PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

ANNUAL REPORT 2021

TLP:WHITE = Disclosure is not limited.

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

CONTACT DETAILS AND FEEDBACK

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

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

Table of Contents

From the Chair	4
Program Overview	**7**
Overview	8
Member Updates	**11**
Australia	12
Cook Islands	18
Fiji	20
Kiribati	22
Marshall Islands	24
New Zealand	26
Niue	34
Palau	35
Papua New Guinea	37
Samoa	47
Solomon Islands	52
Tokelau	56
Tonga	62
Tuvalu	70
Vanuatu	73
Partner Updates	**75**
Cybersecurity and Infrastructure Security Agency	76
Reserve Bank of Fiji	82
Working Groups	**84**
Awareness Raising	85
Capacity Building	87
Communications	89
Partners	90
Future Plans – 2022	**91**
Acnkowledgements	**92**
Glossary	**95**

From the Chair

Welcome back to the Pacific Cyber Security Operational Network (PaCSON) Annual Report! Our entire PaCSON Community warmly extends its thanks to our stakeholders and partners for their continued support and encouragement. During a further year of turbulence and uncertainty, CERT Tonga has been privileged to hold the position of PaCSON Chair. I am proud to present this report and its reflections on our PaCSON efforts during 2021.

Throughout 2021, our PaCSON Community continued to perform a vital role for our region. In the spirit of collaboration, we pulled together with our stakeholders and partners virtually for another year of socially-distanced engagements. Our increased reliance on digital connectivity in 2021 resulted in innovative digital transformation and connectivity as we managed the demands of working, educating, shopping, connecting and living online.

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

Cyber security is a matter of great significance, and as I echo the remarks from our 2020 Chair, I too am glad to witness such excellent collaboration among our Pacific community. Cyber security is a complex recipe, with collaboration and cooperation as its two key ingredients. Without these, working alone does not yield tangible results for our Pacific community. Relationships built on collaboration and cooperation continue to be crucial for achieving success, as we are stronger together than apart. The significance of our collective maturity and ability to respond to cyber events has positioned PaCSON as the focal point of cyber security coordination. I feel incredibly blessed to be able to lead our magnificent PaCSON Community.

Cyber threats against the Pacific region have increased in pace, scale and sophistication. The current threat landscape across the Pacific is one of uncertainty and responsive reaction. PaCSON is key to enabling cyber security officials to learn from each other and exchange ideas on how, together, we can address the growing number of cyber threats affecting our region. Working together on cyber security is vital, as is ensuring the robust nature of our most valuable partnerships. By working together, we are ensuring that our cyber security capabilities and professional competencies grow in line with our increasing reliance on cyber and digital mechanisms.

Simple acts of information-sharing, awareness raising and aapacity building are incredibly impactful and assist in improving the cyber security posture and readiness of our Pacific region. This is a noble and important cause – one which our PaCSON Community looks forward to continuing and encourages all to engage in. The continued success of PaCSON demonstrates the resilience of the Pacific region's cyber community and reinforces that the PaCSON Community is well placed to contribute to the worldwide effort in confronting the challenges that face an open, free and safe cyber space.

I wish to draw particular attention to our annual awareness raising campaign, Cyber Smart Pacific, which was very successfully redesigned in 2021 with assistance from CERT NZ. The campaign retained the format of four key messages designed to help improve personal cyber security, and it is hoped that the campaign will only increase in strength and value in 2022. The campaigns four key messages were:

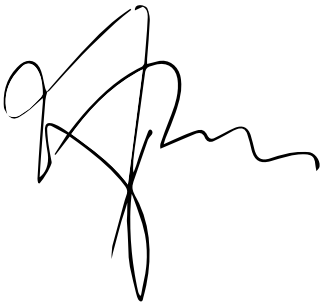
1. Upsize your passwords
2. Upgrade to two-factor authentication
3. Update your apps and devices
4. Uphold your privacy.

Partnerships and cooperation with international stakeholders together form a key pillar for successful cyber security. I was delighted to see our PaCSON Community grow with the addition of the Department of Information and Communications Technology from Papua New Guinea. We will continue to welcome and look forward to building relationships with new members and partners who share the PaCSON values and vision of improving cyber security capabilities and cyber readiness across the Pacific through cooperation and collaboration.

As we continued our online engagements throughout 2021, our Remote Session Series increased in perspective and participation. Delivering eight sessions with more than 230 participants, these sessions provided further opportunities for engagement and skills growth that are crucial to increasing our PaCSON Community's collective knowledge and understanding. These sessions increased our knowledge across a range of topics and facilitated connections with industry partners and other cyber forums. The Remote Session Series showed the power of our community and demonstrates what we can achieve when we all come together to tackle regional challenges.

I wish to share my thanks with our valued stakeholders who have contributed to the success of PaCSON. I would especially like to pass along my appreciation to the PaCSON Secretariat and the Cyber and Critical Tech Cooperation Program within Australia's Department of Foreign Affairs and Trade who have committed their support to PaCSON.

Last year was another year of success and challenge for PaCSON. I wish to reflect on our success and give thanks to those in and around our PaCSON Community. As I look to finalise my privileged time as the PaCSON Chair, I wish the very best of luck and dedicate my ongoing support to the new Executive Committee of 2022 – Tonga, the Cook Islands and Vanuatu. Finally, I wish our Community all the best for the remainder of 2022 and very much look forward to witnessing our future success.



Mr Paula Pouvalu Ma'u
2021 PaCSON Chair

September 2022

Program Overview

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 information infrastructures and constituents. The availability of internet connectivity presents significant opportunities but also exposes users within the Pacific region to increased threats from malicious cyber actors.

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

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

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

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

PaCSON is not a Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT) and does not provide an incident response capability. Rather, the program 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 enables cooperation and collaboration, particularly when a cyber security incident affects the region.

The direction of PaCSON is guided by the Executive Committee (EC), which provides leadership on behalf of the PaCSON Community. The EC is empowered to make decisions on behalf of PaCSON and is responsible for the management and direction of PaCSON. All PaCSON members are eligible to nominate for all EC positions. In 2021, the structure of the PaCSON EC included:

- Chair – Tonga
- Deputy Chair – Cook Islands
- Incoming Chair – Vanuatu.

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

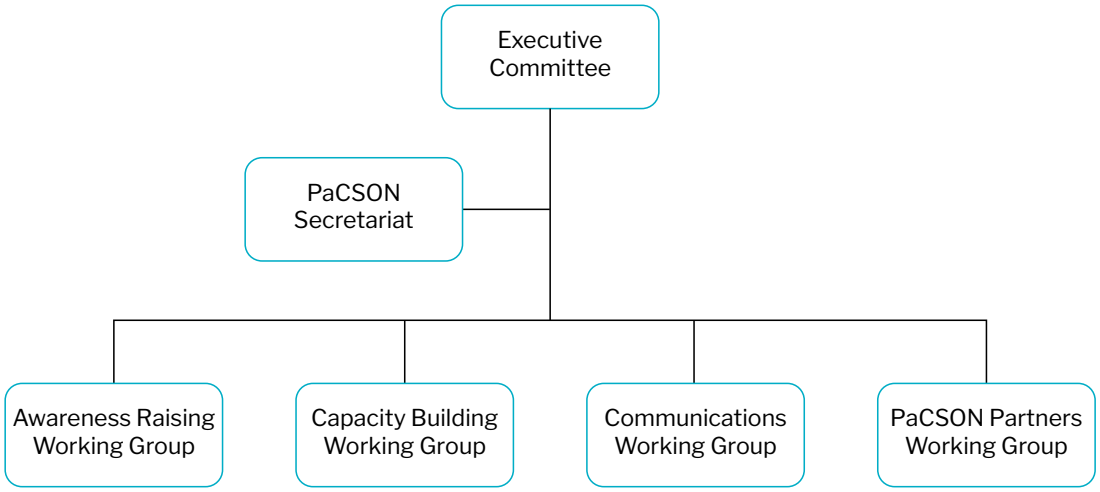


Figure 1: PaCSON network governance structure

Vision

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

Mission

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

2021 Annual General Meeting

Every 12 months, the PaCSON Community comes together to celebrate and recognise its efforts, and to plan for the coming year. In 2021, the PaCSON Annual General Meeting was held virtually over three days and reflected on what we had achieved and planned for where our journey was heading in 2022.

During the three-day program, some of the topics PaCSON discussed included:

- learning about big-data sets; understanding what data is and how it is collected; what threat information can be inferred from collecting data; how it can be used to help set priorities and show areas of concern
- the positive and long-term impacts that can be gained from conducting proactive awareness raising efforts
- the COVID-19 supply chain and how increased attraction from a range of malicious cyber actors can be deterred
- exploring cloud-based solutions and understanding common challenges as well as practical hints and tips to help overcome common barriers

PaCSON looks forward to returning to face-to-face engagement in 2022.

Member Updates

Australia

Overview

Australian Cyber Security Centre (ACSC)

Resourcing and Constituency

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. At the end of the 2020–21 financial year, ASD employees approximately 2,100 full-time equivalent staff.

