
PaCSON
PACIFIC CYBER SECURITY OPERATIONAL NETWORK
ANNUAL REPORT
2023

TLP:CLEAR = Disclosure is not limited.

Sources may use TLP:CLEAR 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:CLEAR 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.

PaCSON 2023 ANNUAL REPORT

Contents

From the Chair

FROM THE CHAIR

The Pacific Cyber Security Operational Network (PaCSON) has been operational for 6 years now, after its launch in 2017, as an initiative by the Australian Government to assist the Indo-Pacific region. Since then, there has been no turning back. From the 16 founding members, PaCSON has extended its collaboration to include 4 critical partners and 3 reputable organisations as friends of PaCSON.

Despite the different challenges we faced in our respective economies, we continue to soldier on, come what may, in any way possible to achieve our shared vision which is to improve cyber security capabilities and readiness across the Pacific.

Throughout 2023, PaCSON continued to serve as a vital platform for collaboration, knowledge-sharing, and capacity-building initiatives among our Pacific member states.

Our collective reports have not only enhanced our ability to address emerging cyber threats but also strengthened the overall cyber resilience of our nations. One of the notable highlights of 2023 was the participation of PaCSON members in the Forum of Incident Response and Security Teams (FIRST) annual conference, held in Montreal, Canada. This global event provided a valuable opportunity for our cyber security professionals to exchange insights, best practices, and technical expertise with their international counterparts, further enriching our collective understanding of cyber defence strategies and tactics.

Additionally, I am pleased to report the successful launch and implementation of the Cyber Smart Pacific (Cyber Up) Initiative, a collaborative effort to promote cyber security awareness and education across the region.

Furthermore, we successfully hosted the 2023 Annual General Meeting (AGM) in the heart of Port Vila, Vanuatu. In conjunction with the FIRST Pacific Symposium, the symposium provided a platform for stakeholders from the government and private sectors across the Pacific to engage in meaningful discussions, share insights, and forge partnerships to strengthen cyber incident response capabilities in the region.

I am also pleased to acknowledge the constant success of each of our working groups, which includes the Awareness Raising Working Group, Capacity Building Working Group, Communication Working Group, and the Partners Working Group. Through their dedicated efforts, these working groups have facilitated information exchange, fostered collaboration, built capabilities through capacity building programs, and promoted best practices in their respective areas, contributing significantly to our collective cyber resilience.

As we look ahead to the challenges and opportunities, PaCSON remains steadfast in its commitment to promoting a safe, secure and resilient cyber ecosystem in the Pacific region. Together, we will continue to leverage our collective expertise, resources and partnerships to address evolving cyber threats, and safeguard the digital future of our nations.

I extend my heartfelt gratitude to all PaCSON members, the 2022–23 PaCSON Executive Committee and the Secretariat for their unwavering dedication, commitment and contributions throughout the past year. Your continued support and collaboration are invaluable as we work together to navigate the complex cyber landscape and build a more secure and prosperous future for our region.

Thank you
Vanuatu, Chair, PaCSON Executive Committee

Program Overview

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 region's 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 made up of Pacific working-level cyber security experts. PaCSON coordinates activities that aim to benefit the regional network of cyber security incident response professionals. Some of the main ways we do this is through training and awareness-raising, which are underpinned by 3 guiding pillars:

- encouraging collaboration on best practice
- increasing sharing on threats and related information
- supporting and developing incident response capability.

The PaCSON community consists of representatives from eligible Pacific governments and private organisations. Membership of PaCSON includes 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 can join the network. Partners are other government organisations, not-for-profit organisations and academia. The partner organisations of PaCSON include the Reserve Bank of Fiji (RBF), the US's Cyber Security Infrastructure & Security Agency (CISA) and Federal Bureau of Investigation (FBI).

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. Instead, the network maintains 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) that 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 any of the EC positions.

The structure of the PaCSON EC included:

	2022	2023
Chair	Tonga	Vanuatu
Deputy Chair	Cook Islands	Kiribati
Incoming Chair	Vanuatu	Cook Islands

The PaCSON Secretariat supports the PaCSON community and the EC in all matters. The Australian Cyber Security Centre (ACSC) performs the function of the PaCSON Secretariat. The ACSC absorbs all the costs associated with this function. The PaCSON Secretariat supports PaCSON members and PaCSON 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.

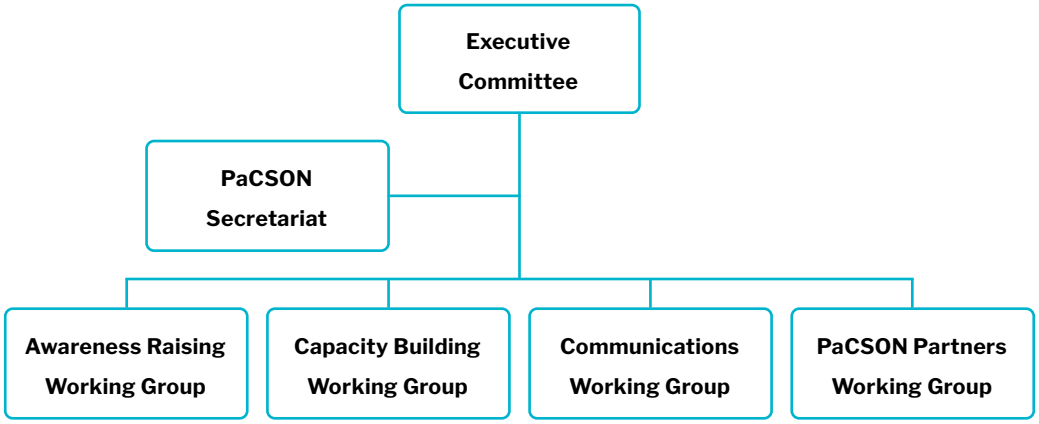


Figure 1. PaCSON governance structure

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.

PaCSON Annual General Meeting

PaCSON ANNUAL GENERAL MEETING

The 2023 PaCSON Annual General Meeting (AGM) was held in Port Vila, Vanuatu from 18 to 22 September, and was an opportunity for the PaCSON community to reconnect in person. PaCSON members, PaCSON partners, friends and observers came together to collaborate and share key cyber security findings in the region.

Figure 2. PaCSON 2023 Annual General Meeting attendees

As this was the largest attendance at an AGM yet, it was the perfect opportunity to reflect on all the work that has been done to make PaCSON what it is today, and to look forward to what it could become in the future.

The AGM provides the community, particularly members, with the chance to work directly alongside each other. It was a great chance to share information and learn from other experts. It was an opportunity to re-establish relationships that had been built over the preceding years. Strengthening these relationships continues to produce an environment of openness and mutual trust, which leads to greater opportunities for learning.

2023–24 Executive Committee

As part of the AGM, the PaCSON community held an election for the Executive Committee membership. Former Chair, CERT Vanuatu and the host of the 2023 AGM, gracefully handed over the role to the Incoming Chair, the Cook Islands. The community excitedly welcomes the new Executive Committee for 2023–24, which is:

- the Cook Islands as Chair
- Papua New Guinea as Deputy Chair
- Kiribati as Incoming Chair.

The new EC will represent and make decisions on behalf of the PaCSON community for the next 12 months.

After the vote, CERT Vanuatu was farewelled as Chair. It was highly commended for its proactive approach to the task and its engagement in the EC. In its role as Chair, CERT Vanuatu served the community thoughtfully and took a hands-on approach, ensuring that decision-making by the EC was always done in the best interest of the community. CERT Vanuatu played a large role in the expansion of the community, exemplified by its endorsement earlier in the year for FIRST to become a partner of PaCSON. FIRST's application was successful, and it officially became a partner in March 2023.

CERT Vanuatu is also commended for its wonderful hospitality, and for its efforts towards ensuring a successful AGM in Vanuatu. The team went above and beyond to facilitate the event, and was ever-present throughout the week to ensure all participants were comfortable and well-supported. Participants particularly enjoyed the cultural leading ceremony, the address from the Prime Minister of Vanuatu, and the various social events hosted by the team. The AGM would not have run as smoothly as it did without the efforts of CERT Vanuatu, and for that, the community is very grateful.

Throughout the 3 days of the AGM, the PaCSON community took part in a range of activities and discussed many topics, some of which included:

- a Capture the Flag Cyber Challenge, which was a favourite among the community, with many PaCSON members taking part and competing to come out on top. Congratulations to the team from Fiji, who ended up capturing the most number of cyber 'flags' and winning the challenge
- sharing information on cyber threats and learning from each other about how to best target and mitigate against these threats
- a presentation from CERT Vanuatu about the cyber incident that occurred in the country. This presentation gave unique insights into a serious cyber incident in a Pacific country, including a walkthrough of the event and advice on how to defend against a similar incident.

Looking ahead to 2024 and the AGM in the Cook Islands

The 2023 AGM provided members, partners, friends and observers the opportunity to come together as a community and share knowledge and experiences. Interacting in person is an invaluable experience for the community, and provides the chance to collaborate and communicate directly with each other. Through this cooperation, the PaCSON community is strengthened and ready to continue defending against cyber threats in the region together.

Throughout the AGM, members discussed what the priorities should be for 2024, and proposed ideas on what could be done to help PaCSON continue to grow and serve the needs of the community. The EC and the Secretariat will start work on sharing these priorities and making progress on exploring and implementing the suggestions raised.

The community is already looking forward to next year's AGM, which will take place in the Cook Islands.

Member Updates

AUSTRALIA

Australian Cyber Security Centre

The Australian Cyber Security Centre (ACSC) is based within the Australian Signals Directorate (ASD). We provide advice and information about how to protect individuals, families and businesses online. The ACSC's cyber security mission is supported by ASD's wider organisation. We lead the Australian Government's efforts to improve cyber security. Our role is to help make Australia the most secure place to connect online. ASD is a statutory agency within the Defence portfolio which reports directly to the Minister for Defence.

All Australians can report a cyber security incident or cybercrime via ReportCyber (cyber.gov.au) or by contacting the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

During the reporting period, the top 3 cybercrime types for individuals were:

- identity fraud
- online banking fraud
- online shopping fraud.

During the reporting period, the top 3 cybercrime types for businesses were:

- email compromise
- business email compromise (BEC) fraud
- online banking fraud.

The primary constituency for the ACSC includes:

- federal, state and territory government agencies
- large organisations and critical infrastructure
- small and medium business
- individuals and families.

Threat landscape

Malicious cyber activity continued to pose a risk to Australia's security and prosperity in the 2022–23 financial year. A range of malicious cyber actors showed the intent and capability needed to compromise vital systems, and Australian networks were regularly targeted by both opportunistic and more deliberate malicious cyber activity.

ASD responded to over 1,100 cyber security incidents from Australian entities in 2022–23. Separately, nearly 94,000 reports were made to law enforcement through ReportCyber – around one every 6 minutes.

In the 2022–23 financial year:

- Average cost (AUD) of cybercrime per report, up 14%:
  - small business: $46,000
  - medium business: $97,200
  - large business: $71,600
- Nearly 94,000 cybercrime reports, up 23%:
  - a report every 6 minutes (on average)
  - an increase from 1 report every 7 minutes.

