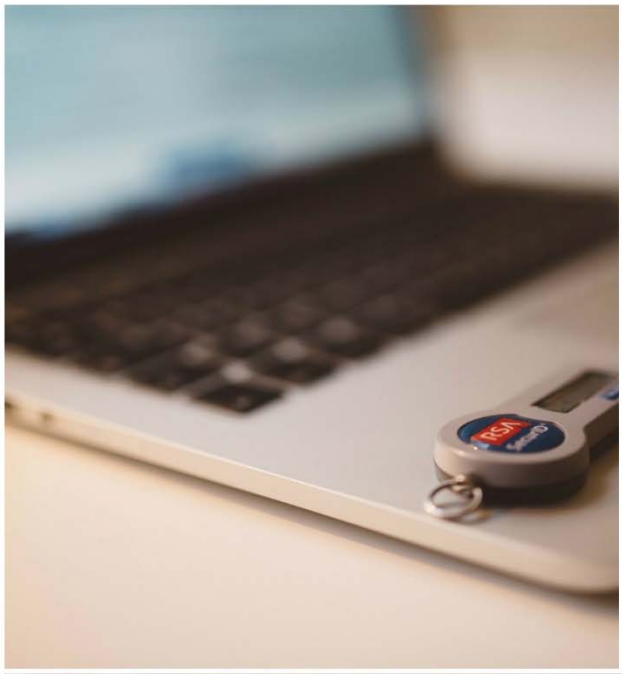
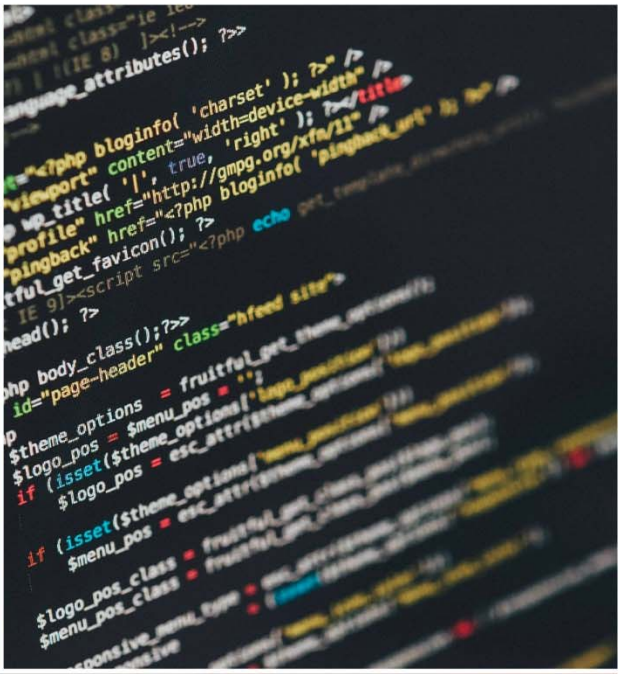
CARICOM Cyber Security and Cybercrime Action Plan





Collaborating Partners

Shaping Caribbean Communications CTU

Organization of American States

The Commonwealth

CARICOM Cyber Security and Cybercrime Action Plan

Contents

1. Executive Summary

The CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) seeks to address the Cyber Security vulnerabilities in each participating Caribbean country and to establish a practical, harmonised standard of practices, systems and expertise for Cyber Security, to which each Caribbean country could aspire in the short and medium terms. It also seeks to build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of Cybercrime and possible linkages to other forms of criminal activity.

This CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) was developed as the main output of the Caribbean Stakeholders Meeting II – Cyber Security and Cybercrime held in Saint Lucia in March 2016.

In order to ensure the success of the CCSCAP, mechanisms must be put in place to facilitate and motivate countries into action, monitoring progress and providing strategic direction. This Action Plan therefore highlights the important role that a Regional Cyber Committee will play in the coordination of initiatives, sharing of information, exchanging of lessons learnt, resources and expertise. There will also be a Cyber Steering Committee comprising the key lead agencies.

The CCSCAP also highlights the need for identifying minimum standards for Cyber Security, which would serve as a basis for all Member States, which are at varying stages of their cyber security readiness, to work towards the region developing common standards for Cyber Security. The plan will also focus on providing an up to date review of the status of the Cyber activity in each country and developing a system for regular reviews making use of existing mechanisms.

This action plan identifies five (5) priority areas of intervention for addressing Cyber Security and Cybercrime issues in the CARICOM region.

1. Public awareness;
2. Building sustainable capacity;
3. Technical standards and Infrastructure;
4. Legal Environment; and
5. Regional and International Cooperation Collaboration - Incident response, cybercrime investigation and capacity building.

Under each priority area, needs are identified, possible solutions put forward and the relevant Agencies/Partners with interest in and/or a mandate to address the specific needs are identified.

Also critical to the success of the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) is the development of Monitoring and Evaluation Mechanisms and the mobilisation of resources.