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

The primary constituency for the ACSC includes:

- Government agencies
- Large organisations and critical infrastructure
- Small and medium business
- Individuals and families.

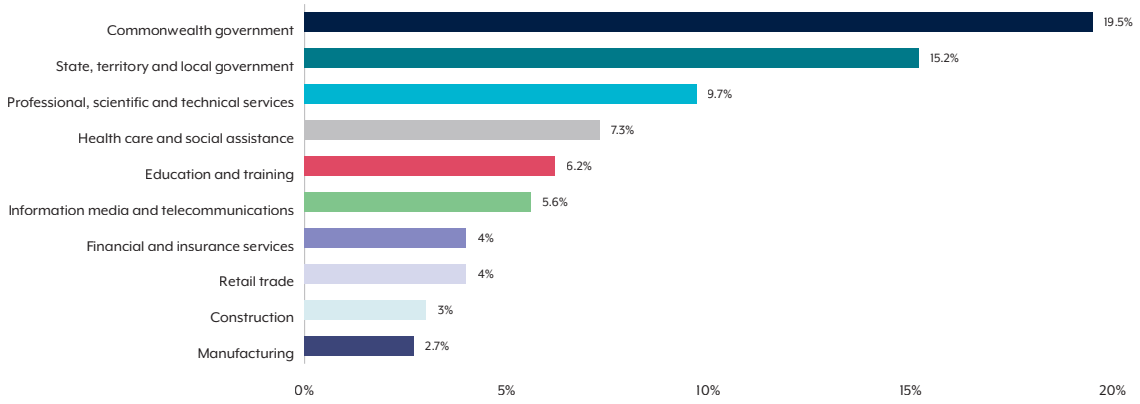


Figure 2: Australia – Cyber security incidents by the top ten reporting sectors for financial year 2020–21

Threat landscape

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

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

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

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

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

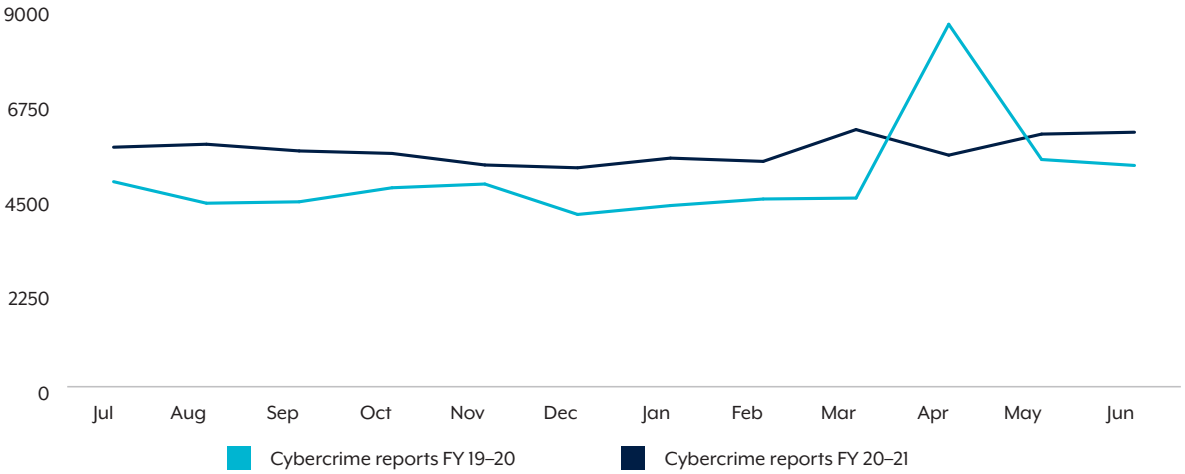
The Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts to improve cyber security. Our role is to help make Australia the most secure place to connect online. We monitor cyber threats across the globe 24 hours a day, seven days a week, so we can alert Australians early on what to do. We provide advice and information on how to protect yourself and your business online. When there is a cyber security incident, we provide clear and timely advice to individuals, businesses and critical infrastructure operators. We work with our business, government and academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats.

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

- Web shell malware
- Ransomware
- Phishing and scam emails
- Malicious insiders
- Remote access scams
- Denial of service
- Hacking attacks.

In the 2021 calendar year, the ACSC received approximately 73,100 cybercrime reports via ReportCyber and responded to nearly 1,340 cyber security incidents. Over this period, approximately 90 per cent of cybercrime reports to ReportCyber were made by individuals and nearly two-thirds of all cyber security incidents affected medium-to-large organisations. The ACSC encourages the reporting of all cybercrime and cyber security incidents, via our ReportCyber website (www.cyber.gov.au). The ACSC uses reported incidents to enhance national situational awareness of the cyber security environment in Australia, identify emerging trends, and support timely and tailored advice and assistance to Australian organisations.

Awareness raising



Note: The notable spike in April 2020 relates to a bulk extortion campaign, resulting in nearly half of the cybercrime reports for that month.

Figure 3: Australia – Cybercrime reports by month for financial year 2020–21 compared with financial year 2019–20

In 2021, ACSC launched an online cyber security learning platform called Learn Hub to support Australian small businesses, older Australians and families with practical, actionable cyber security advice. Learn Hub is hosted on the cyber.gov.au website and includes content for audience groups with a lower digital maturity. Content has been written at a level to be plainly understood by an average 10 year old, and is in line with best practice web guidelines in addressing low technological literacy and target audience confidence levels.

ACSC's Learn Hub also provides a number of downloadable resources in the form of toolkits, and also references existing ACSC products and resources such as step-by-step guides, prevention and response guides (ransomware and email security), ACSC's Small Business guide and Personal Cyber Security guides. In-language translations of products are also available for culturally and linguistically diverse (CALD) audiences in the following languages: Chinese Traditional, Chinese Simplified, Arabic, Hindi and Indonesian.

The ACSC produces several types of news, publications or advisories. These are all available on our website through the view all content function.

In 2021, the ACSC released:

- 1 ACSC Annual Cyber Threat Report
- 18 news items
- 22 new publications and guidance
- 7 advisories
- 28 alerts.

Case Study 1: Australia – Accellion File Transfer Appliance (FTA)

In January 2021, a new vulnerability was identified that targeted the Accellion file transfer appliance (FTA).

Vulnerabilities can have a significant impact on organisations, and when such a vulnerability is released, our teams spring into action to understand the issues and impact that it may have on Australia.

According to open source reporting, there were 13 of these devices easily identifiable within Australia. While a figure of 13 does not sound like much, all of the devices were being used by large organisations so a significant number of Australians were likely to be impacted.

The ACSC was asked to assist in dealing with one of these compromises and, during that investigation, we uncovered a novel way to identify the exfiltrated data and help organisations with their response.

The original web shell that was deployed had attempted to clean up after itself to disguise the attack. While it removed some indicators, quite a few remained behind. Log entries in the Apache rewrite log were not removed as part of the clean-up, and allowed our investigation to determine the exact timing that the attack took place.

With the time of the attack known, the next step was to turn our attention to what other artefacts were created as part of the compromise.

The investigation identified a large number of symbolic links that were created within the /home/seos/apps/1000/ folder, all with timestamps that were shortly after the identified time of the compromise.

By using 'log2timeline' over the disk image, a comprehensive timeline of changes that occurred to the disk was extracted and the investigation uncovered a pattern with these link files. They contained two sets of numbers separated by a period. In this case, the first set of numbers was 8,888, and the second was a unique number.

The investigation set out to identify the meaning behind these numbers with the intent to understand what had occurred during the compromise.

The focus of the investigation shifted to the FTA database where a 'files' table was identified within the 'mbox1_1000' database. This table contained a field with similar numbers inside the 'file_id' column.

The data was extracted to a CSV file allowing us to automate the analysis using command line tools. The investigation identified that the second series of numbers in the name of the symbolic link matched the 'file_id' column in the 'files' table.

The incident responders at the ACSC wrote a short script that searched the data and output a list of files that had been accessed illegitimately. This information was unable to be identified via the traditional audit logs as the attack directly accessed the database and did not use any of the legitimate access methods.

Once the list of files was identified, the ACSC worked with the customer to confirm that the information we had uncovered was correct. Using the file sizes from the database, and then aligning them with net flow data for the time, we got a pretty close match. While such outcomes are never perfect, it was a strong indicator that our investigation had successfully identified the exfiltrated files.

All of our findings were passed to the victim organisation, allowing them to make the necessary reports and take action to protect the information contained in the exfiltrated files.

The tradecraft from this investigation contributed to a collaborative effort by the cyber security authorities of Australia, New Zealand, Singapore, the UK, and the US on the Exploitation of Accellion FTA, which can be accessed from: https://www.cisa.gov/uscert/ncas/alerts/aa21-055a

Cook Islands

Overview

ICT Division, within the Office of the Prime Minister (OPM ICT)

Resourcing and constituency

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

Threat landscape

There is no formal process for cyber incidents reporting. In terms of online financial incidents, the reporting is made to the Financial Supervisory Commission (FSC).

Informal reporting can be submitted to the ICT Division through email and in person.

