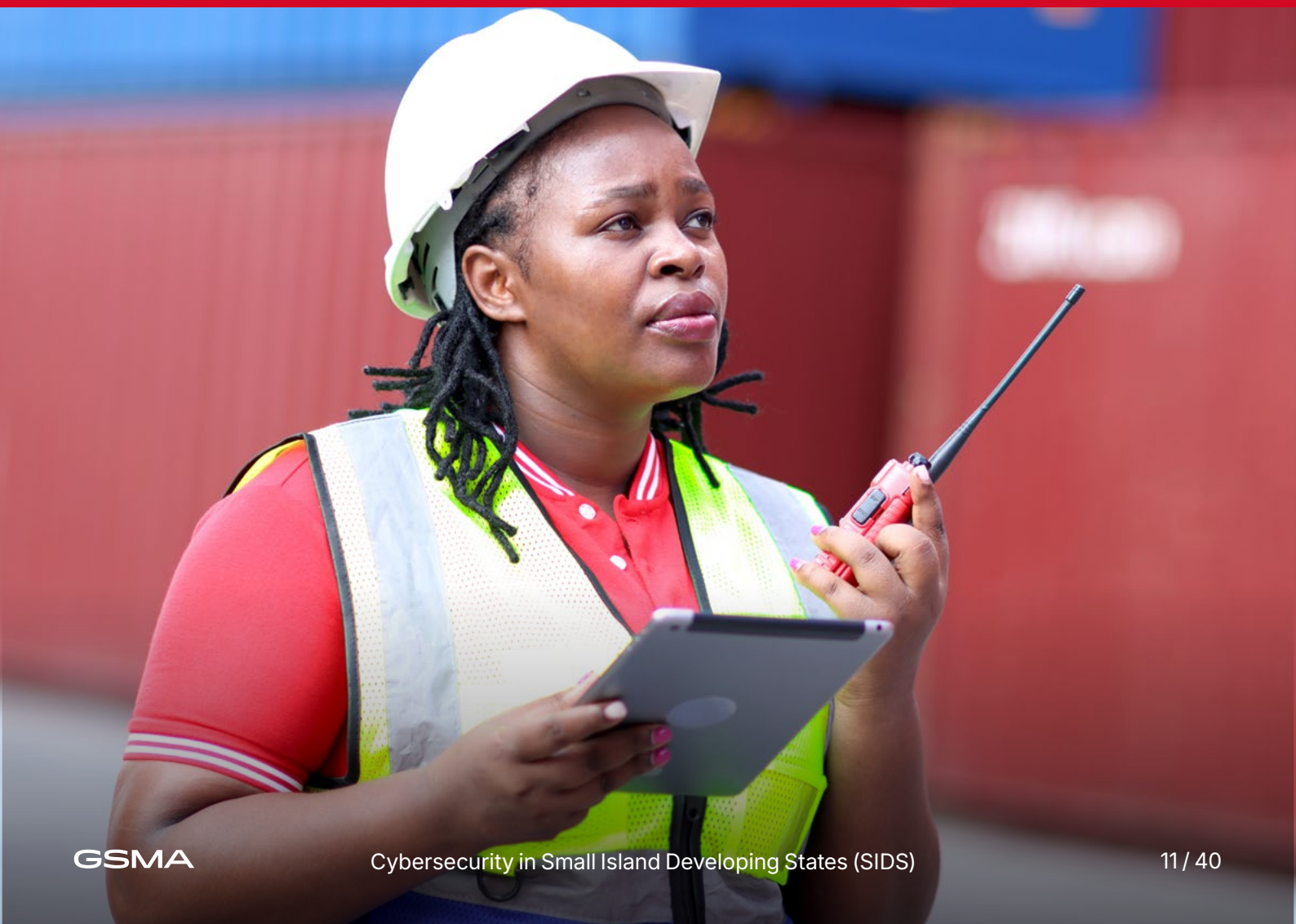
Exposure to Transnational Threats

The Caribbean's openness and integration into global digital markets increase exposure to transnational cyber threats. Regional financial services sectors, which collectively support millions of retail and business accounts, are frequently targeted by volume-driven phishing campaigns. According to the European Union Agency for Cybersecurity(ENISA), more than 90% of data breaches begin with phishing or social engineering. Caribbean institutions, with limited internal threat-hunting capacity, can be attractive targets for opportunistic actors seeking to exploit credential theft as an entry point into larger networks.

Threat actors often operate across jurisdictions, exploiting regulatory fragmentation and uneven enforcement capacity. World Bank estimates show that 60% of Least Developed Country SIDS have not yet adopted formal national cybersecurity strategies, and many lack published cybercrime laws aligned with international frameworks. This creates gaps in legal authority for cross-border investigations and mutually supportive enforcement. Smaller states such as Dominica and Saint Vincent and the Grenadines may depend on mutual legal assistance treaties (MLATs) or regional police organizations to pursue transnational cases; however, MLAT processes can take months rather than weeks, limiting timely access to crucial digital evidence.

These dynamics reinforce the importance of regional cooperation, information sharing, and harmonized legal frameworks. Without collective approaches to addressing transnational cybercrime, individual Caribbean SIDS risk becoming weak links within an increasingly interconnected regional digital ecosystem.

4. The Caribbean Cyber Threat Environment



Dominant Threat Vectors

Regional reporting and recent incidents indicate that ransomware, phishing/social engineering, insider/privilege misuse, and DDoS remain among the most consequential threats to Caribbean SIDS, with public-sector systems and SMEs particularly exposed due to legacy IT, inconsistent patching, and limited backup/recovery capacity.

Ransomware and extortion-driven disruption

Caribbean organizations have experienced ransomware attacks that have caused immediate service disruption and long-term recovery costs. For example, the Caribbean Telecommunications Union cites a 2023 ransomware incident affecting Telecommunications Services of Trinidad and Tobago, in which personal data of over one million customers was stolen.

In Jamaica, national threat reporting has also underscored the role of privileged access in facilitating ransomware: a Government of Jamaica communication reports that "over 70% of ransomware attacks" (contextualized as a global 2023 pattern) were facilitated by compromised privileged accounts. These patterns are consistent with the high systemic impact of ransomware in small states, where limited redundancy can turn a single incident into a multi-agency disruption.

Phishing and social engineering are the leading initial vectors

Social engineering continues to drive compromise across the region, especially against public employees, financial institutions, and SMEs. A LACNIC cybersecurity analysis reports that phishing accounted for 74% of reported cases in the Latin American and Caribbean region. This aligns with observed targeting of government-facing services and citizen portals, as evidenced by the 2025 cyberattack that crippled Jamaica's Office of the Registrar-General website, illustrating how attacks on high-value public services can quickly affect citizens and businesses.

DDoS and service availability risk

The Caribbean's reliance on online public services and digitally mediated tourism/commerce increases the harm of availability attacks. Globally, DDoS activity continues to surge: Cloudflare reports that in Q4 2025, DDoS attacks increased 31% quarter-over-quarter and 58% compared with 2024, with network-layer attacks comprising 78% of observed DDoS activity.

Telecommunications and service providers are among the most frequently targeted sectors in DDoS reports, a fact that is directly relevant to Caribbean mobile operators and ISPs that underpin essential services and emergency communications.

SIM swap, signaling abuse, and management-plane threats

Mobile ecosystems face distinct fraud and recall risks, notably SIM swap-enabled account takeover and attacks on network management systems. A concrete Caribbean example is Jamaica's Financial Investigations Division reporting convictions in a J$61 million (USD 390,000) SIM-swap-linked fraud and money-laundering case. As networks transition to virtualized, cloud-native architectures, the expansion of API surfaces, vendor dependencies, and orchestration layers further underscores the need for security-by-design, robust access controls, and continuous monitoring in mobile network environments.

Underreporting and Limited Visibility

Cyber incidents across the Caribbean are frequently underreported due to reputational concerns, uneven disclosure obligations, and limited trust in reporting channels. This undermines situational awareness and weakens evidence-based policymaking, particularly where governments and regulators are still developing baseline incident-response and monitoring capacity.