Raising awareness

The ACSC answered over 33,000 calls to the Australian Cyber Security Hotline, up 32%:

- 90 calls per day (on average)
- an increase from 69 calls per day.

In the 2023, ASD's ACSC:

- responded to over 1,100 cyber security incidents, similar to last year
- noted that 10% of all incidents responded to included ransomware, similar to last year
- notified 158 entities of ransomware activity on their networks, compared to 148 last year, roughly a 7% increase
- Cyber threat intelligence sharing partners grew by 688% to over 250 partners.

The Cyber Hygiene Improvement Program (CHIP):

- issued 103 high-priority operational tasking reports, up 110%
- distributed 4,900 reports (up 16%) to approximately 1,360 organisations (up 32%).

The Critical Infrastructure Uplift Program (CI-UP):

- completed 3 CI-UPs covering 6 CI assets
- 3 CI-UPs in progress
- sent 20 CI-UP Info Packs
- held 5 CI-UP workshops
- notified 7 critical infrastructure entities of suspicious cyber activity, up from 5 last year
- published or updated 34 PROTECT and Information Security Manual (ISM) guidance publications
- published 64 alerts, advisories, and incident and insight reports on cyber.gov.au and the Partnership Portal.

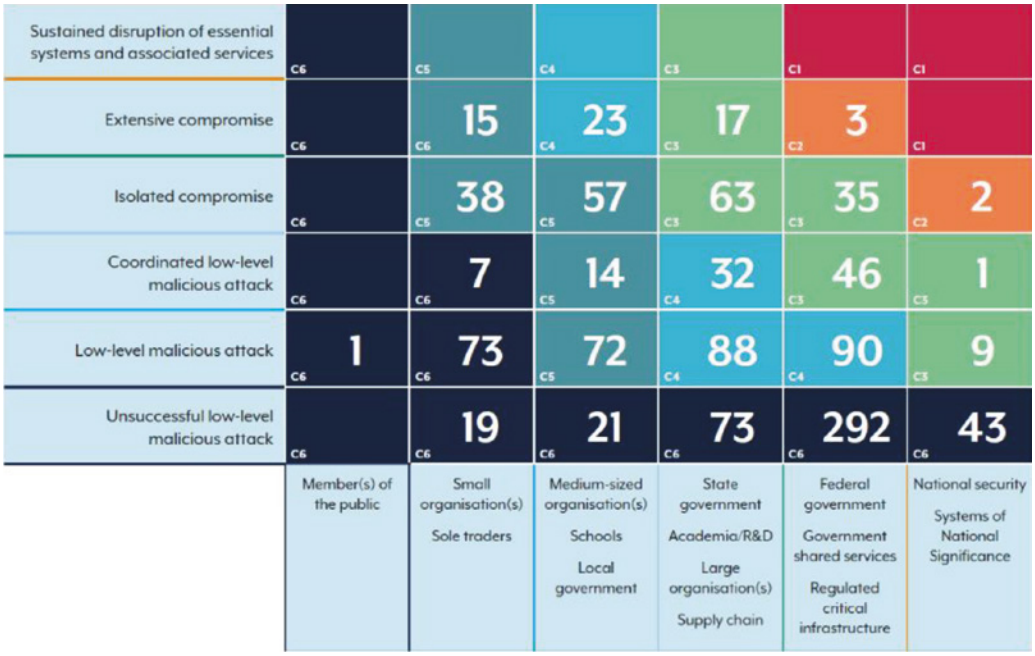


Figure 3. Cyber security incidents by severity category for FY 2022–23 (total 1,134)

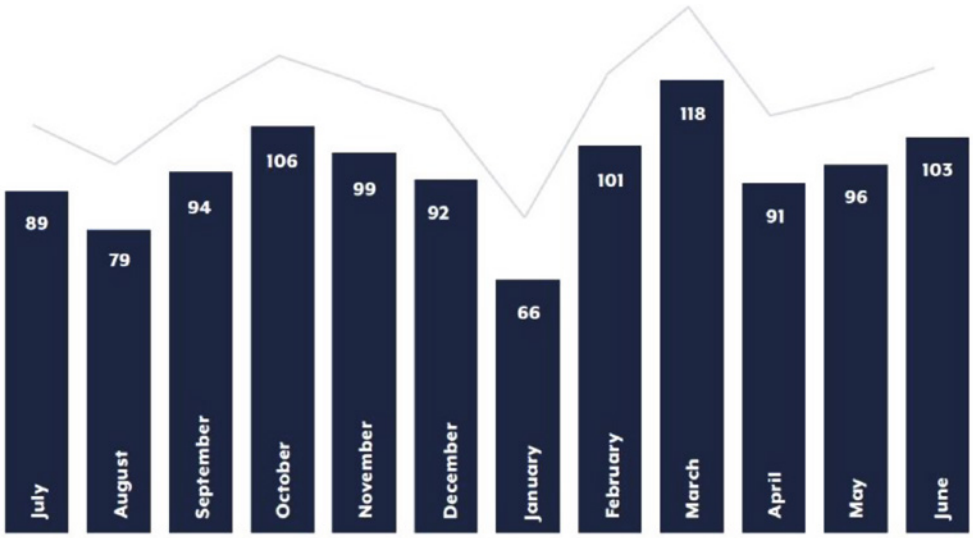


Figure 4. ASD responded to over 1,100 cyber security incidents, around the same as in the last financial year

In the 2023 calendar year, ASD's ACSC:

- released the ASD 2023 Cyber Threat Report
- published or updated 34 PROTECT and ISM guidance publications
- published 64 alerts, advisories, and incident and insight reports on cyber.gov.au and the partnership portal.

Case studies

In January 2023, a federal government entity engaged a cyber security company to conduct penetration testing on its systems. The company identified serious vulnerabilities in a software product used by the entity. The software was installed on the entity's network and was part of its Software-as-a-Service (SaaS) offerings.

Once informed of the vulnerabilities, the entity contacted other known users of the software, including other government entities. The entity also authorised the cyber security company to report the identified vulnerabilities to both the software vendor and ASD. ASD, using the CHIP scanning capability, identified and informed other impacted entities that were operating the same software. ASD also warned international partners of the vulnerabilities.

The identification of the vulnerable software and the subsequent notification to impacted parties gave users the opportunity to mitigate the threat of potential exploitation, while the software vendor developed and released patches. As a result of these actions, no instances of compromise were detected.

COOK ISLANDS

National ICT Office

The ICT Office is a division of the Office of the Prime Minister (OPM), and maintains the government network by providing IT services to 45 government agencies and state-owned enterprises (SOEs). It administers funds for software, licensing, data services and capital investments. The division has 5 core staff reporting to the Director of ICT who reports to the Chief of Staff. Private contractors, that are based locally and overseas, also support the organisation. Citizens can report cyber incidents in the Cook Islands directly to the police, the Financial Intelligence Unit, the Department of Internal Affairs or to the ICT Division of the OPM.

Threat landscape

In 2023, there was an increase in cyber incidents inside our borders. During the reporting period, the top 3 cyber incidents were:

- spam
- viruses and malware
- phishing.

These issues were addressed by filtering and informing users to block and delete (spam); using a quarantine process and, if necessary, deleting and cleaning affected devices (viruses and malware); and informing users to block and delete emails (phishing).

Awareness raising

OPM is a partner of getsafeonline.org.ck, and leads media releases on major cyber events. Advisory notes are provided directly to government users via the gov.ck domain.

Case study

During the reporting period, there was much work undertaken in infrastructure upgrades, including migration of servers to the data centre, upgrades to the Vodafone MPLS fibre network, outer island 03B satellite 4G connectivity, and rollout of MS360 licensing and Fortinet.

Policies released in the period included:

- National Security Policy (including cyber security)
- National ICT Policy 2023
- Cook Islands E-commerce Acceleration Work Plan June 2023
- National Digital Strategy 2024–2030.

Development of a national cyber security policy and cyber investment plan is underway, along with legislative reviews of cybercrimes.

FIJI

Ministry of Communications

There are 3 departments under the Ministry of Communications:

- Department of Communications
- Digital Government Transformation Office
- Department of Information, Technology and Computing Services.

The Minister for Trade, Co-operatives, Small and Medium Enterprises, and Communications is the Hon Manoa Seru Kamikamica, with Mr Shaheen Ali as the Permanent Secretary, and Ms Tupou'tuah Baravilala as the Director-General for Digital Government Transformation, Cybersecurity and Communications. Our primary constituencies are the ministers, general public, telecommunication sector stakeholders, private sector and government.

Depending on the nature of cyber incidents and cybercrimes, reports can be made to the following entities:

- Fiji Police Force: https://www.police.gov.fj/
- Fiji Independent Commission Against Corruption (FICAC). For more information refer to website: https://ficac.org.fj/
- Fiji Financial Intelligence Unit (FIU): https://www.fijifiu.gov.fj/
- Online Safety Commission (OSC). For more information refer to website: https://onlinesafetycommission.com/.

Threat landscape

During the reporting period, the top 3 types of cyber incidents were:

- malware
- phishing
- distributed denial of service (DDoS).

We monitor and respond to security incidents on the government network such as phishing emails received by the users, malware/ransomware detections on the devices, DDoS attacks on our network, brute force attacks, DNS tunnelling, etc. There has been an increase in the number of detected security incidents in general that we triage and investigate based on our monitoring and security tools in place within the organisation.

Raising awareness

Within the civil service and also for the public, when launching national initiatives, cyber security is a core component in our communications and PR strategy.

Security advisories, ITC advisories and awareness raising of critical vulnerabilities are also disseminated to government ministries and agencies.

Case study

2023 achievements

Successfully hosted the 2023 Asia Pacific Telecommunity Policy and Regulatory Forum (APT PRF 23)

Fiji hosted the 23rd Asia Pacific Telecommunity (APT) Policy and Regulatory Forum (PRF) from 20 June to 22 June 2023. This three-day event brought together 155 member representatives, of which 79 representatives from Australia, China, India, Indonesia, Kiribati, Malaysia, Samoa, Sri Lanka, Thailand, Tonga, Vanuatu and Vietnam were present in person.

Lagatoi Declaration

On 28 August 2023, the Pacific ICT ministers and senior delegates from 13 countries and territories met at APEC Haus, Port Moresby, Papua New Guinea. The Lagatoi Declaration was signed at this meeting and is a significant step forward for the Pacific region in addressing legacy challenges and coordinating efforts to harness the power

of ICT and digital transformation for sustainable development. The Declaration provides a comprehensive roadmap for action, and the Pacific ministers are committed to working together to achieve its goals.

Starlink licensed in Fiji

On 10 November 2023, Starlink, a leading provider of low Earth-orbiting satellite systems, had been granted a spectrum licence by the Ministry of Trade, Co-operatives, SMEs and Communications, and a telecommunications licence by the Telecommunications Authority of Fiji. This marks a significant step for Fiji – granting the rights to Starlink to provide internet services to businesses and customers in Fiji, providing low latency, high speeds and a simple plug and play setup.