For the Cook Islands, common types of cyber threats include:

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

Occurrences of financial scams and viruses on the Government network are the major types of incidents to which the ICT Division responds.

In 2021, there were two incidents that came through OPM ICT:

- an email informing of an allegation of extortion. This was forwarded to the National Security Office and the Financial Intelligence Unit to investigate in collaboration with police.
- vulnerability attacks on the Exchange Mail Server. The attacks were mainly from China and the US. In response, an IP geo-block was put in place.

Awareness raising

With financial support from Get Safe Online, the Cook Islands we engaged a local contractor to produce cybercrime awareness content for publishing via radio, television and social media. The awareness campaign made reference to the Get Safe Online national site, https://www.getsafeonline.org.ck/

With the support of Get Safe Online, the following was achieved:

- Get Safe Online – Cook Islands Facebook page
- Radio and Live Stream
- Cook Islands Television
- Print Media
- Text Blast.

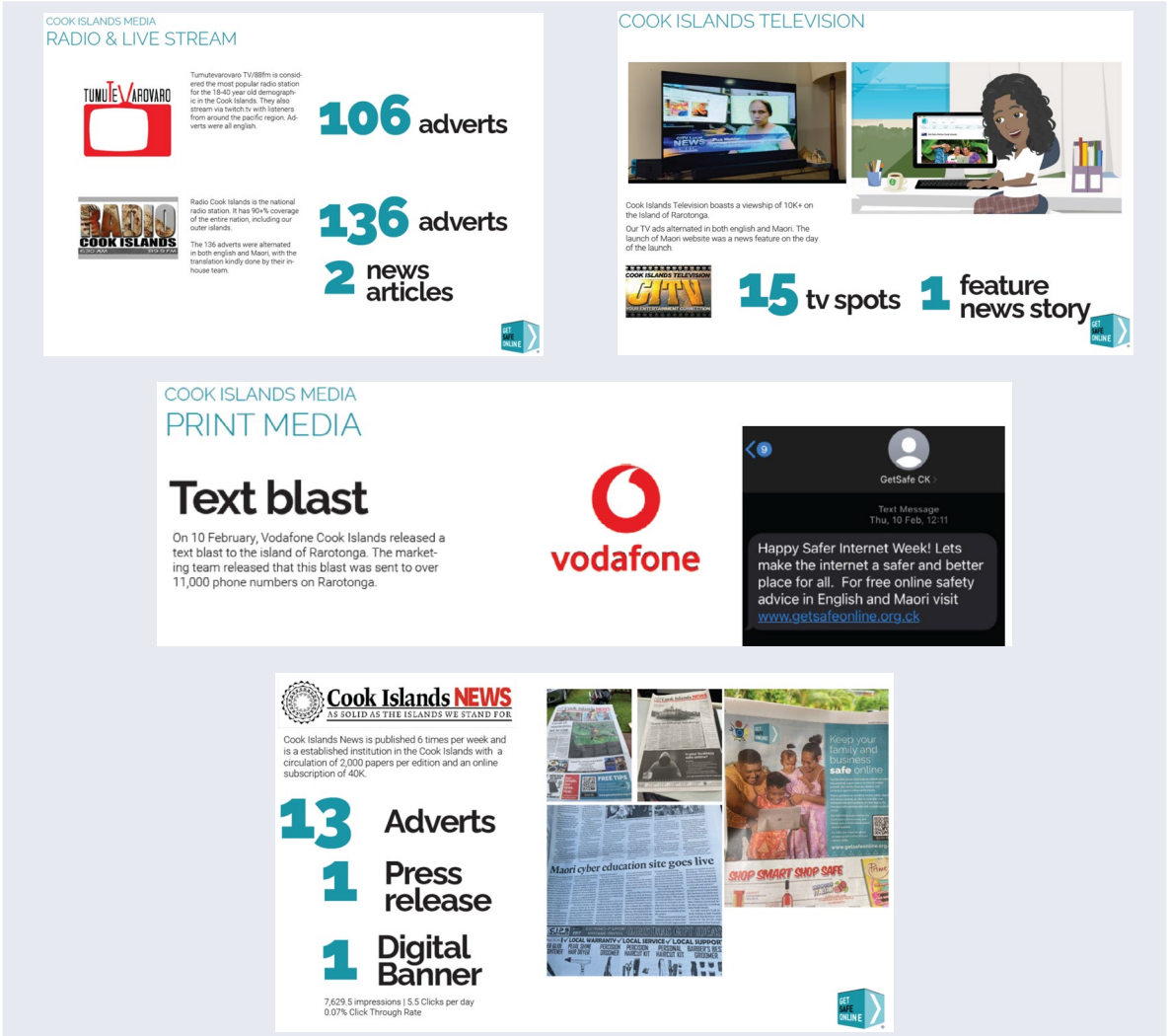


Figure 4: Cook Islands – Get Safe Online initiatives

Fiji

Overview

Ministry of Communications

Resourcing and constituency

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

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

In terms of high-level management, Hon Aiyaz Sayed-Khaiyum is the Minister for Communications and Ms. Tupou'tuah Baravilala is the Acting Permanent Secretary for Communications.

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

- Fiji Police Force
  For more information, refer to website – 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)
  For more information, refer to website – https://www.fijifiu.gov.fj/
- Online Safety Commission (OSC)
  For more information, refer to website – https://onlinesafetycommission.com/

Threat landscape

In Fiji, common threats to our cyber landscape include:

- website defacement
- phishing
- malware and ransomware
- financial fraud or financial crimes, including pyramid schemes
- business email compromise.

In 2021, Fiji continued to experience and respond to several cases of misinformation, disinformation, fake news and mal-information, including information related to COVID-19.

The Ministry of Communications responds to, thoroughly investigates, and resolves cyber incidents that affect government networks and infrastructure.

Awareness raising

The Ministry of Communications supports awareness raising initiatives within the civil service and also the public. When launching national initiatives, cyber security is a core component in our communications and public relations strategy.

Security advisories and awareness on critical vulnerabilities are disseminated out to government ministries.

Kiribati

Overview

Ministry of Information, Communications and Transport (MICT)

Resourcing and constituency

The Digital Transformation Office (DTO) of the MICT comprises six units, one of which is the Government Computer Emergency Response Team (CERT) with three permanent staff members, including the Government Chief Information Security Officer, the Senior Information Security Analyst, and an Information Security Analyst. The CERT is housed within the DTO and is headed by the Government National ICT Director, who also heads the other five units of the DTO. The DTO was established as part of a government restructure and all government ICT personnel are now being absorbed under it. The Government Chief Information Security Officer will lead the National CERT and report to the National ICT Director. The National ICT Director reports to the Secretary of the MICT and the Honourable Minister of the MICT.

Our primary constituencies are the government ICT sector, critical national infrastructure providers, the public, and local businesses.

Threat landscape

The National CERT has not yet formalised procedures on reporting cyber incidents; however, cyber incidents are often reported to the MICT/National CERT via direct telephone calls, law enforcement and direct emails.

Common threats to the cyber landscape in Kiribati include:

- social media phishing attacks
- financial scamming online
- disinformation
- usage of unlicensed or cracked software/malware/ransomware infected software
- unpatched systems (vulnerable systems usage).

We do not have the formal capability to respond to cyber incidents; however, in certain cases we are able to provide limited response to severe cyber incidents on government networks, critical infrastructure and service providers.

We have not formally lodged any incidents thus far, although MICT/National CERT have provided response capability on a few separate incidents. During the reporting period, MICT provided considerable support to the COVID-19 response for the Kiribati Government.

Awareness raising

The DTO and National CERT raise cyber security and cyber safety awareness in schools via the MICT's Cybersecurity Awareness School Campaigns. They also raise community awareness through cyber safety tips and advice on best practices for staying secure on the internet. This is an annual effort.

The MICT provides advisories to government ICT professionals on cyber security issues. We have also published national cyber security guidelines for government agencies. Email is our primary means of notification.

Marshall Islands

Overview

Marshall Islands Police Department (MIPD)

Resourcing and constituency

The MIPD is part of the Ministry of Justice. Headed by a Police Commissioner and made up of approximately 200 sworn police officers, the MIPD is responsible for serving a population of 70,000 people who inhabit 34 coral atolls and more than 1,000 islands.

The MIPD supports government, business and small enterprises, private industry and the public as its primary constituency.

Threat landscape

The Marshall Islands is able to receive cyber-related reporting through multiple sources, which include community outreach and engagement activities and police business.

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

- fraud, identity theft and other types of crimes targeting the financial sector
- scams designed to build doubt in trusted brands and extract money from victims
- business email compromise and ransomware
- malware and phishing attacks
- DoS attacks and malicious activities against the health sector.

The MIPD responds to and supports efforts for a variety of cyber and criminal incidents.

The MIPD does not currently collect reporting data on cyber incidents.

Awareness raising

The MIPD conducts various community engagement and awareness raising efforts. The MIPD uses social media to support information sharing and conducts various general public safety and awareness raising efforts.

Case Study 2: Marshall Islands – COVID-19 focus

During 2021, the Marshall Islands experienced a number of cyber incidents, which were influenced by COVID-19. The health and financial sectors, and the government more broadly, experienced increased threats, demonstrating how the Marshall Islands was affected by cyber criminals and malicious actors during this period.