This Action Plan represents the way forward for raising awareness; building new skillsets; establishing appropriate legal and technical frameworks; establishing effective mechanisms for

responding to threats and incidents; and cultivating the global collaborative relationships, all of which are essential for improving Cyber Security and dealing with Cybercrime in the region.

2. Background

There has been significant growth in Cybercrime in the Caribbean - Government websites have been hacked, child online exploitation has infiltrated schools and the increasing use of crypto currencies to fund criminal activities are but a few of the manifestations of criminal activity in cyberspace impacting the region. According to the Commonwealth "Major cybercrimes reported in the region to date include the theft of $150 million from an international bank in 2014; individuals claiming to be local ISIS supporters hacking government websites in 2015; and, in the same year, hackers infecting tax authorities with ransomware, which blocks users from accessing their systems and demands money". These activities point to the existence of significant cyber security vulnerabilities in the protection frameworks for persons, possessions and privacy and which extend more generally to the information and critical national infrastructures. Cybercrime could have a devastating impact on national security and, if not addressed urgently, could severely hamper social and economic development of our Caribbean States.

Reference is made to the CARICOM Crime and Security Strategy, adopted at the Twenty-Fourth Inter-sessional Meeting of the Conference of Heads of Government of CARICOM, in February 2013, where ***Cybercrime*** is listed under "Tier 1 – Immediate Significant Threats" with strategic goal 8 being "Strengthening CARICOM's Resilience to Cyber Crime".

In the Strategic Plan for the Caribbean Community 2015-2019, ***Cybercrime*** is listed as an obstacle and threat to social and sustained economic development in CARICOM. Strengthening Cyber Security is seen as a strategy to achieve technological resilience but is also linked to strategies needed to achieve social resilience and citizen security.

Caribbean governments are being approached by numerous agencies with their solutions for Cyber Security and combatting Cybercrime. However, the Caribbean in its nascent stage of development in cyber security and cybercrime has been grappling with the wherewithal to navigate its way through the various capacity building efforts globally and more specifically the diversity of assistance from various international Cyber Security programs, which appear to be operating in silos. In response, the Caribbean Telecommunications Union (CTU), the Commonwealth Secretariat, the Organisation of American States (OAS/CICTE) and CARICOM Implementation Agency for Crime and Security (CARICOM IMPACS) have been collaborating to develop a comprehensive programme for Caribbean Cyber Security and Cybercrime. Recognizing that each agency has its own mandate and different areas of focus (e.g. Commonwealth Secretariat focuses on cybercrime; OAS/CICTE on Cybersecurity; CTU on ICT, including Cyber Security; and CARICOM IMPACS' mandate is Regional Crime and Security), the initiatives have been aimed at strategically coordinating efforts at the regional level.

The Caribbean Stakeholders' Meeting (CSM I) was first held in Trinidad and Tobago in May 2014, and served to raise awareness of the potential impact of Cybercrime. Commonwealth Secretariat, the OAS/CICTE and the CTU convened the meeting, which was supported by CARICOM IMPACS. At the CTU's 25th Anniversary ICT Week held in February 2015, the issue of Cyber Security and Cybercrime was again highlighted and in this case the meeting reviewed and updated the Caribbean Cyber Security Framework, which had been developed by the CTU and the OAS in 2012. Based on the recommendation of the meeting, the Commonwealth Secretariat conducted Cyber Security and Cybercrime needs assessments in five Caribbean countries and identified common needs/weaknesses, which the Secretariat concluded would be applicable to most countries given the commonality in the stage of development and regional experiences.

The second Caribbean Stakeholders' Meeting (CSM II) was convened by the Commonwealth Secretariat and CTU with support from OAS/CICTE and CARICOM IMPACS in Saint Lucia in March 2016. This meeting was designed to build on the previous initiatives and to develop a comprehensive Action Plan for Cyber Security and Cybercrime in the Caribbean; one that would holistically address all aspects of the challenges and gaps identified. Development agencies were also invited to support the process and to identify their areas of interest.

CSM II considered emerging cyber threats in the Caribbean by first presenting the results of the five needs assessments and then identifying areas of deficiency, gaps and vulnerabilities. Representatives of all other participating Caribbean countries were also given the opportunity to contribute their specific country perspective, which resulted in it being determined that the situation in terms of each country's needs was generally the same.

Delegates agreed on the following priority areas for intervention, which were very closely aligned with the Caribbean Cyber Security Framework:

1. Public awareness;
2. Building sustainable capacity;
3. Technical standards and Infrastructure;
4. Legal Environment; and
5. Regional and International Cooperation Collaboration - Incident response, cybercrime investigation and capacity building.

The meeting also allowed delegates the opportunity to propose additional elements for consideration. As a result, the process was fully consultative as the input for the plan came from the participants from the various Caribbean countries with representation at the Ministerial and senior technical level including the judiciary. Importantly delegates presented practical solutions for addressing the needs identified, which serve as the basis for this Action Plan.