Girls in ICT Day

The ministry hosted the inaugural Girls in ICT Day in the country with Vunimono High School being selected as the pilot school. This is a United Nations – International Telecommunications Union initiative. A regional opening was conducted, followed by a series of training and mentorship programmes at Vunimono High School over a period of 4 months. A cohort of 55 girls were a part of this programme ranging from 15 to 18 years old. This is an ongoing programme.

Upgrade of end-to-end cyber security solution

Implementation of these solutions allows ITC to analyse traffic on the network and uncover unknown threats. It will be able to detect early stages of attacks or unusual behaviour within the environment.

Overall, the protection the above upgrades provides in combination with existing platforms, is world-class and will give the ITC team members and users a lot of confidence in the security of the environment. With the introduction of these cyber security solutions, it will enable ITC to fulfil its long-term plan on security monitoring.

KIRIBATI

The Kiribati National Computer Emergency Response Team

In 2023, the Kiribati National Computer Emergency Response Team (CERT-KI) undertook a series of impactful cyber security initiatives aimed at enhancing awareness, resilience and response capabilities across various sectors.

Awareness Raising

Establishing CERT-KI

The establishment of the National CERT is enshrined and legalised under the Digital Government Act 2023, which was passed by Parliament in August 2023. The Act also gives CERT its obligations and roles both in government and on a national level on cyber security, both in a response and prevention (proactive) role.

Cyber security awareness programs

Conducted cyber security awareness programs targeting schools, communities, non-government organisations (NGOs) and ministries. These initiatives aim to educate Kiribati citizens (internet users) about the importance of cyber security, common threats and best practices for staying safe online. Our focus this year is on scams and phishing emails, especially on social media.

Enforcing two-factor authentication

CERT-KI successfully enforced two-factor authentication (2FA), or the use of multifactor authentication, enhancing security measures for accessing sensitive information. Efforts are ongoing to expand 2FA implementation to all line ministries, NGOs and state-owned enterprises (SOEs). The Digital Government Act 2023 also enshrines and acts as an instrument to compel government agencies to use 2FA or any security mechanism that will improve overall security.

Participating in training and international forums

CERT-KI represented Kiribati in the UN Cybercrime Treaty negotiation voicing a need for greater respect of human rights for intrusive powers under this treaty. One of our team members was also certified as an Interpol-certified trainer to assist our law enforcement in cybercrime training needs. The team also represented Kiribati at the council of Europe's Cyber Crime Convention bi-annual meeting to indicate Kiribati's deposit of accession instruments in 2024.

Responding to cybercrime cases

In 2023 there were 2 major incidents involving government agencies being targeted and becoming victims of spear phishing attacks. We have observed that phishing emails have also been very convincing and are hard to detect that they are not authentic emails. One case was pretending to be an API Security Review which clicking on a button to review will land users on a fake sign in page. We saw the importance of 2FA and how it can prevent further potential intrusion to any system. As such we have rolled out an enforcement of 2FA for public-facing systems across government.

Training in cyber security for ICT taskforce and law enforcement officials

Organised cyber security training sessions for the ICT Taskforce & Law Enforcement officials. These training sessions, led by CERT NZ and the Council of Europe, provide valuable insights on cyber security threats, digital forensics and incident response, and strengthened the capacity of law enforcement personnel in identifying, investigating and prosecuting cybercrime activities.

Sharing information

Facilitating the sharing of threat intelligence and best practices among government agencies, private sectors and other stakeholders.

NAURU

The Department of Information, Communication and Technology

The department sits under the Ministry of Telecommunications and is currently made up of 26 staff members, plus the Head of the Department, the Minister and the Deputy Minister.

Threat landscape

Citizens of Nauru report their cyber concerns directly to the Nauru Police Force through direct walk ins, phone calls or Facebook chats. Public service employees report to us either in person or via phone call and email.

Our most commonly reported cyber threats were:

- lack of citizen awareness and skills
- phishing
- pyramid schemes.

Awareness raising

ICT used materials from PaCSON to conduct workshops within the government departments, schools and communities. We also conducted radio announcements in both English and Narau to raise cyber awareness in society. A National Cyber Roadmap has been developed and is in its consultation stages for approval. More information about ICT in Narau can be found on the Republic of Nauru official website at http://www.nauru.gov.nr/.

Important cyber milestones in 2023 include:

- CERT NZ in-country visit in May 2023
- Nauru Cyber Maturity Model review by Oceanic Cyber Security Centre (OCSC) in late 2022 and a report was completed in early 2023. A draft roadmap has been developed from this also in 2023.
- During the Nauru Government Annual Public Service Day in November 2023, ICT had a stall set up where ICT responsibilities, services and equipment were explained to the public. PaCSON Cyber Up materials were also shared for awareness raising.

NEW ZEALAND

Computer Emergency Response Team New Zealand

In 2023, the Computer Emergency Response Team New Zealand (CERT NZ) was integrated into the Government Communications Security Bureau (GCSB) as part of the National Cyber Security Centre (NCSC). The objective of the integration was to create a single leading cyber security agency for New Zealand that addresses the needs of nationally significant organisations, critical infrastructure, and businesses and individuals.

CERT NZ currently has 36 staff working in operations, communications and engagement, governance, and analytical reporting. CERT NZ also has a contact centre to receive incident reports.

CERT NZ specifically 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.

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 incident response counterparts when they identify affected New Zealand organisations in their investigations.

CERT NZ also has a dedicated Pacific Partnership Team that works closely with Pacific incident response counterparts and the wider regional cyber community. Our Pacific programme delivers 2 primary lines of effort, which are business-as-usual collaboration and standalone response programming.

Business-as-usual activities include:

- sharing information
- developing good practice
- engaging community and developing rapport
- mentoring, both formal and informal
- directing incident response support
- reaching out to communities
- contributing to PaCSON, including convening the PaCSON Capacity Building Working Group
- supporting, advising, and contributing to national, regional and global cyber capacity building.

Responsive programming since January 2023 has included:

- PaCSON Remote Session Series – 6 sessions for 135 participants in 2023
- Awareness Raising Working Group – collaborating on developing and delivering the Cyber Smart Pacific (Cyber Up) annual regional awareness raising campaign
- Pacific Data and Insights Project with the Shadowserver Foundation – providing localised data to each PaCSON member
- in-country bilateral meetings and training with Tonga, Kiribati and Nauru
- partnering with SamCERT to deliver Samoa's first Cyber Smart awareness raising roadshow
- partnering with CERT Tonga to deliver Tonga's first Cyber Smart Week
- sharing CERT NZ reporting templates
- continuing collaboration with CERT Tonga on a Cyber Security Workforce Development Program
- publishing the Vulnerability Disclosure Policy and process.

Incidents can be reported to CERT NZ through an online reporting tool, by phone, or through our referral partners. Full contact details are available here:

- CERT NZ website: https://www.cert.govt.nz/about/contact-us/
- for Individuals and Businesses: https://www.cert.govt.nz/individuals/report-an-issue/
- website for IT Specialists: https://www.cert.govt.nz/it-specialists/report-an-incident/.

Threat landscape

In 2023, there were 7,935 incidents reported to CERT NZ. Individuals, small businesses and large organisations from all over New Zealand submitted incident reports.

Of those reported, 24% included some form of financial loss, with a combined total loss of NZD $18.3 million.

The top 3 incident categories in 2023 were:

- phishing and credential harvesting
- scams and fraud (accounting for over 85% of all reported financial losses)
- unauthorised access.

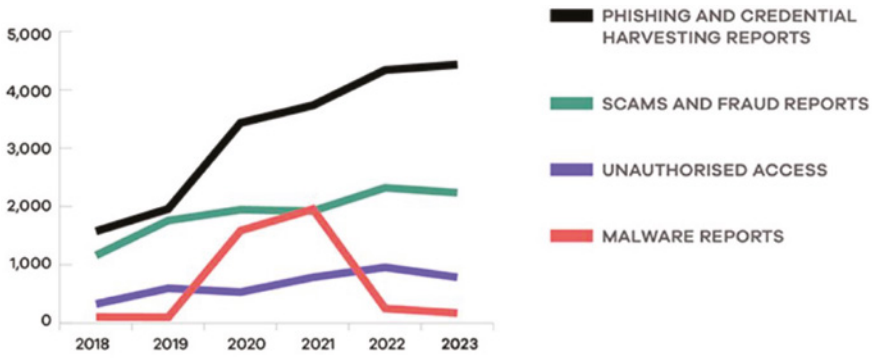


Figure 5. Trends in incidents reported to CERT NZ, 2018–23

CERT NZ supports victims with any form of cyber security incident. These may include:

- ransomware incidents
- phishing and credential harvesting
- malware
- scams and fraud
- unauthorised access
- website compromise.

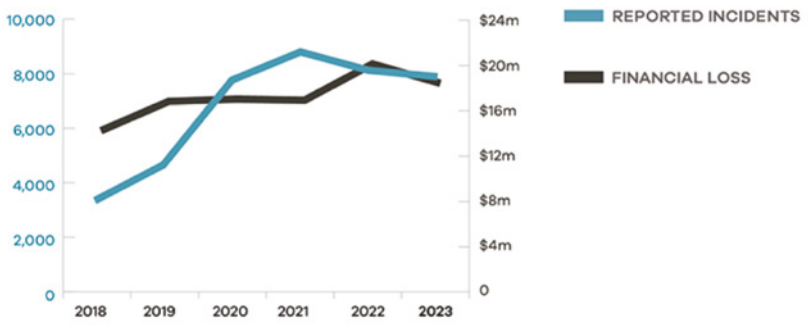


Figure 6. Report trends received by CERT NZ and impacts, 2018–23

CERT NZ reviews and assesses any threats reported, and uses this information to develop mitigation advice that it can share with those reporting the incident as well as with the rest of the community.

When CERT NZ receives a report, it also assesses whether that report is best investigated by a partner agency and, if so, refers the incident to them. Information provided to CERT NZ is confidential and consent is sought before sharing any details of a report.

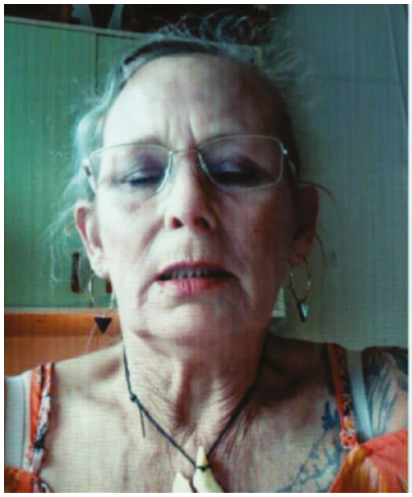
There has been a slight decrease (3%) in the number of reports received in 2023 compared to 2022.

Awareness raising

In October, CERT NZ delivered the seventh annual NZ Cyber Smart Week. CERT NZ had 7 key industry partners, and over 1000 organisations sign up as supporters to help share the message with their extensive customer base.