New Zealand

Overview

CERT NZ

Resourcing and constituency

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

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

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 IR counterparts and the wider regional cyber community. The Pacific program delivers a program of on-going activity and collaboration, plus a number of standalone projects.

Our ongoing work includes the following:

- information and good practice sharing and development
- community development and engagement
- formal and informal mentorships
- direct incident response support
- community outreach
- contribution to PaCSON, including convenorship of the PaCSON Capacity Building Working Group (CBWG)
- support, advice, and contributions to New Zealand, regional, and global cyber capacity building.

Standalone projects initiated since January 2021 include the following:

- organising the PaCSON Remote Session Series
- spearheading the collaborative development and delivery of the Cyber Smart Pacific annual regional awareness raising campaign
- supporting the establishment of SamCERT
- trialing the translation of good practice materials
- sharing of CERT NZ reporting templates
- collaborating with CERT Tonga on a Cybersecurity Workforce Development Program.

See http://www.cert.govt.nz for more information.

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

The online tools can be accessed here:

https://www.cert.govt.nz/individuals/report-an-issue/ (for individuals and businesses)

https://www.cert.govt.nz/it-specialists/report-an-incident/ (for IT Specialists)

Full contact details are available here: https://www.cert.govt.nz/about/contact-us/

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

Threat landscape

The top five incident categories reported to CERT NZ in 2021 are:

- 3,709 phishing and credential harvesting, up 9 per cent on 2020
- 1,930 malware reports, up 24 per cent on 2020
- 1,897 scams and fraud reports, down 1 per cent on 2020
- 760 unauthorised access reports, up 50 per cent on 2020
- 106 website compromise reports, up 90 per cent on 2020.

Malware has continued its upward trend and overtaken ‘scams & fraud’ as the second most common incident reported to CERT NZ in 2021, while ‘phishing & credential harvesting’ has remained the top reported incident.

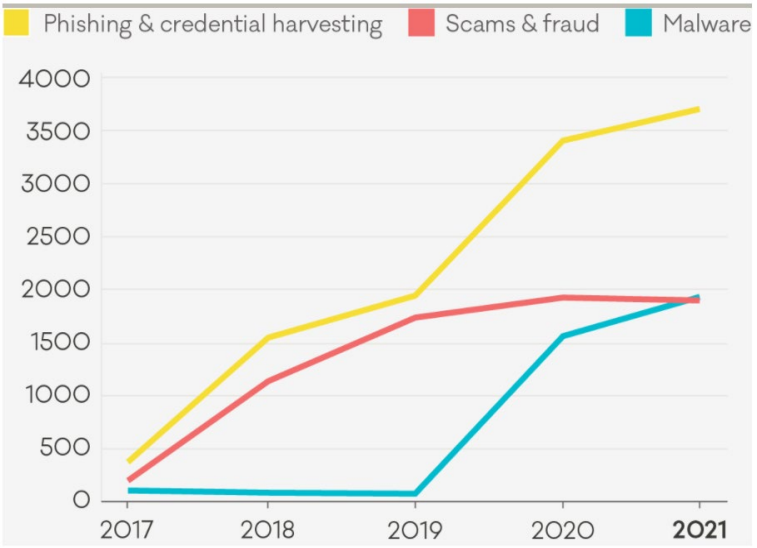


Figure 5: New Zealand – cyber threat trends 2017 – 2021

Of the reports received by CERT NZ in 2021, 15 per cent included a direct financial loss, with a combined total of NZD $16.8 million.

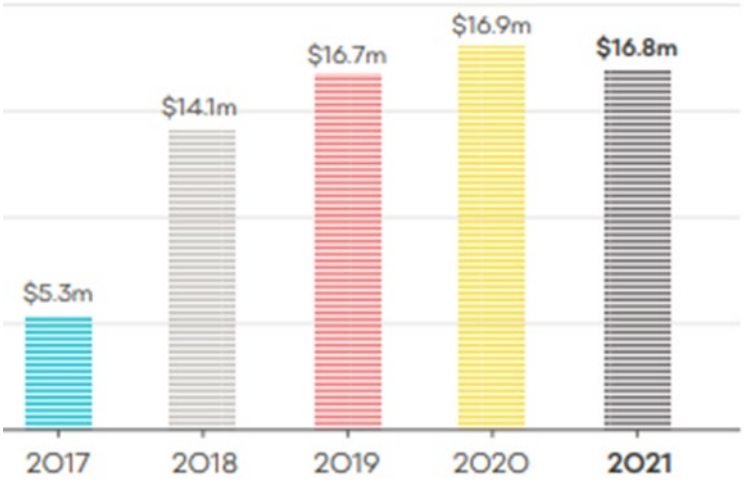


Figure 6: New Zealand – financial losses 2021 due to cyber attacks

CERT NZ accepts reports of any kind on cyber or online threat or incident. We operate a 'no wrong door' policy, where we refer incidents to other partners, where they are better placed than us to deal with them. For example:

- Scams or frauds, where there has been a loss of money or identity theft, are referred to the New Zealand Police.
- Online objectionable material is referred to the Department of Internal Affairs.

In terms of threats, vulnerabilities and incident response, CERT NZ's key services are:

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

In 2021, a total of 8,831 incidents were reported to CERT NZ, a 13 per cent increase on 2020.

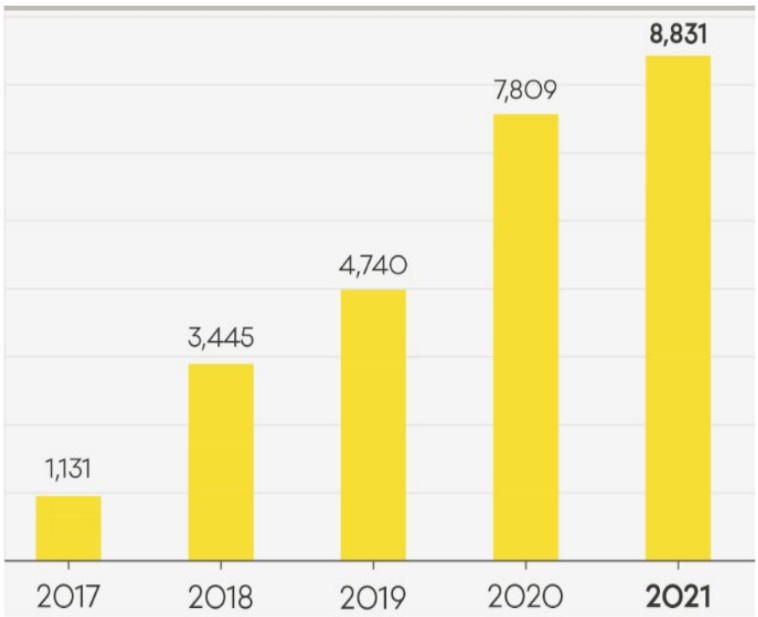
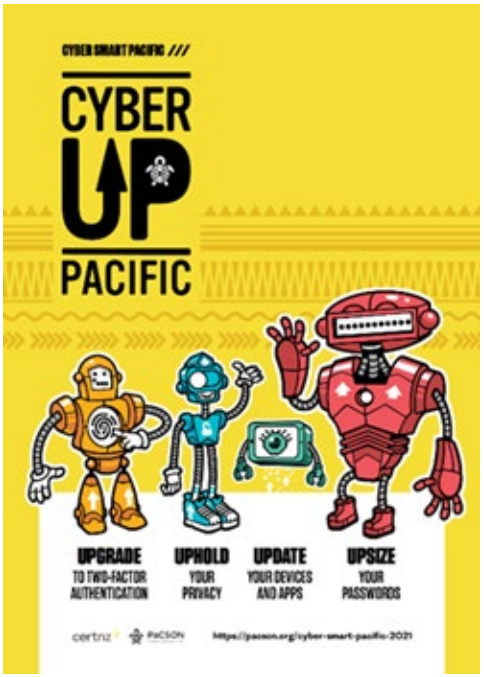


Figure 7: New Zealand – incident reports in 2021

Awareness raising

In October 2021, as part of International Cyber Awareness Month, CERT NZ supported the development of the collaborative Cyber Smart Pacific initiative for its second year, through the PaCSON Awareness Raising Working Group (ARWG).



Similar to 2020, the ARWG proposed and voted on a range of themes, taglines, and materials. The outcome included the launch of several local and regional websites and awareness efforts, including numerous localised and translated posters.

Domestically, CERT NZ ran its 5th annual Cyber Smart Week, also taking place in October.

CERT NZ engaged with partners from across the government and private sectors to share the four simple steps all New Zealanders could take to be more secure online. During the campaign, CERT NZ worked with 290 partner organisations to help amplify the reach and impact of the campaign. A wide range of resources – from graphics to editorial content – were available for partners to use and share. CERT NZ also ran a password-focused campaign in 2021, with supporting content including videos. 'Password perfect' was a mini campaign targeting 54 to 64 year-olds to get better at creating strong passwords by using passphrases that are stronger and easier to remember.

