UK COMMONWEALTH CYBER SECURITY PROGRAMME

A SELECTION OF SIX CASE STUDIES

APCO worldwide

Microsoft

Foreign &
Commonwealth
Office

COMMONWEALTH
UK CHAIR-IN-OFFICE 2018-20

CONTENTS

FOREWORD

It seems like only yesterday that representatives of 53 countries got together at the Commonwealth Heads of Government Meeting (CHOGM) in London in 2018, to agree a vision for strengthening national and collective cyber security. From that meeting a unique document was born – the Commonwealth Cyber Declaration.

As Chair of the Commonwealth, the UK has focused on supporting the implementation of the Declaration and we are delighted to report significant achievements. Some of these we have illustrated through a selection of case studies that best capture the depth, breadth and scale of our programme.

As we look ahead to the next CHOGM in Kigali, we will aim to build on the progress to-date in the implementation of the Cyber Declaration, and aim to support Rwanda's ICT and Innovation agenda for the Commonwealth. In doing so we will:

- reduce the threat from those seeking to harm;
- increase resilience to cyber threats;
- make the technologies we depend on more trustworthy and secure;
- strengthen Commonwealth and international cooperation; and
- promote prosperity , skills and research.

In the meantime, I do hope you enjoy reading these case studies and find them useful. I would like to take this opportunity to thank all involved in our Commonwealth Cyber Programme, including all of the countries for their various levels of support and participation, project implementers and partners, and contributions from UK government departments. And a special thanks to Microsoft and APCO Worldwide, who helped to produce these case studies.

Andrew Dinsley
Head of Programmes – Cyber Security
Foreign & Commonwealth Office

TORCHLIGHT INCIDENT RESPONSE

Establishing cyber security incident response capability across the Commonwealth

Experts and delegates at the Caribbean workshop hosted in St Lucia

THE CHALLENGE

As countries develop, access to digital systems is key. The internet enables huge opportunities for business and communication, but also some threats and risks. Every country with access to the internet needs to have strong cyber security to ensure trust – understanding the risks and being able to respond to them builds confidence within national and international communities, which is especially important for winning foreign investment and trade. At the beginning of 2018, 24 of the 40 low-and middle-income countries in the Commonwealth had no to little cyber security incident response capability. That is why the UK Foreign and Commonwealth Office (FCO), as part of the UK's commitment to maintaining a free, open inclusive and secure cyber space, partnered with the Singaporean Government and a commercial consortium, consisting of Torchlight Group, Protection Group International and Venues & Events, to support governments in developing this important capability. By bringing people together and providing technical advice, the objective is to support public and private sector bodies in the participating Commonwealth countries developand mature their own national cyber incident response capabilities.

APPROACH

To address the differences between these Commonwealth countries, three regional events were held for African, Caribbean, and Asia Pacific countries. This enabled more locally tailored and therefore fruitful discussions, as the mix of delegates present were likely to face similar issues and share experiences. This cross-pollination was important given that in many cases, countries do not normally communicate on these issues and because in some cases experiences mirrored those across rather than within a region (e.g. Caribbean and Asian Pacific island states). Each event consisted of a three-day programme, comprised of a mixture of workshops, forums, and keynote speeches delivered by experts in the field of cyber security. National delegates received tailored support, with countries with less mature incident response capabilities receiving guidance on how to establish these frameworks, whilst states with mechanisms already in place receiving support on refining and improving these. At the end of the conference, both groups came together for a final plenary session to discuss standards and best practices. Delegates from these countries also enjoyed continued access to subject matter experts through a dedicated advisory service, operating through to February 2020.