As noted in the official communique from the meeting, the draft action plan, as presented, was endorsed by all attendees and commitment was given to continue working together to finalize the plan and to implement the action items as identified (Appendix 1 – CSM II Communique).

This CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) therefore represents a consolidated vision for raising awareness; building new skillsets; establishing appropriate legal and technical frameworks; establishing effective mechanisms for responding to threats and incidents; and cultivating the global collaborative relationships, all of which are essential for improving Cyber Security and dealing with Cybercrime in the region.

The purpose of this document is to provide a framework within which all initiatives of Cyber Security and Cybercrime in the region will be developed, implemented and controlled in order to ensure they are properly synchronised, duplication is eliminated and the benefit to the region is maximised.

It should also be noted that the issues of Cyber Security and Cybercrime are borderless, hence this CARICOM Cyber Security and Cybercrime Action Plan will serve as the platform for other Caribbean countries (non-members of CARICOM) to collaborate with the CARICOM Member States and Associate Member States.

3. Overview of the CARICOM Cyber Security and Cybercrime Action Plan

The CARICOM Cyber Security and Cybercrime Action Plan seeks to address the Cyber Security vulnerabilities in each participating Caribbean country and to establish a practical, harmonised standard of practices, systems and expertise for Cyber Security, to which each Caribbean country could aspire in the short and medium terms. It also seeks to build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of Cybercrime and possible linkages to other forms of criminal activity. The plan will therefore address:

i. The establishment of a proper governance framework, including a Regional Cyber Committee;
ii. The identification of minimum standards for Cyber Security for each country;
iii. An updated (desk) status review of each country;
iv. Identification of mechanisms for implementation of the relevant action items - Common Needs, Solutions and agencies/partners with interest (present or potential**)**; and
v. Monitoring and evaluation of activities to ensure that objectives are being achieved.

It should be noted that the purpose of the Action Plan is to guide and coordinate efforts within the region recognising that while this does not itemise a conclusive list of needs, it seeks to layout capacities that are needed throughout the region as a whole. It is believed that if comprehensively addressed there will be considerable improvement in the ability of the Region to respond to cyber

threats. Importantly, all agencies with interest in the area of Cyber Security and Cybercrime can use this Action Plan to guide their activities targeting the Caribbean Region.

4. Governance Structure for the Action Plan

In order to develop a structured approach, one of the first elements of the plan is the formulation of a governance structure which will be used for the implementation of the various activities to ensure proper monitoring, coordination and evaluation. This will also serve as an excellent platform for the collaboration of representatives of the Ministries with responsibility for ICT, Telecommunications, Security, Judiciary, etc., who have a vested interest in Cyber Security and Cybercrime initiatives.

Coordination Lead - CARICOM IMPACS has oversight responsibility for Regional Crime and Security with the Regional Intelligence Fusion Centre (RIFC) as one of its sub agencies that provides intelligence support to regional and international stakeholders in furtherance of the security imperatives mandated by CARICOM. Against this background CARICOM IMPACS is best placed to be the Coordination Lead for the Plan and will use its existing governance structure of, and access to, the CARICOM Council of Ministers responsible for National Security and Law Enforcement (CONSLE) and the CARICOM Heads of Government in the implementation of the Plan.

Steering Committee – The implementation of the Plan will be guided by a *Steering Committee*, comprising representatives from the following organisations, which have already been collaborating to ensure that all activities in the area of Cyber Security and Cybercrime in the region are properly coordinated and are in accordance with this Action Plan: -

- CARICOM IMPACS
- Caribbean Telecommunication Union (CTU),
- The Commonwealth Secretariat,
- The Organization of American States, Inter-American Committee against Terrorism (OAS/CICTE), and
- A representative of the Ministry of National Security from the country whose Prime Minister has lead responsibility for security in CARICOM.

The Steering Committee will also seek to continue collaboration with other organisations with interest in the area of Cyber Security and Cybercrime (e.g. International Telecommunication Union (ITU), INTERPOL, etc.).

It will act in an advisory capacity to the Regional Intelligence Fusion Centre (RIFC). Steering Committee member organisations will also implement projects as seen necessary within the ambit and scope of their own mandates in accordance with this Action Plan.

At the Regional Level – Given the need for a regional approach as it relates to Cyber Security and Cybercrime, the role of CARICOM IMPACS' ***Regional Intelligence Fusion Centre (RIFC)*** will be expanded by improving its capacity to monitor Cyber Security and Cybercrime as it increases its sphere of regional intelligence analysis.