To launch Cyber Smart Week 2023, CERT NZ created 'EXPOSED: Through the Lens of a Hacker', a free public exhibition of photographs featuring real New Zealanders who have been affected by an online incident and want to share their experiences.

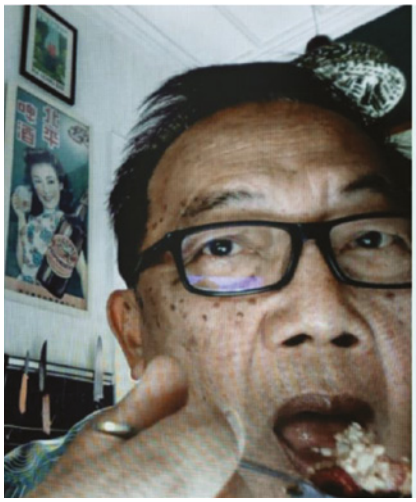
These stories were also shared across various social platforms to raise awareness of the very real harms of cyber incidents to everyday New Zealanders. CERT NZ also provided content to partners and supporters to share with relevant stakeholders.



In real time scam

Subject name: Glenis
Incident Type: Phone scam

Glenis was the target of a scam phone call. She was contacted by a woman who claimed to be from the bank. They told Glenis they were investigating her account due to a few interesting transactions, all the while discussing specific and accurate account information. Glenis panicked and gave up way too much information too quickly. She had been a target of a scam before and wanted to cooperate. She then watched in distress as her money was transferred from one account to another and then go out of her account completely, all in real time. For Glenis, the emotional toll has been far worse than the financial one.



Hostage in Manila

Subject name: William
Incident Type: Impersonation scam

William was the target of an impersonation scam. He was on holiday in Malaysia when he received a text from a friend who travels regularly, saying he was being held hostage at his hotel in Manila. The hostage takers wanted $800 before they would release him and his passport. The texts kept coming, sounding more and more desperate each time so William transferred the money. As soon as the money was gone, he realised he had been scammed. His friend was safe at home, and he was out of pocket. He regrets not picking up the phone and calling his mate first.

Figure 7. Cyber incidents stories shared with CERT NZ. See ownyouronline.govt.nz for more information

In addition to these awareness raising activities part of October International Cyber Awareness Month, CERT NZ supported the development and refresh of the collaborative Cyber Up initiative. It is the third year CERT NZ has been a part of the initiative, through the PaCSON Awareness Raising Working Group.

Figure 8. Cyber Up Pacific campaign creative

In 2023, the working group – led by SamCERT – proposed and voted on themes, developed additional characters and messaging, taglines, and materials, building on the messaging and success of the 2022 Cyber Up Pacific Campaign. To support the Cyber Up Pacific Campaign, CERT NZ developed 6 awareness raising videos which focused on the key steps individuals, communities and businesses can take to be secure online.

Figure 9. Cyber Up Pacific campaign awareness raising video

CERT NZ regularly publishes Advisories and Guides and make these available on the CERT NZ website.

In addition, CERT NZ's quarterly 'Cyber Security Insights' continued in 2023. Two reports are published each quarter:

- Quarterly Insights: Highlights document, focusing on selected cyber security incidents and issues
- Quarterly Insights: Data Landscape document, providing a standardised set of results and graphs for the quarter.

In 2023, CERT NZ launched a brand new awareness raising platform, 'Own Your Online', as part of the New Zealand Government's work on raising understanding of cyber security issues for individuals and business. The development of the program and associated campaign was underpinned by consumer research from 2022 to better understand how to motivate New Zealanders to take action in cyber security.

A key pillar of 'Own Your Online' was a focus on stories of real New Zealanders that had been victims of cyber attacks. The campaign involved a photographic exhibition, giving a view of the victim in the eyes of the attacker, at the moment they were hacked. This was then supported with a series of videos, a social media and traditional media campaign telling similar stories across various platforms.

Case study

Scam Alert!

While scammers prefer a widespread campaign, hoping to catch anyone who is unaware, they sometimes hone in on specific groups they see as susceptible to their messages. CERT NZ saw a targeted scam of this type in the last quarter of 2023 which was aimed at Mandarin speakers living in New Zealand on visas.

Starting in early November, a spate of calls occurred from a source impersonating Immigration New Zealand, telling recipients there were serious problems with their visas. While calls of this nature – pretending to be from a government agency and targeting people who would interact with that agency – are not new, this particular series was remarkably high in number. Together, CERT NZ and Immigration New Zealand received over 800 reports in only 6 weeks. Because most incidents go unreported, we estimated the actual number of phone calls was much higher. The callers did not start with the knowledge of peoples' immigration status or background. So, while the content of the scam was targeting a certain demographic, anyone with a New Zealand phone number could have received the call.

The nature of the call

This scheme was specifically designed to target Mandarin speakers. The callers masked their originating numbers by 'spoofing' the phone numbers of unsuspecting individuals. The call started with a voice message asking the recipient to choose a language: English or Chinese. Selecting English ended the call. Those who selected Chinese were directed to a scammer who told them that there were issues with their visas and, in some cases, asked them to return promptly to China. The callers collected personal and sensitive information (including visa numbers), and sometimes asked for payment to help sort out visa problems.

Getting the message out

CERT NZ worked with Immigration New Zealand which used its platform and connections to get the message out to people who could be targeted. The Chinese Consulate also engaged with us and promptly disseminated information in the community. The number of reports reduced significantly in December and eventually died out, with the last case reported to us on 23 December.

Figure 10. CERT NZ working with Kiribati MICT during a training session in Tarawa

Figure 11. CERT NZ and CERT Tonga at Tonga's first Cyber Smart Week

Figure 12. Nauru ICT Ministry of Communications and Media Secretary Geoff Harris, and Director CERT NZ Pacific Partnerships Team Lefaoali'i Meremine Auelua

Figure 13. Cyber Smart Roadshow in Savai'i, Samoa led by SamCERT and CERT NZ

PALAU

Bureau of Public Safety

As its primary constituency, the Bureau of Public Safety provides support to government, law enforcement, business and small enterprises, private industry and members of the public.

The Bureau of Public Safety receives cyber-related reporting through formal reporting frameworks. Additionally, the Bureau uses social media to engage with the public.

Threat landscape

During the reporting period, the top threats were:

- ransomware
- malware
- phishing attacks
- money laundering
- identity theft and fraud
- illegal online gambling.

Technical expertise is lacking in the cyber environment. Apprehension of online gambling among offenders has proven fruitful as a number of cases were prosecuted, but not to the fullest extent.

Awareness raising

The Bureau of Public Safety conducts various community engagements and awareness raising efforts. In 2023 engagement via social media platforms was common. Cyber awareness has been put into most outreach programs and officers are more aware now. The public also has more access to this advice as other entities are helping to put information out there.

The Bureau of Public Safety use the Ministry of Justice's Facebook page to send out information on the services we offer in our department. We also use the National Broadcasting Service to send out messages and air our public announcements. Congress has been drafting bills for major cyber infrastructure guidance.

PAPUA NEW GUINEA

National CERT of Papua New Guinea

The National CERT of Papua New Guinea (PNGCERT) operates within the National Information & Communications Technology Authority (NICTA).

Our primary constituency is the country of Papua New Guinea.

Members of the public, businesses and organisations can report cyber security incidents directly to PNGCERT by reaching out to us via our email address, or through our website.

Email: report@pngcert.org.pg Website: https://www.pngcert.org.pg

PNGCERT provides advisories on how to be safe online; it is up to each entity to implement safeguards, based on their budget.

Threat landscape

Ransomware still a threat

During the past year, we have seen dramatic ransomware attacks impacting PNG companies. Well-known and public cases are NCSL and the Department of Finance (two years ago), but there have been may others, that have not been reported. Usually, ransomware attacks happen for two reasons, firstly, bad configuration of systems in the perimeter of the companies and, secondly, phishing emails being opened by company users. Ransomware is definitely one of the biggest threats in PNG. At least 90% of the hacking attacks seen in PNG are ransomware or phishing related.

Social media such as Facebook and Tiktok, issues with fake accounts and cyber bulling

This is also a huge issue in PNG. In particular, stealing of Facebook accounts is rampant in PNG for various reasons (for example, a weak password that can easily be guessed). Cyberbullying happens a lot too. Sadly, victims rarely report this to the police because they feel ashamed or because they simply don't know that cyber bulling is a crime according to the Cyber Security Act released by the Government 3 years ago.

Website defacement

This issue is particularly affecting public agencies and authorities. Website attacks are very common in PNG.

Scammers

Scamming is on the rise. Scammers are not very sophisticated in PNG. Scams are usually related to family matters or simple subjects. It is, however, becoming a bigger threat. In countries like Australia or the US, scammers set up fake websites selling products that you will never receive after you pay. But this is not currently happening in PNG. Instead, common scams in PNG involve sending an SMS saying that you have won a prize from Trukai (this one is quite usual) and then try to bring you to a situation where you need to transfer some money in order to receive this prize. A very unsophisticated type of attack, but common.

Artificial Intelligence (AI)

AI in PNG is something new. Although we are aware of its increasing use, there are no known cases of AI-related incidents yet.

Awareness raising

The Safer Internet Day is an awareness raising initiative conducted by NICTA to encourage cyber safety. It is designed to help internet users in our country practise safer behaviours when using the internet.

Cyber awareness information is also available through the NICTA website and NICTA Facebook account.

NICTA also uses the awareness raising materials provided by PaCSON as part of our community engagement activities.

Department of Information and Communications Technology

The Department of Information & Communications Technology (DICT) is a PNG government agency under the Ministry of ICT which is responsible for providing leadership in ICT.

We provide timely policy advice to the Minister for ICT on communication and information matters, coordinate digital government programs and initiatives, create awareness, and disseminate government development information.

The mission of DICT is to harness the potential of ICT to make PNG become a smart, networked and knowledgeable society. We continue to achieve our mission by providing and empowering all agencies with the tools, methods, practices and policy guidance they need to deliver digital services effectively and efficiently to our constituents nationwide. These are primarily citizens, businesses, infrastructure and the government as a whole.

People or organisations who experience a cyber incident can report it directly to www.ict.gov.pg or directly to the NCSC via email: info@ncsc.gov.pg.

Some of the most common cyber threats experienced include:

- scamming
- phishing attacks
- misinformation
- malware
- ransomware attacks
- distributed denial of services (DDoS) attacks
- identity theft and fraud.

Within the year 2023, we had seen an increase in the number of incidents reported to the National Cyber Security Centre and responded to as well.

Through the National Cyber Security Centre and Social Media Management Desk, we can respond to malware, phishing, ransomware attacks and misinformation or disinformation.

Awareness raising

DICT continues to raise awareness through its social media pages on Facebook and LinkedIn. DICT also supports PNG Government by spreading awareness through official communication channels. Our organisation also provides printed materials, videos and graphics online to the community and raises awareness through local talk-back radio shows.

