Cybersecurity in the Commonwealth: Building the Foundations of Effective National Responses in the Caribbean

08 March 2019
Introduction

The April 2018 Commonwealth Heads of Government Meeting (CHOGM), held in London, saw the creation and the adoption of the Commonwealth Cyber Declaration (‘the Declaration’). The Declaration outlines the framework for a concerted effort to advance cybersecurity practices to promote a safe and prosperous cyberspace for Commonwealth citizens, businesses and societies.

In this context, Chatham House’s International Security Department (ISD) embarked on a new project, Implementing the Commonwealth Cybersecurity Agenda, in June 2018. This initiative aims to develop a pan-Commonwealth platform to take the Commonwealth Cyber Declaration forward by means of a holistic, inclusive and representative approach. The objective is to improve cyber policymaking by broadening knowledge. To achieve this, the project has the following objectives:

1. Initiating a structured dialogue on cyber capacity-building in the Commonwealth, based on ongoing initiatives under the Declaration to discuss progress, challenges, mitigation measures and best practices;

2. Creating an informal network that connects key Commonwealth policy influencers with capacity builders and sources of expertise at Commonwealth and global levels; and

3. Sharing and developing a common understanding of best practices.

The main project activities include four workshops and subsequent reports summarizing the main discussion points, conclusions and key considerations.

The first three workshops and reports will focus on one of the three pillars of the Declaration. The fourth and final workshop and report will build on the previous outputs and provide an overview of the progress achieved in 2018–20 in respect of the Declaration by the UK Foreign & Commonwealth Office’s (FCO) Commonwealth Cyber Programme.

Workshop 2 summary

The second workshop of this project took place in Barbados, on 8 March 2019, under the title ‘Cybersecurity in the Commonwealth: Building the Foundations of Effective National Responses in the Caribbean’. The workshop considered the second pillar of the Declaration – Build the foundations of an effective national cybersecurity response – and its eight action points.

The participants at this workshop included representatives of the public and private sectors from Caribbean countries, as well as regional and international organizations conducting work in the Caribbean. The workshop was made up of four thematic sessions.

---

2 The first workshop under this project was held on the 4th of October 2018 at Chatham House in London addressing the issue of Supporting Economic and Social Development and Rights Online. For the workshop’s summary, see https://chathamhouse.soutron.net/Portal/Default/en-GB/RecordView/Index/182669
3 For workshop agenda, see Annex.
Session 1: Cybersecurity capacity-building in the Caribbean: Gaps & opportunities

Session 1 of the workshop focussed on the challenges faced by Caribbean countries in developing their cybersecurity capacities, including the financial constraints and difficulties in gaining political buy-in. The session outlined how cooperation on a national, regional and international basis can help fill some of the gaps in capacity-building in the Caribbean.

Key discussion points

- Cooperation in cybersecurity capacity-building in the Caribbean is vital to protect the countries relatively small economies. Caribbean countries should not operate in isolation from one another but rather assist each other, share information and follow the same best practices.
- Capacity-building is difficult to address when cybersecurity is not a priority for governments of some developing countries with limited budgets. Some Caribbean countries, for example, need to prioritize investment in housing, protection from natural disasters, or improving the physical security of critical infrastructure, before they can invest in cybersecurity. Therefore, the provision of international support to Caribbean cybersecurity capacity-building is essential.
- Cybersecurity capacity-building requires investment and momentum. Therefore, the political leadership of a country must be convinced of the importance of cybersecurity and of the risks of not prioritizing it. Political support for prioritizing cybersecurity must be maintained throughout political change, which was highlighted as a salient issue across Caribbean countries.
- There was a consensus that the establishment of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) are vital to cybersecurity capacity-building, and at present there are few examples in the Caribbean. There was also a consensus that the level of cooperation between CERTs and CSIRTs should be heightened at the national, regional and international levels.4

Recommendations

- A repeated theme of the session, and the workshop, was whose responsible for capacity-building. For example, ‘Digital Champions’ (individuals appointed to promote the benefits of living in a digital society) were suggested as an effective means of raising awareness and driving standards – but there should be no reliance on one single measure. Capacity-building requires multi-stakeholder collaboration and a whole-society approach and it is therefore important that all stakeholders assume a degree of responsibility.
- Capacity-building initiatives already in existence in the Caribbean should be fully utilized by countries seeking to develop their cybersecurity capacities. It would be beneficial to map out the various capacity-building initiatives and programmes taking place in the Caribbean to help spread awareness of the current or potential support available to each Caribbean country. This would also help improve the level of regional and international cooperation in cybersecurity across the Caribbean, which was often highlighted in the workshop as insufficient.

---

4 Latin America and Caribbean Network Information Centre (LACNIC) has several initiatives that promote this. For example:
- LACNIC Warning Advice and Reporting Point (WARP): a point of reporting and coordination to manage cyber incidents for LACNIC members; a free of charge, confidential service to all citizens of member countries.
- LACNIC AMPARO: ‘A program that seeks to increase computer security incident response capabilities through applied research initiatives, promoting CSIRT creation, providing training at regional level, and generating collaboration opportunities, among other activities.’