To support the RIFC, a ***Regional Cyber Committee (RCC)*** will be formed. Membership of the RCC will be National Cyber Points of Contact (NCPOC) from each participating territory. The RCC will be chaired by a representative of CARICOM IMPACS, who will therefore bring together and coordinate the NCPOCs. The responsibilities of the RCC will be to: -

1. Serve as the mechanism for the sharing of information as it relates to cybercrime activities (with possibly links to other criminal activities) nationally and/or regionally;
2. Serve as a mechanism for the exchange of lessons learnt, resources and expertise as they relate to cyber security and cybercrime from a regional perspective;
3. Be an effective mechanism that will aid in the coordination of projects aimed at sustainable capacity building initiatives;
4. Disseminate information, through the NCPOCs, ensuring that each member of the Committee is responsible for the communication and coordination within the jurisdiction which they represent as it relates to the activities of the Committee. This will also entail working along with other stakeholders and other points of contact personnel within their jurisdiction (e.g. OAS/CICTE – National Points of Contact); and
5. Provide relevant reports to the various stakeholders including the Steering Committee, IMPACS Standing Committees, CONSLE, etc.

At the National Level – Each member state will be required to nominate two (2) ***National Cyber Points of Contact (NCPOC)***, who will serve as members of the RCC. These individuals should be senior level officials with the authority to both represent and make decisions on behalf of their respective countries. Given the cross-cutting nature of Cyber related issues representatives may be chosen from any area, however it is recommended that consideration be given to: -

i. Law enforcement authority, intelligence agency or military unit nominated by the appropriate national security authority
ii. Ministries responsible for ICT and Telecommunications
iii. Parliamentary Sub-Committee
iv. Judiciary

These representatives will serve as the main focal points for the purposes of this action plan and their responsibility will be to represent their member state as it relates to:-

1. Establishing and leading a national community of practitioners;

2. Gathering of relevant information so as to provide status updates on Cyber related projects and activities;
3. Collating information as it relates to incidents, experiences and lessons learnt; and
4. Identifying national resources and expertise.

5. Identification of Minimum Standards for Cyber Security

Currently Caribbean countries are at varying stages in their Cyber security efforts, in terms of its ability to secure its cyberspace and withstand or address cybercrime incidents. In an effort to adopt a regional collaborative approach and to maximise our limited resources there is a need to identify some initial standards or baselines to be used for the evaluation of each country.

As such, the first main task of the Regional Cyber Committee (RCC) will be to analyse the priority areas identified in CSM II and subdivide each one into a number of specific areas. Minimum standards will then be identified for each of the specific areas, and these will form the baselines against which each country will be evaluated and continuously monitored.

For example: -

Priority Area	Specific Areas	Minimum Standard
Legal Environment	National Cyber Security Policy	Law enacted/Approval Obtained
	National Cyber Security Strategy	Approved
	National Cyber Security Authority	Established
	Data Privacy Act	Legislation enacted
Public awareness	Government Ministers	One off sensitization
	Government Officials	One off sensitization
	Public Sector	Media Campaign established
	Private Sector	Campaign established as part of CSR
	Schools	School Awareness Program implemented at various levels

6. Update and Status Review

An effective Action Plan for the Caribbean must include steps to ensure that there is an understanding of the current state of Cyber Security and Cybercrime in each country. While there

have been a number of assessments/studies conducted within the region, the environment is very dynamic and continues to evolve.

The update and status review will entail a desk analysis of the recent assessments/studies and a comparison of the results to the minimum standards as identified in item (5) above with the aim of constantly updating and documenting the progress/status within each country. This information will then be supplemented by feedback from the National Cyber Points of Contact (NCPOC) and will facilitate the identification of gaps in each country.

The following provides a listing of the recent studies completed which will be used to form the basis of the assessment: -

1. OAS and Symantec – June 2014 - Latin America and Caribbean Cyber Security Trends
2. OAS and Trend Micro – 2015 – Report on Cybersecurity and Critical Infrastructure in the Americas
3. OAS and IDB – 2016 - Cybersecurity – Are we ready in Latin America and the Caribbean?
4. Commonwealth Secretariat – 2014 - Cyber Security Needs Assessments in Five Countries

The output of this phase will be: -

1. An updated report outlining a gap analysis for each country
2. A mechanism for constantly updating this gap analysis based upon initiatives implemented
3. A mechanism for periodic reporting on the status of each country through the Regional Cyber Committee (RCC).

7. Identification of mechanisms for implementation of the relevant action items - Common Needs, Solutions and agencies/partners with interest (present or potential)

The output of CSM II identified five (5) priority areas for intervention together with associated common needs and possible solutions which serves as the basis for this Action Plan. The priority areas are: -

1. Public awareness;
2. Building sustainable capacity;
3. Technical standards and Infrastructure;
4. Legal Environment; and
5. Regional and International Cooperation Collaboration - Incident response, cybercrime investigation and capacity building.

The following provides details as it relates to each priority area, the common needs, possible solutions and in some cases implementing partners who may be doing work or have an interest in

the identified need. (It should be noted that this is not a conclusive list of the potential implementing partners *. While some current and possible agencies/partners have been identified, others may exist that were not identified at the time of the finalization of this Action Plan): -

7.1. Public Awareness

An effective Cyber Security framework requires that all individuals and organisations be aware of the issue of Cybercrime and the need for a culture of Cyber Security. Public awareness is a collective responsibility of all stakeholders and therefore requires different approaches to ensure that the message of Cyber Security reaches all citizens.

