
PaCSON
PACIFIC CYBER SECURITY OPERATIONAL NETWORK
ANNUAL REPORT
2020

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CONTACT DETAILS AND FEEDBACK

Feedback about this report is welcome, and should be directed to:

The PaCSON Secretariat: pacson.secretariat@defence.gov.au

Table of Contents

From the Chair

Welcome to the inaugural Pacific Cyber Security Operational Network (PaCSON) Annual Report. It has been a privilege to hold the PaCSON Chairmanship for an extended period – this PaCSON Community is one which is essential to supporting the development of our Pacific region's cyber security. I am proud to present this report as an opportunity to reflect on our combined efforts throughout 2020, and I welcome future reports as a key initiative designed to summarise our activities and promote awareness.

PaCSON is a regional network of cyber security incident response professionals collaborating on best practice, sharing information and developing incident response capability. Since its establishment in 2017, PaCSON has continued to grow and prosper in both memberships and partnerships and also in the work that we undertake. Our PaCSON Community encourages development, shares cyber security information, enhances technical skills and knowledge, builds relationships with other cyber-related programs and progresses work through our four Working Groups – Awareness Raising, Capacity Building, Communications and Partners. Together, we are strengthening cyber security for our Pacific region.

Cyber security is of global significance, and I am glad to see such excellent collaboration from our Pacific community. Collaboration has been crucial to our success thus far, as we are stronger together than apart. As a diverse group, with wide-ranging skills, a key focus of the Community is to work together to improve the collective knowledge of all involved. The greatest success of PaCSON is the participation and valuable outcomes delivered for our members and partners. It is through their collaboration that PaCSON is contributing to boost the cyber security strength of the Pacific region. I truly value the emerging Pacific maturity and believe PaCSON is positioned as a leader for Pacific-focused cyber security.

As the 2020 Chair, I offer my heartiest congratulations to the PaCSON Community for their contribution and commitment. 2020 was unprecedented in so many ways, but the continued success of PaCSON has helped to strengthen the resilience of the Pacific region's cyber community. Our PaCSON community is well placed to contribute to the worldwide effort of confronting the challenges of an open and free cyber space, while taking maximum benefit from the opportunities presented.

Those cyber threats affecting the Pacific region are increasing in scale and sophistication. To combat these threats and to anticipate the future threat environment, it is important that we work together to develop robust cyber security capabilities and enable professional competencies to protect our increasingly connected identities. PaCSON is key to enabling the Pacific's cyber security officials to learn from each other and exchange ideas on how, together, we can address the increasing number of cyber threats affecting our region's small and vulnerable countries.

There has never been a more important time to join together. The impacts of COVID-19 have shown us all how critical connectivity is to achieving and maintaining success. To assist with connectivity, education and awareness are vital in keeping our societies informed on what they can do to prevent potential cyber security attacks. Cyber Smart Pacific, our inaugural awareness raising campaign, was a tremendous success. The campaign focused on four key messages to help improve personal cyber security. Based on this success, the campaign will become an annual fixture for PaCSON's awareness raising efforts.

The challenge of COVID-19 saw our PaCSON Community pivot towards new ways of meeting and learning. In 2020, the Remote Session Series was launched with incredible success. More than 10 Remote Sessions were attended by over 190 participants. These sessions increased our knowledge across a range of topics and facilitated connections with industry partners and other cyber forums. The Remote Session Series shows the power of our community and demonstrates what we can achieve when we all come together to tackle regional challenges.

International cooperation is a key pillar for cyber security. It has been wonderful to see our PaCSON community grow as we welcomed the Reserve Bank of Fiji and the U.S. Cybersecurity & Infrastructure Security Agency as PaCSON partners. We will continue to welcome, and look forward to building relationships with, new members and partners who share the PaCSON values and vision of improving cyber security capabilities and readiness, across the Pacific, through cooperation and collaboration.

I also give thanks to our various stakeholders who have contributed to the success of PaCSON – without you our community would not be what it is today. I would especially like to pass along my appreciation to the PaCSON Secretariat and Australia's Department of Foreign Affairs and Trade's Cyber and Critical Tech Cooperation Program, who have committed their support to PaCSON.

The last year was undoubtedly a big challenge for PaCSON. I would like to acknowledge and thank everyone for the continual faith and dedication to our PaCSON community during this unprecedented time. As I finish my time as PaCSON Chair, I wish the very best of luck, and dedicate my ongoing support, to the new Executive Committee of 2021 – Tonga, the Cook Islands, and Vanuatu – I have faith that you will lead our community strongly.

Finally, I wish our community all the best for what remains of 2021 and very much look forward to seeing what we can achieve together in the future.

Mr Fualau Talatalaga Mata'u Matafeo
PaCSON Chair 2018–2020
30 September 2021

Program Overview

Established in 2017, the Pacific Cyber Security Operational Network (PaCSON) was created to foster regional cooperation and collaboration, and to ultimately protect the Pacific regions respective information infrastructures and constituents. The availability of internet connectivity presents significant opportunities but also exposes users within the Pacific region to increased threats from malicious cyber actors.

PaCSON is an operational cyber security network of regional working-level cyber security experts in the Pacific. PaCSON coordinates activities which aim to benefit the regional network of cyber security incident response professionals. These activities are underpinned by three guiding pillars:

- encouraging collaboration on best practice
- increasing threat and information sharing
- supporting and developing incident response capability through training and awareness raising activities.

The PaCSON network, commonly referred to as the 'PaCSON Community', consists of representatives from eligible Pacific governments or private organisations. Membership of PaCSON includes representatives from Australia, the Cook Islands, Fiji, Kiribati, the Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, the Solomon Islands, Tokelau, Tonga, Tuvalu and Vanuatu.

In support of PaCSON, partners – including other government organisations, not-for-profit organisations and academia – are able to join the network. The partner organisations to PaCSON include the Reserve Bank of Fiji, and the U.S.'s Cybersecurity Infrastructure & Security Agency (CISA).

PaCSON is not a Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT) and does not provide an incident response capability. The program maintains an operational cyber security points of contact and empowers members to share cyber security threat information; provides opportunities for technical experts to share tools, techniques and ideas; and is an enabler of cooperation and collaboration, particularly where a cyber security incident affects the region.

The direction of PaCSON is guided by the Executive Committee (EC), who provides leadership on behalf of the whole PaCSON Community. The EC is empowered to make decisions on behalf of PaCSON and is responsible for the management and direction of PaCSON. All PaCSON members are eligible to nominate for all EC positions. In 2020, the structure of the PaCSON EC included:

- Chair – Samoa
- Deputy Chair – Vanuatu
- Incoming Chair – Tonga.

The PaCSON Community and the EC are supported in all matters by the PaCSON Secretariat. The function of the PaCSON Secretariat is performed by the Australian Cyber Security Centre (ACSC). The ACSC absorbs all the costs associated with this function. The PaCSON Secretariat supports PaCSON members and partners to be part of a cooperative and collaborative community; maintains records and updates documentation; arranges and supports EC meetings; and coordinates arrangements for annual-general meetings, cyber security information exchanges and cyber security workshops.

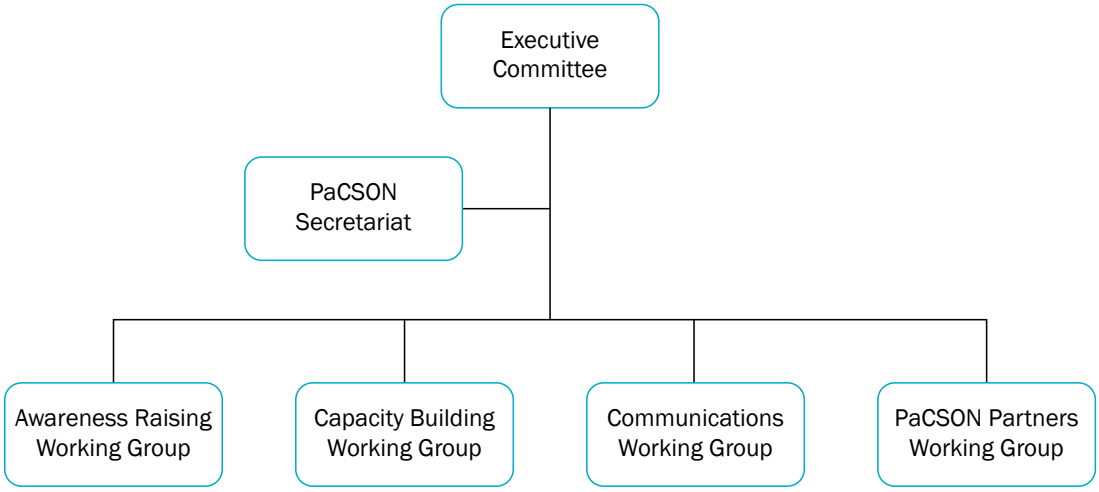


Figure 1: PaCSON network governance structure

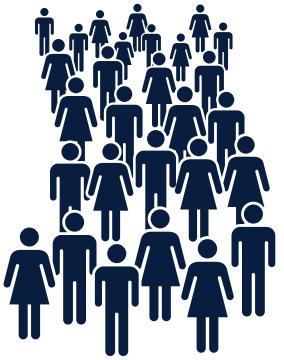
Vision

Improve cyber security capabilities and readiness across the Pacific through cooperation and collaboration among those responsible for coordinating national responses to cyber security incidents.

Mission

Work together across the Pacific to cooperatively and collaboratively develop collective cyber security incident response capabilities; enhance technical skills and knowledge; share cyber security threat information; and reflect best practice in order to strengthen our cyber security defences.

Figure 2: 2020 Remote Sessions



190 *Participants attended*

16

Economies participated from across the Asia-Pacific region

2 NEW PaCSON PARTNERS IN 2020

WELCOME

Reserve Bank of Fiji
US Cybersecurity and Infrastructure Security Agency (CISA)

Membership Updates

AUSTRALIA

Overview

Australian Cyber Security Centre (ACSC)

Resourcing and Constituency

The ACSC is a group within the Australian Signals Directorate (ASD). ASD is a statutory agency – within the Defence portfolio – that provides foreign signals intelligence, supports ACSC's cyber security mission, and reports directly to the Minister for Defence.