Session 2: Towards a better cyber safety framework in the Commonwealth: legal, organizational and strategic

In Session 2, the discussion focussed on the importance and the challenges of national strategic cybersecurity planning and incident response capabilities in Caribbean countries. It also explored the potential for information sharing across Caribbean countries and the means of enhancing cooperation between government, law enforcement and industry on a national, regional and international basis.

Key discussion points

- Previous reports have demonstrated that cybersecurity standards in Caribbean countries have generally been low, and it was acknowledged during the workshop that the region is susceptible to cybercrime. However, several projects are attempting to establish a baseline of standards in cybersecurity across the Caribbean. For example, on a regional level, CARICOM’s Implementing Agency for Crime and Security (IMPACS) in its Cyber Security and Cybercrime Action Plan (CCSAP), contains a monitoring and evaluation component to ensure its work is current and meets the needs of the region. On an international basis, the Commonwealth is conducting several cybersecurity projects in the Caribbean including the Commonwealth Cybercrime Initiative.

- The cyber safety frameworks of Commonwealth countries do, however, need different types and levels of development. Commonwealth countries are, for example, at different stages of development and compliance with legislation: some need completely new legislation, while others are closer to complying. Part of the challenge, therefore, is to identify gaps and priorities.

- Jamaica’s recent strategic cybersecurity planning highlights some of the challenges faced by Caribbean countries in developing a cyber safety framework. Jamaica began establishing a national CERT in 2015 and today only has five approved positions – which took over three years to fill. The skills shortage in cybersecurity is a challenge faced by governments across the world, but it is especially acute in developing countries with financial constraints.

Recommendations

- The two vital components of improving cybersecurity capacity and creating a strategy are public awareness and political buy-in. Political buy-in can be gained by prioritizing cybersecurity over politics by, for example, conducting regular threat assessments. Awareness can be raised through campaigns such as Jamaica’s ‘Be Cyber Safe’, which aims to raise public awareness and promote a cybersecurity culture throughout the country’s population.

- There are unique challenges facing Caribbean (and other Commonwealth) countries and they should therefore be treated on an individual basis. It is up to the individual countries to take the advice of regional and international organizations, to make it their own and to create national schemes that improve the country’s overall cyber safety framework.

- Countries should be willing to take small steps to develop their cyber safety frameworks. It is important that countries use up-to-date, current data to support these efforts because data in cybersecurity expires quickly.

---

Session 3: Supporting a culture of cyber hygiene to foster cyber resilience

Session 3 focussed on how Caribbean countries can raise cybersecurity awareness and promote cyber hygiene, how the skills shortage in cybersecurity can be addressed, and what efforts governments can take to support businesses and their customers.

Key discussion points

- Phishing is an extremely easy and cheap form of cyberattack from which an attacker can make a good living, even with a small success rate. It is impossible to eliminate this problem entirely, as such work should be focussed on minimizing the risks by promoting a culture of cyber hygiene. Achieving cybersecurity requires a culture of public awareness and education.
- A culture of cyber hygiene can be engendered by conducting public awareness campaigns. However, several challenges of conducting these were flagged:
  - Different people respond to different messaging and not all groups of people can be targeted in the same way. Messages and incentives should therefore be tailored to different audiences – for example, different age groups.
  - There is too much focus in cybersecurity on telling people NOT to do certain things, which can serve to reinforce the behaviour that messaging is trying to curb. It is important to understand the psychology of people and what types of messaging are most effective in promoting cyber hygiene.
- From an organizational perspective, it is important to promote a culture that errs on the side of caution. It is important that individuals at all levels of the organization understand the risks because large-scale, sensitive data breaches can be designed to be triggered by any position within an organization.

Recommendations

- When developing and implementing cyber awareness campaigns, Caribbean countries could utilize and build on the existing services and advice of organizations with long expertise in this field. For example, the Cybersecurity Awareness Toolkit by the Organization of American States (OAS) provides guidance and resources for developing cybersecurity awareness campaigns. Also, Get Safe Online is delivering services to Caribbean countries in 2019–20, which are open and free.
- Caribbean countries can learn from other national cyber awareness campaigns such as Jamaica’s ‘Be Cyber Safe’ campaign. Through sharing lessons learned and best practices, Caribbean countries can create a repository of information on promoting public awareness and education in cybersecurity, which can be distributed to relevant bodies, institutions and individuals. Information that is fed into this repository need not be limited to cybersecurity knowledge, as lessons gained through other awareness and education campaigns, such as those for public health or natural disasters, can prove equally useful and provide their own unique insights.
- Continue to consider the best ways in which to communicate advice to different audiences, because raising awareness is a continual process. Focusing on education is key and cyber hygiene should be included in school curricula to ensure that future generations have appropriate cybersecurity behaviours ingrained in them.

---

Session 4: Building security from the ground up: secure by default

In Session 4, discussion focussed on the unique challenges of securing the Internet of Things (IoT), the potential means of incentivizing manufacturers and vendors to comply with standards, and how to navigate the traditional security problem of spreading user awareness.