Delegates taking part in the Asia-Pacific workshop hosted in Singapore

OUTCOME

The final workshop, hosted in London, was attended by representatives from 29 out of the original 40 participating Commonwealth countries. Three of these countries (Seychelles, St Vincent & Grenadines, Kiribati) declared that they expected to formally launch their nCSIRT capability in February 2020. By September 2020, indications are that approximately 80% of those countries without an established nCSIRT capability (currently around 18) would have an operational capacity. In addition, an estimated 12 countries stated they have instituted some form of international standard in relation to cyber security –set against a project target of 4 countries. Twenty countries have so far completed a self-assessment of their current cyber security maturity, with further countries following suit in 2020.

> Twenty countries have so far completed a self-assessment of their current cyber security maturity, with further countries following suit in 2020.

PGI AFRICAN FELLOWSHIP NETWORK

Building a network of cyber policy leads and experts in Africa

Fellows attending the first regional Fellowship meeting in Accra, Ghana in March 2018

THE CHALLENGE

Africa is a large and diverse region made up of more than 50 countries. Because there are large variations in income, digital infrastructure and skills between countries, approaches to addressing cyber security across the continent are inconsistent. To tackle this the UK Foreign and Commonwealth Office (FCO), as part of the UK's commitment to maintaining a free, open inclusive and secure cyber space, partnered with Protection Group International to establish a network of cyber security policy experts in the African region. By bringing experts together and creating a network of trustworthy connections between countries, the objective is to enhance regional cyber capability and enable countries to work together on cyber issues and share expertise and best practice.

Fellow-led discussions were used to identify and agree priority work areas for the network

OUTCOME

Since its inception in 2018 the Fellowship has helped create a network cyber security leaders across Africa who are influential, have strong ideas, and are willing to support each other. The list of active participants, which grew organically from an initial short list, now counts 43 different Fellows from 12 countries, while links have also been established with key regional organisations including the Economic Community of West African States; East African Communications Organisation; Africa Search; and the New Partnership for African Development (NEPAD). Crucially, the network established by the African Fellowship programme is set to continue after the formal end of the project in March 2020 as the existing Fellows have already pledged to continue working together to build on this popular network. They have also established a new 'Women in Cyber' sub-group within the Fellowship and begun planning a pilot project which aims to pool resources and training capability between Uganda, Botswana, Zambia, Sierra Leone and Malawi.

APPROACH

In cyber security, trust is key: it facilitates the sharing of information, expertise, and development of joint solutions to shared issues. Trust-building is the central premise of the African Fellowship: the success of this initiative goes beyond the knowledge shared at its two core meetings a year, and comes instead from the formal and informal connections and ongoing dialogue developed in between.

The focus and activities of the bi-annual meetings are shaped by the participants. For example, Fellows from Sierra Leone, Rwanda and Tanzania expressed an interest in female representation and child protection in cybersecurity. This led to a decision to hold a workshop on Women in Cyber initiatives and an Online Child Protection Masterclass in 2020.

Aside from the formal meetings, the Fellows use ongoing informal communications to draw attention to issues and ask for advice. In this way the project helps create a self-sustaining network of trusted regional experts able to work on and solve joint problems and share cyber security expertise tailored to the region.

> “Since its inception in 2018 the Fellowship has helped create a network cyber security leaders across Africa who are influential, have strong ideas, and are willing to support each other.”

BANK OF ENGLAND

Enhancing cyber resilience among central banks and financial regulators

Cyber security specialists networking at London's Guildhall

THE CHALLENGE

Cyber security is vital to financial stability: if a central bank is attacked, it can impact other financial institutions as well as the wider economy and society. This was highlighted by the 2016 attack on the Bank of Bangladesh, in which a partially successful attempt to steal US $1 billion was made. The potential impacts of such incidents on ordinary people and businesses can be huge: companies may not be able to pay their workers and consumers may struggle to get cash from ATMs. As countries are so interlinked, the damage and knock-on effects could be catastrophic. Some Commonwealth countries may be seen as weaker targets because of their varying levels of cyber readiness. This is why the Foreign and Commonwealth Office (FCO), partnered with the Bank of England to promote best practices across the Commonwealth and help countries improve cyber resilience in their banking sectors. This partnership was designed to support our commitment to a free, open, inclusive and secure cyber space, as agreed in the Commonwealth Cyber Declaration.