The ACSC leads the Australian Government's efforts on national cyber security. It brings together cyber security capabilities from across the Australian government to improve the cyber resilience of Australian society.

Our role is to help make Australia the most secure place to connect online, and we have a long history of cyber security excellence, providing advice and information about how Australians can protect themselves online.

The primary constituency for the ACSC includes:

- individuals and families
- small and medium business
- large organisations and critical infrastructure
- government.

Cybercrime is becoming more sophisticated and cyber criminals target individuals, businesses and government. ReportCyber is the reporting tool for Australians and is available at cyber.gov.au/acsc/report.

Reporting to ReportCyber is not a formal police statement and not all reports are investigated by law enforcement agencies. However, the reports can help to disrupt cybercrime operations and to make Australia a safe place to connect online.

Threat landscape

The scale and sophistication of cyber threats to Australia and the Indo-Pacific is increasing. Australia cannot, and does not, act in isolation in addressing cyber threats. International partnerships create opportunities for information sharing, operational collaboration and support, and cooperation to build technical capacity.

Some of the most common cyber security threats experienced in Australia include:

- ransomware
- phishing and scam emails
- malicious insiders
- remote access scams
- denial of service (DOS)
- hacking attacks.

The ACSC monitors cyber threats across the globe 24 hours a day, seven days a week, so we can alert Australians early on what to do. We provide advice and information on how to protect Australians and their business online. When there is a cyber security incident, we provide clear and timely advice to individuals, businesses and critical infrastructure operators. We work with our business, government, academic partners, and experts in Australia and overseas to investigate and develop solutions to cyber security threats.

In Australia, some of the types of incidents that the ACSC responds to include:

- web shell malware
- ransomware
- phishing and scam emails
- malicious insiders
- remote access scams
- DOS
- hacking attacks.

In the 2020 calendar year, the ACSC received 65,617 cybercrime reports via ReportCyber, and 2,223 reports of cyber security incidents. Approximately one-third of cyber security incidents reported during the 2020 calendar year affected critical services, such as the electricity, water, education, banking and finance, health, communications, and transport sectors. The ACSC encourages the reporting of all cybercrime and cyber security incidents, via ReportCyber. The ACSC uses reported incidents to enhance national situational awareness of the cyber security environment in Australia, to identify emerging trends, and to support timely and tailored advice and assistance to Australian organisations.

Awareness Raising

In 2020, ACSC conducted market research that highlighted a widespread desire among Australians to better understand how they can protect themselves online. ACSC's Act Now, Stay Secure advertising campaign was launched on 30 November 2020.

The campaign encourages Australians to protect themselves against cybercrime and increases awareness of ACSC. The campaign warns Australians about online threats and directs people to the official ACSC website – www.cyber.gov.au, for a wide range of practical resources including several types of news, publications or advisories.

In 2020, the ACSC released reports, media releases and 25 advisories and alerts.

COVID-19

Since early March 2020, when COVID-19 was first recorded in Australia, there has been a significant increase in COVID-19 themed malicious cyber activity within Australia.

Malicious cyber actors are actively targeting individuals and Australian organisations with COVID-19 related scams and phishing emails.

In Australia, Scamwatch has received over 6,415 scam reports that referenced the coronavirus, with more than $9,800,000 (AUD) in reported losses since the outbreak of COVID-19. Common scams include phishing for personal information, online shopping, and superannuation scams.

Scamwatch is aware of scams relating to COVID-19 vaccines both in Australia and overseas. These include:

- requests for payment for vaccines or for early access to vaccines
- offers to mail vaccines
- offers of money as a return on an investment opportunity in the Pfizer vaccine
- fake surveys related to vaccines that offer prizes or early access.

COOK ISLANDS

Overview

ICT Division, Office of the Prime Minister

Resourcing and Constituency

The ICT Division is headed by the Director of ICT and consists of five technical staff and a Project Management Unit (PMU) of three staff. Our primary constituency is the Government.

Threat landscape

In the Cook Islands, there is currently no formal process for cyber incidence reporting. In terms of online financial incidences, the reporting is made to the Financial Supervisory Commission (FSC).

Common cyber threats to the Cook Islands include:

- spam
- scams (e.g. pyramid schemes) and phishing
- ransomware
- fraudulent employee data use (data theft and data deletion)
- social engineering through social media (trying to access social media accounts).

Mostly, the ICT Division responds to scams and virus on the Government network.

For 2020, the ICT Division was unable to provide concrete figures regarding incidents responded to. But scams number more than a thousand. The challenge is ensuring recipients of the scams do not respond. This is usually done with an email, to all users on the network, telling them to block and delete emails from certain sources and containing certain subjects.

Awareness Raising

The Cook Islands has no formal cyber awareness raising program in place. Responses to awareness were triggered by incidents reported on social media platforms.

General cyber-related advice includes:

- the KukiWise advertisement on local TV and social media, to inform the community of the types of online scams and who to contact
- the 'Get Safe Online Cook Islands' website: https://www.getsafeonline.org.ck/

COVID-19

For the Cook Islands, there was minimal impact in 2020 from COVID-19 to our cyber landscape.

FIJI

Overview

Ministry of Communications

Resourcing and Constituency

There are four departments under the Ministry of Communications. These departments are:

- Department of Communications
- Department of Information
- Department of Information Technology and Computing Services (ITCS)
- Digital Government Transformation Office (DGTO).

The Ministry of Communications is led by the Minister Hon Aiyaz Sayed-Khaiyum, followed by Acting Permanent Secretary Tupou'tuah Baravilala, who oversees the four departments. Each of the departments has department heads who report to the Acting Permanent Secretary.

Within Government, the ministries report all cyber incidents to ITCS. ITCS also identifies if any cyber incident has occurred within the Government network. ITCS has a team that monitors and attends to cyber incidents and threats within the Government.

Outside the Government network, cyber incidents are usually reported to the Fiji Police's Cybercrime Investigations Unit. Cybercrime is a severe criminal offence which is investigated by the Fiji Police Force. Cyber incidents are also reported to Online Safety Commission and Fiji Financial Intelligence Unit.

Threat landscape

Common cyber threats to Fiji include:

- website defacement
- phishing
- malware
- ransomware
- financial fraud
- business email compromise.

The ITCS department responds to incidents such as website defacement, malware, business email compromise and phishing attacks within the Government network.

During 2020, the ITCs department responded to 15–20 cyber incidents.

Awareness Raising

Awareness raising efforts conducted by the ICTS department included critical information being disseminated to all IT officers, including secure communications within the group to quickly address evolving issues. Security advisories and awareness on critical vulnerabilities are disseminated to government ministries.

COVID-19

Many companies and businesses in Fiji quickly introduced online shopping for their customers so that the businesses could keep operating during the pandemic, while adhering to all the COVID-19 safe business protocols and policies advised through the Fijian Government. This rapid introduction of e-shopping increased the surface of attack for cyber criminals. However, despite the surge in uptake of e-shopping we have not noticed any significant increase in cyber incidents at a national level.

It has been noted that misinformation and disinformation regarding COVID-19 is circulating on social media platforms, as is evident globally. A notable example is the misinformation about the COVID-19 vaccines, whereby people are posting that vaccines are not safe as we do not know what they consist of and that the vaccines contain microchips to track people. This misinformation started trending on social networking sites and translated into a lot of questions regarding the credibility and integrity of the vaccines. The Fijian Government, through the Ministry of Health and Medical Services, has been rolling out awareness campaigns through traditional and social media platforms to educate people, and through targeted and focused community engagement to address the misinformation and disinformation.

KIRIBATI

Overview

Ministry of Information, Communication, Transport and Tourism Development (MICTTD)

Resourcing and Constituency

The ICT Policy and Development Division of MICTTD comprises seven personnel: the ICT Director, three senior ICT officials, one ICT officer and two helpdesk officers. The Director of ICT directly reports to the Secretary of MICTTD.

Primary constituencies for MICTTD are the Government ICT sector, the general public and local businesses.

The ICT division has not yet formalised procedures on reporting cyber incidents; however, cyber incidents are often reported to the ministry via direct telephone calls and emails.

Threat landscape

Malware infections, phishing, social-engineering scams and misinformation, harmful content (violent content and child-inappropriate content), and web defacement are the most common types of cyber threats in Kiribati.

MICTTD does not have the formal capability to respond to cyber incidents; however we have certain cases where we provides a response capability, to a limited extent, to severe cyber incident cases on government networks.

We have not formally lodged any incidents thus far, although the Ministry have provided response capabilities on two separate incidents.

Awareness Raising

Awareness raising efforts by the MICTTD ICT Division include conducting cyber security and cyber safety awareness to schools, via the MICTTD Cybersecurity Awareness School Campaigns, and awareness to communities on cyber safety tips and best practices on staying secure on the internet.

Every year the MICTTD also hosts an MICTTD Day, where the ICT Division conducts focused awareness programs on current, persisting cyber security issues.

During International Girls in ICT Day, and National Youth Day, the ICT Division also conducts awareness on cyber safety and digital citizenship.

The MICTTD does not have formal publications on advisory but does provide advisories to government ICT professionals on cyber security issues. The MICTTD has also published a National Cybersecurity Guideline for government agencies.

COVID-19

Kiribati has seen a surge in usage of the internet by the general population during the COVID-19 pandemic. A few months back, Kiribati imposed a curfew as a response to the first COVID-19 confirmed border case. Many school-aged children turned to the internet to access school materials, as did the general population to communicate with families, friends and to access COVID-19 advisories from the Government and the World Health Organisation.

This surge in usage also came with a few downsides as more people tended to get COVID-19 information from the internet, often from social media platforms where there was a high volume of trending anti-vaccine information and misinformation about COVID-19. This has had grave consequences for the way people perceive the pandemic and vaccination campaigns. We have also observed an increase in the number of scams during this time, including pyramid schemes and social-engineering scams.