A practical indicator of under-maturity, and the likelihood of underreporting, is highlighted in a Caribbean-wide business survey reported by the Jamaica Gleaner, which found that fewer than 30% of more than 2,000 businesses across the region had upgraded their cybersecurity, despite growing awareness of cyber threats. While this statistic speaks directly to investment gaps, it also implies limited detection and response tools, conditions that are commonly associated with lower incident discovery rates and reduced formal reporting.

At the national and regional level, cybersecurity maturity differentials also shape reporting consistency. An EU external action service analysis, citing the ITU Global Cybersecurity Index tiering, notes that only Cuba, the Dominican Republic, Jamaica, and Trinidad and Tobago were placed in Tier 3, with the rest of the Caribbean in Tier 4 or Tier 5. Lower maturity typically corresponds to weaker monitoring capacity, fewer standardized reporting pathways, and less consistent incident classification, all of which reduce the quality and comparability of incident data across jurisdictions.

For mobile operators and regional providers operating across multiple islands, inconsistent national expectations increase compliance complexity and can reduce incentives for open information sharing. This creates a negative cycle: limited reporting reduces the sharing of threat intelligence, which in turn constrains preventive action and coordinated responses.

Natural Disasters as a Cyber Risk Multiplier

Natural hazards are a defining feature of the Caribbean risk landscape, regularly disrupting power, connectivity, and physical infrastructure. During disaster response and recovery, cybersecurity controls may be relaxed or deprioritized to restore service quickly, creating windows of heightened vulnerability precisely when reliance on digital communications is greatest.

The scale of disaster impact in small Caribbean states is well documented. The IMF reports that the Caribbean is seven times more likely to be affected by natural disasters than larger states and that average disaster damage (as a share of GDP) is six times higher for Caribbean countries than for larger states. These structural conditions mean that disasters can simultaneously degrade physical infrastructure and erode cyber resilience through staff displacement, emergency network reconfiguration, and disrupted supply chains.

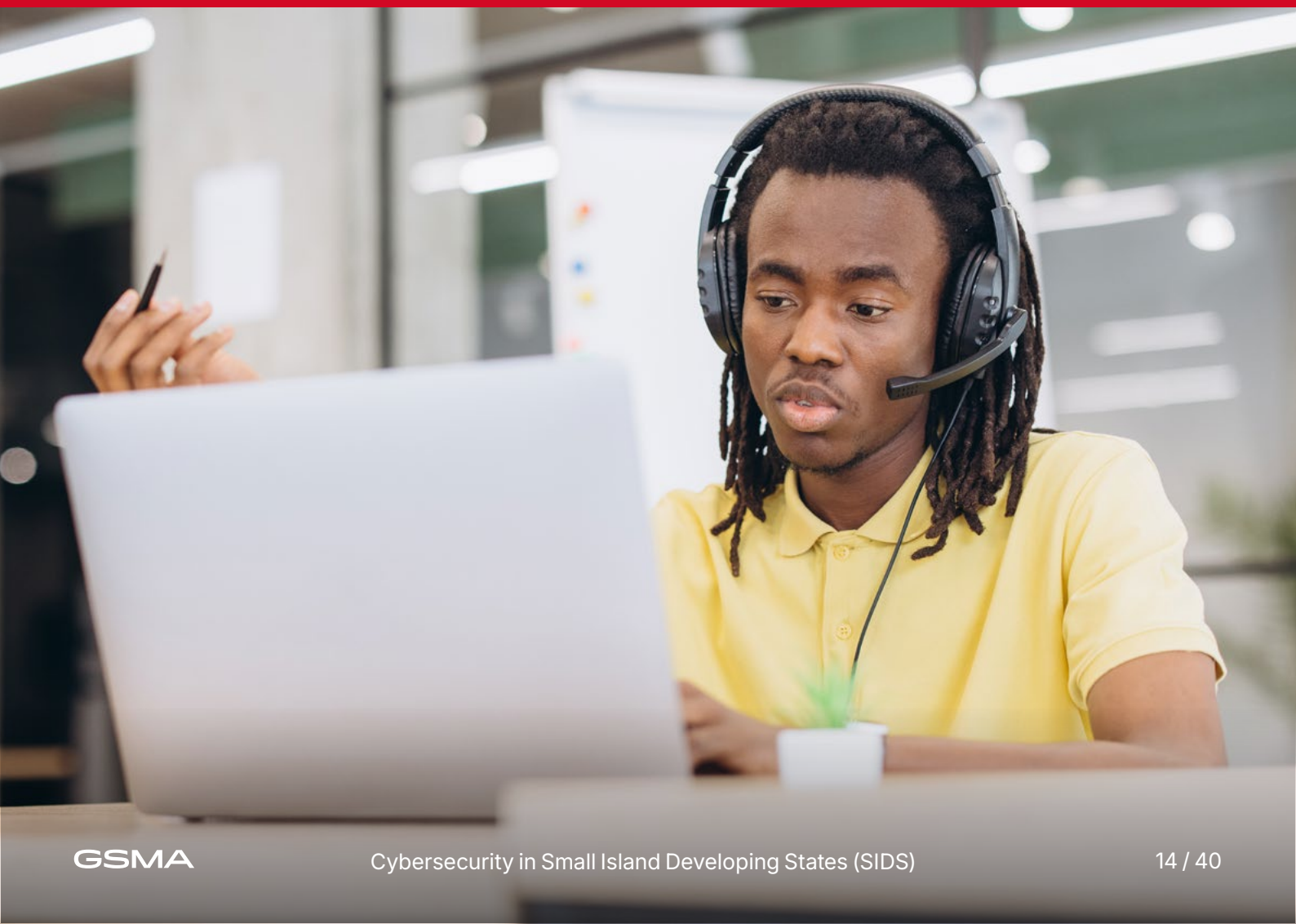
Concrete examples underscore the magnitude of these shocks:

- Dominica (Hurricane Maria): World Bank/ GFDRR reporting notes damages and losses amounting to 226% of 2016 GDP (and extensive housing damage), demonstrating how a single event can overwhelm institutional capacity and infrastructure resilience.

- St. Vincent and the Grenadines (Hurricane Beryl): The World Bank notes that a single event like Beryl can cause damages equivalent to more than 20% of GDP, illustrating the fiscal and operational stress disasters impose on small administrations.

Mobile networks are central to disaster response, supporting emergency communications, public alerts, remittances, logistics coordination, and the continuity of government services. Disaster-driven power instability, emergency routing changes, and reliance on temporary connectivity solutions can increase exposure to misconfigurations, opportunistic phishing, fraud spikes, and service availability attacks. This makes integrated planning for physical and cyber resilience essential, including redundant power, secure emergency access procedures, and tested disaster-recovery and incident-response playbooks.

5. Limitations of Conventional Cybersecurity Models



Global cybersecurity frameworks are frequently designed for jurisdictions with sizeable public budgets, mature institutions, and deep cybersecurity labor markets. These assumptions are not held in many Caribbean SIDS, where capacity and implementation bandwidth are structurally constrained. At the global level, the World Economic Forum highlights widening "cyber inequity" and capability gaps. In practice, this means Caribbean states can face a mismatch between framework requirements (e.g., standalone national operations centers, full-spectrum incident response, extensive compliance monitoring) and feasible delivery models.

A concrete indicator of the region's uneven ability to operate conventional approaches is cybersecurity maturity benchmarking. The ITU Global Cybersecurity Index (GCI) 2024 moved from rankings to five performance tiers. An EU/EEAS regional assessment, applying the ITU tiering notes, reports that only Cuba, the Dominican Republic, Jamaica, and Trinidad and Tobago are placed in Tier 3, while the rest of the Caribbean region falls into Tier 4 or Tier 5. This disparity matters because conventional "national-centric" models often assume that each country can sustain comparable baseline capabilities, whereas the Caribbean reality is a patchwork of maturity levels—making replication of "one-country, one-stack" cybersecurity models prone to fragmented implementation and unsustainable outcomes.

This fragmentation is also evident in the uneven scaling of national efforts across pillars. Some states may prioritize legislation and awareness but lack sustained operational capability, whereas others may establish incident response arrangements without consistent sector-wide reporting or minimum baselines. In multi-island or small-market contexts, requiring each jurisdiction to implement the full institutional and technical architecture of large-economy frameworks can lead to duplicative costs, gaps at the weakest links, and dependence on short-term project funding rather than durable national capacity.