CERT NZ publishes media releases, guides, advisories and alerts, which are available on the CERT NZ website.

CERT NZ produces a quarterly report analysing and summarising incident reports made to CERT NZ over the previous quarter. As well as a highlights document, we published a 'Data Landscape', providing a standardised set of results and graphs for the quarter.

2021 saw CERT NZ update its Critical Controls, which is CERT NZ's best practice guide for business.

With the growing prevalence of ransomware, CERT NZ published several new pieces of content to help organisations understand and how to best mitigate any attack. This included the 'How ransomware happens and how to stop it' guide and infographic for IT specialists available at: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

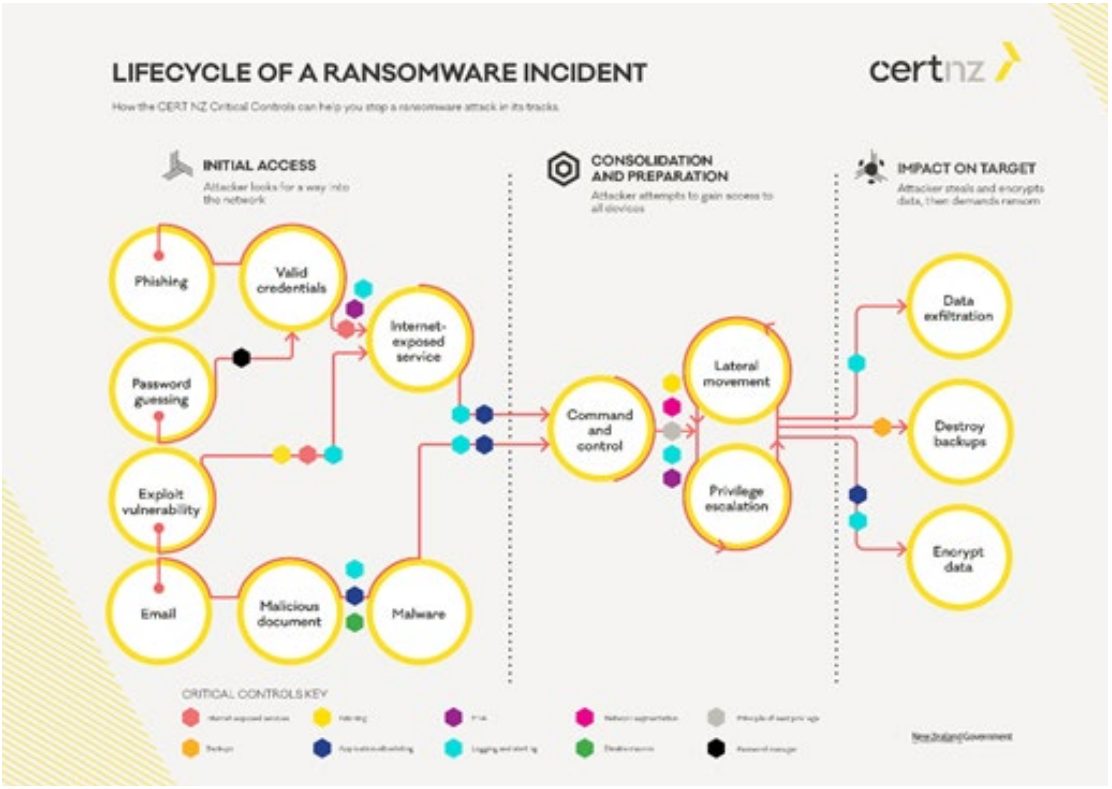


Figure 8: New Zealand – Cyber Smart Week, lifecycle of a ransomware incident

A business version can be found at https://www.cert.govt.nz/business/guides/protecting-from-ransomware/

CERT NZ increased its use of social media in 2021 as a way to reach our constituency. As well as building on our existing use of Twitter (@CERTNZ) and Facebook page: https://www.facebook.com/certnzgovt

CERT NZ launched a LinkedIn page to target businesses: https://www.linkedin.com/company/certnz/

Case Study 3: New Zealand – Log4j vulnerability

In December 2021, a critical security vulnerability in a component of open-source software Log4j was made public.

What is Log4j?

Log4j is widely used in software applications, which means the vulnerability immediately put thousands of businesses and organisations in New Zealand at risk. An update was quickly made available; however, any lag in discovering the software's use on systems and applying the update provided a window for attackers to seek access to those systems.

Log4j is a Java-based logging software component used to carry out numerous tasks including recording and communicating warning or error messages. Common examples include recording what types of devices are accessing your website or when someone tries to access a missing file on your website resulting in a "404 error" message. Log4j is part of a software supply chain which means it is used in many software applications.

A software supply chain is similar in function to a physical supply chain. For example, Log4j is like a component in car manufacturing, such as an airbag. The car manufacturer buys the airbags from another supplier and installs them into every car across various models. In day-to-day use you will not notice it is there, but if there is a critical fault with the airbag, the manufacturer may need to do a mass recall. If you do not hear about the recall, or take appropriate action, you could be at risk.

With so many software applications and services using Log4j, many companies still may not know that it is bundled together into the software they use.

Log4Shell is relatively easy for attackers to exploit, for example some of the first public activity noticed was the malicious code executed in the chat functions of the video game Minecraft.

How does the vulnerability affect systems?

The Log4j vulnerability, known as Log4Shell, allows attackers to run their own malicious code on a system. The results of this attack can vary and could include a system being controlled remotely, data being stolen, or the system being locked down with ransomware. Once the system is infiltrated, other systems within the organisation can be targeted.

Any applications that use Log4j could be affected. The vulnerability works by running code logged to the system. This means attackers can send lines of code and instead of logging the text, the system will execute it. This is also known as code injection or execution vulnerability.

Attackers may access systems but do not always take advantage of the access immediately, meaning the compromise may not be discovered until they decide to carry out an attack.

Exploitation of the Log4j vulnerability may be difficult to detect because it allows attackers to carry out various types of compromise, making it more difficult to identify the root cause.

CERT NZ response

CERT NZ was the first government organisation internationally to release advice on the Log4j vulnerability. This information was quickly picked up and circulated by international agencies and media, helping raise awareness of the risk and share advice to help protect against compromise.

Our IR team worked with local and international agencies to establish an incident coordination and response function, and shared information about how the incident was progressing.

CERT NZ anticipates that impacts from this vulnerability will continue and encourages all businesses and organisations to implement and maintain good cyber security practices.

Key Takeaways

- Log4j is a software component used by millions of systems around the globe.
- Attackers are actively scanning for the vulnerability.
- Larger organisations are likely to be targeted first. Due to ease of exploitation, attackers will likely target smaller businesses once larger organisations have patched all systems and are no longer easy to exploit.
- The extensive use of Log4j means some vulnerable software may still be undiscovered, leading to a potential "long-tail" of attacks.
- It may be difficult to determine if a compromise originated through exploitation of the Log4j vulnerability, because:
  - attackers can hide on systems for long periods of time before being discovered
  - the exploit allows attackers to carry out other malicious activity.

Niue

Overview

Telecom Niue Limited

Resourcing and constituency

Telecom Niue Limited is a company incorporated in Niue and owned 100 per cent by the Government of Niue. Telecom Niue employs a moderate size workforce including administrative officials, technicians and labourers.

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

Threat landscape

Generally, Niue Island's experience of cyber security threats is similar to that of the broader Pacific region. Some common types of cyber threats include:

- ransomware
- malware
- phishing attacks
- cyber bullying
- malicious software and fraud.

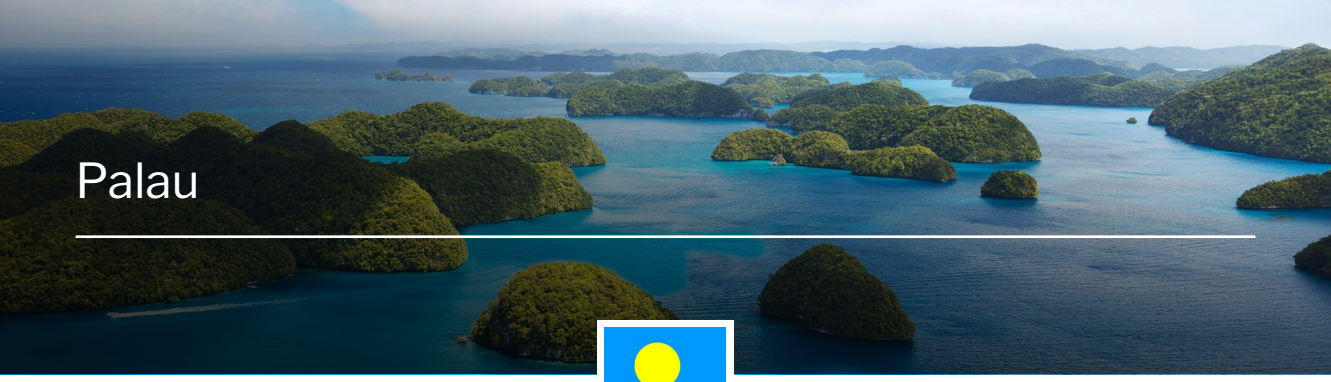
The types of incidents that Telecom Niue responded to were cyber-attacks reported to the Government of Niue through official reporting channels.