On our website (www.ict.gov.pg) DICT regularly supports awareness raising initiatives by promoting cyber security awareness materials for communities and government users.

Cyber security publications, news or advisory bulletins are posted online regularly on DICT's Facebook page and on pamphlets, banners and posters used for big events or workshops. A major accomplishment for DICT in 2023 was seeing the National Cyber Security Centre (NCSC) come into full operation.

Case study

In 2023, a cyber incident occurred to one of our constituents. It was a ransomware attack to which the NCSC responded immediately to analyse and detect where the attack came from and provided advice and recommendations for the agency going forward.

Figure 14. DICT joined other organisations to talk about cyber security careers to national high school students and teachers, Port Moresby

Figure 15. Attendees at the October 2023 Cyber Security Awareness Month

Figure 16. Social media post about DICT Cyber Security In-house Awareness Campaign

Figure 17. Cyber Up awareness with students from the Port Moresby National High School

Figure 18. Georgina Kiele from DICT and Andirauga Nongkas from NICATA, being interviewed live on radio by Cullingan Tanda from FM100, to raise awareness on cyber security

Figure 19. Bank of Papua New Guinea Cyber UP Banner. The Central Bank of PNG joined the October 2023 Cyber Security Awareness Month

Figure 20. University of Technology students joining the October 2023 Cyber Security Awareness Month. Bachelor of Computer Science students showing infographic materials

Figure 21. 'Cyber Up Pacific with PaCSON' in DICT the newspaper

Figure 22. 'Cyber Up Pacific with PaCSON' campaign posters on the DICT office staff notice wall

Figure 23. October 2023 Cyber Security Awareness Month social media posts

Figure 24. Vulnerability awareness campaigns on social media

SAMOA

The Samoa Computer Emergency Response Team

The Samoa Computer Emergency Response Team (SamCERT) has been making significant progress in enhancing cyber security awareness and preparedness in Samoa. Recently, SamCERT organised a Cyber Smart Roadshow across colleges in Savaii, under the theme 'Samoa e, Mataala', emphasising the importance of staying vigilant online. This initiative took a multi-stakeholder approach, with representatives from the Ministry of Police, Ministry of Education, Office of the Regulator, and Ministry of Communications and IT (MCIT) as well as guests from CERT NZ and NetSafe.

Awareness raising

The roadshow not only targeted students but also included sessions for teachers, parents and community members such as church ministers, Matais and other community leaders. Engagement with various stakeholders highlighted the collaborative effort to promote cyber security awareness and best practices across different segments of society. It was a full-on program and was worth it.

Following the successful roadshow, a special session was held for members of Parliament to share feedback and findings from the event. MCIT plans to replicate this initiative in Upolu and Manono, further extending the reach and impact of cyber security education in Samoa.

Case study

In October 2023, a Cyber Week was conducted with support from the Australian Cyber Security Centre, where the IT community was invited to participate in sessions covering areas such as Essential 8, risk assessment processes and technical workshops on topics like Capture the Flag and hacking. The Cyber Week received positive feedback from participants, particularly on the technical exercises, demonstrating the value of hands-on learning in cyber security.

Additionally, Retrospect Labs visited Samoa to further strengthen technical skills in incident handling, risk assessment and management, benefiting both the SamCERT team and the broader community. These efforts reflect the commitment of SamCERT to building a resilient cyber security ecosystem in Samoa and equipping individuals and organisations with the knowledge and skills to combat cyber threats effectively.

MCIT, through SamCERT, extends its heartfelt gratitude to CERT NZ, the ACSC, Retrospect Labs, the GFCE, NetSafe, and our Pacific community for their unwavering support and valuable contributions. Through emails and Zoom meetings, we have been able to exchange ideas, receive support and establish our operations in Samoa. Your assistance has been instrumental in strengthening our cyber security initiatives and enhancing our capabilities to safeguard our digital landscape. Thank you for your continued partnership and commitment to building a more secure and resilient cyber environment in Samoa.

Figure 25. Samoa Mataala Roadshow

Figure 26. SamCERT visit to Salelologa Primary School, Savaii. MCIT CEO, Afioga Lefaoalii Unutoa Auelua-Fonoti giving out a lecture to all the students at Itu o Tane College. Savaii Sisifo College Principal Tuua Tamala and Amanda from CERT NZ after their session in the morning

Figure 27. Reverend Soti Roma and the Faletua Community Session after a visit to the college in the morning

Figure 28. PTA, School Community and Teachers Session

Figure 29. Minister of Communications and IT, and former prime minister and opposition leader Tuilaepa Sailele Malielegaoi who both attended the session for Parliament Members. This was the last session for the roadshow

Figure 30. Official photo after the opening ceremony of Cyber Week 2023

Figure 31. Acting Prime Minister and Deputy Prime Minister the Honorable Tuala Ponifasio delivering the keynote address to open the Cyber Week

Figure 32. Cyber Week participants engaged in the week's activities

Figure 33. The winning team for the Retrospect Labs from Australia who were also part of the Cyber Week 2023. Dr Rory and Connor. Eleitino and her team took the winning prize. Congrats to the winning team

Figure 34. Photo of the ACSC team who organised Cyber Week

SOLOMON ISLANDS

Solomon Islands Government Information & Communication Technology Services

The Solomon Islands Government Information Communication Technology Services (SIG ICT Services) is under the Ministry of Finance Corporates Services. SIG ICT Services was mandated in 2011 to provide ICT service delivery to the Solomon Islands Government. This includes all ministries, provincial governments and related agencies. SIG ICT Services has 38 staff that includes technical, management and administration positions. SIG ICT Services provides technical operational and development support through the teams Information Systems, Client Support Services, Infrastructure, Digital Transformation and Strategic Projects, Cyber Security and Admin and Finance, and Management.

Cyber incidents are reported to the Royal Solomon Islands Police Force, SIG ICT Services, or to the organisation to which people work for or are a member of. This is due to the work on establishing a formal communication channel on cyber security is still in progress. Reports are received from various global or regional bodies for which organisations subscribe to, for example, Shadow Server, PaCSON or the Cyber Security and Infrastructure Security Agency (CISA) in the US.

Threat landscape

The 3 common cyber security threats in the Solomon Islands include:

- phishing
- malware
- insider threats.

Our organisation is equipped with specialised response strategies to handle incidents related to phishing attacks, malware and insider threats. For phishing attacks, we quickly neutralise threats by identifying and blocking malicious content, and educating our users on recognising such attempts. In the case of malware, we use detection tools (anti-virus) to isolate and remove infections quickly, analysing the attack to prevent future breaches.

SIG ICT Services Initiative

In 2023, our team established a Security Information and Event Management (SIEM) system, significantly enhancing our cyber security capabilities by improving visibility across our network. The main functions of the SIEM system include log management, event correlation, real-time monitoring and alerts, and incident response.

Our log management aggregates and centralises the collection of log data from various sources across the network, facilitating easier analysis and management. Our event correlation analyses and correlates events from different sources to identify patterns that may indicate a potential security threat or incident. Our real-time monitoring and alert function provides real-time visibility into network activity and generates alerts for suspicious activities, enabling immediate action. For incident response, we investigate and respond to security incidents with tools for analysis, tracking, and reporting, helping to quickly mitigate threats. Overall, these functions help strengthen our security and protect our organisation from cyber threats.

Prior to establishing the SIEM system, it was difficult to indicate if there is was an increase in cyber incidents. However, with visibility, there are certainly daily attempts to comprise government services, especially through phishing attacks and supply chain attacks. On that note, our organisation is striving to remain vigilant and proactive in adapting our security measures and response strategies to effectively address these challenges. We're committed to safeguarding our systems and data against potential threats, constantly enhancing our capabilities to respond to incidents as they arise.

Awareness raising

Our organisation is dedicated to enhancing cyber security awareness through ad hoc training sessions, and ongoing awareness campaigns for staff and communities. Establishment of awareness training with the Public Service Training Institution for government officers. These initiatives are aimed at ensuring employees are well-informed and vigilant, creating a strong culture of cyber safety.

Our organisation primarily focuses on fostering a culture of cyber security awareness through a dedicated cyber safe campaign, which includes the dissemination of emails to all staff. These emails serve as our primary method of communication, offering the latest insights, advice, and updates on cyber security best practices, emerging threats and protective measures. While we may not produce a wide range of news, publications or advisory bulletins, these emails are carefully made to ensure all employees stay informed and proactive in safeguarding against cyber threats.

While we are still in the early stages of this year and actively working towards our major annual goals, we haven't reached any significant milestones yet and our teams are diligently working towards our set goals, and we're optimistic about the progress and outcomes. Our most recent significant achievement was last year's involvement in the Pacific Games event. Our team at SIG ICT Services played a crucial role in the success of the games, which stands as a testament to our dedication and capability.

TONGA

Tonga Computer Emergency Response Team

The Tonga Computer Emergency Response Team (CERT Tonga) is the Kingdom of Tonga's National Computer Emergency Response Team and point of contact for cyber security issues (incident response, awareness raising, trainings, digital forensics, and cyber security bulletins and advisory). CERT Tonga is one of the departments operating under the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (MEIDECC). CERT Tonga's revised organisational structure consists of 3 established staff and contracted staff under the CERT Tonga Cyber Security Workforce Development Program (CWDP), capacity building project funded by CERT NZ (since November 2021 to December 2025).