A SIDS-Appropriate Approach: Scalability, Cooperation, and Proportionality

A Caribbean SIDS–appropriate approach must prioritize scalability, cooperation, and proportionality, shifting from a purely national-centric lens toward shared services and regional public goods. This direction is reflected in recent Caribbean policy developments. In October 2025, CARICOM launched the updated CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP), positioning it as a regional framework to strengthen cyber resilience through coordinated action.

Complementing this, the underlying CCSCAP framework structure explicitly emphasizes region-wide coordination mechanisms (including governance and minimum standards), capacity building, and operational cooperation:

- Harmonized approaches and shared governance: The updated CCSCAP is framed around regional alignment and collective capacity, reinforcing that a shared blueprint can reduce fragmentation across laws, reporting expectations, and operational readiness.
- Joint capacity-building and operational uplift: Regional technical communities and partners are already running practical cyber resilience initiatives. For example, ARIN reports strong Caribbean interest in routing security (RPKI) workshops delivered through regional network operator forums, illustrating an actionable model for pooled training and operational improvement that individual SIDS may struggle to sustain independently.
- Critical infrastructure resilience framing: The Caribbean Telecommunications Union has emphasized the need for deeper harmonization and collaboration to manage critical digital infrastructure dependencies in the region, a framing that supports shared approaches to baseline controls, incident coordination, and resilience planning.

Recognizing the role of MNOs as system integrators is essential within this model. In practice, operators sit at the convergence of cross-border submarine cable connectivity, terrestrial fiber, satellite backhaul, data centers, and cloud-native services. A SIDS-appropriate approach, therefore, leverages operator capabilities, such as security monitoring, redundancy planning, and network-level threat mitigation, while using regional institutions to coordinate on standards, information sharing, and capacity building. This alignment directly addresses the maturity-tier realities reflected in ITU benchmarking and reduces the weakest-link problem in a tightly interconnected regional ecosystem.

6. Cybersecurity as a Regional Public Good

Cyber risks do not respect national borders, and the Caribbean's digital ecosystem is inherently regional. Interconnected mobile and internet infrastructure, particularly shared submarine cable systems, regional cloud dependencies, and cross-border service providers, means that vulnerabilities or disruptions in one jurisdiction can have spillover effects across neighboring markets.

This is why regional frameworks increasingly treat cybersecurity as a collective-resilience issue rather than a purely national technical function.

Treating cybersecurity as a regional public good enables cost-sharing and pooled capacity, thereby reducing "weakest-link" exposure across regions with varying national maturity levels. The CCSCAP design explicitly anticipates this logic by calling for regional governance mechanisms, such as a Regional Cyber Committee and the identification of minimum cybersecurity standards across Member States. In practice, this approach helps smaller administrations avoid duplicating high-cost capabilities (e.g., full-scale 24/7 monitoring, specialized forensics) while still benefiting from coordinated standards, shared operational support, and region-wide learning.

How Regional Cooperation Reduces Fragmentation and Compliance Burdens

Regional cooperation can support shared threat intelligence platforms, federated incident response arrangements, and harmonized regulatory frameworks that reduce fragmentation and compliance burdens, particularly for mobile operators and providers operating across multiple jurisdictions. The Caribbean's operating environment includes multi-country networks, roaming dependencies, and region-wide interconnections, which means inconsistent reporting rules, varying disclosure thresholds, and divergent baseline security expectations can increase compliance complexity and hinder time-sharing.

A concrete example of how regional coordination works in practice is CARICOM IMPACS' role in supporting region-wide cyber capacity initiatives and alignment activities aligned with CCSCAP priorities. In the Eastern Caribbean, for instance, OECS and CARICOM IMPACS have collaborated on cyber awareness and resilience initiatives aligned with CCSCAP objectives. While awareness is only one pillar, these initiatives demonstrate the operational value of regional vehicles that can deliver common programs once, on a scale, rather than requiring each country to build and fund separate efforts.

Emerging Multilevel Approaches: Caribbean Digital Support Facility and UNDP–ITU Cooperation

Initiatives such as the Digital Facility for the Caribbean (DFC), often referenced as a regional digital support facility housed within UNDP's regional digital work, illustrate an emerging multilevel approach to strengthening resilience through pooled expertise, structured knowledge sharing, and implementation support. The DFC model is designed to help countries move from vision to implementation by providing technical advice, implementation support, financing pathways, and capacity development. This is directly relevant to cybersecurity because it strengthens the institutional and delivery conditions needed to implement and sustain cyber risk management as part of digital transformation.

Complementing this, SIDS-focused international cooperation is increasingly explicit about cybersecurity capacity building. The World Economic Forum notes that UNDP and the International Telecommunication Union (ITU) are collaborating on a joint program on cyber development and capacity building to support safe and resilient digital ecosystems. For Caribbean SIDS, such multilevel programming is valuable because it can support common foundational needs, workforce skills, baseline controls, incident coordination procedures, and governance templates, while avoiding duplicative country-by-country buildouts.

UNDP's DFC "service offer and experience overview" reports that an online knowledge series (Feb–Jun 2025) attracted over 1,200 registrants from more than 20 Caribbean and extra-regional countries, demonstrating the scale benefits of regional convening and shared learning mechanisms.

MNOs as Critical Infrastructure Operators

MNOs are critical national infrastructure in Caribbean SIDS, as mobile networks underpin day-to-day public services and serve as the primary backbone for communications during emergencies. This role is reinforced by regional disaster governance: the Caribbean Disaster Emergency Management Agency (CDEMA) coordinates regional telecommunications preparedness activities (e.g., its annual regional telecommunications exercise, which tests procedures and networks across participating states) and currently comprises 19 Participating States. The practical implication is that telecom resilience is not only a commercial service issue but also a regional public-safety dependency. Some concrete examples:

- Disaster restoration + continuity: Jamaica, 2025. After Hurricane Melissa (Oct. 2025), Jamaica's Government reported that Digicel restored 46% of mobile sites, 86% of its fixed network, and 75% of business connections during early restoration efforts. A Digicel restoration update issued via the Private Sector Organization of Jamaica further quantified the service continuity effect: 46% of sites operational, serving 72% of mobile customers. These figures illustrate a core "critical infrastructure" point of the white paper: partial physical restoration can still yield majority service coverage if networks are engineered with redundancy, prioritization, and rapid repair capability.

- Security risks that affect critical services: Mobile identity and accounting integrity are increasingly tied to national economic activity (banking, payments, authentication).

- High reliance and high exposure: In high-penetration, high-dependency environments such as the Caribbean, outages or security incidents can propagate rapidly across sectors (government services, commerce, emergency response), strengthening the case for proportionate, risk-based regulation that recognizes MNOs' critical infrastructure role and encourages investment in network security, redundancy, monitoring, and restoration capabilities.

MNOs as Development Enablers

Beyond infrastructure provision, Caribbean MNOs are major enablers of digital inclusion and economic activity, supporting e-government access, tourism and logistics operations, SME digitization, and, during crises, the rapid restoration of connectivity to enable recovery and continuity. Some concrete examples:

- Disaster recovery as a development function: Jamaica, 2025. The same post-hurricane restoration metrics also serve as a signal of development enablement. Restoring 75% of business connections and achieving 72% customer coverage, with 46% of sites operational, supports the recovery of commerce, logistics, and essential services during the most economically fragile period after a disaster. In tourism-dependent economies, maintaining communications and payment functionality is foundational to reopening airports/ports, coordinating supply chains, and restoring visitor services.

- Regional emergency communications capability: CDEMA's regional telecommunications exercise (and broader emergency communications planning) demonstrates that telecommunications, including mobile networks, are systematically integrated into disaster preparedness across participating Caribbean states. This is a development issue because resilient mobile communications support early warning, coordination, remittances and digital payments, and continuity of government operations during and after hazards.

- Positive externalities of operator cybersecurity investment: When MNOs strengthen controls against fraud (e.g., SIM-swap), improve monitoring, harden management-plane access, and secure interconnect/signaling, the benefits accrue across the economy—especially to financial services, e-government authentication, and SMEs that depend on mobile connectivity and mobile-based identity.

