Commonwealth island states collaborate to strengthen cyber security

Delegates to the Asia-Pacific workshop on establishing national response teams for computer security incidents in Singapore, September 2019.

Tonga has benefited from training and mentoring support (from the Commonwealth Cyber Security programme) in building its national Cyber Security Incident Response strategy. Moreover, this small state has also built relationships with other Commonwealth countries and is sharing and learning in ways that are mutually beneficial.

CHOGM THEME
A more secure future

PROJEC T TITLE
The Cyber Security Programme

COUNTRY
Tonga

IMPLEMENTING PARTNERS
Torchlight, Protection Group International (PGI)

Tonga is a Polynesian archipelago in the southern Pacific Ocean, comprising 169 islands, of which 36 are inhabited. Despite its small population of just over 100,000 people, the country is not immune to cyber security threats. "Just recently we received a 'business email compromise' where a small business in Tonga was instructed to redirect a payment – at the last minute – to a different bank account during an overseas transaction," explained Siosaia Vaipuna, the Director of the country's national Computer Security Incident Response Team (nCSIRT). Other threats faced by Tonga include botnet attacks and even more recently, the use of the coronavirus pandemic as a pretext to persuade less-informed citizens to deviate from well-established banking processes.

Commonwealth nations, to develop their nCSIRTs. nCSIRTs provide a crucial first line of defence against cyber security attacks, by establishing dedicated teams that can respond swiftly to any threats to national digital infrastructure. However, for smaller counties like Tonga, developing the capacity and specialist expertise to build an effective nCSIRT can be challenging. The Commonwealth Cyber Security Programme helped to address this issue by building relationships between member states. This encourages peer learning and collaboration as a tool to overcome their resource and capacity constraints.

T
h
e

Commonwealth 18 –20 Fund has supported Tonga, along with 40 other

Networking to solve problems

“Networking [between nations] has been a very important part of this initiative for smaller Commonwealth nations like Tonga in the Pacific, Antigua and St. Kitts in

A breakout discussion at the Asia-Pacific workshop in Singapore.

Caribbean," said Siosaia. While the focus of the project is on developing a cyber security incident response, small countries also benefited from the networking opportunities provided by the project's capacity building events. "We lack skills to develop approaches in the same way as larger countries," said Siosaia. "My division falls under just one ministry, the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Climate Change and Communications – and to address all these big issues [is challenging as] we have limited resources."

Siosaia attended two workshops run by the project in Singapore and London. The workshop facilitators, specialists in cyber security approaches, introduced Siosaia to the SIM3 self-assessment framework. This is a tool that helps countries understand their cyber security gaps.

'The SIM3 assessment took [Tonga] to the next level. It helped us see what we needed to do, the tasks and activities required to put in place a corporate plan.'

Siosaia Vaipuna

The workshops also gave Siosaia and other delegates the opportunity to meet and discuss common problems.

During one event, Siosaia was approached by another project delegate, Gordina Hector-Murrell, Director of Cyber Security for the Antigua and Barbuda Ministry of Information, Broadcasting, Telecommunications and Information Technology. In the first instance, Gordina asked Siosaia if Tonga would be willing to share their draft Cyber Crime Legislation. "She then requested information to help with job descriptions," said Siosaia. "Today we are happy to help Antigua, in the knowledge that at some time down the line, Antigua will help Tonga."

Learning by example

Good cyber security rests on having the strong systems and processes in place as well as recruiting people with the right knowledge and skill sets. Small Commonwealth nations in the Pacific and Caribbean such as Tonga, Antigua and Barbuda, and St. Kitts and Nevis must persuade their governments to prioritise cyber security and open new positions in the civil service. "Although we have people with the right skills and knowledge in the country, they don't usually have degrees. We could take them through that process, but first we have to persuade our government to open positions and then relax the rules for recruitment," said Siosaia. Degrees are mandatory at key levels. This problem of recruitment and qualifications was also raised by Ophelia Blanchard, the E-Government Coordinator in the Department for Information Technology at the Ministry of Justice, Legal Affairs and Communications in St. Kitts and Nevis, at the final nCSIRT Capacity Building Workshop, in London in December 2019. "Governments may have to change their recruitment requirements. If we can tell them that rules have been relaxed in another country that helps." Networking and regular communications ensures delegates can use examples of progress in other countries to further their own strategies.

Howie Nichol, Programme Manager from Torchlight Group (the project's implementing partner) agrees, but noted, "When it comes to networking, smaller nations like Tonga have made real gains and collaborative working is often a necessity. Larger Commonwealth countries may be more sensitive about sharing information on cyber security. Even if

'When it comes to networking, smaller nations like Tonga have made real gains.'

Howie Nichol

nations are part of the Commonwealth, it doesn't mean they will always see eye to eye." Howie, continued, "At all our capacity building events we tell delegates that there are enormous gains that can be made by building trust, working together and sharing information."

While Tonga has lent a helping hand to Antigua and Barbuda, Tonga has looked to Brunei in order to inform the development of the nation's own cyber security policy and strategy. Mr Vaipuna has been in regular contact with another project delegate, the director of the Brunei National Computer Emergency Response Team (BruCERT). BruCERT was formed in collaboration with Brunei's Authority for Information and Communications Technology Industry to become the one-stop referral agency in dealing with computer and internet-related security incidents. "In Tonga, we are very interested in Brunei because they are ahead of us… this company is a hybrid combining the private sector and the government perspectives. Tonga wants a similar centralized system for dealing with cyber security both inside government and in the private sector," said Siosaia.

Tongan government issues warning of hacked email and webcam scams.