Table 1 – Public Awareness – Needs, Solutions and Agencies/Partners with interest

Ref	NEEDS	SOLUTION	AGENCIES/PARTNERS WITH INTEREST (PRESENT OR POTENTIAL)*
1	Development, publication and dissemination of a public awareness strategy as a component of the National Cyber Strategy. This will also include the relevant Legislative elements.	Undertake the development, publication and dissemination of national cyber strategy	Council of Europe (CoE) – Cybercrime (T-CY) OAS/CICTE
2	Awareness raising amongst senior officials, ministers, parliamentarians and policy makers on the issues of Cyber security and cybercrime and the importance of policy and legislation	• Conduct regional awareness raising sessions targeting senior officials, ministers, parliamentarians and policy makers. • Establish an Academy of ICT Essentials for Government Leaders using UN cyber security standards at the broader level and localized for adoption by Member States	CoE OAS/CICTE ComSec UNODC
3	Comprehensive Cyber Security and Cybercrime Awareness Program for all levels of society	• Develop a media campaign involving print & electronic media. Revise school curriculums to support/promote a cultural change. For example cyber security could be adopted as part of the UWI management	Media Houses Caribbean Broadcasting Union (CBU) Caribbean Examination Council (CXC) Financial Institutions

		program as well as part of CXC and CAPE programmes • Encourage companies to adopt cyber security awareness mechanisms as part of their Corporate/ Social Responsibility	Telecommunication Providers Telecommunication Regulators

7.2. Building Sustainable Capacity

The security of national networks as well as the prevention, detection and prosecution of Cybercrime requires a wide range of skills. In order to ensure relevance in the dynamic area of cyber security and cybercrime, it is important that skills are not only developed, but that such expertise is continuously upgraded.

Table 2 – Building Sustainable Capacity – Needs, Solutions and Agencies/Partners with interest

Ref	NEEDS	SOLUTION	AGENCIES/PARTNERS WITH INTEREST (PRESENT OR POTENTIAL)*
1	Enhance training for judges and prosecutors in electronic evidence and cybercrime	• Conduct regional training workshops and ensure maximum participation • Include Cyber Security as part of law school curriculum	• CoE - Cybercrime (T-CY) Committee of the Council of Europe, • Comsec • OAS/REMJA (Ministers of Justice and Attorneys General of the Americas) training programs • Regional International Law Enforcement Academy (ILEA) programs (USDOJ) • Canada Dept of Justice
2	Training for law enforcement first responders, investigators and prosecutors in the areas of electronic evidence gathering, preservation and presentation; ensuring that proper chain of custody is	• Conduct training courses geared towards law enforcement first responders and investigators • Upgrade of curriculum at police training colleges/academy	• OAS/REMJA (Ministers of Justice and Attorneys General of the Americas) training programs • OAS/CICTE • UNODC

	maintained in cases of cybercrime	• Conduct training courses geared towards prosecutors and members of the judiciary	● CoE - Cybercrime (T-CY) Committee of the Council of Europe, ● Regional International Law Enforcement Academy (ILEA) programs (USDOJ)
3	Develop capabilities in cyber security and cybercrime for Information Technology staff (including the area of National Critical Infrastructure entities)	• Conduct and ensure participation in regional training opportunities and request assistance from international partners • Establishment of a regional academic centre of excellence focused specifically on cyber security and cybercrime • Standardize basic components of training programs among institutions and customize, where necessary, according to how the country is structured • Cooperate with UWI and other tertiary institutions to establish courses in cyber security and cybercrime	• UWI and tertiary institutions • Private Sector Companies/Providers of critical infrastructure • OAS/CICTE
4	Crisis Management	• Review of existing training initiatives in this area to ensure that cyber security and cybercrime are included as areas of threat • Ensure that crisis management is included in other forms of training as it relates to cyber security and cybercrime	• CDEMA • CARICOM IMPACS • EU/EEAS
5	Change Management - In order to include cyber security and cybercrime as part of public thinking it will require significant change	Include change management practices as an aspect of all training programmes. This process will: ○ Reduce the impact of changes;	

	management as it entails changing the culture of organisations, communities and people	○ Identify new issues and risks as a result of changes raised; and ○ Ensure that changes do not negatively affect the ability to achieve the objectives of the various activities.	

7.3. Technical Standards and Infrastructure

This forms the backbone of all information systems. In order to ensure that information can be communicated across networks in a secure manner, appropriate technical standards and infrastructural requirements need to be identified and adhered to by all stakeholders.