APPROACH

A three-day seminar titled 'Beyond Prevention: cybersecurity and the resilience of the financial sector' was held in October 2019 in London. The seminar was attended by senior-banking officials from the central banks of 23 Commonwealth States. The demand for insight on these issues was so high that we are considering organising another seminar in the near future. The seminars covered cybersecurity issues from both technical and social perspectives, including the importance of appropriate regulation of the financial sector's digital networks and establishing good incident response frameworks, as well as the importance of international cooperation, stakeholder engagement and establishing strong cybersecurity cultures within financial institutions. Seminar speakers came from a range of backgrounds and organisations, including the Bank of England and other financial institutions, law enforcement and national security agencies, and a networking event hosted by the FCO at London's Guildhall also involved representatives from the Fintech industry.

Delegates taking part in the cyber security seminar

OUTCOME

Feedback for all sessions and the seminar was very positive. Participants gave the event an overall rating of 4.2 out of 5, and many shared their learning with colleagues back home afterwards. The seminar has already started to have an impact:

Dembo Sankareh, Deputy Director, Central Bank of the Gambia – *"Upon return from the BoE seminar, I made a recommendation to management to constitute a multi-stakeholder committee with a view to drafting a cybersecurity framework for the financial sector in the Gambia. The recommendation was approved and we are in the process of holding our maiden meeting".*

Jacques Henning, Divisional Head, RSD Prudential, South Africa – *"The information and experience gleaned from the seminar will assist tremendously and have a positive impact on our supervisory processes. We are now in the process of developing a cyber questionnaire that will be completed on an annual basis by our supervised entities".*

Aside from the content of the seminars, the value of this initiative came from bringing together policymakers, central bankers and regulators from a wide range of countries to share best practice and identify potential partners to help them build capacity.

> "The value of this initiative came from bringing together policymakers, central bankers and regulators from a wide range of countries to share best practice and identify potential partners to help them build capacity."

COMMONWEALTH SECRETARIAT

Strengthening cooperation, law enforcement and judiciaries across the Commonwealth

Teaching Caribbean judges, police and legal experts learn how to use electronic evidence in cybercrime cases

THE CHALLENGE

In a technology-driven world, international cooperation in cyber crime investigations is critical, not least because a large proportion of cases involve a transnational element. But while an increasing number of Commonwealth countries have programmes and legislation in place to improve resilience and tackle cyber threats, a focus on prevention alone is unlikely to be effective. Alongside this, traditional methods of policing, gathering and interpreting evidence, and prosecuting cases need to evolve to ensure that cyber crimes can be dealt with effectively across entire criminal justice systems.

Accordingly, the UK's Foreign and Commonwealth Office (FCO) provided funding to the Commonwealth Secretariat's Cyber Crime Unit to implement projects aimed at tackling cyber crime and promoting international cooperation across the Commonwealth. The Commonwealth is committed to maintaining a free, open, inclusive and secure cyber space.

APPROACH

To promote better use of electronic evidence in cross-border criminal investigations a series of workshops and exercises was held, looking at cyber crime as not simply a matter for law enforcement, but part of a shared challenge affecting different parts of the criminal justice system. The project brought stakeholders together from across the Commonwealth and provided an environment in which shared solutions to key issues could be developed. For example, law enforcement officials were asked how they would go about collecting and analysing evidence that might be on a computer or mobile device, while judges discussed the utility of different types of evidence.

Better cooperation in criminal investigations was also an ambition with the expansion of the Commonwealth Network of Contact Persons (CNCP) to improve electronic evidence sharing. Live role-playing scenarios were held at three regional events in Barbados, South Africa and Australia, to provide a forum for key contacts in Commonwealth countries to test their collaboration skills. A virtual exercise was also held to test that skills were embedded by the electronic evidence training.

