Cybersecurity and AI

Developing Cybersecurity Capacity in the Pacific

In conversation with Cameron Boardman, CEO, Oceania Cyber Security Centre.

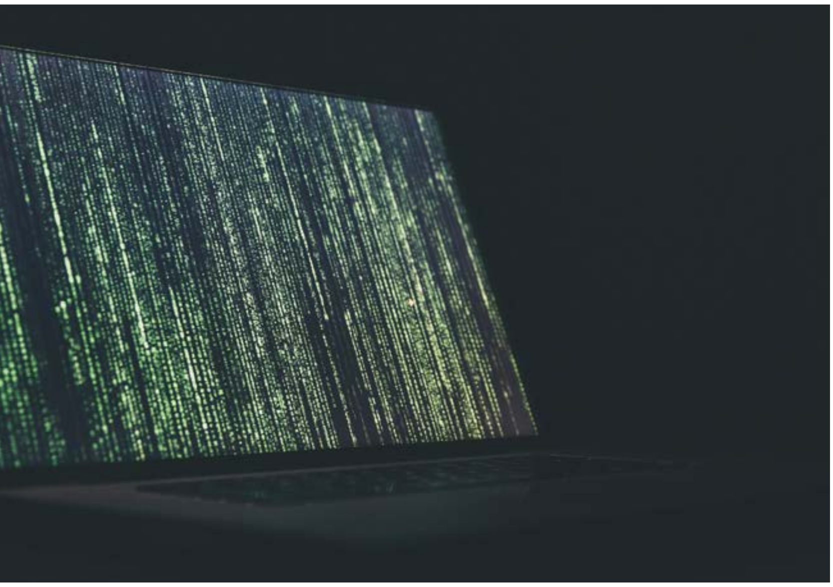
The Oceania Cyber Security Centre (OCSC) engages with industry, academia and government to conduct research, develop training opportunities and build capacity for responding to current and emerging cyber security issues in Oceania and beyond. The OCSC is the regional research and deployment partner of the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford for the Cybersecurity Capacity Maturity Model for Nations (CMM), conducting national cybersecurity capacity reviews and related research in the Pacific. In this interview, CEO Cameron Boardman discusses emerging cybersecurity threats in the Pacific region and the impact of the CMM.

What are the foremost cybersecurity challenges facing the Pacific region?

I will start with a little bit of context as to why cybersecurity is a key challenge in the Pacific. It has been a deliberate policy of the Australian government, and to some extent the US government, to invest significantly in undersea cables which connect all the Pacific island nations with the east coast of Australia and the west coast of Canada and the US. This is motivated by a desire to fulfil the UN Sustainable Development goals concerning the development of communication infrastructure and the right of access to digital technologies. This has resulted in an investment programme, running into the billions of dollars, that has given some Pacific Island nations world class connectivity.

However, small populations and still developing economies have meant that whilst many countries in the Pacific have great connectivity, they do not necessarily have the correlating skill base and expertise on the ground to effectively run these networks. What this means is that the uptake of digital technologies is quite high but public awareness, capabilities, skills, resilience, governance, management, and preparedness to respond in the event that something goes wrong is lacking. Whilst the technology to cope with a denial of service or malware attack is there, the human capabilities do not match up in a lot of instances. Even if an attack could be stopped, we then have to think about how a country's judicial and legislative processes are equipped to hold a perpetrator responsible. These capabilities are not fully developed throughout our region.

What we have seen in terms of global cyber policy for a number of years, as highlighted by the UK government in 2016, is that there is no point making investments in digital and communications technologies unless those investments correlate with on the ground skills and capability enhancement. In accordance with this, the UK adopted the concept of cybersecurity maturity which was the genesis of the Cyber Security Capacity Maturity Model for nations (CMM). This model enables a country to understand where they sit on the scale of cybersecurity maturity, allowing them to understand where they need to target investments, what policy and regulatory changes they need to make to enhance their cybersecurity posture and resilience, and how those policies and investments align to their capabilities. Without understanding the baseline of each cybersecurity dimension, you cannot have a fruitful discussion surrounding cybersecurity.



> “there is not a singular way to implement digital change and each country's specific circumstances, culture and geography must be taken into consideration at every level of the policy development phase.”

How does the Cyber Security Capacity Maturity Model for nations (CMM) framework deployed by the OCSC help nations in the Pacific assess their cybersecurity capacity to protect their national sovereignty and security?

The CMM identifies where the gaps, limitations, and spaces for improvement in a country's cybersecurity policy and infrastructure are. There are five dimensions that the CMM uses to analyse cybersecurity maturity: cybersecurity policy and strategy; cyber culture and society; building cybersecurity knowledge and capabilities; legal and regulatory frameworks; and standards and technologies.

Note that technology itself is only one of the five dimensions. Most of the areas we concentrate on focus on the human element required to ensure cybersecurity, because most successful cyber-attacks target the human element of a system. Usually, such attacks target weak passwords, susceptibility to phishing attacks, or involve grooming an individual to gain some degree of network access. Until you invest in skills and resilience in the human interface, you are going to end up having the best policies, the best standards, the best regulation and the best technology but not actually be secure.

The model looks holistically at a whole-of-government framework to analyse, under those five dimensions and two hundred sub dimensions, how developed a governments cybersecurity ecosystem is. These findings are then used to plot a roadmap for a government to address those gaps. This starts at a macro level, looking at whether a government even has a cybersecurity policy and then drills down into the minutiae of cybersecurity development.

Increasingly, countries are using the CMM as the basis for liaising with international donors, allowing them to use an evidence-based approach to request funding, rather than being told by the international community what they are going to receive funding for. This model means nations are empowered by using the CMM evidence framework to highlight the projects that are going to be the most valuable and the most impactful to them. Pacific nations do not want to be preached to and want to guide their own destiny.