Table 3 – Technical Standards and Infrastructure – Needs, Solutions and Agencies/Partners with interest

Ref	NEEDS	SOLUTION	AGENCIES/PARTNERS WITH INTEREST (PRESENT OR POTENTIAL)*
1	Ensure that networks are properly configured and that the appropriate infrastructure is used	Implementation of international standards in the configuration of network	• CTU • ITU
2	Development of policies and procedures to facilitate the effective detection, diagnosis, remedying and review of cyber-attacks (including National Critical Infrastructure entities) (May also have a Capacity Building Component)	• Adopt and comply with ISO Standards (including training) • Adopt a top down approach to policy development and include civil society and the internet society in setting standards	
3	Increase use of cyber forensic software	• Updating of cyber forensic software licenses • Increase the number of cyber forensic labs available • Training in the use of cyber forensic software	OAS/CICTE

7.4. Legal Environment

In order for security to exist there must be adequate legislative controls. Cybercrime is a multi-disciplinary and complex issue and as a result the introduction of a legislative framework plays a key role in the Action Plan. This framework should include legislation focused on Cyber Security elements and crime prevention as well as the appropriate mechanisms to allow for lawful prosecution in the event that there is a breach of the security elements. Harmonisation of legislation among Caribbean states in the fight against Cybercrime is also widely recognised as a critical key for success.

Table 4 – Legal Environment – Needs, Solutions and Agencies/Partners with interest

Ref	NEEDS	SOLUTION	AGENCIES/PARTNERS WITH INTEREST (PRESENT OR POTENTIAL)*
1	Development, publication and dissemination of a National Cyber Security Strategy in each Caribbean country. This forms the basis of addressing the issue Cyber Security and Cybercrime as it makes a national statement as to how the country intends to address the issue of Cyber Security which then impacts on the issue of Cybercrime.	Undertake the development, publication and dissemination of National Cyber Strategies.	• OAS/CICTE
2	Enactment of appropriate Cyber legislation	• Develop and/or review existing draft legislation • Identify champions to move draft legislation towards enactment • Utilise Commonwealth Computer and Computer related Crime Model legislation or use Budapest Convention as the basis for national cybercrime legislation	• Cybercrime (T-CY) Committee of the Council of Europe • OAS/REMJA (Ministers of Justice and Attorneys General of the Americas) training programs • Commonwealth Secretariat

		• Countries which have enacted legislation can also be used as models and/or assistance	
3	Establishment of effective data retention legislation which balances public safety with human rights, privacy and data protection regimes	Identify countries with existing legislation (e.g. DR) and use as model for development	• OAS/REMJA (Ministers of Justice and Attorneys General of the Americas) training programs • UNODC • Cybercrime (T-CY) Committee of the Council of Europe • Commonwealth Secretariat
4	Develop a mechanism and infrastructure for dealing with online child pornography While there are many facets of Cyber which need to be included and addressed this element was specifically singled out because of the high level of interest which it generated in the assessments	• Develop the appropriate legislation. • Develop and adopt a national or regional online reporting mechanism. • Develop appropriate response mechanism.	CoE

7.5. Regional and International Cooperation Collaboration - Incident response, cybercrime investigation and capacity building

While we seek to improve the capacity and capability of Caribbean countries to secure their network and cyber infrastructure no amount of security will totally prevent the occurrence of cybercrime or incidents. As such there is also a need to plan response mechanisms so as to minimise the effect of such incidents should they occur. Additionally, because of the varying level of the risk/threat of cybercrime and incidents across the region and the borderless nature of such activity there is a need for a national as well as a regional approach to address such situations.

Table 5 - Regional and International Cooperation Collaboration – Needs, Solutions and Agencies/Partners with interest

Ref	NEEDS	SOLUTION	AGENCIES/PARTNERS WITH INTEREST (PRESENT OR POTENTIAL)*
1	Establishment of Computer Emergency/Incident Response Teams (CERTs) at a national level	Request assistance from international partners to establish CERTs at the national level. However due to lack of capacity and capability, a regional hub should also be explored for some countries.	ITU OAS/CICTE
2	Improved cooperation between national CERTs	Utilise OAS collaboration platforms and participate in ITU cyber drills.	• OAS/CICTE • UNODC
3	Develop mechanisms for the pooling of forensic resources across the region	Consider development of regional collaboration agreement to share technical resource	CARICOM IMPACS
4	Improved informal international cooperation between law enforcement agencies	• Ensure participation in Commonwealth Network of Contact Persons, Interpol and other networks offering assistance in the investigations of cybercrime and related offences • Establish 24/7 network for law enforcement points of contact for electronic evidence (USDOJ)	• OAS/REMJA (Ministers of Justice and Attorneys General of the Americas) training programmes • UNODC • Cybercrime (T-CY) Committee of the Council of Europe • Commonwealth Secretariat • CARICOM IMPACS
5	Intelligence Cyber Security Framework	• Establishment of Regional Cyber Committee (RCC) – coordinated by CARICOM IMPACS - Regional Intelligence Fusion Centre (RIFC) and	• CARICOM IMPACS • Commonwealth Secretariat

		comprising the National Cyber Points of Contact (NCPOCs) • Build capacity at the RIFC through training and equipment acquisition to further develop this Regional Agency.	
6	Establishment of a Regional Capacity Centre for Cyber Security and Incident Response	• Identify the skill set required • Identify the Human Resources within the Caribbean Region • Provide the relevant Training • Develop mechanism/SOP for operations	• CARICOM IMPACS • Commonwealth Secretariat • ITU • OAS/CICTE

8. Monitoring and Review

In recognition of the fact that some of the activities, as outlined above, are long term and that approaches to Cyber Security and Cybercrime must be continuously developed, the need for decisive action and the implementation of immediate "quick wins" cannot be overemphasized. It should also be noted that some activities are already in progress and are in alignment with this action plan (e.g. Strategy development, Policy development, training, etc.).