7. Governance and Regulatory Frameworks

Regional Policy Initiatives

CARICOM's CCSCAP is the Caribbean's primary regional policy framework for addressing shared cyber risks and is explicitly designed to reflect the realities of Small Island Developing States by emphasizing resilience, capacity building, and cooperation. A key milestone in this process was the launch of the updated CCSCAP in October 2025 in Port of Spain, Trinidad and Tobago, which reaffirmed cybersecurity as a collective regional priority. CARICOM IMPACS has characterized CCSCAP as a definitive roadmap for strengthening national and regional cybersecurity frameworks, supporting legislative harmonization, and advancing digital safety across Member States.

CCSCAP incorporates concrete operational mechanisms intended to translate policy objectives into practical action. It calls for establishing a regional governance framework, including a Regional Cyber Committee, and developing minimum cybersecurity standards that all Member States can work toward. These measures are designed to address uneven levels of national readiness by reducing weakest-link vulnerabilities while still allowing countries to scale capabilities at different speeds. The plan also emphasizes regional and international cooperation in incident response and cybercrime investigations, recognizing the need for shared capacity-building mechanisms and coordinated action to address transnational cyber threats.

The importance of such regional policy initiatives is underscored by persistent gaps in national preparedness. The Inter-American Development Bank's 2025 Cybersecurity Report indicates that, as of 2020, only 13 countries in Latin America and the Caribbean had adopted a national cybersecurity strategy, and just 9 had specific plans to protect critical infrastructure. While progress had been made by 2025, it remained modest, with only 15 countries reaching a maturity level of three or higher in national strategy development. In this context, regional blueprints, such as the CCSCAP, play a critical role in accelerating implementation by providing shared priorities, governance models, and common baselines that smaller administrations can adopt without independently building full frameworks.

Effective implementation of the CCSCAP in the Caribbean context will depend on several enabling conditions. Sustained political prioritization is essential, particularly to support ongoing monitoring and evaluation and to mobilize the resources required to implement agreed actions.

Equally important is alignment with national legal and regulatory regimes. CCSCAP can only function as intended if national legislation, regulators, and sectoral authorities, including those responsible for telecommunications, finance, and critical infrastructure, align their requirements with regional objectives, thereby avoiding gaps, duplication, and inconsistent application across the region.

Regulatory Harmonization

Fragmented legal and regulatory frameworks remain a material barrier to cyber resilience in Caribbean SIDS. In practice, differences in the scope and enforcement of cybercrime legislation, data protection rules, and incident-reporting requirements increase compliance costs for operators operating across multiple jurisdictions and weaken the region's collective ability to respond to transnational cyber threats. These challenges are particularly acute in an environment characterized by shared digital infrastructure, cross-border service provision, and regional operator group structures, where inconsistencies in national rules can create gaps and delays in incident response.

To address these challenges, several Caribbean-focused harmonization mechanisms have been developed. The ITU-led HIPCAR initiative was established to assist CARIFORUM countries in harmonizing ICT policies, legislation, and regulatory procedures, including by developing model policy guidelines on privacy and data protection.

As a long-standing regional instrument, HIPCAR provides a practical legislative template that countries can adapt to national contexts while maintaining regional alignment, thereby reducing legal fragmentation and supporting more consistent enforcement. In parallel, CARICOM Data Protection and Privacy Rules have been issued to promote common approaches to personal data protection and cross-border data flows across the region. These regional rulesets are increasingly important as government services, financial institutions, and mobile operators rely on cloud hosting and regional service platforms that routinely involve cross-border data handling.

The urgency of regulatory harmonization is underscored by persistent disparities in national cybersecurity readiness. The Inter-American Development Bank's 2025 Cybersecurity Report indicates that, as of 2020, only 13 countries in Latin America and the Caribbean had adopted national cybersecurity strategies, and just 9 had plans to protect critical infrastructure.

This uneven baseline creates predictable "weakest-link" effects in interconnected markets, where gaps in one jurisdiction can undermine resilience across the region. Harmonization helps mitigate these risks by standardizing core expectations and enabling more effective mutual support among states.

In practical terms, regulatory harmonization in Caribbean SIDS should prioritize several key areas. Alignment of cybercrime statutes and investigatory powers is essential to streamline cross-border investigations and facilitate timely evidence sharing. Harmonization of data protection standards can reduce legal uncertainty for operators and public services that depend on regional and cloud-based systems.

Finally, standardizing incident-reporting requirements, including thresholds, timelines, and safe-harbor provisions, would reduce complex compliance for operators and improve disclosure, information sharing, and regional situational awareness, thereby strengthening collective cyber resilience across the Caribbean.

8. Economic Dimensions of Cybersecurity

Cyber incidents impose both direct and indirect economic costs across Caribbean SIDS, including immediate service disruption, technical recovery and forensic expenses, increased fraud losses, and longer-term erosion of consumer and investor trust. In Jamaica, for example, the Office of the Registrar-General (ORG), the national repository for birth, marriage, and death records, reported that a cyber incident disrupted the availability of its systems and left some services "temporarily impacted or unavailable" while recovery proceeded, illustrating how attacks on digital public services can impose economy-wide friction for households and businesses that depend on official documentation and verification services.

In Trinidad and Tobago, Telecommunications Services of Trinidad and Tobago (TSTT) reported that attackers attempted unauthorized access and that a ransomware group claimed the incident; in its public update, TSTT noted it had "continuously invested millions of dollars" in security resources and that the data accessed totaled 6GB, which it assessed as less than 1% of the petabytes of data the company produces and stores—demonstrating both the scale of operator security costs and the economic burden of incident response, data validation, and customer assurance measures even when only a subset of records is implicated.

Private-sector exposure to ransomware is illustrated by the Caribbean's largest recorded data breach in 2022, when the Hive ransomware group targeted a major regional supermarket chain, exposing over 700,000 files containing sensitive employee and customer information, including salaries, identification documents, wire transfer details, and passport data. The attack forced the suspension of customer-facing systems and required engaging international cybersecurity experts to contain and restore them. The incident exemplifies the vulnerability of Caribbean retail and private-sector SMEs to ransomware attacks, which account for nearly half of all cyber incidents in Latin America and the Caribbean.

The breach highlighted insufficient baseline security measures in sectors beyond traditional critical infrastructure, including inadequate encryption, access controls, and backup protocols. Following the attack, the affected organization implemented enhanced security measures, including data encryption, regular security audits, and improved incident response capabilities. The case underscores how organized crime groups increasingly target Caribbean businesses that combine valuable customer data with limited cybersecurity investment, creating opportunities for extortion while simultaneously funding broader criminal activities.

For Small Island Developing States, where retail and tourism sectors are economically vital and often digitally connected through mobile payment systems and customer databases, such attacks demonstrate the cross-sector nature of cyber risk and the need for minimum security standards that extend beyond telecommunications and government infrastructure to encompass all data-handling businesses serving both residents and international visitors.