During the reporting period, Telecom Niue assisted with response to three major events.

Awareness raising

Telecom Niue conducts various community engagement and awareness raising efforts. In 2021, engagement through social media was common.

Telecom Niue promotes news via our social media accounts.



Palau

Overview

The Bureau of Public Safety

Resourcing and constituency

The Bureau of Public Safety exists within the Republic of Palau's Ministry of Justice and is part of the Executive Branch.

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.

Threat landscape

The Bureau of Public Safety receives cyber-related reporting through formal reporting frameworks. Additionally, the use of social media is common.

Palau experiences many cyber security threats common to the broader Pacific region, which include:

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

In Palau, the Bureau of Public Safety responds primarily to money laundering reports from the Financial Investigations Unit, on occasions when it needs assistance. We also respond to online gambling but with limited resources, mostly due to our inability to gain network access or continue tracing.

The Bureau of Public Safety has not yet experienced the challenges of major cybercrime disruptions.

Awareness raising

The Bureau of Public Safety conducts various community engagement and awareness raising efforts. In 2020, engagement via social media platforms was common.

The Bureau of Public Safety uses the Ministry of Justice's Facebook page to send out information on services offered by our department. We also use the National Broadcasting Service to send out messages and air our services.

Case Study 4: Palau – COVID-19 impact

For Palau, there was minimal impact in 2021 from COVID-19 and cyber-related events. During the year, Palau continued to experience a range of cyber issues, but thankfully did not experience any major challenges. Support from international partners was key for Palau being able to maintain a favourable cyber security position during 2021.

Papua New Guinea

Overview 1

PNG Computer Emergency Response Team (PNGCERT), within the National Information and Communications Technology Authority (NICTA)

Resourcing and Constituency

PNGCERT was established by the Government and is operated under the auspices of the same, centrally facilitated through NICTA. PNGCERT works to promote awareness, provide advisory assistance, and coordinate responses to cyber security incidents in PNG.

The NICTA is a government agency responsible for the regulation and licensing of information and communications technology (ICT) in PNG. The below figure explains NICTA's structure.

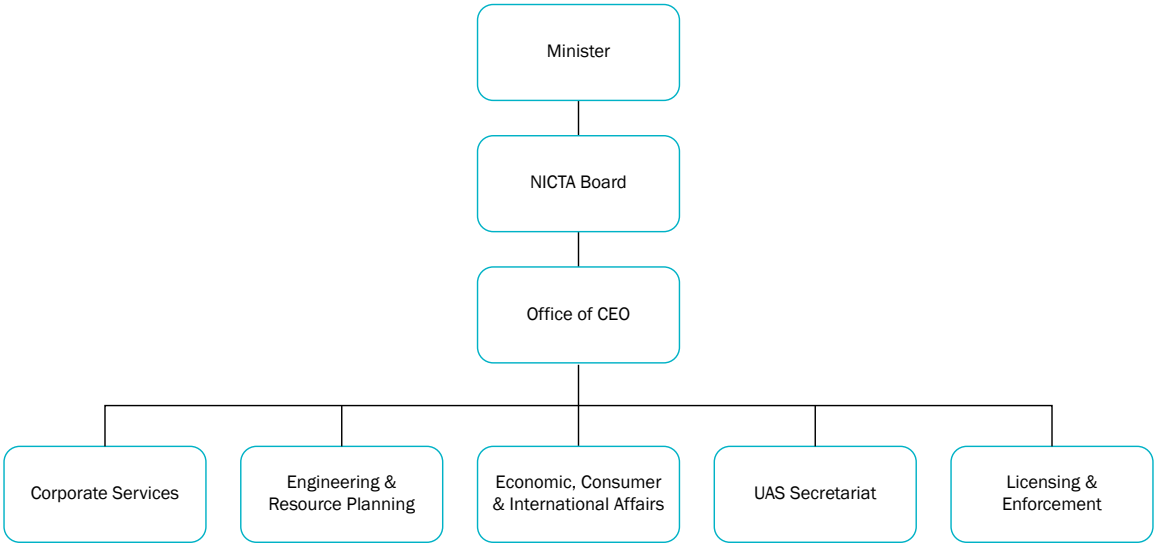


Figure 9: Papua New Guinea – NICTA organisation structure

Office of the Chief Executive Officer (CEO)

Three branches: Corporate Legal Services, Special Projects, and Corporate Secretariat Services.

The CEO is responsible for:

- managing NICTA in accordance with the policy direction of the Board
- advising the Board on matters concerning NICTA
- carrying out the operational and administrative functions of the organisation with the assistance of the Executive Management Team.

Corporate Services Department (CSD)

Three branches: Human Resources and Administration, Finance, and Information Technology.

CSD is responsible for:

- training, staff development and recruitment functions including administering employees' terms and conditions of employment
- compiling Papua New Guinea Telecommunication Authority (PANGTEL) annual budget estimates, debt collection, insurance and personnel matters
- coordinating the IT needs and requirements for line technical departments.

Engineering & Resource Planning Department (ERPD)

Two branches: Resource Planning and ICT Standards & Policy.

ERPD is responsible for:

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

Economics, Consumer and International Affairs (ECIA)

Three branches: Economic Regulation, Consumer Affairs, and International Affairs.

ECIA is responsible for:

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

Universal Access Scheme Secretariat (UAS)

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

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

Licensing & Enforcement Department (LED)

Two branches: Licensing & Business Relations, and Enforcement and Compliance.

LED is responsible for:

- ensuring all ICT Operators have appropriate authorisations (licences, permits, certificates, etc.)
- maintaining cordial working relationship with licensees and stakeholders
- inspecting and surveying all radio and telecommunications equipment and services operating in PNG
- carrying out surveillance of radio frequency spectrums, setting up of equipment standard specifications, and consequent testing of imported radio communications equipment.

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

- broadcasting
- radio communications
- telecommunications.

Threat landscape

In PNG, cyber incidents can be reported through formal government or business frameworks. Additionally, both PNGCERT and NICTA have an online enquiries site where incidents can be reported. Reports can also be provided in person or over the phone.

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

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

Ransomware attacks continue to be a major threat to PNG. In 2021, a major ransomware event impacted payment systems to the Department of Finance.

Working with colleagues from other government departments, NICTA assisted by providing advice and expertise in response to several cyber events in 2021. In addition, some advice and procedural guidance was provided by the National Cyber Security Centre (NCSC) a by the WithYouWithMe initiative. General advice is available for computer users and ICT managers to continually do updates, install or upgrade their firewalls, and install antivirus software.

Awareness raising

NICTA supported various virtual community engagement and awareness raising efforts, including through community outreach and engagement via social media. Unfortunately, due to COVID-19 and consequent measures designed to protect our participants from sickness, many of the engagements NICTA had planned needed to be cancelled.

In 2021, NICTA and PNGCERT were pleased to participate in the PaCSON Cyber Smart Pacific Campaign. We continue to promote and provide tips for safe online practices and behaviour through our Get Safe Online PNG website – https://www.getsafeonline.org.pg/