NEW ZEALAND

Overview

CERT NZ

Resourcing and Constituency

CERT NZ is a branded business unit within the Ministry of Business, Employment and Innovation. It has around 35 staff, including operations, communications and engagement, governance and analytical reporting. CERT NZ also has a contact center to receive incident reports.

CERT NZ is New Zealand's Computer Emergency Response Team, and works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. CERT NZ provides trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand. See http://www.cert.govt.nz for more information.

Anyone can report a cyber security incident to CERT NZ, from members of the public, businesses, and government agencies to IT professionals and security personnel. We also receive incident notifications from our international CERT counterparts when they identify affected New Zealand organisations in their investigations.

Incidents can be reported to CERT NZ through an online reporting tool, by phone, or through our referral partners.

- The online tool can be accessed here:
- https://www.cert.govt.nz/individuals/report-an-issue/ (for individuals and businesses)
- https://www.cert.govt.nz/it-specialists/report-an-incident/ (for IT Specialists)
- Full contact details are available here: https://www.cert.govt.nz/about/contact-us/

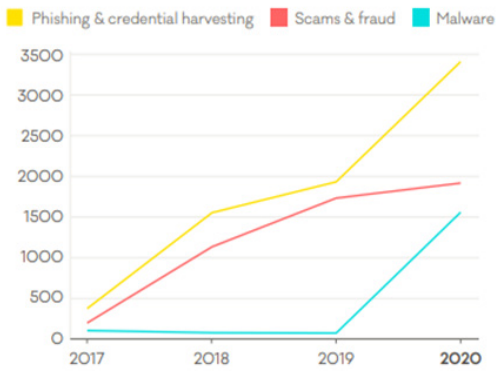
CERT NZ also has a Coordinated Vulnerability Disclosure Policy and process. More information can be found here: https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/

Threat landscape

The top incident categories for 2020 were:

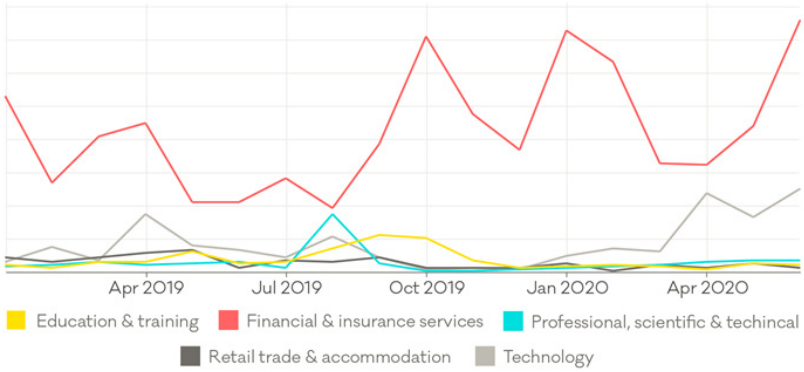
- phishing and credential harvesting, with 3,410 reports
- scams and fraud reports, with 1,920 reports
- malware, with 1,560 reports.

The top incident categories in 2019 were phishing and credential harvesting; scams and fraud; and unauthorised access.



The top three targeted sectors reporting incidents in 2020 included:

- financial and insurance services, with 1,058 reports
- technology, with 200 reports
- public administration and safety, with 54 reports.

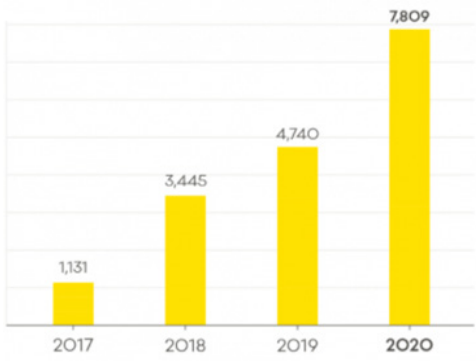


Full details can be found at https://www.cert.govt.nz/about/quarterly-report/

CERT NZ's key services are:

- Threat identification: We analyse the international cyber security landscape and report on threats.
- Vulnerability identification: We analyse data and report on vulnerabilities in New Zealand.
- Incident reporting: We triage reported incidents and assist businesses, organisations and individuals in getting help and pass some incidents on to appropriate organisations, with the reporter's consent.
- Response coordination: We lead the response to some incidents, coordinate the response to others and we support the national emergency response process.
- Readiness support: We raise awareness of cyber security risks, mitigations and impacts and deliver up-to-date, actionable advice on cyber security best practice.

In 2020, 7,809 incidents were reported to CERT NZ, a 65% increase from 2019.



Awareness Raising

In October 2020, CERT NZ ran its fourth cyber security awareness campaign, Cyber Smart Week. CERT NZ engaged with partners from across the government and private sectors to share the four simple steps all New Zealanders could take to be more secure online. During the campaign, CERT NZ worked with 122 partner organisations, achieving a combined five million impressions. A wide range of resources – from graphics to editorial content – were available for partners to use and share, with the backing of CERT NZ.

For the first time, CERT NZ ran a campaign specifically targeted at businesses – Trade Smart Online. This was a joint campaign with Consumer Protection, which promotes secure online trading and shopping practices among businesses and consumers. The campaign was heavily promoted online but also included television ads.

As part of October International Cyber Awareness Month, CERT NZ proposed and supported the development of the collaborative Cyber Smart Pacific initiative through the PaCSON Awareness Raising Working Group. The Working Group proposed and voted on a range of themes and taglines, resulting in a regional campaign that included the launch of several local and regional websites and awareness efforts, including numerous localised and translated posters.

CERT NZ regularly publishes Advisories and Guides available on the CERT NZ website. In addition, CERT NZ's quarterly reporting continued in 2020, with the publication of two reports each quarter:

- Quarterly Report: a highlights document, focusing on selected cyber security incidents and issues
- Quarterly Report: a data landscape document, providing a standardised set of results and graphs for the quarter.

2020 saw CERT NZ publish our updated critical controls, which included 'securing internet exposed services' as a control for the first time. CERT NZ also published numerous pieces of content in response to people shifting to remote working arrangements due to the COVID-19 pandemic.

CERT NZ has also increased its use of social media in 2020 as a way to reach our constituency. As well as building on our existing use of Twitter (@CERTNZ), CERT NZ launched a Facebook page in October 2020 – https://www.facebook.com/certnzgovt.

COVID-19

Over the course of COVID-19, CERT NZ has registered several trends, including a continued increase in incident reporting.

CERT NZ noted a significant increase in reporting in Q1 and Q2 of 2020, with 3,120 reports as compared to 4,740 for all of 2019. April alone accounted for 820 of these reports, correlating with New Zealand's entry in to COVID-19 Alert Level 4 lockdown.

While the increase covered a range of report types, the drivers were scams and fraud, with a 230 percent increase from Q1 2020 to Q2 2020. Unlike in many other countries; however, only three percent of these reports were directly COVID-19 themed. Within the scam and fraud category, extortion and blackmail related reporting accounted for the majority of the April spike, however the notable trend was a gradual and sustained growth in scams related to buying and selling online.

Increased reporting numbers have continued into Q3 2020 with 2,610 reports and 2,097 reports in Q4. Since Q3 2020, Phishing and credential harvesting and malware have overtaken scams and fraud as the top reported incident categories.

NIUE

Overview

Telecom Niue Limited

Resourcing and Constituency

Telecom Niue Limited is a company incorporated in Niue and owned 100% by the Government of Niue. Telecom Niue employs a moderate workforce which includes administrative officials, technicians and labourers.

Telecom Niue supports government, business and small enterprises, private industry and members of the public as its primary constituency.

Threat landscape

Telecom Niue is able to receive cyber related reporting through our website and social media.

Generally, Niue experiences many of the same cyber security threats as the broader Pacific region. Some common types of cyber threats include:

- ransomware
- malware
- phishing attacks.

The types of incidents that Telecom Niue responds to include any cyber attacks that the Government of Niue receives.

In the 2020 reporting year, Telecom Niue responded to 3 major incidents.

Awareness Raising

Telecom Niue conducts various community engagement and awareness-raising efforts. In 2020, engagement on social media was common.

COVID-19

For Niue, there was minimal impact in 2020 from COVID-19, as the Island remained completely illness free.

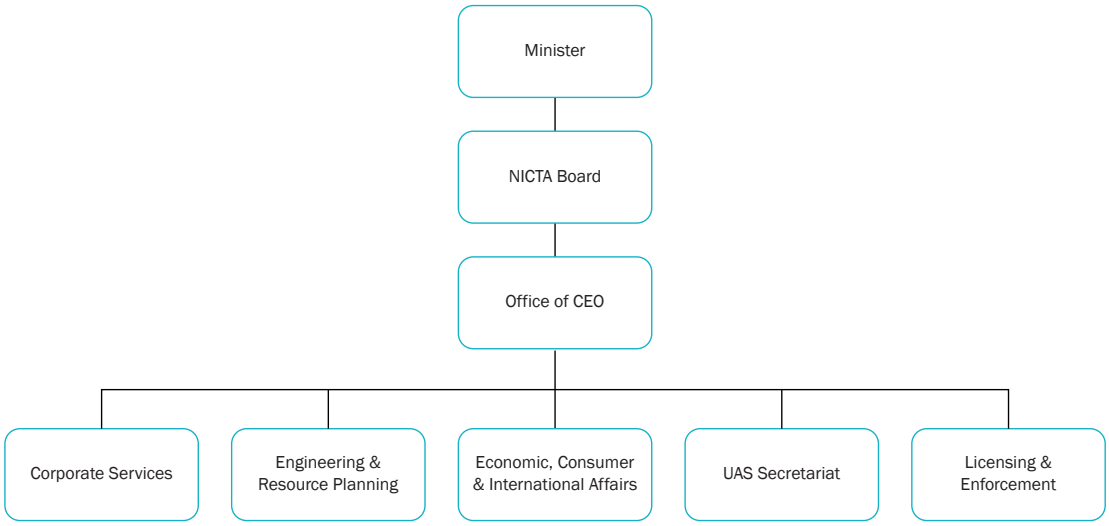
PAPUA NEW GUINEA

Overview

The National Information and Communications Technology Authority (NICTA)

Resourcing and Constituency

NICTA is a government agency responsible for the regulation and licensing of ICT in Papua New Guinea. The diagram below explains how NICTA is structured:



Office of the Chief Executive Officer (CEO)

The CEO is responsible for management of NICTA in accordance with the policy direction of the Board. The CEO is required to advise the Board on matters concerning NICTA and carries out the operational and administrative functions of the organisation with the assistance of the Executive Management Team.