Delegates from Commonwealth countries discuss the importance of international cooperation in criminal justice matters

OUTCOME

The electronic evidence training project has helped establish professional, well-trained law enforcement and prosecution services across the Commonwealth which are equipped with the resources and skills needed to address the demands of modern crime.

The Hon Justice Maria Wilson, a High Court Judge in Trinidad and Tobago stated that "I thought the final exercise, which was a practical exercise on giving evidence in Court, was very useful. It confirmed for me the point that that both Judges and Prosecutors and Police officers should be on the same page with the kind of evidence that is required to prove a cyber crime in court. This would assist Judges in assessing the relevance of evidence and consequently whether the evidence is admissible".

The project has led to the establishment of a designated focal point for electronic evidence for 47 out of 53 member countries. Eighteen countries attended a working group meeting on electronic evidence, sharing information and knowledge around the latest developments in their countries, as well as challenges and good practice in the implementation of laws on electronic evidence. A series of recommendations were agreed by Commonwealth Law Ministers leading to a revision of the Commonwealth Model Law on Electronic Evidence.

> "Judges and Prosecutors and Police officers should be on the same page with the kind of evidence that is required to prove a cybercrime in court."

ORGANIZATION OF AMERICAN STATES

Protecting democratic processes in the americas

Stakeholders from the Commonwealth gathered in the OAS' Washington D.C. headquarters to discuss regional challenges

THE CHALLENGE

The cornerstone of democracy is the electoral process, which should be **conducted in a free, fair and open environment.** However, while foreign electoral interventions have not been new, the use of technology to do so has become increasingly prevalent in recent years. Consequently, **there is a need to not only educate the public on how cyber incidents affect the electoral process, but also to develop tools** that can be useful to **politicians, citizens and the media** to secure the election system **against cyber-attacks.** To address this, the UK Foreign and Commonwealth Office (FCO), as part of the UK's commitment to maintaining **a free, open inclusive and secure cyber space**, partnered with the Organization of American States (OAS) to increase understanding of common cybersecurity challenges in the Americas. The overall **objective is to bring together stakeholders** from the 12 Commonwealth countries in the region to develop a series of **best practice guides** that can be used to enhance cybersecurity around all processes and actors within democratic societies, including **public administration, elections and the media.**

APPROACH

The project began with an initial **benchmarking exercise** of current issues and practices across all 35 independent states of the Americas. **A variety of methods** were used to develop a thorough understanding of the overall issues landscape across this broad range of countries. These included a **workshop introducing participants** to the **importance of cybersecurity efforts in democratic processes**, and a survey of countries' efforts to establish relevant **capabilities and infrastructure.**

Given the broad range of stakeholders within each member country **who could be affected by cyber threats**, the OAS then conducted a **mixture of qualitative, quantitative and desk research** to better understand the issues facing actors on the ground. Workshops were held in Oxford, UK and Washington D.C., USA with cyber incident response **teams, parliamentarians, and election commissions**, to identify **key challenges** and develop specific resources tailored to each sector and the region. Each two-day workshop followed a format of a day of presentations on **strengthening democratic processes** followed by working **group sessions**, where the contents of the best practice guide was developed.

The discussions resulted in a publication that will be available in the OAS' four official languages

OUTCOME

This best practice guide, published in **both English and Spanish by March 2020**, provides a useful resource that can be used by all stakeholders involved in democratic processes throughout the Americas. **Almost 70%** of electoral authorities interviewed **have used the recommendations developed** for the guide.

Of significant note was the level of engagement of the **key actors in the democratic process** such as policy makers, incident response teams, electoral commission personnel and ever parliamentarians. **92% of participants** reported that **they had changed their behaviour** towards cybersecurity following the workshops. In the feedback survey, one attendee wrote that "Even though my country does not yet have electronic voting, the workshop made me **realise that the more advanced we are technologically, the greater the risk".**

> "92% of participants reported that they had changed their behaviour towards cybersecurity following the workshops."