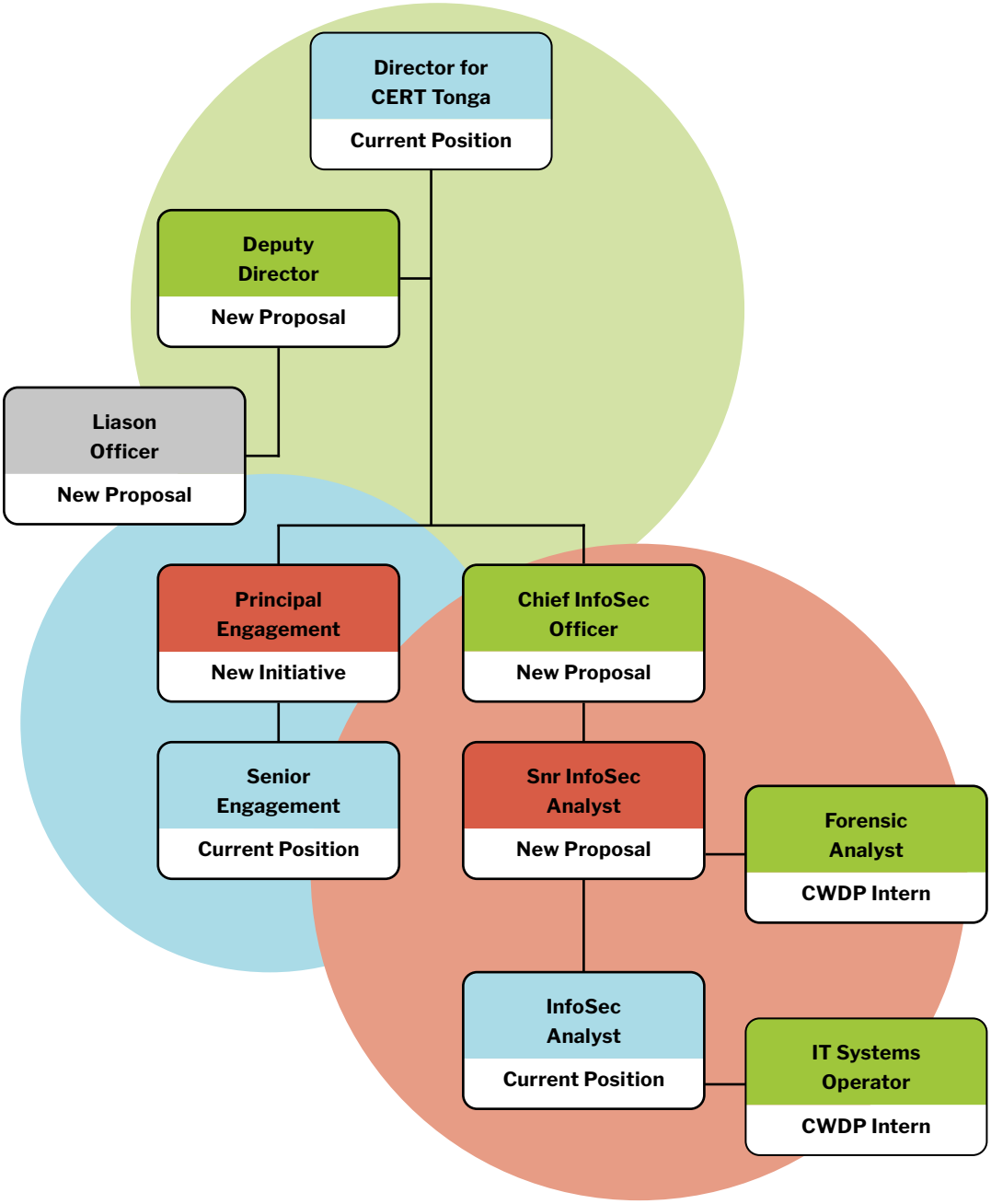


Figure 35. Structure of the CERT Tonga department

The CERT Tonga department consists of 3 divisions: Oversight and Compliance (OC) Division (GREEN); Coordination & Communication, Plan, Response and Technology solutions (CCPRT) Division (BLUE); and Incident Management, Detection, Vulnerability & Forensic Analysis Division (RED). Previously there were only 2 divisions, the Engagements and Technical divisions.

There are only 3 current established positions: the Director, the Senior Engagement Officer, and Security Analyst. There are 3 positions currently filled by CWDP contracted staff, being the IT System Operator (apprentice), the Assistant Security Analyst (secondment) and the Security Analyst/Forensic Analyst (intern) that will run from October 2023 to March 2025 (up to December 2025). The other new proposal positions are still drafted due to no budget and no new recruitment policy (until further notice). Those positions are Senior Information Security Analyst, Chief Information Security Officer (CISO), Liaison Officer and Deputy Director positions. CERT Tonga's constituents are government ministries, departments and agencies, private sectors, public enterprises, and NGOs.

Reports of cyber incidents can be via e-mail at report@cert.gov.to, telephone +676 2378, social media platform (CERT Tonga Face Book), the CERT Tonga website CERT.gov.to, or face to face.

Threat landscape

CERT Tonga's top 3 most common cyber security threats include:

- hackers (scrip kiddies)
- masquerade (fraud actors)
- international malicious actors (professionals exploiting vulnerable IP address and DNS).

CERT Tonga interprets cyber risks the following way:

- Cyber Security Risks = Threats x Vulnerabilities x Assets (Diplo Academy Foundation).

Common incident types:

- phishing emails (scam emails)
- ransomware (to a limited extent, mainly coordinating stakeholders and third parties)
- fraud emails (coordination and collaboration with stakeholders and third parties).

CERT Tonga has often been requested by the Cybercrime Working Group (comprising the Attorney-General's Office and Tonga Police) to assist with social media electronic communications abuse offensive cases (misinformation and disinformation) regarding government officials and high profile cases.

There was a dramatic increase of incidents at the beginning of 2023 (early February) then followed with a few IP exploitation reports. There were a few fraud cases during the year, with cyber security awareness raising campaigns to the country and outer islands to mitigate this.

Awareness raising

CERT Tonga provided cyber awareness training to high schools, in last quarter of 2022 and to the 2 outer islands middle schools and high schools, as well as key government ministries, departments, and agencies (including NGOs and public enterprises). There was also a Cyber Resilience Week in the beginning of the 2023–24 financial year, with events and activities to promote a safe and secure digital environment for the Kingdom of Tonga and its citizens.

CERT Tonga news and publications

- System Administration Hardening Guide (in collaboration with Cyber CX)
- draft Information Security Policy (in collaboration with Trustwave)
- draft Information and Classification Handling Standard (in collaboration with Trustwave)
- draft Log Management and Monitoring Standard (in collaboration with Trustwave)
- draft Malicious Code Standard (in collaboration with Trustwave)
- Patch Management and Vulnerability Standard (In collaboration with Trustwave)
- Tonga Incident Response Standard (in collaboration with Trustwave)
- monthly Security Bulletin and Advisory (to be resumed soon).

CERT Tonga did accomplish the Cyber Resilience Week (7th Anniversary Commemoration of its establishment since July 2016) with the co-hosting with CERT NZ, PaCSON and the ACSC. The cyber awareness raising to the Outer Islands accomplished more than 50% outreach to the ‘Eua Island and the main Island of Ha’apai.

Case study

A major cyber event that occurred this year (since last quarter of 2023) in Tonga has been selected out of 8 other countries to be the Hub Country in the Pacific Region for the new Global Action against Cybercrime Enhanced (GLACY-e) Project.

TUVALU

The Department of Information and Communications Technology

The Department of Information and Communications Technology (ICT) underwent a transition in February 2024, shifting from the Ministry of Justice, Communications, and Foreign Affairs to the Ministry of Transport, Energy, Communication, and Innovation. Responsible for overseeing the government's technological landscape, ICT plays a pivotal role in various sectors. While certain government departments employ IT specialists that tailor their work to specific requirements, the broader spectrum of technological affairs falls under the purview of ICT.

Under the leadership of the Director and 2 senior officers, ICT is organised into key teams such as networking and database management. These teams are further subdivided to also address critical areas including cyber security (which collaborates closely with virtual CERT) and regulatory compliance. It also spearheads the Government of Tuvalu's ambitious digital transformation objectives.

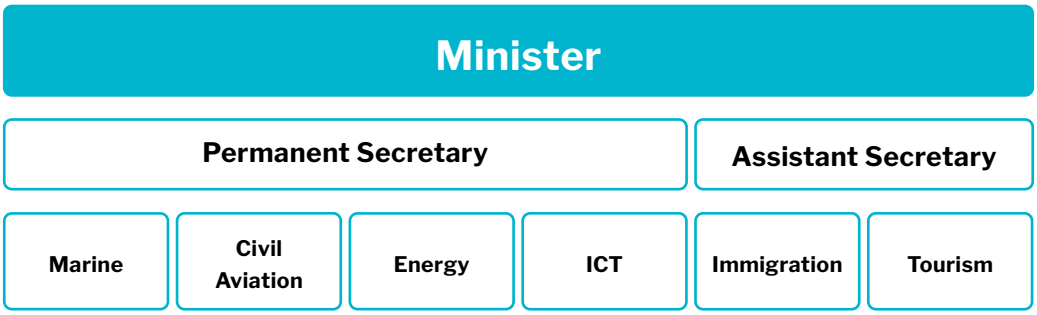


Figure 36. Ministry of Transport, Energy, Communication and Innovation structure

Our CERT team is more a virtual collaboration between ICT, Tuvalu Telecom, Tuvalu Police and the Attorney-General's Office. This collaboration extends the awareness programs like cyber security awareness, Pasifika, PaCSON, Get Safe Online and PILON to primary school students, as well as to the wider community.

The World Bank is funding a submarine cable project for Tuvalu. While that is forthcoming, further collaboration to expand satellite internet bandwidth is in progress, with timely introduction of Starlink satellite services to boost connectivity speeds and reliability. Our virtual cyber security team will continue to educate the general public on how to stay safe online. There have been a few workshops held by the Cyber Safety Pasifika Team from the Tuvalu Police, in the capital and some on the outer islands.

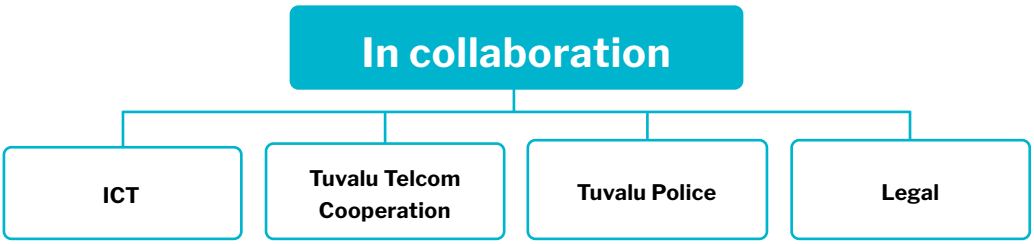


Figure 37. Collaborative partners of CERT threat landscape

Threat landscape

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

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

- malware
- phishing attacks
- scams
- identity theft and fraud
- ransomware.

Awareness raising

The Department of ICT, in collaboration with the Tuvalu Police, supported various community engagement and awareness raising efforts during the reporting period, including through community outreach, visits to schools, and engagement via social media. Our office, and police, are always available to the public if there are any cyberattacks or any online issues.

The Department of ICT uses social media accounts as a platform to share cyber security and cyber safety updates. The Department of ICT tries to share the security advisories from PaCSON partners like CERT Tonga, CERTVU, CERT NZ and even CISA, on various social media outlets like government Facebook pages and Tuvalu news pages.

VANUATU

Computer Emergency Response Team Vanuatu

Computer Emergency Response Team Vanuatu (CERTVU) is the cyber security arm of the Government of Vanuatu, established under the Office of the Government Chief of Information Officer (OGCIO), within the Ministry for the Prime Minister. CERTVU currently has 4 dedicated staff, 3 of whom are employed on a full-time basis and one on a contracted basis. CERTVU is Vanuatu's national CERT; therefore, it serves the entire nation of Vanuatu – government, businesses and civil society.

People report cyber incidents through the following measures:

- submit an online incident report via CERTVU's website: https://cert.gov.vu/index.php/services/incident-resolution
- phone contact, +67833380
- our social media platform
- by coming into the office to report any cyber incident, CERTVU has an open-door policy.

Threat landscape

There has been an increase in cyber incidents in 2023. During the reporting period, the top 3 threats were:

- targeted phishing attacks
- business email compromises
- ransomware.