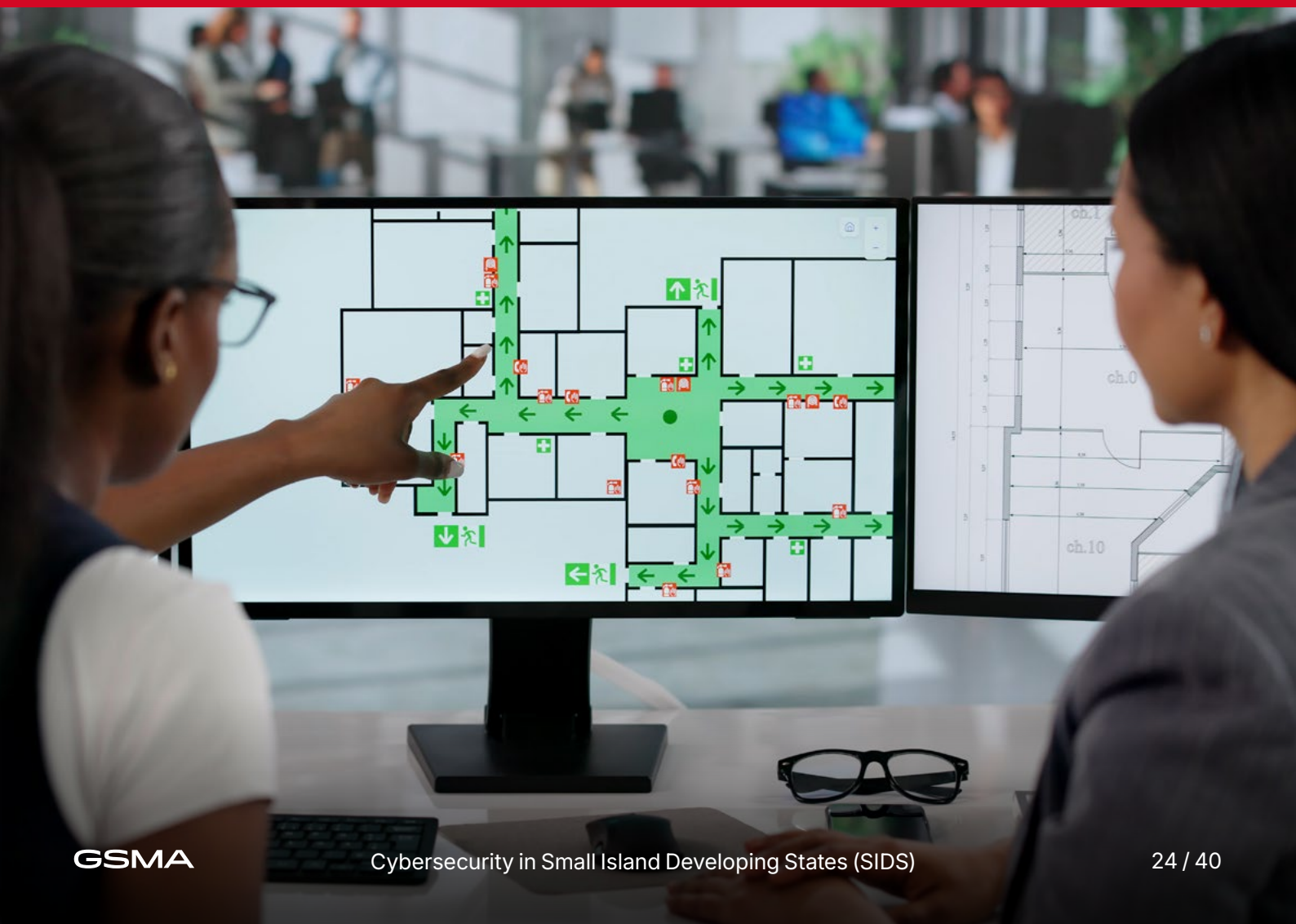
For Caribbean SIDS, these impacts can be disproportionately large because national systems and markets are smaller, redundancy is limited, and a disruption to a single high-dependency platform (telecommunications, identity, payments, government services) can cascade rapidly across sectors. This is precisely why cybersecurity investment should be treated as an enabler of digital growth rather than a discretionary cost.

The World Bank's Cybersecurity Economics for Emerging Markets argues that stronger cybersecurity supports growth and notes that a developing country that reduces cyber incidents could boost GDP per capita by 1.5% within a decade, reinforcing the policy logic that cyber resilience is an investment in productivity and competitiveness.

Public–private collaboration can improve the efficiency and sustainability of this investment, particularly where operators already maintain advanced security capabilities that can be leveraged for broader national benefit. In the ORG case, the agency reported activating an incident response plan that included containment, digital forensics, and notification of relevant authorities—an approach that relies on established coordination among institutions and the broader security ecosystem.

Public–private collaboration improves security investment efficiency, as demonstrated by TSTT's engagement with international cyber security experts during its 2023 ransomware incident (detailed above).

9. Infrastructure, AI, and Emerging Risks



The Caribbean's shift toward virtualized, cloud-native mobile networks is already underway through the region's early 5G rollouts and the increasing use of cloud platforms for core network functions and service delivery, which expands the cyber-attack surface while also enabling more flexible security controls. A practical example is the Cayman Islands, where FLOW framed its 2024 5G launch as a major network evolution milestone for the territory, reflecting the region's move toward next-generation architectures that rely more heavily on software, orchestration, and remote management.

Therefore, it requires stronger hardening of management planes, identity controls, and continuous monitoring.

In Barbados, FLOW's "5G+" rollout was initially concentrated on 22 high-impact sites, illustrating how early-stage 5G deployments in SIDS often begin with targeted coverage footprints in which cyber-resilience requirements (for slicing, virtualization layers, and cloud interconnects) must be embedded from the outset. AI is increasingly positioned as a tool to strengthen this security posture, particularly for anomaly detection, event correlation, and automated triage; for example, a telecom-focused industry report summary noted that 59% of communications service provider executives cited AI use for network security threat detection as a widespread application, reflecting the mainstreaming of AI-driven security operations in telecom environments.

At the same time, AI introduces new risks relevant to Caribbean operators and regulators, including model exploitation, automation of phishing and social engineering, and the strain that AI-driven bot traffic can place on digital services and online ecosystems; Cloudflare reported that during 2025, AI bot traffic averaged 4.2% of all HTML requests, peaking above 6% at points in the year, underscoring the growing scale of automated activity that security teams must distinguish from legitimate usage.

Infrastructure resilience remains inseparable from cybersecurity in Caribbean SIDS because connectivity is heavily dependent on a limited number of physical and logical chokepoints, particularly submarine cables, national spectrum policy, and the availability of local/regional data-center capacity.

Subsea cable risk is not hypothetical: globally, ~200 subsea cable faults occur per year (2013–2024), and the vast majority are associated with fishing and anchoring activities, demonstrating how routine physical hazards can generate really cyber and service-continuity consequences when redundancy is limited.

A 2025 risk assessment further identified 44 publicly reported cable damages in 2024–2025, highlighting how limited redundancy and repair capacity can amplify the impact of outages, conditions that mirror the vulnerability profile of many island networks. This dependence is clearly illustrated in the Turks and Caicos Islands (TCI): the regulator notes that the country's sole international communications gateway is the ARCOS-1 submarine cable landing on Providenciales, while other inhabited islands depend on microwave links that have become oversaturated as demand has grown, constraints that have pushed some residents toward satellite alternatives.

The same consultation paper documents an attempt to regularize satellite internet demand, noting that Starlink applied on 8 Oct. 2024 for an ISP license capped at a maximum of 500 subscribers, before withdrawing as the regulator moved toward a dedicated satellite licensing framework, an example of how satellite systems are becoming part of the region's resilience toolkit, while also raising governance and jurisdictional challenges for cybersecurity oversight.

Parallel investments in data-center infrastructure can reduce latency and improve resilience (e.g., by keeping services local during upstream disruptions), but they also concentrate risk if security, power resilience, and interconnection diversity are weak; one Caribbean market assessment estimated the regional data-center market at US$62 million (baseline) with growth to US$120.4 million by 2027 (CAGR 11.7%) and identified 15 existing data centers, a growth trajectory that increases the importance of data-center security controls, incident response integration, and trusted interconnection arrangements. Finally, spectrum management is a foundational "enabler layer" for secure network evolution.

10. Strategic Imperatives and Recommendations

To address the evolving cyber risk landscape and support sustainable digital transformation, Caribbean SIDS must adopt a set of strategic imperatives tailored to their structural realities and regional interdependence. Central to this approach is the recognition of cybersecurity as a regional public good. Given the interconnected nature of Caribbean digital infrastructure, particularly mobile networks, submarine cables, cloud services, and cross-border platforms, cyber risks and vulnerabilities in one jurisdiction can have cascading effects across the region.

Treating cybersecurity as a shared responsibility enables cost-sharing, reduces weakest-link vulnerabilities, and strengthens the Caribbean's collective capacity to engage effectively with global technology providers, development partners, and threat intelligence networks.

Strengthening regional coordination and information sharing is therefore a critical priority. Caribbean states should deepen cooperation through existing regional institutions and mechanisms to support shared threat intelligence, coordinated incident response, and joint capacity-building initiatives. Federated arrangements for information exchange and incident coordination can help overcome national capacity constraints, improve situational awareness, and ensure more timely and effective responses to transnational cyber threats. Harmonized approaches also reduce duplication and allow smaller administrations to benefit from collective expertise and resources.