The Office of the CEO has three branches: Corporate Legal Services, Special Projects, and Corporate Secretariat Services.

Corporate Services Department (CSD)

CSD has three branches: Human Resource and Administration, Finance and Information Technology. CSD is responsible for:

- training, staff development and recruitment functions including administering employees' terms and conditions of employment.
- compiling PANGTEL's annual budget estimates, debt collection, insurance and personnel matters as well as coordinating the IT needs and requirements for line technical departments.

Engineering & Resource Planning Department (ERPD)

ERPD has two branches: Resource Planning and ICT Standards & Policy. ERPD is responsible for:

- formulating regulatory policies, plans, guidelines, standards and specifications for all radio communications services including broadcasting.
- spectrum management in PNG, including the establishment of spectrum usage policies, spectrum pricing, spectrum planning and allocation of the radio frequency spectrum.

Economics, Consumer and International Affairs (ECIA)

ECIA has three branches: Economic Regulation, Consumer Affairs, and International Affairs. ECIA is responsible for:

- promoting competition through an open-access regime (infrastructure sharing, interconnection, national roaming).
- enhancing and promoting consumer welfare and encouraging responsible use of ICT services.
- technical co-operation and activities with donor agencies, foreign governments and international organisations, including International Telecommunication Union (ITU), Asia-Pacific Telecommunity (APT), etc.

Universal Access Scheme Secretariat (UAS)

UAS is responsible for improving availability of ICT services in PNG, particularly in rural and underserved areas, by:

- improving affordability of ICT services
- improving access and availability of emergency services
- ensuring sustainability of implemented projects
- managing the UAS fund.

Licensing & Enforcement Department (LED)

LED has two branches: Licensing & Business Relations, and Enforcement and Compliance. LED is responsible for:

- ensuring all ICT Operators have appropriate authorisations (licenses, permits, certificates, etc.).
- maintaining cordial working relationships with licensees and stakeholders.
- inspecting and surveying all radio and telecommunications equipment and services operating in Papua New Guinea.
- carrying out surveillance of radio frequency spectrum and setting up equipment standard specifications and consequent testing of radio communications equipment imported into Papua New Guinea.

As its primary constituency, NICTA provides regulatory support to government, business and small enterprises within Papua New Guinea. As part of our responsibilities, NICTA regulates:

- broadcasting
- radio communications
- telecommunications.

In Papua New Guinea, cyber incidents can be reported through formal government or business frameworks. Additionally, NICTA also has an online enquiries site where incidents can be reported, and reports can also be provided in person or over the phone.

Threat landscape

Generally, Papua New Guinea shares many similarities, regarding cyber security threats, with the broader Pacific region. Some common types of cyber threats include:

- malware and ransomware attacks
- phishing attacks
- identity theft and social engineering to conduct fraud and theft.

During 2020, ransomware attacks were reported in Papua New Guinea. The advice and recommended procedures, provided by the UK's National Cyber Security Centre (NCSC) and our partner WithYouWithMe, was to continually do updates, install or upgrade firewalls and install antivirus software.

Awareness Raising

NICTA supported various community engagement and awareness raising efforts, including through community outreach and engagement via social media.

As a function of NICTA, the Papua New Guinea Computer Emergency Response Team (PNGCERT) works to promote awareness, provide advisory assistance and coordinate responses to cyber security incidents in Papua New Guinea.

COVID-19

During the reporting period, Papua New Guinea's threat landscape changed in response to COVID-19. New threats experienced during this time related to misinformation regarding the pandemic and increased network traffic which created strain, and increased ransomware incidents.

SAMOA

Overview

Ministry of Communications and Information Technology (MCIT), Samoa

Resourcing and Constituency

MCIT is the Policy Advisor and central planning agency to the Government of Samoa on all broadcasting, postal, telecommunications, and ICT and cyber security policies for Samoa. The Ministry comprises the National Computer Emergency Response Team (SamCERT), Policy and Planning Development Division, ICT Secretariat Division, Broadcasting Services Division and Corporate Services Division. In addition to these Divisions is the Office of the Minister of Communications and Information Technology. Currently in the pipeline is the establishment of the Digital Transformation Authority (DTA) to oversee the Government's digital transformation agenda and activities. MCIT currently operates from three separate locations in the city of Apia, with a combined workforce of 50 employees.

The Ministry plans, designs and develops plans and policies in all areas stated above for all government agencies and offices to adhere to. In addition, the Ministry conducts educational and awareness campaigns, and capacity development programmes for government, private sector, communities, schools and businesses. Lastly, through the newly established SamCERT, the Ministry will directly liaise with private businesses, non-governmental organisations (NGOs), government bodies and academic institutions in relation to all cyber incidents.

Currently, all crimes, including cyber incidents, are reported to the Samoa Ministry of Police and Prisons (SMPP), with additional support provided by MCIT for cyber-related attacks and incidents. However, with the newly established SamCERT under our Ministry, it is intended that SamCERT will be the focal point for all cyber incident reporting, responses and handling within Samoa.

Threat landscape

The top cyber security threats for Samoa include:

- DOS
- Distributed Denial of Service (DDOS)
- email spam
- pyramid scams

In addition, the rise of fake news, disinformation, cyber-bullying and cyber-harassment has been witnessed in Samoa and across the Blue Pacific Region.

In the past few years, Samoa has been fortunate to have not been pressed with any major cyber incident. The Ministry; however, through its partners in Government, mainly the ICT Technical Working Group for Government (ICT-TWG), has provided extensive support for awareness and response to two concerning incidents. The first was an incident concerning the health sector of which one of its entities faced a ransomware attack. This incident was quickly resolved with the assistance of the ICT-TWG, which was equipped to handle such incidents through technical training over the years, as the interim-team to respond to cyber security incidents for the Government. The second incident involved a domestic bank being affected by a massive DDOS attack. This incident was also managed and successfully recovered through the technical support provided by the ICT-TWG, the bank's security firm in New Zealand and the internet service provider. Apart from these two cyber incidents, there is no record of any further incidents occurring to date.

Awareness Raising

The Ministry, as well as its sector partners and stakeholders, continues to place more emphasis on the importance of cyber security, with ongoing cyber security awareness programs and capacity development training initiatives across the country. Much of this cyber security training awareness targeted the ICT-TWG on various cyber security topics and best practices for Government and private businesses. Additional support in this area is provided by member groups, including the Samoa Information Technology Association (SITA), which deals directly with the community and other sectors of the Government through various cyber security training and awareness programs. SITA also hosts an annual conference on cyber security for both public and private sectors.

In February 2021, the Ministry, in collaboration with all its partners in the cyber security domain, held its first National Cybersecurity Awareness Week. The National Cybersecurity Awareness Week was used to create new skills for all technical staff from both the private and public sector in terms of working together, forging new relationships and partnerships in handling and responding to cyber threats. The National Cybersecurity Awareness Week also featured a roll out of massive billboards across the main island, printed posters for all schools, government offices, and private businesses, talkback shows on Radio 2AP and cyber commercial advertisements on local television. It also coincided with the official launch of the PaCSON website, the GetSafeOnline Samoa website, and the revamped MCIT cyber security webpage. The National Cybersecurity Awareness Week will be an ongoing event that will be led by the newly established SamCERT.

MCIT continues to develop a variety of cyber security awareness materials that are distributed to different sectors of the economy. These include posters for schools and public and private sector offices, and cyber security bulletins distributed to all ICT-TWG members, via email on a monthly basis, as well as CS-Advisories on an as-needed basis.

As Samoa builds its tools of cyber security and cyber-safety, we have striven for these to be well established; hence, Samoa now has a GetSafeOnline portal or website, made available in both Samoan and English languages – https://www.getsafeonline.ws/. This platform also includes materials which provide education about and understanding of the different threats emerging in cyber space, including awareness materials. It was launched during the 2021 National Cybersecurity Awareness Week. Additionally, the platform includes the material published as a result of the collaborations between the Ministry and its international partners, such as PaCSON, CERTNZ, Asia Pacific Network Information Centre (APNIC), and other cyber security entities of the region.

COVID-19

As Samoa adapts to the new environment brought by the COVID-19 pandemic, the Ministry, in close collaboration with its local, regional, and international partners, continues to find ways to manage the growing amount of misinformation circulated in cyberspace. This contest is waged between those who try to improve the flow of relevant constructive information and those who exploit this information flow to cause havoc and victimize those who are caught in the crossfire. Samoa, like many of its neighboring countries, is not immune to these changes in cyberspace where, at times, Samoa has experienced incidents that involve the circulation of misinformation concerning COVID-19, via social media platforms and emails. This has caused major problems with the security of the country, with the use of fake news to pivot watering-hole attacks luring users to visit sites that have malicious content which also seek to harm devices and systems.

Similar to these campaigns is the rise of phishing attacks targeting those in the financial industry with messages related to COVID-19 insurance, and promises of financial support related to COVID-19 assistance. The Ministry recognised that attackers are becoming very creative in their attacks, using a composite of disinformation and misinformation to draw in their victims and using sophisticated attack vectors to achieve their intent. There have been sightings of ransomware, Fileless viruses and Living off the Land (LOL) attacks within Samoa; however, these have been very few and only affected a small portion of the workforce, with affected entities being able to manage and report in a timely manner for a quick response and recovery. These incidents; however, are still a major threat as, if they were amplified on a major level, that will lead to levels that affected national security, and could be something that Samoa does not want to see. In many ways, this could play out as a digital COVID-19.

Special Note –

Samoa looks forward to the great opportunity that SamCERT presents in protecting and managing Samoa's cyberspace and national critical infrastructure. The existence of SamCERT will open new doors for regional collaboration to strengthen not only Samoa's digital and cyberspace profile as a secure and safe country for digital collaboration and digital economies, but also to improve the cyber security structure for the region as a collaborative effort, in improving the life of the inhabitants of our Blue Pacific population.