What are the recurring issues detected by the CMM in the Pacific?

There are three recurring themes that usually become clear after a CMM report has been carried out in the Pacific. Firstly, most countries in the Pacific region have a low level of cybersecurity maturity. Now whilst this may not come as a surprise, before they have gone through the process of compiling the report, which necessitates having an honest discussion with themselves and identifying where their significant limitations are, nations are perhaps not as aware of their shortcomings as they should be.

The second issue is that an aspiration towards global standards, which come from documents like the Budapest convention, or the Delhi communique, or in the Pacific - the Boe Declaration, is not necessarily attainable for all nations. What we have found is that whilst international standards are ambitious, there is no one size fits all policy and there has to be an honest assessment of the incrementality of change that countries are capable of making.

The third recurring theme is that even though there is an increasing capability through networks of global cooperation to detect cyber-attacks, the legislative and regulatory frameworks to do anything about such risks, even when a threat actor is clearly identified, are underdeveloped. This is not just a problem in developing nations and is something that advanced western democracies are struggling with as well. The Australian Federal Police, for example, have investigated cybercrimes over many months, even years and built a compelling evidence base, yet fail to secure successful prosecutions because the legislation and regulation is not responsive to the digital or technical elements of the crime itself. Improving judicial understanding of the technical aspects of a crime is also a challenge.

Do Small Island Developing States in the Pacific region face unique cybersecurity challenges?

One thing that you have to consider when thinking about the Pacific is that every country is a collective of cultures and subcultures, and languages and sub-languages. Whilst English is a standard, it is not necessarily the societal language and, in some cases, you still have levels of village or tribal regulation. Often the norms of the past have not been adapted or adjusted into what we consider a modern framework. Coupled with a significant technology change, this can create challenges. We have to acknowledge that many nations in the Pacific are not cyber-mature and that their digital transformation is very embryonic.

There is also the key issue that there is not a singular way to implement digital change and that each country's specific circumstances, culture and geography must be taken into consideration at every level of the policy development phase. Whilst this is true of many regions in the world, these issues are intensified due to the Pacific's geographical isolation, very small population, low GDP and significant dependency on international aid, not just as it relates to digital improvement but for all of their infrastructure development. Couple this with an occasionally volatile political environment, and you are faced with a cocktail of complication.

We have found on the positive side, that almost without exception, there is a genuine enthusiasm within the seven countries that we have deployed the CMM model and in the six that are lining up to do it, to learn about how cyber maturity can be improved and what they need to do to invest in their people, systems, and skills. There is a very strong partnership mentality whereby Pacific countries understand that they cannot develop these capabilities in isolation and that they need to learn from Australia, New Zealand and fellow Pacific states that have been through the process so that they can share expertise on a basis that prioritises continuous improvement in each states' cybersecurity posture and resilience.

> “Until we get the basic fundamentals of appropriate regulatory systems that can adequately respond to violations, it is going to be very difficult to improve cybersecurity world over.”

PAPUA NEW GUINEA
NAURU
KIRIBATI
KIRIBATI
SOLOMON ISLANDS
TUVALU
TOKELAU
SAMOA
WALLIS AND FUTUNA
AMERICAN SAMOA
FRENCH POLYNESIA
VANUATU
FIJI
NIUE
TONGA
COOK ISLANDS
AUSTRALIA
NEW CALEDONIA
NEW ZEALAND

Commonwealth countries in the Pacific/Oceania

How is the dynamic threat environment in the Indo-Pacific impacting the cybersecurity of Commonwealth nations in the region?

It goes without saying that the Belt and Road style-initiatives are very attractive. They represent a lot of money and a lot of political influence, sometimes particularly apparent in Pacific political dynamics.

It is true that because of the sophistication and technology of submarine telecommunications cables a number of the Pacific Islands whether knowingly or otherwise have been used for proxy attacks into Australia, Canada, New Zealand, and the United States. This takes us back to the core reason why establishing cybersecurity and the correct skill base is so important, it is because these types of activities may be occurring without a given state's knowledge, and even if they do know, they may not be able to respond or prevent it.

This is a real-life scenario, there are a number of Pacific Islands who have had their broadband networks invested in through Belt and Road type initiatives. It is not for me to say whether this has led to an increase in activities which may not adhere to global standards, values and legislative standards, however evidence would suggest presence of threat actors. More recently, pre-Covid, there was a hack on the parliament of Australia, which the Australian government openly stated was sponsored by China, which China has not denied. If a developed and well-resourced organisation such as the Parliament of Australia can be susceptible to such an attack, you can imagine how difficult it can be for less developed organisations to cope.

If you could implement just one policy to improve cybersecurity capacity in the Pacific, what would it be?

I think the most significant limitation we face at the moment in tackling cybercrime is in law enforcement and the judiciary, not just in the Pacific, but across the globe. Until we get the basic fundamentals of appropriate regulatory systems that can adequately respond to violations, it is going to be very difficult to improve cybersecurity world over. Implementing these sorts of policies is difficult. We have witnessed effective policy be put in place in the commercial sector that has curbed malfeasant activity. For example, when British Airways faced a GBP183m fine for the breach of its security systems in 2018. Whilst British Airways stated at the time that hackers had carried out a "sophisticated, malicious criminal attack" the British Information Commissioner's Office defended the record fine by stating that companies have a fundamental obligation to protect individual privacy rights and that increased scrutiny will be applied to those who don't take appropriate steps. Therefore, companies are making sure that they are obeying the rules and thinking about privacy, data protection and security. I would like to see similar policies come into play in the international arena as they are the key to tackling international cybercrime in consistent adherence to global standards at all levels including government, industry and civil society.