This White Paper further highlights the importance of supporting operator-led resilience through proportionate, risk-based regulation. Mobile network operators play a dual role as critical infrastructure providers and key enablers of digital inclusion and economic activity. Many operators already invest significantly in network security, redundancy, monitoring, and disaster recovery, often exceeding minimum regulatory requirements. Policy and regulatory frameworks should recognize this role, avoid imposing fragmented or duplicative obligations, and instead incentivize continued investment in resilience by setting clear, consistent, and proportionate regulatory expectations aligned with regional objectives.

Sustained investment in human capital and skills development is also essential. Cybersecurity capacity in Caribbean SIDS is constrained by limited pools of specialized expertise and high competition for skilled professionals. Governments, regulators, operators, and regional institutions should prioritize coordinated training programs, workforce development initiatives, and partnerships with academic and international organizations to build and retain cybersecurity talent. Regional training and certification programs can help achieve economies of scale and reduce reliance on short-term external assistance.

Finally, integrating cybersecurity into disaster-resilience planning is imperative in the Caribbean context. Natural hazards such as hurricanes and floods regularly disrupt power, connectivity, and physical infrastructure, creating periods of heightened cyber vulnerability during emergency response and recovery. Cybersecurity considerations should therefore be embedded into national and regional disaster risk management frameworks, including emergency communications planning, infrastructure restoration protocols, and continuity of government operations. Aligning cyber resilience with broader disaster preparedness efforts will help ensure that digital infrastructure remains secure and reliable when it is most critical to public safety and economic recovery.

11. GSMA Cybersecurity Frameworks in Caribbean SIDS

Mobile Threat Intelligence Framework (MoTIF - FS.57)

MoTIF is a classification framework inspired by MITRE ATT&CK, designed to describe how adversaries attack and exploit mobile networks through tactics, techniques, and procedures (TTPs). It structures threats into phases (kill chain stages) to enable systematic analysis, intelligence sharing, and defense building. The main steps/phases include:

1. **Reconnaissance**: Adversaries gather information about the target network or users, such as monitoring radio interfaces to collect cell configuration parameters or subscriber data (e.g., via broadcast channels or victim identity gathering). This preparatory step helps tune subsequent attacks.

2. **Initial Access**: Gaining a foothold, often through techniques like exploiting signaling protocols or social engineering to compromise devices or accounts.

3. **Execution**: Carrying out malicious actions, such as running unauthorized code on network elements or devices.

4. **Persistence**: Maintaining access, e.g., by installing backdoors or modifying configurations to ensure long-term control.

5. **Privilege Escalation**: Elevating access rights, often via compromised privileged accounts (a factor in over 70% of ransomware attacks).

6. **Defense Evasion**: Avoiding detection, such as obfuscating traffic or disabling security controls.

7. **Command and Control**: Establishing communication channels to control compromised systems.

8. **Exfiltration**: Stealing data, like customer information or network configurations.

9. **Impact**: Achieving objectives, such as service disruption (e.g., DDoS) or data extortion.

In resource-limited SIDS like Jamaica or Trinidad and Tobago, MoTIF can be incorporated by integrating it into regional threat-sharing platforms under the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP). For example, mobile network operators (MNOs) could use MoTIF to map TTPs from local incidents (e.g., the 2023 TSTT ransomware attack) during reconnaissance and privilege escalation phases, enabling pooled intelligence hubs via the Caribbean Telecommunications Union (CTU).

This fosters collaborative monitoring without overburdening small teams (<10 staff), and links to disaster planning by prioritizing threats during post-hurricane recovery, when networks are vulnerable to evasion tactics.

Network Equipment Security Assurance Scheme (NESAS)

NESAS is a voluntary assurance scheme jointly developed by GSMA and 3GPP, focusing on secure network infrastructure product development, lifecycle processes, and network equipment security evaluation for mobile networks (especially 5G). It involves two main assessment processes: Vendor Development and Product Lifecycle Process Audit, and Network Product Evaluation. The steps are:

Vendor Processes Assessment Steps:

1. **Define Security Processes (Preparatory)**: The equipment vendor establishes and documents security-related processes for product development and lifecycle management, ensuring "security by design" principles like domain separation, least privilege, and vulnerability disclosure.

2. **Self-Assessment and Conformance Claim**: The vendor assesses their processes against NESAS requirements (e.g., FS.16 security requirements) and declares conformity.

3. **Independent Audit**: An accredited audit team (appointed by GSMA) conducts an audit of the vendor's product development processes to verify compliance.

4. **Audit Report**: The audit team prepares a report, agrees on findings with the vendor, and issues recommendations for improvements, if appropriate.

Network Product Evaluation Steps:

1. **Build and Declare Compliance (Preparatory)**: The vendor develops the network product in accordance with the audited product development processes and declares compliance with the security requirements defined in relevant 3GPP Security Assurance Specifications (SCAS).

2. **Evidence Evaluation**: An accredited test laboratory reviews the vendor's compliance declaration and supporting documents.

3. **Product Testing**: The test laboratory evaluates the product against the SCAS defined security test cases (e.g., for network functions like gNB or AMF), including vulnerability scans and security requirement verifications.

4. **Evaluation Report**: The test laboratory documents results, including any issues identified, and the product evaluation report can be published and made available by the product vendor.

NESAS requires periodic reassessments, evolving with threats like quantum computing

NESAS can be incorporated into procurement and regulatory frameworks in SIDS reliant on external infrastructure. For instance, regulators in the Bahamas or Barbados could mandate NESAS audits for 5G rollouts by operators like FLOW, ensuring equipment resilience against combined cyber-physical threats during hurricanes. Regional bodies like CARICOM could recognize the outcome of NESAS process audits and product evaluations to avoid incurring costs, aligning with CCSCAP for harmonized standards, reducing supply chain risks in virtualized networks, and enhancing trust in cloud-native architectures amid API expansions.

GSMA Baseline Security Controls (FS.31)

FS.31 provides a set of foundational controls (not strictly sequential steps) to build a strong security posture, grouped into business and various technological categories. It includes a checklist for compliance and maturity assessment, with implementation viewed as iterative steps:

1. **Assessment and Gap Identification**: Use the provided checklist (Annex A) to identify and compare implemented controls, and their maturity, against GSMA's recommendations, assigning implementation and monitoring tasks across teams (e.g., business controls for policy and risk management).

2. **Business Controls Implementation**: Establish organizational foundations, such as defining security policies, conducting risk assessments, ensuring supplier security, and training staff.

3. **Technological Controls Implementation**: Apply controls across network elements, e.g., (e)UICC management (secure SIM provisioning), radio network operations (access controls), core network (encryption), and security operations (monitoring and incident response).

4. **Verification and Improvement**: Perform active verifications like penetration testing, vulnerability scans, or red team exercises; update controls implementation and gap analysis based on findings.

5. **Ongoing Maintenance**: Regularly review and update (e.g., version 5.0 adds tables for assignment and refines descriptions for NFVI virtualization and core controls).

Incorporation in Caribbean SIDS: In SIDS with legacy IT and inconsistent patching (e.g., public systems in Jamaica), FS.31 can be incorporated as minimum standards in national cybersecurity strategies, many of which are underdeveloped. MNOs could start with the checklist for self-assessments, then collaborate via CTU for regional training on technological controls like slice security in 5G networks. This addresses phishing (74% of regional cases) through access controls and supports SMEs by integrating into public-private partnerships, enhancing resilience in tourism-dependent economies like Saint Lucia during availability attacks.

These frameworks complement each other; for example, MoTIF informs threat modeling in NESAS audits, while FS.31 provides baseline controls for implementation. In Caribbean SIDS, incorporation emphasizes regional public goods, leveraging initiatives like UNDP-ITU programs for capacity building to overcome talent shortages and foster sustainable digital resilience.

12. Conclusion

The Caribbean's digital transformation is reshaping how economies function, how governments deliver services, and how societies respond to shocks. Mobile networks now underpin essential public services, financial systems, disaster response, and economic activity across the region. At the same time, this growing digital dependence has elevated cybersecurity from a technical concern to a strategic imperative for national resilience, economic stability, and public trust. For SIDS, where institutional redundancy is limited and recovery capacity constrained, cyber incidents can have systemic effects that extend far beyond individual organizations or sectors.