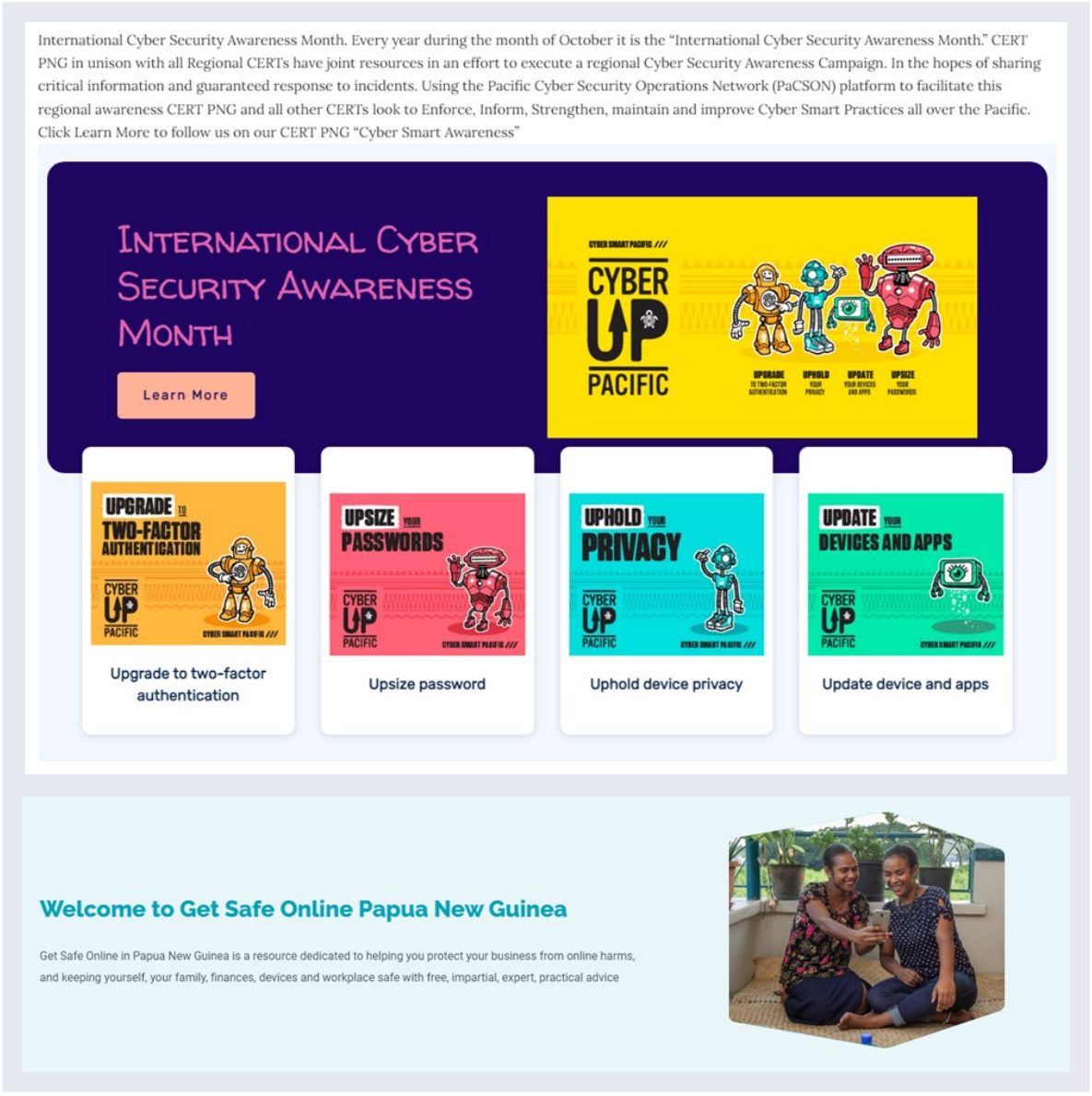


Figure 10: Papua New Guinea – 2021 Get Safe Online

As a function of NICTA, PNGCERT works to promote awareness, provide advisory assistance and coordinate responses to cyber security incidents in PNG. We use our website as a mechanism to promote the latest cyber security news and tips.

Case Study 5: Papua New Guinea – government cyber hardening practices

We always practice and prepare to defend against a cyber attack. In October 2021, multiple areas of the PNG government were required to put this planning into action as we responded to a ransomware attack against our Department of Finance's Integrated Financial Management System.

NICTA was available to provide assistance and support to the Department of Finance and other cyber functions of the PNG government as they worked to recover from this event.

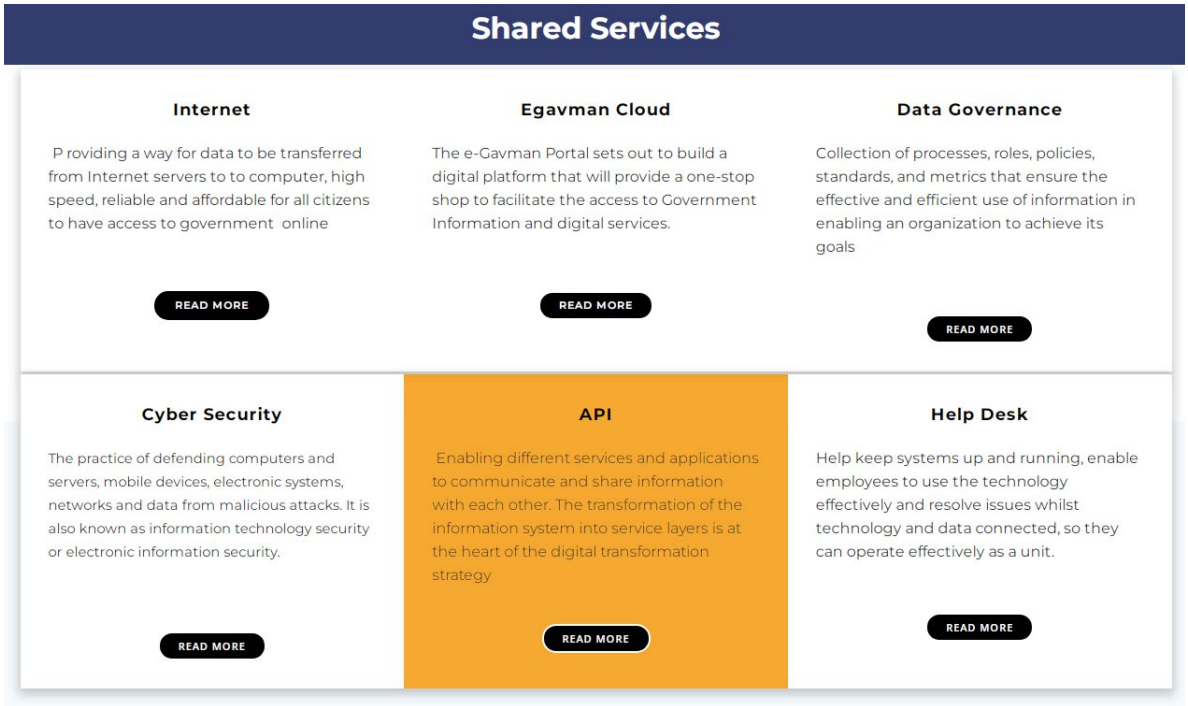
Overview 2

Department of Information and Communications Technology (DICT)

Resourcing and constituency

DICT is a government agency established through a Ministerial Determination and is responsible for providing timely policy advice to the Minister for ICT on communication and information matters. DICT also coordinates digital government programs and initiatives to raise awareness and disseminate government IT development information.

As its primary constituency, DICT provides cyber security services through the NCSC and other digital government-shared services support to PNG government departments.



DICT's Mission

The DICT mission is to harness the potential of ICT to make PNG a smart, networked and knowledgeable society and help bring government closer to the people through effective governance, improved service delivery and socio-economic growth. DICT aims to transform how government learns, builds, delivers, and measures digital services in the 21st century.

DICT sets out to achieve its mission by providing all agencies with the tools, methods, practices, and policy guidance they need to deliver effective and accessible digital services to all PNG residents. DICT's goal is to ensure the use of appropriate and affordable digital technologies through a transformative and inclusive approach across sectors of the economy for the benefit of all.

At DICT, we are committed to improving people's experience of government services by putting people first, improving skills both within government and outside government to deliver these services. DICT values:

- customer focus
- innovation and change
- standards
- teamwork and collaboration
- transparency
- honesty
- listening
- employees
- professionalism.

We are committed to working as one team at all levels of our operations to ensure the effective and efficient delivery of digital services to government, business and the citizens of the country.

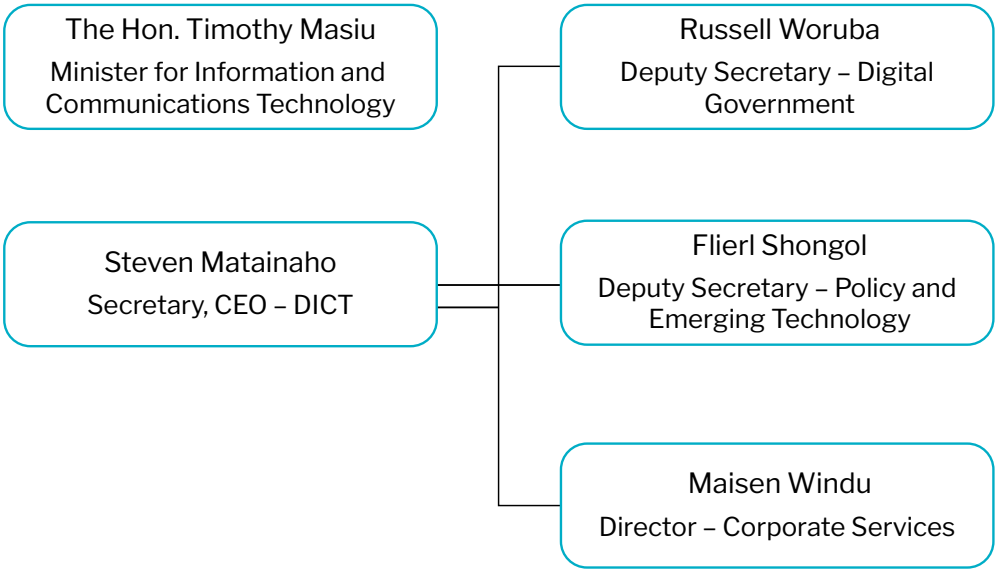


Figure 11: Papua New Guinea – DICT organisation structure

DICT's Vision

It is DICT's vision that the use of ICT will:

- promote collaboration, interaction and participation
- promote innovation and learning
- provide an open and transparent government
- provide citizen-centered services, and knowledge-based industries.

This vision is one where all citizens are empowered and can interact and collaborate with the Government.

Threat landscape

Occurrences of cyber incident reporting to DICT can be submitted directly to the NCSC or through our website – http://www.ict.gov.pg

PNG's experience of cyber security threats is similar to that of the broader Pacific region. Some common types of cyber threats include:

- malware
- ransomware attacks
- phishing attacks
- DDOS attacks
- identity theft and social engineering used by cyber criminals to conduct acts of fraud and theft.