Samoa would again like to thank its Pacific Member Governments and people in keeping the momentum of the PaCSON family moving towards positive changes in the cyber security spectrum of cyberspace. For this, MCIT would like to extend its sincere appreciation to the Government of Australia, through the ACSC, in strengthening cyber security in the region, through the PaCSON family, and of fighting this ongoing battle of securing and keeping our Blue Pacific Cyberspace safe for the collective good of our region.

SOLOMON ISLANDS

Overview

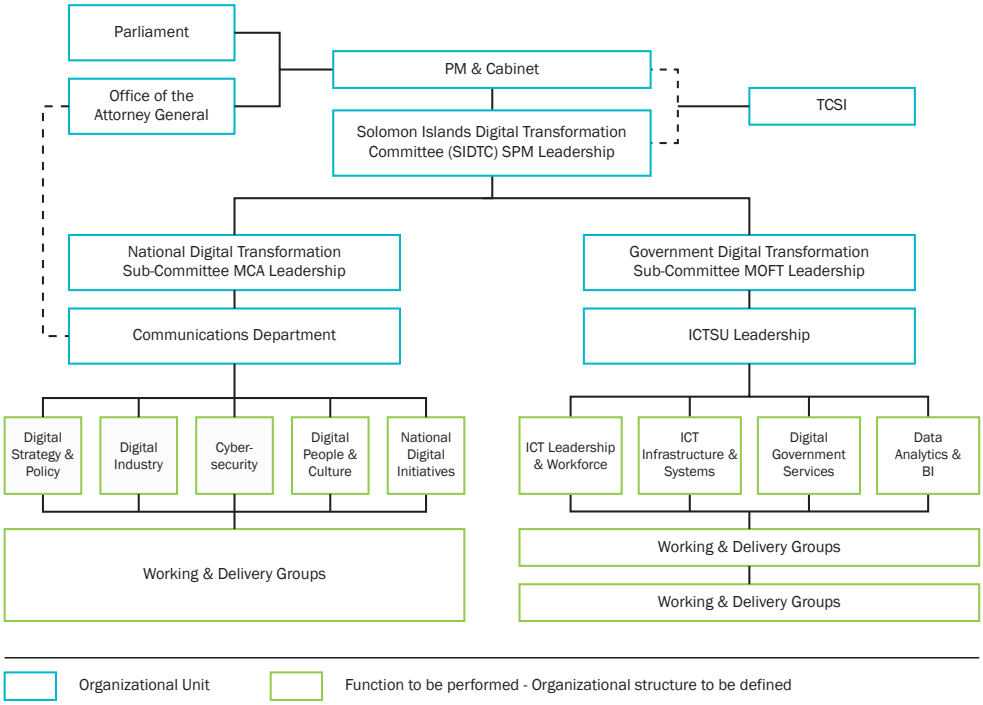
Solomon Islands Government Information Communication Technology Services (SIG ICTS)

Resourcing and Constituency

The SIG ICTS is an office with 34 technical staff and 6 in management and administration.

Currently we sit under the Ministry of Finance Corporates Services, reporting to the Deputy Secretary Corporate Services, and providing services on three fronts: Client Support, Information Systems, and Infrastructure. There is still a huge resource gap in terms of capacity, and an organisational structural review is in progress to clearly ascertain roles and responsibilities, which will result in additional recruitment and capacity development.

With a whole-of-government approach, a Digital Transformation Institutional Framework has been developed (in draft) to capture this. See below for the proposed structure of the SIG ICTS five years ICT Strategic Plan.



Solomon Islands Digital Transformation Institutional Framework (Draft)

SIG ICT services delivery is mandated by the Government, so our primary constituency is the Solomon Islands Government. This includes all government ministries, provincial governments and related agencies.

There is no fully-functional mechanism in place specific to cyber incident management and reporting, as this is currently being developed through the implementation of a security operations center within SIG ICTS, which is still in its infancy.

However, reporting is done via our Helpdesk support system through:

- emails
- phone calls
- direct communication.

Threat landscape

In the Solomon Islands, common types of cyber security threats include:

- phishing
- information leakage
- malware
- ransomware
- scams.

SIG ICT responds to incidents, such as:

- phishing:
  - identify
  - analyse links and report to portals such as virus total
  - awareness to end users.
- malware:
  - identify
  - patch and upgrade/update system
  - awareness to end users
- information leakage:
  - log analysis and email audit
  - identify and report.

In 2020, SIG ICT managed responses to a few incidents. These included:

- the leaking of confidential documents and emails, which prompted an audit and analysis of our exchange facility
- the recent Solarwinds exploit, which prompted the team into action
- a vulnerability due to an out-of-date Windows patch, which was exploited, resulting in our file server being infected.

Awareness Raising

SIG ICT awareness-raising efforts are delivered via newsletters that are sent through emails, phishing simulation and links to updates from related sites. We also send regular emails to our users on specific issues.

To date, there has not been any direct awareness raising programs/workshops targeting our constituents.

Other types of awareness raising efforts include news releases via email, and plans are in place to have a dedicated page via the Solomon Islands Government portal.

COVID-19

COVID-19 has spiked internet usage in the Solomon Islands as a lot of people surf online to get updates on latest news releases. However, this spike presents cyber security threats as well, including:

- increase in phishing emails
- scams regarding donor funds
- scams about positive cases in the Solomon Islands
- scams about a local antidote for COVID-19.

TONGA

Overview

Tonga's Computer Emergency Response Team (CERT Tonga)

Resourcing and Constituency

CERT Tonga consists of three full-time staff and liaison officers within domestic partner organisations. There are also a handful of volunteers who assist the team from time to time.

CERT Tonga operates under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (MEIDECC) and is the national Computer Emergency Response Team for the Kingdom of Tonga.

CERT Tonga's constituents are government ministries, the private sector, public enterprises, and NGOs.

Cyber reporting to CERT Tonga can be made:

- at the Hotline number 2378 to call and report any cyber incident
- People or organisations can also report via email report@cert.gov.to; and
- via our website https://www.cert.gov.to/.

Threat landscape

For Tonga, our most common cyber threats include:

- business email compromise
- phishing email/scams
- botnets
- brute force activities.

The types of incidents that we respond to are mostly botnet activities, dark net activities, brute force activities and business email compromise (BEC) and phishing.

Awareness Raising

CERT Tonga has an awareness program it provides to government ministries, public enterprises, the private sector and NGOs. Examples of our awareness programs are below.

GOVERNMENT

CERT Awareness on Emotet with System Administrators /IT officers: CERT Tonga facilitated an awareness session to local systems administrators and IT officers from different organisations.

Ministry of Lands & Natural Resources: awareness session with the Natural Resource Division.

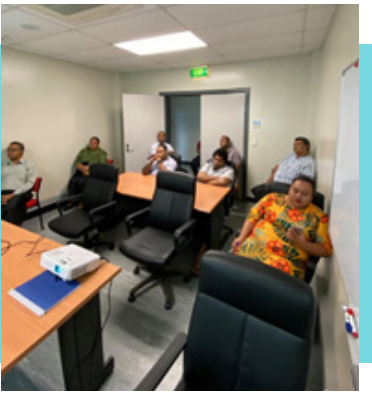
Ministry of Finance (MOF): CERT Tonga provided two awareness sessions with different divisions from MOF.

Ministry of Internal Affairs (MIA): CERT Tonga provided three awareness sessions with different departments from MIA.

Public Service Commission (PSC): CERT Tonga provided an Awareness session with PSC staff at their office.

PUBLIC ENTERPRISES

Tonga Cable Limited (TCL): an awareness session with TCL staff provided by Saia Vaipuna and CERT Tonga.



PRIVATE BUSINESS

Office Equipment: a session with staff from Office Equipment in making sure that they are aware of who CERT Tonga is and what we do.

NON-GOVERNMENT ORGANISATIONS (NGOS)

Tonga Women in ICT: women from different organisations have a passion for IT here in Tonga, so CERT Tonga provided a session with them.

CERT Tonga website: provide awareness through our website during the Cyber Smart Week (October 2020).

Other awareness-raising activities conducted by CERT Tonga include publishing advisories to assist constituents in resolving imminent threats and vulnerabilities observed to be exploited in the wild. We provide Monthly Security Bulletins about different vulnerabilities encountered within that month. An email advisory is also sent out to our constituents, via a mailing list, to notify of any possible attacks and when they were detected.

This is all in addition to:

- using social media platforms – CERT Tonga uses Facebook and Twitter to share our advisories, security bulletins as well as security tips
- disseminating news – we also use the government portal as a platform to publicised news.

COVID-19

CERT Tonga has not seen much of an increase in cyber attacks in-country, but we have seen other countries impacted by COVID-19 scams. In response our team decided to put out an advisory just so that people and organisations were aware of such misinformation.

TUVALU

Overview

Department of Information and Communications Technology (ICT)

Resourcing and Constituency

The Department of ICT is under the Ministry of Justice, Communications and Foreign Affairs. The department management is led by Director of ICT, together with two senior officers looking after Networking and Applications Development. The Department reports to the Permanent Secretary, as well as the Assistant Secretary of the Ministry. Other functions include coordinating cyber security capacity developments, regulating the telecommunications sector, and also the wider digital transformation goals of the Government.

The Department of ICT supports the Tuvalu Government's IT services. As its primary constituency, the Department of ICT provides support to all government departments. The Department does offer support to the private sector, in terms of capacity building, and cyber safety for schools and the general public.

In Tuvalu, cyber incidents can be reported to the police, the Department of ICT or the Office of the Peoples' Lawyer who is the major legal aid/service for the general public.

Threat landscape

Generally, Tuvalu shares many similarities regarding cyber security threats as the broader Pacific region. Some common types of cyber threats include:

- malware
- phishing attacks
- identity theft and fraud.

Awareness Raising

The Department of ICT, in collaboration with the Tuvalu Police, supported various community engagement and awareness raising efforts, including through community outreaches, visits to schools and engagements via social media. The newly launched Get Safe Online website in Tuvalu is a huge boost for Tuvaluans, especially with translations to the local language.