The Caribbean's digital transformation is reshaping how economies function, how governments deliver services, and how societies respond to shocks. Mobile networks now underpin essential public services, financial systems, disaster response, and economic activity across the region. At the same time, this growing digital dependence has elevated cybersecurity from a technical concern to a strategic imperative for national resilience, economic stability, and public trust. For SIDS, where institutional redundancy is limited and recovery capacity constrained, cyber incidents can have systemic effects that extend far beyond individual organizations or sectors.

This paper has shown that the cybersecurity challenges facing Caribbean SIDS are structurally distinct from those of larger economies. Limited fiscal space, small talent pools, heavy reliance on externally owned digital infrastructure, and high exposure to natural hazards create a risk environment in which conventional, national-centric cybersecurity models are often ill-suited. Attempting to replicate standalone frameworks designed for large markets can lead to fragmented implementation, duplicated costs, and unsustainable outcomes. Instead, cybersecurity in the Caribbean must be approached as a shared regional challenge, embedded within broader digital, economic, and disaster-resilience strategies.

Treating cybersecurity as a regional public good offers a more effective and proportionate pathway forward. Regional policy initiatives, such as the CARICOM Cyber Security and Cybercrime Action Plan, demonstrate how shared governance mechanisms, harmonized standards, and coordinated capacity-building can help address uneven national readiness and reduce weakest-link vulnerabilities within an interconnected digital ecosystem. Strengthening regional coordination and information sharing—through federated incident response, shared threat intelligence, and aligned regulatory frameworks—can enhance situational awareness, improve response effectiveness, and reduce compliance burdens for operators active across multiple jurisdictions.

Treating cybersecurity as a regional public good offers a more effective and proportionate pathway forward. Regional policy initiatives, such as the CARICOM Cyber Security and Cybercrime Action Plan, demonstrate how shared governance mechanisms, harmonized standards, and coordinated capacity-building can help address uneven national readiness and reduce weakest-link vulnerabilities within an interconnected digital ecosystem. Strengthening regional coordination and information sharing—through federated incident response, shared threat intelligence, and aligned regulatory frameworks—can enhance situational awareness, improve response effectiveness, and reduce compliance burdens for operators active across multiple jurisdictions.

Mobile network operators occupy a central position in this resilience agenda. As critical infrastructure operators and key enablers of digital inclusion, emergency communications, and economic activity, MNOs already invest significantly in network security, redundancy, and operational resilience.

Recognizing and supporting this role through proportionate, risk-based regulation is essential. Well-designed policy frameworks can incentivize sustained investment in cybersecurity while ensuring affordability, service quality, and innovation, thereby generating positive spillovers across the broader economy.

Looking ahead, sustained investment in human capital, skills development, and institutional capacity will be critical to closing cybersecurity gaps in Caribbean SIDS. Equally important is the integration of cybersecurity into disaster risk management and climate resilience planning, given the region's exposure to natural hazards and the central role of digital infrastructure in emergency response and recovery. Cyber resilience and physical resilience are increasingly inseparable, and both must be addressed in a coordinated manner.

Looking ahead, sustained investment in human capital, skills development, and institutional capacity will be critical to closing cybersecurity gaps in Caribbean SIDS. Equally important is the integration of cybersecurity into disaster risk management and climate resilience planning, given the region's exposure to natural hazards and the central role of digital infrastructure in emergency response and recovery. Cyber resilience and physical resilience are increasingly inseparable, and both must be addressed in a coordinated manner.

By aligning regional and national policy frameworks, leveraging operator capabilities, investing in people and infrastructure, and embedding cybersecurity into broader resilience strategies, Caribbean states can mitigate cyber risks while unlocking the full benefits of digital transformation. Collective action, regional cooperation, and sustained public–private partnership offer the most credible and effective path toward a secure, inclusive, and resilient digital future for Caribbean Small Island Developing States.

By aligning regional and national policy frameworks, leveraging operator capabilities, investing in people and infrastructure, and embedding cybersecurity into broader resilience strategies, Caribbean states can mitigate cyber risks while unlocking the full benefits of digital transformation. Collective action, regional cooperation, and sustained public–private partnership offer the most credible and effective path toward a secure, inclusive, and resilient digital future for Caribbean Small Island Developing States.

13. References

International Organizations & Policy Documents

[1] Caribbean Community (CARICOM), "Updated CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) launched," Nov. 3, 2025. [Online]. Available: https://caricom.org/updated-caricom-cyber-security-and-cybercrime-action-plan-ccscap-launched/.

[2] Caribbean Telecommunications Union (CTU), "CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP)," 2021. [Online]. Available: https://ctu.int/wp-content/uploads/2021/02/CARICOM-Cyber-Security-and-Cybercrime-Action-Plan_Final_Ver3-copy.pdf.

[3] Caribbean Telecommunications Union (CTU), "3 key strategic imperatives to achieve ICT infrastructure resilience in the Caribbean." [Online]. Available: https://ctu.int/3-key-strategic-imperatives-to-achieve-ict-infrastructure-resilience-in-the-caribbean/.

[4] World Economic Forum, Global Cybersecurity Outlook 2026. Geneva, Switzerland: World Economic Forum, 2026. [Online]. Available: https://www.weforum.org/reports/global-cybersecurity-outlook-2026.

[5] K. N. Massally and L. Hildrebrandt, "Small Island Developing States can lead in digital transformation for climate resilience. Here is how," World Economic Forum, May 31, 2024. [Online]. Available: https://www.weforum.org/stories/2024/05/sids-small-island-developing-states-digital-climate/. Accessed: Feb. 2, 2026.

[6] International Telecommunication Union (ITU), Global Cybersecurity Index 2024. Geneva, Switzerland: ITU, 2024. [Online]. Available: https://www.itu.int/itu-d/cybersecurity/global-cybersecurity-index.

[7] International Telecommunication Union (ITU), "HIPCAR: Privacy and data protection model policy guidelines," 2012. [Online]. Available: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/privacy_and_data_protection_model%20policy%20guidelines.pdf.

[8] World Bank, Digital Connectivity and Resilience in Small Island States. Washington, DC, USA: World Bank, 2025. [Online]. Available: https://www.worldbank.org/en/publication/digital-connectivity.

[9] World Bank, Cybersecurity Economics for Emerging Markets. Washington, DC, USA: World Bank, Oct. 9, 2024. [Online]. Available: https://www.worldbank.org/en/topic/digital/publication/Cybersecurity-Economics-for-Emerging-Markets.

[10] World Bank, Digital Development in the Caribbean: Infrastructure, Services, and Resilience. Washington, DC, USA: World Bank, 2025. [Online]. Available: https://www.worldbank.org.

[11] World Bank, "How tailored national cybersecurity strategies enable safe, inclusive and resilient digital transformation," Jun. 8, 2022. [Online]. Available: https://blogs.worldbank.org/en/digital-development/how-tailored-national-cybersecurity-strategies-enable-safe-inclusive-and.

[12] World Bank, "How the World Bank crisis toolkit is empowering Caribbean small states," Apr. 28, 2025. [Online]. Available: https://www.worldbank.org/en/news/feature/2025/04/28/how-the-world-bank-s-crisis-toolkit-is-empowering-caribbean-small-states.

[13] Global Facility for Disaster Reduction and Recovery (GFDRR)/World Bank, "Dominica: Post-disaster needs assessment following Hurricane Maria," Sep. 18, 2017. [Online]. Available: https://www.gfdrr.org/en/publication/dominica-post-disaster-needs-assessment-following-hurricane-maria.

[14] Inter-American Development Bank (IDB), 2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean. IDB, 2025. [Online]. Available: https://publications.iadb.org/publications/english/document/2025-Cybersecurity-Report-Vulnerability-and-Maturity-Challenges-to-Bridging-the-Gaps-in-Latin-America-and-the-Caribbean.pdf.

[15] International Monetary Fund (IMF), "Building resilience in the Caribbean to climate change," Finance & Development, Mar. 2018. [Online]. Available: https://www.imf.org/en/publications/fandd/issues/2018/03/otker.

[16] European External Action Service (EEAS), "A cyber wall for the Caribbean," Nov. 6, 2025. [Online]. Available: https://www.eeas.europa.eu/eeas/cyber-wall-caribbean_en.

[17] United Nations Development Programme (UNDP), "Digital Facility for the Caribbean," UNDP Digital Hub. [Online]. Available: https://www.undp.org/latin-america/digitalhub4/digital-facility-caribbean.