Based on the input of the representatives of the Caribbean countries at CSM II, it is clear that there is a need for a structured approach in order to ensure that all activities are adequately coordinated, that there is no duplication of effort and that resources are effectively used. Based on the aforementioned, there is the need to ensure that the Action Plan is constantly monitored and reviewed. This will also ensure that the plan is appropriately amended in response to the changing environment.

The monitoring and review process will include the following elements: -

1. Periodic reports from the RCC to the Steering Committee through the Regional Intelligence Fusion Centre (RIFC), which is responsible for coordinating the activities of the RCC.
2. Meeting of the Steering Committee – The Steering Committee will meet on a mutually agreed schedule to review the work being done by the RCC and make appropriate recommendations for appropriate action by the RIFC. It should be noted that the Steering Committee will only function in an advisory capacity.
3. CSM Meetings – The Steering Committee will seek to host Caribbean Stakeholders Meetings (at least annually), in order to update all stakeholders on the work being

done in the area of Cyber Security and Cybercrime in the region, to seek the input of stakeholders in a structured manner and to update the Action Plan, if required.

4. Report to Heads of Intelligence and Financial Investigative Units – As part of the CARICOM framework for the management of crime and security, one of the Standing Committees which provides direction to CARICOM IMPACS and its Sub Agencies is the Heads of Intelligence and Financial Investigative Units. As such the work of the RCC will be of significant importance to this standing committee, the feedback from which will form part of the monitoring and review aspect of this Action Plan
5. Report to CONSLE – CARICOM IMPACS reports to CONSLE on all aspects of its operation and will also report on the progress of activities as they related to the implementation of this Action Plan

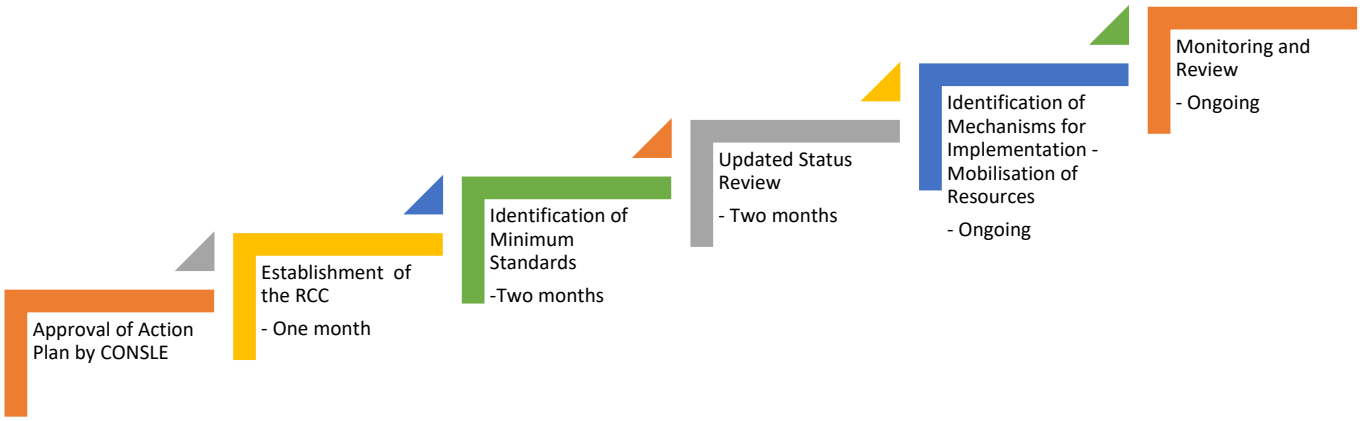
9. Funding

While various entities have already begun work in the region in terms of Cyber Security and Cybercrime, this Action Plan seeks to facilitate and enable a coordinated approach to these efforts. Activities already completed or in progress would have already received funding from various sources. It is anticipated that national governments and corporate entities will fund some of the country specific needs. However, this comprehensive Action Plan will provide additional justification for regional agencies (including members of the Steering Committee) when they seek international funding for regional projects not currently funded. Preliminary discussions have already been conducted with some funding agencies by the Steering Committee and some initial indications of their areas of interest collected and collated.

10. Time Line

It is expected that with concerted efforts of the key stakeholders, the activities outlined in this action plan can take place within five (5) years. Its achievement will certainly be affected by a number of factors including the availability of resources (finance, human and technical) the support of multiple stakeholders. While some estimated timeframes have been assigned, the Steering Committee will make use of the monitoring and review elements as outlined in item 8 above to ensure that all activities are coordinated in accordance with this Action Plan and that the needs as outlined are appropriately addressed.

