A more cyber-resilient Pacific

by James Boorman and Joe Fulwood

7 March 2024

OCSC

It is a truth universally acknowledged that digital developments have shrunk space and time, and nowhere is this more evident than in the Pacific. The arrival of undersea cables and the availability of satellite connectivity have provided faster and more reliable access to the global digital economy, enabled progressive digitisation of government services and supported rapid digitisation in response to COVID-19.

But this improved connectivity has opened a dangerous new frontier for external aggression towards Pacific island countries (PICs), which brings with it harms already prevalent globally that jeopardise sustainable prosperity. Island nations that were once distanced from the world by vast ocean expanses now find themselves face to face with the world's most sophisticated and ruthless criminals, with limited capacity to defend themselves.

This challenge has called forth an international collective effort to lift cyber capacity across digitally advancing nations. Cyber Capacity Building (CCB) is a multi-stakeholder effort by people and communities working both locally and across countries to share skills, knowledge, and resources in order to build a safer digital environment. In the Pacific, which faces significant geographical and financial barriers to development, CCB programs are essential if local stakeholders are to strengthen their capacity to reduce cyber harms.

However, almost a decade in, the quest to strengthen the Pacific's cyber capacity has been characterised by an oversaturation of well-meaning but uncoordinated CCB activity that often duplicates effort and is rarely tailored to the local context.

Thankfully, a collective reset by many of the region's international donor partners has set the stage for a new era in CCB. In 2023, the countries that make up the Partners in the Blue Pacific (PBP) laid the groundwork for improved cyber collaboration and coordination with their Pacific counterparts.

An informal mechanism for improving support and engagement in the Pacific, the

PBP's goal is to support regional priorities under the guidance of Pacific leaders. In October 2023, the PBP invited the Oceania Cyber Security Centre (OCSC) and the Global Forum on Cyber Expertise (GFCE) Pacific Hub to organise a regional forum to help them support the cyber priorities outlined in the Pacific Islands Forum's 2050 Strategy for the Blue Pacific Continent and 2019 Boe Declaration Action Plan. Subsequently, as one of the PBP's first regional initiatives, the inaugural Pacific Cyber Capacity Building and Coordination Conference (P4C) was held in Nadi, Fiji, in October 2023.

The P4C afforded Pacific stakeholders a unique opportunity to engage in the co-design of a new framework for CCB in the region by providing space for frank discussions between donors and Pacific stakeholders. The PBP, OCSC, and GFCE Pacific Hub collectively designed a conference program that would bring together Pacific cyber leaders with the international donor community to discuss in an effective way, with Pacific needs and perspectives front and centre, the difficulties of cyber-development in the Pacific and possible solutions. The aim was to ensure discussion would genuinely inform the re-design of CCB programs to include localised priorities and insights, aligned with existing strategies.

Cognisant of the depth and diversity of expertise represented at the P4C, and in keeping with the Chatham House Rule, the organising team made careful notes on the issues, priorities, and learnings articulated. These anonymised notes were analysed for key themes to inform future CCB activity in the region. The resultant PBP P4C Outcomes Report summarises the CCB challenges discussed at the P4C under five key themes, and presents 10 recommendations to lift cyber maturity across the region. The starting point for an ongoing process of co-design between PICs and the international donor community, the Outcomes Report and its recommendations present a practical pathway toward more efficient CCB program design and delivery for the future.

Greater donor collaboration, contextualisation of interventions, and adherence to Pacific perspectives are routinely presented as the answers to cross-cutting and persistent development challenges. However, each of these things is easier said than done. The Outcomes Report presents actionable ways of implementing these generalised solutions in the CCB context.

Recommending a mix of short and long-term interventions, the Outcomes Report stands as a contextualised overview of the Pacific CCB landscape and may be used by CCB donors, recipients, and implementers as a guiding framework for designing and delivering future programs and responding to requests for support. It offers for the first time a genuinely collaborative pathway to progress that is responsive to the region's needs rather than prescriptive.

While there is no universal rulebook for improving CCB, the Outcomes Report lays the foundations for practical change in the Pacific. Now that PICs and their donor partners have this toolkit to improve the efficiency and impact of CCB, only time will tell how they use it.

Disclosures:

Joe Fulwood and James Boorman are employees of the not-for-profit Oceania Cyber Security Centre and were part of the managing team who organised the inaugural Pacific Cyber Capacity Building and Coordination Conference. They do not speak on behalf of the Partners in the Blue Pacific who funded the P4C or the GFCE who were their co-organisers.

Author/s:

James Boorman
Dr. James Boorman is the Head of Research and Capacity Building at Oceania Cyber Security Centre (OCSC).

Joe Fulwood
Joe Fulwood is the Research Project Officer and Marketing and Communication Manager at Oceania Cyber Security Centre (OCSC).

Link: https://devpolicy.org/a-more-cyber-resilient-pacific/