WORLD BANK

Supporting economic development in Africa through robust cyber security

Sharing experiences and lessons learned from African countries
The Gambia
Lesotho
Botswana
Ghana

THE CHALLENGE

While cybersecurity has long been recognised as important, recent high-profile incidents like WannaCry and NotPetya have highlighted the crippling effects that attacks can have on public institutions and the vital services that ordinary citizens and businesses rely on. This is of additional importance in regions like Africa, which are undergoing rapid economic and social development. With the World Bank planning to digitally enable every African government, citizen and business by 2030, as part of its Digital Transformation Initiative, ensuring countries have effective cybersecurity capabilities in place is more vital than ever.

To support the Commonwealth's commitment to maintaining a free, open inclusive and secure cyber space, the UK's Foreign and Commonwealth Office funded the World Bank to provide national cybersecurity capacity reviews based on the Cybersecurity Capacity Maturity Model for Nations (CMM) of the Global Cyber Security Capacity Centre (GCSCC) of the University of Oxford. The reviews help African and Asian Commonwealth countries to understand the maturity of their cybersecurity capacity across and priority areas for development. All Commonwealth countries committed to voluntarily undertake a review by the next Commonwealth Heads of Government Meeting (CHOGM) in Kigali, 2021. This undertaking is set out in the Commonwealth Cyber Declaration's Implementation Plan, agreed at the last CHOGM in London.

APPROACH

The World Bank's approach to developing cybersecurity maturity is premised on country ownership and commitment. As such, for each of the African and Asian countries taking part in this initiative, the World Bank encourages participating countries to take the lead in the national cybersecurity assessment. The assessment begins with desk research of each country's current cybersecurity capabilities. Key national stakeholders from different sectors then take part in focus group workshops lead by the World Bank who then develops a cybersecurity capacity and gaps analysis, and drafts a report including recommendations to increase maturity in the various dimensions of cybersecurity as defined by the CMM. These plans are verified by the participating Government and then reviewed by the GCSCC, who developed the CMM. On completion, countries can choose to publish the review report and proceed to implementation. This process puts the essential building blocks in place so that participants have a robust, country-specific cybersecurity roadmap which complements their wider economic development objectives. Regional clinics were also organised in East and West Africa to build links between countries by highlighting common challenges and opportunities and encouraging regional cooperation.

OUTCOME

This process of capacity building provides a secure foundation to support the development of the digital and physical economy in Africa. By elevating cybersecurity from solely being the preserve of the defence and security community, and making it a key part of the day-to-day work of government, African countries are able to transform their governance, public services and financial systems, and achieve wider development objectives. As a result of the capacity building and analytical assessments that are being undertaken, the World Bank has received an increase in requests from African countries to include cybersecurity components in their digital projects. These requests also include countries that were not part of the CMM assessments conducted by World Bank but either benefitted from the study tours, regional clinics or CMM done by the GCSCC or one of its other partners.

> “All Commonwealth countries committed to voluntarily undertake a review by the next Commonwealth Heads of Government Meeting (CHOGM) in Kigali, 2021.”

Since the Commonwealth Heads of Government Meeting in 2018, the UK has provided extensive support to Commonwealth countries to help them meet the commitments in the Commonwealth Cyber Declaration. Over £5m has been invested through the UK's Commonwealth Cyber Programme with 100 events in over 30 countries.

Through pan Commonwealth, regional and national level activities, the Programme has helped strengthen cyber security across the Commonwealth, creating stronger networks to exchange knowledge and expertise, raising understanding of risks, and facilitating civil society engagement. All Commonwealth countries benefited from UK cyber security capacity building activity during the UK's Chair in Office.

APCO worldwide®

Microsoft

Foreign &
Commonwealth
Office

COMMONWEALTH
UK CHAIR-IN-OFFICE 2018-20