[18] United Nations Development Programme (UNDP), "Digital Facility for the Caribbean: Service offer and experience overview," Dec. 2025. [Online]. Available: https://www.undp.org/sites/g/files/zskgke326/files/2025-12/digital_facility_for_the_caribbean_service_offer_and_experience_overview.pdf.

[19] Caribbean Community (CARICOM), "CCS data protection and privacy rules," 2020. [Online]. Available: https://caricom.org/wp-content/uploads/CCS-Data-Protection-and-Privacy-Rules-GC.pdf.

[20] CARICOM Implementation Agency for Crime and Security (IMPACS), "Building robust, long-term defence against cyber threats," Sep. 4, 2025. [Online]. Available: https://www.caricomimpacs.org/articles/building-robust-long-term-defense-against-cyber-threats.

[21] Caribbean Disaster Emergency Management Agency (CDEMA), "Participating states," May 10, 2018. [Online]. Available: https://www.cdema.org/index.php/component/content/article/497-participating-states-1?Itemid=741.

[22] Caribbean Disaster Emergency Management Agency (CDEMA), "Exercise Region Rap to test communications procedures, plans and networks," Feb. 18, 2020. [Online]. Available: https://www.cdema.org/index.php?Itemid=280&catid=54%3Ast-kittsnevis&id=1239%3Acommunity-response-teams-to-be-trained&option=com_content&view=article.

Industry Reports & Analysis

[23] GSMA. (2024, April 3). FS.57 Mobile Threat Intelligence Framework (MoTIF) principles. https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-57-mobile-threat-intelligence-framework-motif-principles/

[24] GSMA, The Mobile Economy: Latin America and the Caribbean 2025. London, UK: GSMA, Jun. 2025. [Online]. Available: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/latam/.

[25] GSMA, Mobile Networks and Digital Resilience, GSMA Policy Series. London, UK: GSMA. [Online]. Available: https://www.gsma.com.

[26] GSMA. (2026). Network Equipment Security Assurance Scheme (NESAS). GSMA Services. https://www.gsmaservices.com/assurance-services/network-equipment-security-assurance-scheme-nesas/

[27] S&P Global Market Intelligence, "Latin America and the Caribbean mobile market overview," Sep. 9, 2025. [Online]. Available: https://www.spglobal.com/market-intelligence/en/news-insights/research/2025/09/latin-america-and-the-caribbean-mobile-market-overview.

[28] LACNIC, "Cybersecurity in Latin America: Key threats and responses," Jun. 23, 2025. [Online]. Available: https://blog.lacnic.net/en/cybersecurity-in-latin-america/.

[29] Cloudflare, "DDoS threat report for 2025 Q4," Cloudflare Radar, Feb. 2026. [Online]. Available: https://radar.cloudflare.com/reports/ddos-2025-q4.

[30] Cloudflare, "The 2025 Cloudflare Radar year in review: The rise of AI," Dec. 15, 2025. [Online]. Available: https://blog.cloudflare.com/radar-2025-year-in-review/.

[31] AIBusiness, "AI, cloud critical for telecommunications, report finds," Feb. 26, 2025. [Online]. Available: https://aibusiness.com/ai-policy/ai-cloud-critical-for-telecommunications-report-finds-mobile-world-congress-2025.

[32] Submarine Networks, "Statistics on subsea cable fault and repair," Jun. 28, 2025. [Online]. Available: https://www.submarinenetworks.com/en/nv/insights/statistics-on-subsea-cable-fault-and-repair.

[33] Recorded Future, Insikt Group, "Submarine cable security at risk amid geopolitical tensions and limited repair capabilities," Jul. 17, 2025. [Online]. Available: https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats.

[34] Arizton, "Caribbean data center market – investment analysis and growth opportunities 2022–2027," updated Mar. 2024. [Online]. Available: https://www.arizton.com/market-reports/caribbean-data-center-market.

Government & Regulatory Sources

[35] Government of Jamaica, Jamaica Information Service (JIS), "Organisations urged to take immediate steps to strengthen their cyber security defences," Sep. 26, 2025. [Online]. Available: https://jis.gov.jm/organisations-urged-to-take-immediate-steps-to-strengthen-their-cyber-security-defences/.

[36] Government of Jamaica, Jamaica Information Service (JIS), "Telecoms companies restoring service to hardest-hit parishes," Nov. 4, 2025. [Online]. Available: https://jis.gov.jm/telecoms-companies-restoring-service-to-hardest-hit-parishes/.

[37] Financial Investigations Division (FID), Jamaica, "Three convicted in J$61M money-laundering and SIM-swap case from joint FID–MOCA–JCF probe," Oct. 20, 2025. [Online]. Available: https://www.fid.gov.jm/fid-moca-jcf-break-61m-fraud-case/.

[38] Telecommunications Authority of Trinidad and Tobago (TATT), "Consultative document on the spectrum plan for the accommodation of public mobile telecommunications services (Version 4.2)," Jan. 30, 2024. [Online]. Available: https://tatt.org.tt/wp-content/uploads/2024/01/Spectrum-Plan-for-the-Accommodation-of-Public-Mobile-Telecommunications-Services-ver-4.2.pdf.

[39] Telecommunications Commission, Turks and Caicos Islands, "Public notice 2025–2: Consultation framework for the licensing of satellite-based internet service providers," Mar. 27, 2025. [Online]. Available: https://telecommission.tc/wp-content/uploads/2025/03/PN-2025-2-Consultation-on-Licensing-of-Satellite-Services.pdf.

Corporate & Telecommunications Providers

[40] Telecommunications Services of Trinidad and Tobago (TSTT), "TSTT update on cybersecurity issue - November 3, 2023," Nov. 3, 2023. [Online]. Available: https://www.tstt.co.tt/news/tstt-update-on-cybersecurity-issue---november-3%2C-2023.

[41] Digicel Jamaica, "Update: Hurricane Melissa," Nov. 3, 2025. [Online]. Available: https://www.psoj.org/wp-content/uploads/2025/11/Digicel-Jamaica-Update-HURRICANE-MELISSA-1.pdf.

[42] Cable & Wireless Communications (FLOW), "Flow applauded for the historic introduction of 5G," Press Release, Jun. 13, 2024. [Online]. Available: https://www.cwc.com/news-and-media/press-releases/flow-applauded-for-the-historic-introduction-of-5g.html.

News & Media Sources

[43] Jamaica Observer, "Cyber attack on Office of Registrar General contained, but services impacted — ORG," Aug. 27, 2025. [Online]. Available: https://www.jamaicaobserver.com/2025/08/27/cyber-attack-office-registrar-general-contained-services-impacted-org/.

[44] Jamaica Gleaner, "Office of the Registrar-General, formerly RGD, hit by cyber attack," Aug. 27, 2025. [Online]. Available: https://jamaica-gleaner.com/article/news/20250827/office-registrar-general-formerly-rgd-hit-cyber-attack.

[45] C. Stephens, "Risk perception of growing cyber threat," Jamaica Gleaner, Feb. 13, 2022. [Online]. Available: https://jamaica-gleaner.com/article/business/20220213/cedric-stephens-risk-perception-growing-cyber-threat.

[46] Bajan Reporter, "Flow reassures public safety as 5G+ rolls out," Nov. 12, 2025. [Online]. Available: https://www.bajanreporter.com/2025/11/flow-reassures-public-safety-as-5g-rolls-out/.

GSMA

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences. For more information, please visit the GSMA corporate website at www.gsma.com.

About the GSMA North America Team

Headquartered in Atlanta, Georgia, USA, GSMA North America represents and leads mobile network operators in the United States, Canada, Greenland and the Caribbean. Working alongside some of the mobile industry's most influential companies, GSMA North America aims to increase the region's commercial opportunities and develop a collaborative and socially responsible and ecosystem. In this mission, GSMA North America convenes several leading annual industry events, provides regulatory expertise and technical knowledge to support network optimization.

Document Editor

GSMA Staff

For further information, please visit:
https://www.gsma.com/northamerica

GSMA NORTH AMERICA
Armour Yards
165 Ottley Drive
Atlanta, GA 30324
USA

GSMA Head Office
1 Angel Lane
London, EC4R 3AB
U.K.
Tel: +44 (0)207 356 0600
Email: info@gsma.com