The Department of ICT tries to share Security Advisories from PaCSON partners like Tonga CERT, Vanuatu CERT, NZ CERT and even CISA, on various social media outlets such as Government Facebook pages and Tuvalu news pages.

COVID-19

For Tuvalu, due the country's remoteness, there was minimal impact in 2020 from COVID-19 as the area remained free from any cases. This was aided by the border lockdown, mostly to flights into the country, and also to most visiting boats, besides the essential cargo shipments.

There was a substantial increase in the country's total bandwidth available for use, due to the Government securing contracts with Pacific, Eutelsat and ABS, but there were not any corresponding numbers of major attacks reported.

There was the odd event of people believing in convincing, but unverified, news.

VANUATU

Overview

CERT Vanuatu (CERTVU)

Resourcing and Constituency

CERTVU was established within the Office of the Government Chief Information Officer (OGCIO), under the Ministry for the Prime Minister's Office. CERTVU has three active staff who handle the entire operation of CERT, from providing incident responses to delivering cyber security awareness nationwide.

We have not distinguished our constituency. CERTVU is the national CERT, hence our constituency covers the government sector, private sector, NGOs and civil society.

Our constituents can report cyber incident to us through the following methods:

- phone
- email
- the web portal
- social media platforms
- assisting partners.

Threat landscape

Common cyber threats to Vanuatu include:

- phishing
- online money scam
- malware attacks
- business email and fraud
- misinformation.

All cyber related incidents are reported by our constituents. During the reporting period, CERTVU responded to 340 reported incidents.

Awareness Raising

Our yearly awareness-raising program involves the following:

- radio talkback shows
- social media platforms
- open air awareness talks
- dissemination of flyers and brochures
- one-to-one sessions with organisations
- video clips
- music (cyber security songs)
- regular rural communities' initiatives
- school educational talks.

CERTVU, during the 2020 period, published five advisories to constituents on certain threats and vulnerabilities.

We have also published our cyber smart flyers online for internet users.

COVID-19

We have seen an increase in cyber security threats and attacks compared to the past two years, as COVID-19 forced organisations and individuals to go online. Money scams are currently the second most prevalent type of attack encountered by internet users. We have also seen activities related to misinformation in relation to COVID-19. Examples include misinformation which relates to the cause of COVID-19 and misinformation surrounding the vaccination for COVID-19. This resulted in a high percentage of the population opting out of the COVID-19 vaccination.

Partnership Updates

CISA

Overview

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)

Resourcing and Constituency

CISA is divided into six divisions:

- Cybersecurity Division (CSD): The CSD leads efforts to protect federal civilian executive branch networks and to collaborate with the private sector to increase the security of critical infrastructure networks. This occurs through the following subdivisions: Capability Delivery; Threat Hunting; Operational Collaboration; Vulnerability Management; Capacity Building; Strategy, Resources & Performance; and Cyber Defense Education & Training.
- Emergency Communications Division (ECD): Established in 2007 in response to communications challenges faced during the attacks on September 11, 2001, and Hurricane Katrina in 2005, the ECD supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. CISA leads the nation's operable and interoperable public safety and national security and emergency preparedness (NS/EP) communications efforts. CISA provides training, coordination, tools, and guidance to help its federal, state, local, tribal, territorial and industry partners develop their emergency communications capabilities. CISA'S programs and services coordinate emergency communications planning, preparation and evaluation to ensure safer, better-prepared communities nationwide.
- Infrastructure Security Division (ISD): the ISD leads CISA's infrastructure security mission. The Division conducts cyber and physical exercises with federal, state, local, tribal, territorial, private sector, and international partners to enhance security and resilience of critical infrastructure. These exercises provide stakeholders with effective and practical mechanisms to examine plans and procedures, potentially identify areas for improvement, and share best practices. These exercises may also inform future planning, technical assistance, training, and education efforts. CISA offers a suite of free exercise services, resources, and materials. ISD conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and state, local, tribal, and territorial partners understand and address risks to critical infrastructure. ISD also provides information on emerging threats and hazards, such as unmanned aircraft systems and cyber security and physical convergence, so that appropriate actions can be taken. Among other critical infrastructure security and resilience programs and services, the division also facilitates vulnerability and consequence assessments as well as tools and training to partners to help partners in government and industry manage the risks to their assets, systems, and networks.

- Integrated Operations Division (IOD): the IOD provides a national capability to deliver CISA services to our stakeholders and partners across state and local governments and the critical infrastructure community. Via CISA Regions, IOD delivers cyber and physical vulnerability assessments; architecture review and design subject matter expertise; incident response support; exercise planning and support; National Special Security Event planning and support; and chemical facility inspections and site security planning to implement Chemical Facility Anti-Terrorism Standards.
- Stakeholder Engagement Division (SED): SED develops partnerships, facilitates dialogue, convenes stakeholders, and promotes awareness to help CISA achieve a secure and resilient infrastructure for the American people. SED coordinates stakeholder engagements and partnerships to support the agency's efforts to reduce national risk. SED focuses on three lines of effort:
- Strategic partnerships: SED builds strategic partnerships with federal, state, local, tribal, territorial, international, and private sector organisations, including critical infrastructure. SED supports national industry and government councils serving critical sectors, facilitating the sharing of vital information and resources, as well as enabling rapid crisis coordination. SED also identifies opportunities for collaboration to address shared needs and links stakeholder organisations with CISA subject matter experts. SED's International Affairs Branch spearheads CISA's international engagement on cyber security and infrastructure security issues worldwide.
- Stakeholder engagement strategy: SED coordinates and governs CISA's stakeholder engagement strategy, offering resources and activities based on stakeholder needs. SED's stakeholder engagement initiatives include developing targeted awareness campaigns on cyber security, infrastructure security, and emergency communications issues, as well as resources to help stakeholders develop the capabilities needed to address these threats.
- Stakeholder relationship management: SED's activities inform CISA's unified, customer-centric approach. Stakeholder relationship management enables SED to continually expand and improve engagements, services, and product offerings.
- National Risk Management Center (NRMC): the NRMC is a planning, analysis, and collaboration center within CISA, leading risk reduction efforts, and working to identify and address the most significant risks to our nation's critical infrastructure. NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to identify, analyse, prioritise, and manage these risks to help advance our nation's collective defense.

Threat landscape

CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors and delivers technical assistance and assessments to federal, state, local, tribal, and territorial stakeholders, as well as critical infrastructure owners and operators nationwide. In addition, CISA pursues collaboration with international partners to promote an open, interoperable, reliable and secure interconnected world within a global, operational and policy environment where network defenders and risk managers can collectively prevent and mitigate threats to critical infrastructure.

Common cyber threats include:

- ransomware
- supply chain
- critical infrastructure.

Awareness Raising

CISA offers seven products which contain a variety of information for users with carried technical expertise. Those with more technical interest can read and/or subscribe to CISA's Insights, Alerts, Analysis Reports, Current Activity, or Bulletins. Users looking for more general-interest pieces can read the Tips and Cyber Essentials.

CISA also recommends reviewing the National Emergency Communications Plan, Goal 6: *Cybersecurity: Strengthen the cybersecurity posture of the Emergency Communications Ecosystem*, which provides guidance on the nation's strategy to strengthen the cyber security posture of the emergency communications ecosystem.

SAFECOM provides technology tools for practitioners that support communications and cyber resilience that can be referenced as a great public resource. These resources can be found at this link: https://www.cisa.gov/safecom/technology

In addition, CISA has consolidated cyber security resources on many topics, including: election security, ransomware, and COVID-19. Our first international strategy, CISA Global, published in February, 2021, describes CISA's international vision and outlines our approach for working with international partners to fulfill our responsibilities, execute our work, and create unity of effort within our mission areas. If you are interested in learning more, please email us at CISAInternationalAffairs@hq.dhs.gov

THE RESERVE BANK OF FIJI

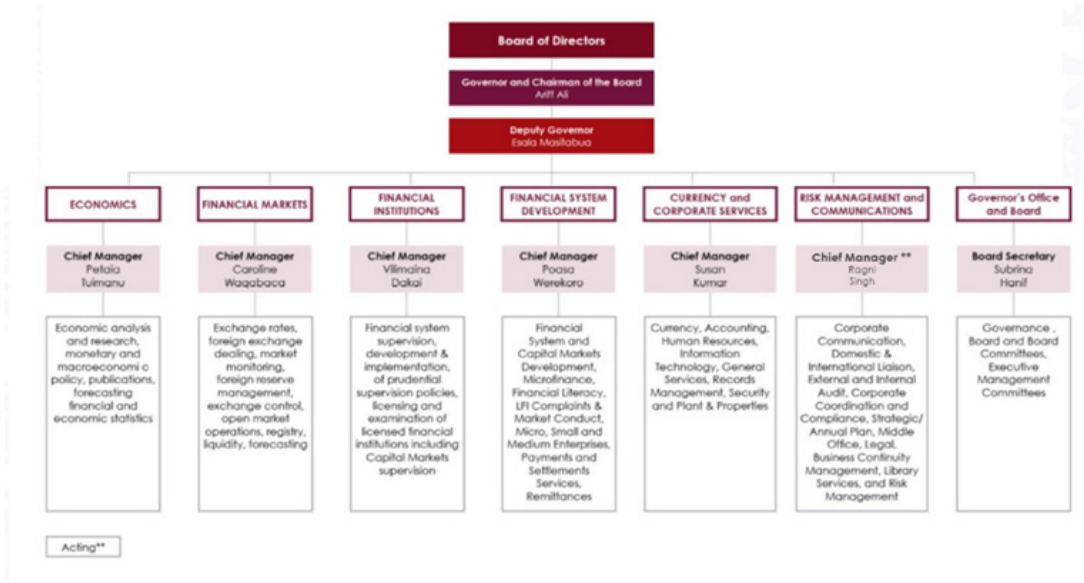
Overview

The Reserve Bank of Fiji (RBF)

Resourcing and Constituency

The RBF is the central bank of the Republic of Fiji, established in 1984 under the *Reserve Bank of Fiji Act (1983).*

As a central bank, RBF issues currency, promotes monetary stability, financial structure and regulates insurance, capital markets and securities industry. It also fosters credit and exchange conditions conducive to the orderly and balanced economic development of the country. Cyber security for financial institutions also forms part of this work which is managed by RBF and the management of RBF operations is overseen by the Board of Directors and the RBF management team.