Awareness raising

Our awareness raising program involves:

- national radio talk shows
- national events participation
- cyber security awareness videos: Cyber Up
- Cyber Up Campaign, a one-to-one community awareness program
- Schools Cyber Awareness Campaign
- business house awareness
- public and private awareness and intelligence sharing
- producing flyers and brochures on cyber security.

Major achievements

- incident response
- Critical Infrastructure Security Framework
- Incident Response Emergency Communication Framework
- hosting the PaCSON AGM in Vanuatu
- hosting of the FIRST Pacific Symposium in Vanuatu
- launching of the National Data Protection Policy
- launching the National Harmful Digital Communication Policy
- launching the Train-the-Trainers (T3) program and resources
- multi-stakeholder Cyber Security, Cyber Safety, Cybercrime Awareness Platform Program
- engaging international partners on incident response.

Case study

2023 marked a very important year for CERTVU, the launching of the Train-the-Trainer (T3) initiative (program and resources). This was a project we commenced in 2022 and, despite various challenges, we launched the training package with 4 cyber security guides. The T3 initiative addressed Cyber Security Priorities (CSP) 1, 2 and 3 of Vanuatu's National Cyber Security Strategy of 2030, which aims to address: cyber resiliency, cyber literacy and capability, and cyber security awareness.

By the end of 2023, CERTVU identified a pilot site for the project and delivered the training there. There were positive remarks from that initiative and lessons learned, which CERTVU has taken into consideration to better the T3 initiative and continue with other local communities.

Figure 38. CERTVU in collaboration with the Youth Challenge Vanuatu (YCV) provides cyber security awareness to Paunangisu Community Youths Efate Island, Vanuatu

Figure 39. CERTVU Cyber Security Capacity Building session with the Youth Challenge Vanuatu Agency

Figure 40. CERTVU implementing the Train the Trainers initiative at Nguna Island

Figure 41. CERTVU Implementing the Train the Trainer initiative at Nguna Island

Figure 42. Deputy CIO Mr. John Jack on CERTVU ICT and cyber security weekly Radio Talk Show segment in collaboration with the Vanuatu Broadcasting Television Collaboration (VBTC) through Radio Vanuatu, reaching an audience of over 200,000 people

Figure 43. CERTVU and the Vanuatu Police Force provide cyber security and cybercrime awareness to the Vilakalaka community on the Island of Ambae

Figure 44. CERTVU on the Cyber Up initiative program at Eles Primary School at Nguna Island

Partner Updates

CYBER SECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE US DEPARTMENT OF HOMELAND SECURITY (DHS)

Cyber Security and Infrastructure Security Agency's (CISA) overarching goal is to have 'A secure and resilient critical infrastructure for the American people'. We aim to support our partners in achieving the same objective for their respective nations. Participation is based on mutual collaboration, and participants are expected to be actively engaged in information sharing, information enrichment, sharing technical tippers, and providing insights about broader campaigns and threat actor activity.

CISA's Joint Cyber Defensive Collaborative (JCDC) brings together organisations and operators from across the public and private sectors, including from state, local, and international government participants. The national Computer Emergency Response Teams (CERT) functions for the US sit with JCDC International, and our office focuses on continual international partnership collaboration with cyber defence organisations to ensure that information about cyber threats is identified and rapidly disseminated. JCDC is a public-private cyber security collaborative that supports uniting the international cyber community on the collective defence of cyberspace.

Department of Homeland Security > CISA > Cyber Security Division (CSD) > Joint Cyber Defence Collaborative (JCDC) > Partnerships Office > International

Threat landscape

Nation-state adversaries, including the People's Republic of China, Russia, North Korea and Iran, pose elevated threats to our national security. These adversaries are known for their Advanced Persistent Threat (APT) activity. Read more here:
https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

CISA's contributions to PaCSON in 2023 were:

- attendance at the 2023 Annual PaCSON Conference
  - conducted 3 days of CISA workshops
- added PaCSON members to CISA distros
- on-boarded more CISA staff at the PaCSON Portal.

Case study

The US, and international cyber security authorities, issued a joint Cyber Security Advisory (CSA) to highlight a recently discovered cluster of activity associated with a People's Republic of China (PRC) state-sponsored cyber actor, Volt Typhoon. Private sector partners have identified that this activity has affected networks across US critical infrastructure sectors, and they also believe Volt Typhoon could apply the same techniques against other sectors worldwide.

The advisory provided from the United States National Security Agency (NSA), the US Cyber Security and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Communications Security Establishment's (CSE's) Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the National Cyber Security Centre (NCSC-UK)

One of Volt Typhoon's primary tactics, techniques, and procedures (TTPs) is 'living off the land', which uses built-in network administration tools to perform its objectives. This TTP allows Volt Typhoon to evade detection by blending in with normal Windows system and network activities, avoid endpoint detection and response (EDR) products that would alert on the introduction of third-party applications to the host, and limit the amount of activity that is captured in default logging configurations. Some of the built-in tools Volt Typhoon uses are wmic, ntdsutil, netsh, and PowerShell. The advisory provided examples of the actor's commands along with detection signatures to aid network defenders in hunting for this activity. Many of the behavioural indicators included can also be legitimate system administration commands that appear in benign activity. The advisory can be accessed here:
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

Visit these links to learn more about CISA

- https://www.cisa.gov/news-events/cybersecurity-advisories
- https://www.cisa.gov/securebydesign
- https://www.cisa.gov/ai

FEDERAL BUREAU OF INVESTIGATION

The US's Federal Bureau of Investigation (FBI) has 57 field offices with a cyber taskforce at each. The FBI has a cyber action team that performs incident response and can deploy globally if a cyber incident meets certain thresholds. The FBI has cyber experts in many US embassies who act as liaisons to host countries. The FBI is willing to conduct cyber investigative training in the Pacific region.

Threat landscape

Common cyber threats:

- business email compromise
- data breaches
- ransomware.

The FBI has provided guidance to law enforcement in the Pacific. The FBI has provided cyber investigative training to Pacific Island countries.

RESERVE BANK OF FIJI

As the Central Bank of the Republic of Fiji, the Reserve Bank of Fiji's (RBF) functions include issuing currency and promoting monetary and financial stability in the economy, while providing policy advice and financial services to the Government. The RBF employs a little over 200 staff who operate from central Suva, the capital of Fiji. A total of 7 departments function together under the leadership of the Board, the Governors and the Executive Management to deliver its statutory responsibilities.

Recently, the RBF reviewed the structure of its IT unit with an aim to better manage operations, cyber security and innovations. From 1 August 2023, the RBF established a Manager of Cyber Security along with a team to focus on cyber safety and cyber initiatives.

Threat landscape

During the reporting period, common threats were:

- phishing and ransomware
- payments system threats
- security gaps and vulnerabilities created with rapid cloud adoption, digitisation and AI
- staff turnover.

Other cyber activities

RBF released the Prudential Supervision Policy Statement (PSPS-2) in March 2023 with full compliance required of users within one year from the effective date. This includes commercial banks, credit institutions, insurance companies, insurance brokers, the securities exchange, management companies of managed investment schemes, stock brokers, the Fiji National Provident Fund, the Fiji Development Bank, and restricted foreign exchange dealers.

a. national cyber security strategy and cyber security maturity model reviews

b. ransomware attacks on multiple organisations in both private and public sector

c. financial scams, for example: https://www.fbcnews.com.fj/news/ebayshop-scam-crosses-2million-mark/

PaCSON contribution

RBF contributions to PaCSON included on-ground information-gathering and advisories to identify capacity building and other cyber security needs.

We also send direct regulatory requirements to licensed financial institutions regarding cyber security.

Publications and news

- RBF strategy and customer feedback: https://www.data3.com/knowledge-centre/customer-stories/reserve-bank-of-fiji/
- managing cyber security risks: https://www.rbf.gov.fj/wp-content/uploads/2023/04/PSPS-No.2_Minimum-Requirements-for-the-Management-of-Cybersecurity-Risk-.pdf
- media releases: https://www.rbf.gov.fj/media/
- we also send direct regulatory requirements to the licensed financial institutions regarding cyber security.

Friend Updates

FRIEND UPDATES

Global Forum on Cyber Expertise Pacific Hub

Overview

The Global Forum on Cyber Expertise (GFCE) Pacific Hub has 5 members, being the Director, 3 senior advisors and a project associate. The Pacific Hub reports to the GFCE Secretariat.

PaCSON contribution

The Pacific GFCE Hub, during conversations with regional and external stakeholders, has consistently highlighted the valuable work undertaken by PaCSON and its ongoing efforts in fostering regional collaboration. It also highlights PaCSON's efforts in connecting cyber security experts and technical specialists from Pacific governments, and facilitating information sharing and resources aimed at improving cyber security across the region.

The Hub also supported and provided assistance to the Cyber Upskill (CUP) program initiative by connecting it with relevant agencies, bodies and individuals in Tonga during filming for the CUP resources.

We actively share initiatives and resources developed by PaCSON.

The Hub also had the opportunity to participate in the PaCSON AGM and conference, by engaging in the discussions and dialogues that took place at the events.

The GFCE Pacific Hub has a virtual presence in the region with members of the team based in different countries across the Pacific. We trust that relevant PaCSON points of contact within those countries will provide relevant information of any incidents or activities from those countries.

The GFCE Pacific Hub would like to highlight the Partners in the Blue Pacific (P4C) Pacific Cyber Capacity Building and Coordination Conference, which was jointly organised by the GFCE Pacific Hub and the OCSC. Many of PaCSON's members and their representatives, including the PaCSON Secretariat, participated in the Pacific-centred dialogue to inform future cyber capacity building efforts in the region.

Working Group Updates

WORKING GROUP UPDATES

Awareness Raising Working Group

In 2023, the Awareness Raising Working Group of the Cyber UP Campaign was very productive. The committee approved an extension of 2 additional themes to the campaign, focusing on upscaling backups and uplifting data security. This decision was a significant step towards enhancing the overall cyber security awareness and practices within the community, especially focusing on data protection and continuity of service.

During the 2023 Annual General Meeting, held in Vanuatu in September, the committee engaged in in-depth discussions and provided valuable feedback on the delivery methods of the campaign. The members brainstormed innovative ways to effectively communicate the importance of backups and data security to a wider audience, ensuring that the message resonated with people across different demographics.

Through collaborative efforts and meetings, the Awareness Raising Working Group successfully presented the new themes for the Cyber UP Campaign. By leveraging various communication channels, educational resources, and outreach initiatives, the committee aimed to raise awareness, educate, and empower individuals and organisations to take proactive steps in safeguarding their digital assets. While things are still in progress, a review on how effective these campaigns have been, and continue to be, in the Pacific is one important matter that was raised.

Overall, the activities of the Awareness Raising Working Group in 2023 demonstrated a strong commitment to promoting cyber security best practices and fostering a culture of vigilance in the digital realm. The extension of themes and the detailed discussions during the AGM reflected the dedication and passion of the committee members towards creating a safer and more secure online environment for the Pacific community.

Figure 45. 'Cyber Up Pacific with PaCSON' banner

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 capability and capacity, and identify ways in which other members of PaCSON may be able to contribute support.