Key discussion points

- There is an insufficient level of accountability surrounding the privacy and security dimensions of IoT devices. It was suggested that equipment manufacturers and vendors should be incentivized to comply with security and privacy standards, and that Caribbean governments should take more responsibility for IoT security as it continues to impact a growing number of citizens.
- IoT security is challenging due to a substantial privacy dimension of the amount of data collected by IoT devices.
- The burden of responsibility to understand the potential privacy and security implications of IoT devices should not be placed on the user. Rather, manufacturers and vendors need to be more forthcoming with this information, and it is up to governments to mandate and incentivize this. Users however, need to be vigilant and understand the security implications of using IoT devices.
- Participants flagged limited resources as an obstacle to promoting and implementing a secure by design approach in the Caribbean.

Recommendations

- Include IoT security and privacy issues in cyber hygiene and awareness campaigns.
- Promote public awareness of secure by design and its benefits and bring the discussion into the public arena. Doing so may incentivize manufacturers and vendors to adhere to security and privacy standards due to the implications of reputational damage.
Final remarks

Throughout the workshop, it was highlighted that events such as these are invaluable forums for facilitating information sharing between private industry, civil society, national governments and regional and international organizations. These discussions are essential preliminary steps to building cybersecurity capacity in Caribbean countries and throughout the Commonwealth, particularly in developing countries with financial constraints and other limitations on resources. However, when countries learn from each other, as opposed to operating in isolation, the process of development is quicker and more cost effective.

In each of the four sessions of the workshop, three prominent challenges arose. Firstly, there was unanimous agreement that there has been an insufficient level of cybersecurity cooperation at the national, regional and international levels in the Caribbean, particularly between national CERTs and CSIRTs. Secondly, it was repeatedly flagged that there are unique challenges facing Caribbean countries, including financial constraints and the risks of national disasters. Such constraints and risks are an additional dilemma for decision-makers when considering the allocation of resources to cybersecurity. Thirdly, there exists the challenge of tailoring messages to different audiences, both to increase the political will to invest in cybersecurity capacity and skills development, and to raise awareness among the general population of good practices of cyber hygiene.

There were, however, valuable discussions on the measures that can be taken to navigate these challenges. Broadly speaking, these emphasized the importance of making use of the existing initiatives and programmes currently available in the region, and of promoting cooperation between governments at the national and regional levels. The recognition that all organizations must understand the audiences they are trying to reach in their efforts to develop cybersecurity capacity was followed by innovative suggestions, including various forms of incentives and regulation, that can be taken forward and practised by the stakeholders in the Caribbean.

While this workshop was focussed specifically on the second pillar of the Declaration – Build the foundations of an effective national cyber security response – the conclusion of the workshop is by no means the end of the discussion on this topic within the ISD project. This pillar, and its related projects under the FCO programme, will be discussed in future activities.

Chatham House plans to convene the third workshop in October 2019. This meeting will focus on the third pillar of the Declaration: Promote stability in cyberspace through international cooperation.
Annex: Workshop 2 Agenda

08:30–09:00  Tea and coffee

09:00–09:30  Welcome, introductions and context

09:30–11:00  Session 1: Cybersecurity capacity-building in the Caribbean: Gaps & opportunities
This session will address action point (8) of pillar two of the Commonwealth Cyber Declaration: Note with concern the challenges faced by Commonwealth developing member countries, particularly less developed countries and small island developing states. Commit to invest in cybersecurity capacity-building, including through the transfer of knowledge and technology on mutually agreed terms, the development of skills and training, the promotion of education and research, awareness raising, and access to good practice.

11:00–11:30  Coffee break

11:30–13:00  Session 2: Towards a better cyber safety framework in the Commonwealth: legal, organizational and strategic
This session will address action point 1, 2, 6 and 7(i) of pillar two of the Commonwealth Cyber Declaration: (1) Note the importance and involvement of all stakeholders within their respective roles and responsibilities in the good governance of cyberspace; (2) Highlight the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime; (6) Recognize the potential for sharing of information across the Commonwealth for improving cooperation between government, law enforcement and industry, with due regard for necessary and proportionate safeguards; and (7) Commit to exploring options to deepen cooperation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities and mitigation measures.

13:00–14:00  Lunch

14:00–15:30  Session 3: Supporting a Culture of Cyber Hygiene as a way to fostering Cyber Resilience
This session will address action point 3 and 5(ii) of pillar two of the Commonwealth Cyber Declaration: (3) Commit to support businesses to implement appropriate measure to protect themselves and their customers from cybersecurity threats; and (5) Encourage investment in cybersecurity and cyber hygiene skills, and to develop skills in the workforce, particularly for women and girls, and public awareness to help the public adopt secure online behaviours and protect themselves from cybercrime.

15:30–16:00  Coffee break

16:00–17:00  Session 4: Building security from the ground up: secure by default
This session will address point 4 of pillar two of the Commonwealth Cyber Declaration: (4) Commit to work towards the development and convergence of approaches for internet-connected devices and associated services, in order to promote user security by design.

17:00–17:30  Final Remarks