Figure 1 – Estimated Time Line



11. Conclusion

The Action Plan involves five (5) priority areas each of which have been broken down into specific needs and associated solutions with the identification of possible Agency/Partners with the relevant interest. It has been made clear from consultations no one need or priority area can address the issue of Cybersecurity and Cybercrime.

What is required is the development of an ecosystem within which all solutions will be implemented to address the needs as identified. The adoption of a multi stakeholder approach is required with input included from civil and internet societies being driven from top down with the appropriate champions to the cause.

As indicated earlier, the issue of Cybercrime is borderless and as such collaboration and coordination from a regional perspective is also required in order for the battle to be won.

APPENDIX 1

The Caribbean Stakeholders Meeting on Cybersecurity and Cybercrime (CSM-II), Saint Lucia 16-18 March 2016

GROS ISLET, COMMUNIQUE

Ministers, high level justice, national security and telecommunications sectors officials, regulators and stakeholders, in charge of the management and administration of cybersecurity and cybercrime of the Caribbean Region, met in Gros Islet, Saint Lucia, from 16 to 18 March 2016 under the auspices of the Commonwealth Cybercrime Initiative in collaboration with the Caribbean Telecommunications Union and the Caribbean Community Implementation Agency for Crime and Security. The meeting identified contemporary challenges and vulnerabilities in cybersecurity and cybercrime as highlighted through the findings of Commonwealth Cybercrime Initiative needs assessments conducted in five countries in the region. The meeting considered appropriate measures and resources to address these challenges and vulnerabilities through a collaborative approach and the development of a draft regional action plan towards effectively tackling the threat of cybercrime in the region.

The meeting:

NOTING with appreciation and gratitude the invaluable support of the Government and people of Saint Lucia, the Commonwealth Secretariat and the Caribbean Telecommunications Union, the Caribbean Community Implementation Agency for Crime and Security, and other partners;

RECALLING the adoption of the Regional Crime and Security Strategy of the Caribbean Community Heads of Government in February 2013 and Strategic Goal 8 of that Strategy which focuses on strengthening the resilience of the Caribbean Community to cybercrime;

RECALLING also the first Caribbean Stakeholders' Meeting held in Port of Spain, Trinidad and Tobago in May 2014, initiated by the Commonwealth Secretariat and supported by the Caribbean

Telecommunications Union, the Inter-American Committee against Terrorism of the Organisation of American States, and the International Telecommunication Union, and its outcomes, which formed the basis of the deliberations of the meeting;

MINDFUL of the rapid growth of internet and mobile penetration in the Caribbean region, with the attendant risk of cyber vulnerabilities and attacks in the region;

MINDFUL also of the needs assessments conducted by the Commonwealth Cybercrime Initiative in 5 countries of the region, which identified good practices, challenges and gaps in ensuring effective cybersecurity and combating cybercrime;

WELCOMING the initiatives of governments of the region in the development of e-Government and other technologically enabled services for efficient and effective service delivery to citizens;

CONSCIOUS of the harmful and devastating socio-economic impact of cybercrime and cyber-attacks on businesses, governments, and the lives of individuals in the region;

RECOGNISING the need for regional collaboration to harness and mobilise resources to jointly tackle cyber vulnerabilities and threats to the region;

1. *Acknowledges* that implementing effective cybersecurity and preventing and combating cybercrime requires a multi-sectoral approach, involving the development of strategies, legislation, criminal justice and information communication technology expertise, awareness raising, and international cooperation, and involves political, private sector, and civil society leadership at the highest level;

2. *Agrees* to work towards strengthened regional cooperation in the prevention and combating of cybercrime in the Caribbean, including *inter alia* through designation of national focal points for cybercrime and electronic evidence for the purposes of the Commonwealth Network of Contact Persons, as well as active participation in that Network;

3. *Requests* countries within the region to work together by utilising virtual community platforms to share information on strengths, successes and good practices, in particular as regards the development of a national cybersecurity and/or cybercrime strategy, legislation, capacity enhancement and training needs;

4. *Endorses* the draft Action Plan, attached hereto, and confirms the commitment of governments, international organisations, private sector organisations, and all stakeholders represented at the meeting to work towards the finalisation of the Plan, and implementation of the actions identified therein, in a spirit of partnership and mutual cooperation, as well as through the exchange of knowledge and experience;

5. *Welcomes* the work of the Commonwealth Cybercrime Initiative and *requests* the international organisations represented at the meeting, including *inter alia*, the Commonwealth Secretariat, the Caribbean Telecommunications Union, the Caribbean Community Implementation Agency for Crime and Security, the Organisation of America States, Interpol, International Telecommunications Union and the Council of Europe, to work closely with governments, the private sector, and other stakeholders to provide technical support and assistance for implementation of the draft Action Plan in accordance with the individual needs of countries.