The primary constituency of RBF is the Fijian nation – including government, business and members of the public.

Threat landscape

As a financial institution, the RBF manages a wide range of cyber threats. The most common cyber threats the RBF experiences include:

- BEC attacks
- whaling attacks
- spearphishing attacks
- port scanning attacks
- malware
- ransomware threats
- Emotet malware attacks.

Awareness Raising

As part of awareness raising efforts, RBF published the *Financial Institution Prudential Standard – Cybersecurity.*

Working Group Updates

The PaCSON Working Groups, established in 2020, are the four bodies that support PaCSON activities, and were formed in order to drive PaCSON forward to achieve whole-of-community benefits.

The PaCSON Working Groups are instrumental to PaCSON moving forward, and help to build and continue momentum. The four PaCSON Working Groups are grounded by a commitment to identify and support reliable communications; increase awareness and information sharing through hosting more regular calls; and encouraging the PaCSON Community to build upon the principles of a trusted network framework.

AWARENESS RAISING WORKING GROUP

The PaCSON Awareness Raising Working Group acts on behalf of the PaCSON Community and takes the lead on the following key initiatives:

- increase cyber security awareness in all PaCSON member nations
- increase regional collaboration among Pacific Island Countries for the purpose of security information sharing
- increase awareness and collaboration with international partners, with the aim of combatting cross-border or transnational cybercrime activities
- effectively work with the PaCSON Secretariat, PaCSON Capacity Building Working Group and the PaCSON Communication Working Group on PaCSON operations.

The Awareness Raising Working Group is responsible for raising cyber awareness on behalf of the PaCSON Community. The purpose of the Awareness Raising Working Group is to advocate the PaCSON Vision and Mission on behalf of the Community.

Figure 3: 2020 Cyber Smart Pacific campaign

2020 ARWG Activities

During the reporting period, the Awareness Raising Working Group successfully launched PaCSON's inaugural awareness raising campaign – the Cyber Smart Pacific campaign. Held during October 2020, as part of National Cyber Security Awareness Month, the Cyber Smart Pacific campaign centered on four simple, yet impactful, actions which were designed to improve the individual user's cyber security.

In 2020, PaCSON members also created seven Cyber Smart Pacific websites using campaign materials, which were kindly provided by CERT NZ under a Creative Commons Attribution Non-Commercial 4.0 International Licence. These websites, listed below, were set up to assist PaCSON members to further educate and raise the awareness of their local constituency.

- MCICT Samoa: https://mcit.gov.ws/2020/10/16/cyber-smart-pacific-2020-samoa/
- CERT VU: https://cert.gov.vu/cybersmart/
- CERT Tonga: https://www.cert.gov.to/?page_id=1305
- CERT NZ: https://www.cert.govt.nz/cybersmart/
- CERT NZ (partner resources): https://www.cert.govt.nz/cybersmart/supporters/
- Pacific Online: https://pacificonline.org/cyber-smart-pacific/
- PaCSON: https://pacson.org/cyber-smart-pacific/cyber-smart-pacific-2020

Some PaCSON members took this campaign a step further and translated the materials into their native language in an effort to encourage their communities to increase their cyber resilience so that they are less vulnerable to attacks.

CAPACITY BUILDING WORKING GROUP

The goal of the Capacity Building Working Group (CBWG) is to identify the practical steps that PaCSON members can take to build their cyber security capabilities and capacity, and identify the way in which other members of PaCSON may be able to contribute to supporting that.

A key goal for this group is to support PaCSON members to have the mechanisms, contacts and plans in place so that if a serious cyber security event were to occur, each member would be able to receive, share information and take steps to protect or recover from it.

2020 CBWG Activities

The PaCSON CBWG officially launched in March 2020 with the first virtual meeting of the Working Group. Since then, the Working Group has rolled out an ambitious agenda, including our flagship PaCSON Remote Session Series and the development of operational partnerships with local, regional, and global partners.

The PaCSON Remote Session Series was established in June 2020 to help keep the PaCSON Community connected in the face of COVID-19 challenges and restrictions and share workshops, good practices, and cases studies across the community. Between June and December 2020, the CBWG organised an hosted 10 Remote Sessions for over 190 participants from 16 economies.

Partnerships and collaboration have been a core facet of the Remote Session Series and the CBWG's initiatives. The Remote Session Series benefited from the expertise of the local, regional, and global community and the CBWG extends its appreciation to everyone who contributed to and participated in our efforts.

As a part of the Remote Session Series, an informal operational collaboration with Cyber Safety Pasifika (CSP) and the Pacific Islands Law Officer's Network (PILON) has been developed to invite members of each network to each other's relevant sessions to share expertise, better coordinate, and bring together the communities.

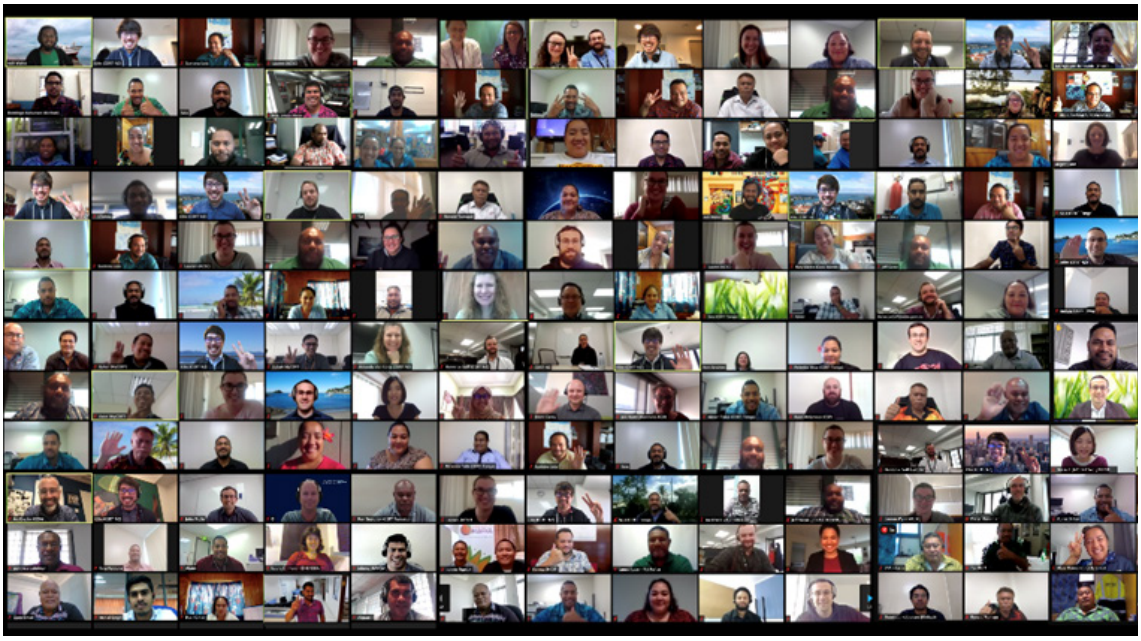


Figure 4: PaCSON Remote Session Series participants' group photo collage.

The CBWG has also worked with the APCERT Secretariat to bring the wider Asia-Pacific and PaCSON incident response communities closer together. This effort kicked off with a Remote Session featuring MyCERT in August 2020.

As part of the PaCSON CBWG-APCERT collaboration, KrCERT/CC also invited PaCSON members to participate in the annual Asia-Pacific Information Security Conference (APISC) Annual CERT Workshop, delivered in November 2020.

Additionally, CBWG worked with the Global Forum on Cyber Expertise (GFCE) to gain PaCSON members access to the GFCE capacity building sessions and workshops in April and November 2020.

The CBWG looks forward to continuing our collaborations throughout 2021.

COMMUNICATIONS WORKING GROUP

The aim of the Communications Working Group is to improve information sharing and the communication tools for the PaCSON Community. During the life of the Communications Working Group, its members will work towards achieving a collective of tools and processes to enable better communication and information sharing within the PaCSON Community. The Communications Working Group will be responsible for improving the communication outlets and information sharing processes on behalf of the PaCSON Community.

2020 Communications Working Group Activities

Throughout 2020, the Communications Working Group worked together to deliver a major outcome for PaCSON – the PaCSON website! The website exhibits many of PaCSON's efforts and is a central source of cyber security news and information. The website provides the PaCSON Community with an online identity and has the ability to amplify awareness, share information and develop capacity.