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

2023 activities

In 2023, the working group continued to deliver the Remote Session Series, organised by CERT NZ. Originally established in June 2020 to maintain community engagement in the face of the COVID-19 pandemic, the series provides a regular opportunity for the PaCSON community to connect. From May 2023 to April 2024, the working group hosted 6 remote sessions with a total of 135 attendees.

Like last year's efforts, external guests and PaCSON Partners were invited to lead sessions for the community. Presentations included from Australia's eSafety Commission, Mandiant, the ACSC and Cyber Security Certification Australia.

The presentations covered a wide range of topics, including a report on a critical Barracuda vulnerability (Mandiant), and the issues of misinformation and disinformation (eSafety Commission). It was encouraging to see the level of engagement and interest from the community within these sessions.

The Pacific Cyber Security Data & Insights, launched at last year's AGM with Shadowserver, started to provide some insights into the region. The addition of this PaCSON grouping to the dashboard allowed members to see what was happening in the region. This initiative will continue into 2024.

Over the past 12 months, as part of the working group, CERT NZ shared 4 advisories to PaCSON Members for vulnerabilities that were relevant to the region.

The working group appreciates the efforts and engagement from the whole of PaCSON as well as our regional and global partners throughout the year. We are looking forward to continuing this momentum and developing new and exciting projects in the coming year.

A goal for next year will be bringing members together to co-create a work plan to help shape the future of the working group as well as elect a co-chair.

Capacity Building Working Group membership:

- Australia
- Fiji
- Nauru
- Papua New Guinea
- Solomon Islands
- Tonga
- Tuvalu
- Vanuatu
- New Zealand – Convenor.

Communications Working Group

The aim of the Communications Working Group (CWG) is to improve information sharing within and communication tools for the PaCSON community. During the life of the working group, members will work towards achieving a collection of tools and processes which will enable better communication and information sharing within the PaCSON community.

2023 activities

In 2023, the working group was proud to publish the PaCSON Annual Report 2022 for distribution to members, partners and stakeholders. This was our main deliverable for the period and we would like to thank members and partners for their contributions in order to make this edition possible.

In addition to publishing the annual report, the working group is also pleased to have published 2 news articles over the course of 2023. The articles focused on the PaCSON delegation that attended the 2023 Annual FIRST Conference in Montreal, Canada, and the 2023 PaCSON AGM. These publications serve the dual purpose, to publicise the important work that PaCSON does and to promote awareness for key initiatives delivered by our members and partners. The working group also shared useful resources, such as translated cyber security information guides originally published on cyber.gov.au.

The Communications Working Group also continued to maintain and sustain the PaCSON website, pacson.org. In 2023, the website saw new features added, including:

- a search function in the portal
- CUP landing site
- a 'subscribe to forums' function
- a new Cyber Smart 2023 Campaign page
- a new 'friends' page
- a new resources content page.

In 2023, the website continued to be 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. Visits to the website during the reporting period were steady, with a high number of visitors discovering pacson.org through keyword searches.

In response to feedback at the AGM, the working group established a Signal group chat that members can opt into in order to receive website updates, alerts and advisories directly to their phone.

The working group also collaborated to create templates and resources to assist members in implementing and sharing the CUP in their communities.

The working group was pleased to continue supporting the ARWG and CBWG throughout 2023, and looks forward to continuing our collaborations in 2024.

PaCSON Partners Working Group

The PaCSON Partners Working Group (PPWG) was established to provide PaCSON partners with opportunities to support and collaborate with the PaCSON primary working groups (Awareness Raising, Capacity Building and Communications) on their planned activities. The PPWG is driven by the aspiration to provide a 'whole-of-community benefit' to PaCSON – working with all PaCSON members to increase their knowledge, capacity and resilience in matters of cyber security. Partners add value to the PaCSON community through their knowledge, resources, experience and capabilities.

In 2023, the PPWG and the PaCSON community was proud to welcome FIRST as the newest organisation to attain partner status within PaCSON. FIRST made a great start, hosting the FIRST Regional Symposium alongside the PACSON AGM in Port Vila. The symposium featured a Capture the Flag activity for PaCSON members and others to take part in, and highlighted presentations from cyber experts working in the region. FIRST brings with it a great network of cyber experts from around the world, with knowledge and experience in cyber incident response. PaCSON looks forward to continuing to work with FIRST to achieve the PaCSON mission of strengthening the Pacific's resilience to cyber threats.

The PPWG will continue to support the PaCSON community to deliver against its mission of working 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.

Future Plans 2024

FUTURE PLANS

In 2024, PaCSON will maintain a high level of commitment to the needs and wants of the PaCSON community. Our PaCSON community may continue to experience an increasing pace and frequency of cyber security events, but we will continue to support each other and improve our regional cyber security capabilities and readiness through cooperation and collaboration.

At the 2023 Annual General Meeting, the PaCSON Forum endorsed the community's priorities for 2023–24. These priorities will guide PaCSON's engagement strategy and goals for the next 12 months and allow the community to track the progress and advances made over the reporting period.

PaCSON's key priorities for 2024

General:

- formalise PaCSON's status as a regional body, such as forming an official relationship with the Pacific Island Forum, and seeking member buy-in
- working groups should be restructured. Clear roles and responsibilities should be defined and co-chairs encouraged. Growth of working groups will ensure members have more ownership of PaCSON
- grow working groups by making them more focused on outcomes. In order to achieve this, working plans should be developed
- review the topics and scope of the working groups
- align the AGM with other relevant conferences and workshops.

Capacity building:

- increase hands-on training opportunities at future AGMs
- commit to working with partners and other players in the region to de-conflict training offerings.

Communications:

- increase traffic to, and use of, the portal:
  - Set up automatic notifications about new forum posts to a WhatsApp or Signal group. This will leverage platforms that members are already using, and allow them to click the link on their mobile and read relevant forum topics
  - Until automatic notifications are set-up, use community-wide emails following forum updates.
- encourage more information sharing via the portal:
  - Encourage members, partners and friends to post updates in the forum to centralise communications.
  - Create a downloadable template for forum posts.

Acknowledgements

ACKNOWLEDGMENTS

PaCSON acknowledges the valuable contributions made by all of our 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 2023, with special thanks to:

ASIA PACIFIC NETWORK INFORMATION CENTRE (APNIC)

APNIC is an open, member-based, not-for-profit organisation, 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 needed for the internet to operate and grow. As part of this service, APNIC is responsible for maintaining the public APNIC Who Is 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.

ASIA PACIFIC COM PUTER 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 https://www.apcert.org/

CYBER SAFETY PASIFIKA (CSP)

CSP is a program led by the Australian Federal Police 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 https://www.cybersafetypasifika.org/

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 the 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 https://www.internationalcybertech.gov.au/

GLOBAL CENTRE FOR CYBER EXPERTISE (GFCE), PACIFIC HUB

The GFCE Pacific Hub endeavours to enhance cyber security capacity and capabilities within the Pacific region by facilitating and coordinating initiatives for cyber capacity building. The aim is to ensure that such initiatives are effective, purpose-driven, and sustainable by promoting the sharing of knowledge and expertise, and fostering coordination among diverse stakeholders, including donors, governments, private sector organisations, and civil society groups.

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 https://pilonsec.org/

Abbreviations

ABBREVIATIONS

2FA	Two-Factor Authentication
ACSC	Australian Cyber Security Centre
AGM	Annual General Meeting
APCERT	Asia Pacific Computer Emergency Response Team
APNIC	Asia Pacific Network Information Centre
ARWG	Awareness Raising Working Group
ASD	Australian Signals Directorate
BEC	Business Email Compromise
CBWG	Capacity Building Working Group
CCTCP	Cyber and Critical Tech Cooperation Program
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERTVU	Computer Emergency Response Team Vanuatu
CERT NZ	Computer Emergency Response Team New Zealand
CISA	Cyber Security Infrastructure & Security Agency (US)
CSA	Cyber Security Advisories
CSD	Corporate Services Department (PNG)
CSD	Cyber Security Division (CISA, USA)
CSIRT	Computer Security Incident Response Team
CSP	Cyber Safety Pasifika
CWDP	Cyber Security Workforce Development Program (Tonga)
CUP	Cyber Upskill Program
DDoS	Distributed Denial-of-Service
DFAT	Department of Foreign Affairs and Trade (Aust)
DGTO	Digital Government Transformation Office (Fiji)
DHS	Department of Homeland Security (US)

DICT	Department of Information and Communications Technology (Papua New Guinea)
DOJ	Department of Justice (US)
DTA	Digital Transformation Authority (the Solomon Islands)
DTO	Digital Transformation Office (Kiribati)
EC	Executive Committee (PaCSON)
ECD	Emergency Communications Division (CISA, US)
ECIA	Economics, Consumer and International Affairs (PNG)
ERPD	Engineering & Resource Planning Department (PNG)
FBI	Federal Bureau of Investigation (US)
FICAC	Fiji Independent Commission Against Corruption
FIRST	Forum of Incident Response and Security Teams
FIU	Fiji Financial Intelligence Unit
GFCE	Global Forum on Cyber Expertise
ICS	Industrial Control Systems
ICSMAs	ICS Medical Advisories
ICT	Information & Communication Technology
IOD	Integrated Operations Division (CISA, US)
IPAM	Institution of Public Administration and Management (the Solomon Islands)
IR	Incidence Response
IRFS	International Revenue Fraud Services
ISD	Infrastructure Security Division (CISA, US)
IT	Information Technology
ITCS	Department of Information Technology and Computing Services (Fiji)
JCDC	Joint Cyber Defence Collaborative (CISA, US)
LED	Licensing & Enforcement Department (PNG)
MEIDECC	Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (Tonga)

MCIT	Ministry of Communications and Information Technology
MICT	Ministry of Information, Communications and Transport (Kiribati)
MSP	Managed Service Providers
NCF	National Critical Functions (CISA, USA)
NCSC	National Cyber Security Centre (PNG)
NGO	Non-Government Organisation
NICTA	National Information and Communications Technology Authority
NRMC	National Risk Management Center (CISA, USA)
OCSC	Oceania Cyber Security Centre
OGCIO	Office of the Government Chief Information Officer (Vanuatu)
OPM	Office of the Prime Minister (the Cook Islands)
OSC	Online Safety Commission (Fiji)
PaCSON	Pacific Cyber Security Operational Network
PILON	Pacific Islands Law Officer's Network
PMU	Project Management Unit
PMO	Prime Minister's Office (Tonga)
PNGCERT	Papua New Guinea Computer Emergency Response Team
PPWG	PaCSON Partners Working Group
RBF	The Reserve Bank of Fiji
SamCERT	Samoa Computer Emergency Response Team
SED	Stakeholder Engagement Division (CISA, US)
SIG	Solomon Islands Government
SIG ICTS	Solomon Islands Government (SIG) Information Communication Technology Services (ICTS)
SIG SOC	Solomon Islands Government Security Operations Centre
SMMD	Social Media Management Desk (PNG)
UAS	Universal Access Scheme Secretariat (PNG)

PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

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