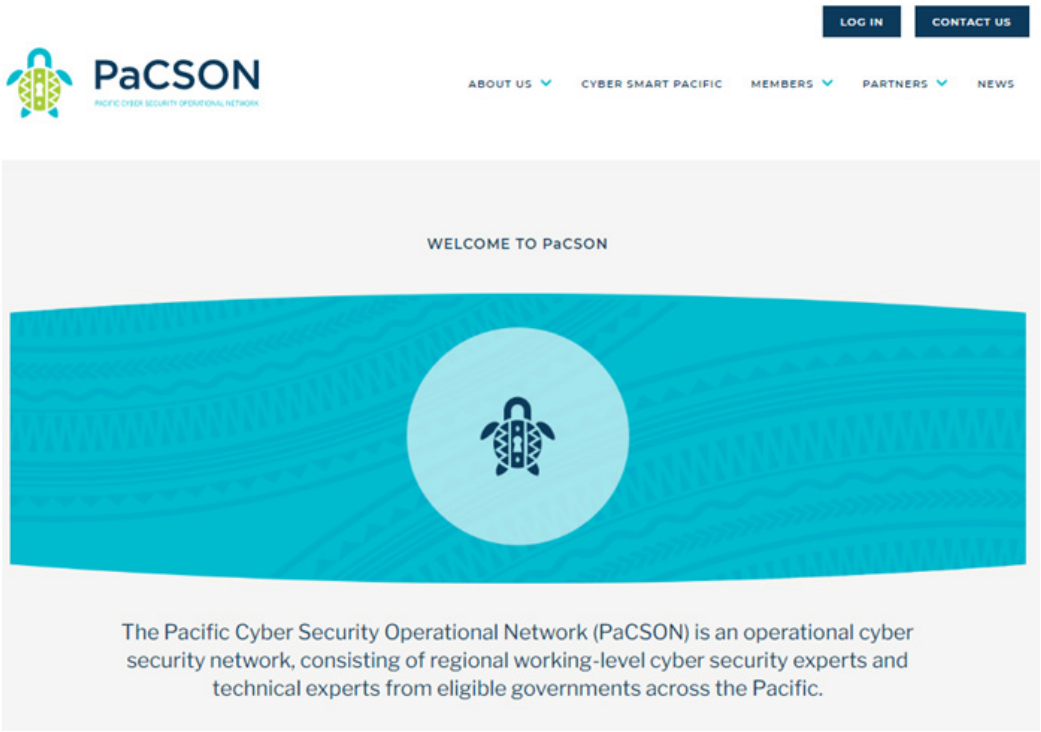


Figure 5: PaCSON webpage

Other achievements of the Communications Working Group, in 2020, include supporting the development of a suite of PaCSON policies and templates, and working collaboratively with the Awareness Raising and Capacity Building Working Groups.

PACSON PARTNERS WORKING GROUP

The PaCSON Partners Working Group is the newest PaCSON Working Group and was established in December 2020 to provide the PaCSON Partners with the opportunity to collaborate with the PaCSON primary working groups on their planned activities.

Future Plans – 2021

In 2021, the activities of PaCSON will remain flexible as the Community continues to face challenges relating to COVID-19. It is clear that, across the Pacific region, cyber criminals are targeting organisations across a range of sectors, including governments, industry, education, health, essential service providers, and operators of other critical infrastructure.

More than ever, our governments and constituencies are aware of the risks and concerned about cyber security. Yet there are few capable and prepared to defend completely against attacks. Cyber security is a shared responsibility and PaCSON is committed to coordinating activities which benefit the Pacific region.

Success in 2021 looks like:

- engaging to raise awareness and build capacity. Especially with our constituents and partners. The updated October 2021 Cyber Smart Pacific campaign will be key to achieving this, as will the increased sharing of cyber security advisories within PaCSON
- building the PaCSON brand as a trusted partner and source of truth amongst cyber security incident response professionals. Welcoming new members and partners will enable PaCSON to contribute further to strengthening the resilience of the Pacific region's cyber security posture.
- continuing to building relationships, conduct engagements and offer training opportunities which focus on the small island context of the Pacific
- delivering specialist and tailored activities that complement our efforts and help to boost the cyber security posture of the Pacific region.

Acknowledgements

PaCSON acknowledges the valuable contributions made by all of our supporting partners. The PaCSON Community is very grateful for the advice, contributions and support of all the government organisations, not-for-profit organisations, private enterprises and academic bodies who work with our network.

This report and the activities of PaCSON are made possible thanks to the support and advice of many individuals and organisations. The PaCSON Executive Committee, on behalf of the entire PaCSON Community, would like to thank everyone who contributed to PaCSON in 2020, with special thanks to:

ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM (APCERT)

APCERT cooperates with CERTs and CSIRTs to ensure internet security in the Asia-Pacific region, based around genuine information sharing, trust and cooperation.

APCERT works to help create a safe, clean and reliable cyber space in the Asia Pacific Region through global collaboration.

To learn more, please visit APCERT

ASIA PACIFIC NETWORK INFORMATION CENTRE (APNIC)

APNIC is an open, member-based not-for-profit organization, whose primary role is to distribute and manage Internet number resources (IP addresses and AS numbers) in the Asia Pacific region's 56 economies. These number resources are the building blocks for the Internet to operate and grow. As part of this service, APNIC is responsible for maintaining the public APNIC Whois Database and managing reverse DNS zone delegations.

APNIC also provides forums for Internet policy development, that are bottom-up and open to everyone.

Furthermore, APNIC helps build essential technical skills across the region, supports Internet infrastructure development, produces insightful research, and is an active participant in the multi-stakeholder model of Internet cooperation and governance.

APNIC performs these activities as part of its commitment to a global, open, stable and secure Internet that serves the entire Asia-Pacific region.

To learn more, please visit APNIC

CYBER SAFETY PASIFIKA (CSP)

Cyber Safety Pasifika is an Australian Federal Police led program and is aimed at increasing cyber safety awareness and education of vulnerable communities in the Pacific region. It is also aimed at upskilling Pacific Police officers in cybercrime investigations.

To learn more, please visit Cyber Safety Pasifika

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE (DFAT)

Australia's Cyber and Critical Tech Cooperation Program (CCTCP) works in partnership with countries in Southeast Asia and Pacific to enhance cyber resilience. Established in 2016, the CCTCP plays an important role in supporting Australia's international cyber engagement which champions an open, free and secure Internet that protects national security and promotes international stability, while driving global economic growth and sustainable development.

The CCTCP supports Australia's commitment to deliver on the United Nations 2030 Agenda for Sustainable Development which recognises the vital role of digital technologies to achieve a better and more sustainable future for all.

PaCSON acknowledges the support and funding provided by the DFAT CCTCP.

To learn more, please visit DFAT Cyber and Critical Tech Cooperation Program

GLOBAL FORUM ON CYBER EXPERTISE (GFCE)

The GFCE strengthens international cooperation on cyber capacity building by connecting needs, resources and expertise and by making practical knowledge available to the global community. The focus of the GFCE is three-fold:

- coordinate regional and global cyber capacity projects and initiatives
- share knowledge and expertise by recommending tools and publications
- match individual needs for cyber capacities to offers of support from the community as a clearing house function.

To learn more, please visit the GFCE

PACIFIC ISLANDS LAW OFFICERS NETWORK (PILON)

PILON works to ensure a safe and secure Pacific by advancing key law and justice issues. PILON is an association of senior law officers from 19 Pacific Island countries and territories.

To learn more, please visit PILON

Glossary

- ACSC – Australian Cyber Security Centre
- APCERT – Asia Pacific Computer Emergency Response Team
- APISC – Asia-Pacific Information Security Conference
- APNIC – Asia Pacific Network Information Centre
- APT – Asia Pacific Telecommunity
- ARWG – Awareness Raising Working Group (PaCSON)
- ASD – Australian Signals Directorate
- BEC – Business Email Compromise
- CBWG – Capacity Building Working Group (PaCSON)
- CCTCP – Cyber and Critical Tech Cooperation Program
- CEO – Chief Executive Officer
- CERT – Computer Emergency Response Team
- CERT NZ – Computer Emergency Response Team New Zealand
- CERT Tonga – Computer Emergency Response Team Tonga
- CERTVU – Computer Emergency Response Team Vanuatu
- CISA – Cybersecurity and Infrastructure Security Agency (US)
- CSD – Corporate Services Department (NICTA, PNG)
- CSD – Cybersecurity Division (CISA, US)
- CSIRT – Computer Security Incident Response Team
- CSP – Cyber Safety Pasifika
- DDOS – Distributed Denial of Service
- DFAT – Department of Foreign Affairs and Trade (Australia)
- DGTO – Digital Government Transformation Office (Fiji)
- DHS – Department of Homeland Security (US)
- DOS – Denial of Service
- DTA – Digital Transformation Authority (Samoa)
- EC – Executive Committee (PaCSON)
- ECIA – Economics, Consumer and International Affairs (NICTA, PNG)
- ECD – Emergency Communications Division (CISA, US)
- ERPD – Engineering & Resource Planning Department (NICTA, PNG)
- FSC – Financial Supervisory Commission (Cook Islands)
- GFCE – Global Forum on Cyber Expertise
- ICT – Information and Communications Technology

- ICT-TWG – ICT Technical Working Group for Government (Samoa)
- IOD – Integrated Operations Division (CISA, US)
- ISD – Infrastructure Security Division (CISA, US)
- IT – Information Technology
- ITCS – Department of Information Technology and Computing Services (Fiji)
- ITU – International Telecommunication Union
- KrCERT/CC – Korea Internet Security Centre
- LED –Licensing & Enforcement Department (NICTA, PNG)
- LOL – Living off the Land (malware)
- MCIT – Ministry of Communications and Information Technology (Samoa)
- MEIDECC – Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (Tonga)
- MIA – Ministry of Internal Affairs (Tonga)
- MICTTD – Ministry of Information, Communication, Transport and Tourism Development (Kiribati)
- MOF – Ministry of Finance (Tonga)
- MyCERT – Malaysia CERT
- NCSC – National Cyber Security Centre (UK)
- NGO – Non-Government Organisation
- NICTA – The National Information and Communications Technology Authority (PNG)
- NRMC – National Risk Management Center (CISA, US)
- OGCIO – Office of the Government Chief Information Officer (Vanuatu)
- PaCSON – Pacific Cyber Security Centre Operational Network
- PILON – Pacific Islands Law Officers Network
- PMU – Project Management Unit (Cook Islands)
- PNGCERT – Papua New Guinea Computer Emergency Response Team
- PSC – Public Service Commission (Tonga)
- RBF – The Reserve Bank of Fiji
- SamCERT – National Computer Emergency Response Team (Samoa)
- SED – Stakeholder Engagement Division (CISA, US)
- SIG – Solomon Islands Government
- SIG ICTS – Solomon Islands Government Information Communication Technology Services
- SITA – Samoa Information Technology Association
- SMPP – Samoa Ministry of Police and Prisons
- TCL – Tonga Cable Limited (Tonga)
- TLP – Traffic Light Protocol (ACSC)
- UAS – Universal Access Scheme Secretariat (NICTA, PNG)

Disclaimer

“The contents of the Membership and Partnerships updates are written by each PaCSON Member or Partner, based on their individual analysis and experience. Responsibility for the information and views expressed in each update lies entirely with the Member or Partner”.

PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

pacson.org