During the 2021 reporting period, DICT received three incident reports.

Awareness raising

To support the increasing need for cyber resilience and safety in PNG, DICT has adopted several awareness raising initiatives, primarily on our website. Here, DICT promotes cyber safety awareness materials for everyday and government users.

As a first step since joining PaCSON in 2021, DICT was pleased to be able to participate in the PaCSON Cyber Smart Pacific campaign.

DICT raises awareness through its social media pages on Facebook and LinkedIn. Some other events that DICT has taken part in for cyber security and cyber safety awareness are Girls in ICT Day, online safety, Cyber Security Awareness Month, and a careers expo for youths.

DICT provides support to the PNG Government through official communication channels. DICT provides pamphlets, graphics online and participates on a radio talkback show.

Case Study 6: Papua New Guinea – 2021 DICT Government's Social Media Mismanagement Desk (SMMD)

The SMMD was established following a 2021 Cabinet decision for the DICT to coordinate countering misinformation and disinformation on social media and other digital outlets.

Since its operations were established, the SMMD has processes in place for monitoring, analysing, and taking necessary actions with relevant government agencies in relation to misinformation.

The public is requested to assist the government in its efforts to counter misinformation on social media platforms, such as Facebook, by filling in the required form and registering any complaints for further deliberation or action.

In relation to this case study, DICT was a member of a cyber investigation team, which investigated a cyber attack on a government department.

Samoa

Overview

Samoa Computer Emergency Response Team (SamCERT), within the Ministry of Communications and Information Technology (MCIT), Samoa

Resourcing and constituency

MCIT is the Government's policy advisor and central planning agency for all broadcasting, postal, telecommunications, ICT and cyber security policies. MCIT comprises the National Computer Emergency Response Team (SamCERT), the Policy and Planning Development Division, the ICT Secretariat Division, the Broadcasting Services Division and the Corporate Services Division. In addition, there is the Office of the Minister of Communications and Information Technology. In the pipeline, is the establishment of the Digital Transformation Authority (DTA) which will oversee the Government's digital transformation agenda and activities.

MCIT currently operates from three locations in the city of Apia, with a combined workforce of over 50 employees. It is a small ministry, but the weight it carries is quite significant in relation to the national support it delivers.

MCIT plans, designs and develops strategies and policies in all areas outlined above for all government agencies and offices to adhere to. In addition, MCIT conducts educational and awareness campaigns, and capacity development programs for government, the private sector, communities, schools and businesses. Lastly, through the newly established SamCERT, MCIT will directly liaise with private businesses, non-government organisations (NGOs), government bodies and academic institutions in relation to all cyber incidents. SamCERT's support is on a national level in that it will respond and provide cyber security assistance to government, local business communities and the general public.

Threat landscape

Currently, all crimes, including cyber incidents, are reported to the Samoa Ministry of Police and Prisons (SMPP), with additional support provided by MCIT for any cyber-related attacks and incidents. Reporting paths have been set up in government for incident support. SamCERT is currently working on developing its own website, which will be the central area for cyber security information distribution and incident reporting. To date, SamCERT information is loaded and facilitated under the MCIT website through the cyber security category of 'information and resources'.

The top five cyber security threats for Samoa are:

1. email spam and business email compromise
2. ransomware
3. misinformation
4. DOS and DDOS
5. insider threats (technical administrators, HR Resources).

In addition, threats are posed by the rise of fake news, disinformation, cyber bullying and cyber harassment in Samoa and across the Blue Pacific region.

During COVID-19 and the 2021–22 financial year, SamCERT responded to three high-level incidents that impacted government organisations. MCIT, through its partners in government – mainly the ICT Technical Working Group for Government (ICT-TWG) – provided extensive support to raising awareness and responded to the following concerning incidents:

1. An infrastructure-related incident which was quickly resolved with the assistance of the ICTTWG (as the collaborative team-extension for SamCERT) given it was equipped to handle such incidents through technical training over the years.
2. A ransomware incident affecting the education sector which was managed and successfully recovered through the technical support provided by the ICT-TWG, SamCERT, and the education entity's IT division, in collaboration with members of PacSON and Australia's Department of Foreign Affairs and Trade's (DFAT) regional support entity, Trustwave.
3. A ransomware infection within a tourism industry-related government organisation to which SamCERT responded and assisted the IT team to manage the incident.

In addition to these three critical incidents, SamCERT provided online security advice to members of the public which had been requested through the MCIT enquires email on its website.

Awareness raising

SamCERT works with MCIT, sector partners and stakeholders to promote the importance of cyber security, with ongoing cyber security awareness programs and capacity development training initiatives available across the country.

Using our various social media accounts, SamCERT promotes cyber security and cyber safety awareness materials. Using the GetSafeOnline materials, SamCERT promotes the message 'Staying safe online is important and we must all understand how to stay safe online'. The GetSafeOnline promotion video is helping SamCERT to create awareness with our communities on matters of cyber safety.

> To watch the full video, visit the MCIT Youtube using this link – https://www.youtube.com/watch?v=V314PkXje8I
>
> To see the Samoa GetSafeOnline website, please visit – www.getsafeonline.ws
>
> Check out the MCIT Samoa Facebook page for more updates and news – https://www.facebook.com/mcitsamoaofficial/

Much of the cyber security awareness training is targeted by the ICT-TWG on various cyber security topics and best practices for government and private business. Additional support is provided by member groups, including the Samoa Information Technology Association (SITA), which deals directly with the community and other sectors of government through various cyber security training and awareness programs. SITA also hosts an annual conference on cyber security for both public and private sectors. During 2021–22, SITA was not able to host a cyber security conference due to COVID-19 lockdown requirements, but the organisation is keen to reinstate this conference annually to boost cyber security understanding domestically across all areas.

SamCERT was also pleased to participate in the 2021 PaCSON Cyber Smart Pacific campaign again – https://mcit.gov.ws/cyber-smart-pacific-2021-samoa/

Through collaboration with the education sector for 2021–22, SamCERT is happy to note that it assisted in promoting cyber security inclusions in various strategic documents for the education sector. This will see the uptake of cyber security courses as well as the inclusion of cyber security materials in national certification programs run by Samoa Qualification Agencies (SQA). The Ministry of Commerce, Industry, and Labour has also started capacity building schemes for officials in the area of ICT, which likewise fall within cyber security SQA accreditation standards. The National University of Samoa is also developing programs and courses that will address the cyber security needs for Samoa, and hopefully attract regional interest in this very specific and technical area.

Following the three critical incident reports that SamCERT submitted, the Samoan Government has set up a Cybersecurity High-Level Taskforce comprised of ministers and CEOs in the relevant areas of support, led by the Deputy Prime Minister, to address all cyber security issues across government. In providing this new level of support, issues related to cyber security will have a sub-committee to the National Security Committee, which will report to Cabinet on a regular basis on the national cyber security status of Samoa.

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

As part of Samoa's efforts to build well-established tools for cyber security and cyber safety, Samoa now has a GetSafeOnline website, available in both Samoan and English. This platform also includes materials which promote understanding of the different threats emerging in the cyber space, including awareness materials launched during the 2021 National Cybersecurity Awareness Week. Additionally, the published materials are the result of MCIT collaborating with international partners, such as PaCSON, CERT NZ, the Asia Pacific Network Information Centre (APNIC), and other regional cyber security entities.

Case Study 7: Samoa – Launch of SamCERT

The launch of SamCERT in May 2021 was a big boost to the cyber resilience of Samoa and the broader Pacific.

As it is an initiative towards strengthening Samoa's cyber security, the capabilities of SamCERT include:

- content monitoring and filtering to primarily deliver safe cyber space to users
- intrusion detection and prevention systems
- centralised virus protection services
- traffic monitoring, auditing and reporting.

The three key areas of activity that guide SamCERT's work are strengthening, improvising and increasing Samoa's national cyber security, cyber safety, and cyber inclusion. SamCERT will not only help raise and improve cyber security awareness, but it will also provide technical support to resolve cyber security incidents and threat management. Furthermore, SamCERT is a key supporter of cyber security for both the public and private sectors.

SamCERT has already proven valuable to strengthening the cyber resilience of Samoa, having assisted in responding to several cyber events within government and the private sector, as well as with the Samoan public.

Solomon Islands

Overview

Solomon Islands Government Information Communication Technology Services (SIG ICTS).

Resourcing and constituency

SIG ICTS is an office with 30 technical staff and 5 in the management level and administration.

Currently, SIG ICTS sits under the Ministry of Finance Corporate Services, reporting to the Deputy Secretary Corporate Services. SIG ICTS provides services on three fronts: client support, information systems, and infrastructure. There is still a huge resource gap in terms of capacity, and an organisational structural review is in progress to clearly ascertain roles and responsibilities, which will result in additional recruitment and capacity development.

With a whole-of-government approach, a Digital Transformation Institutional Framework has been developed (in draft) to capture this. The figure below shows the proposed restructure as per SIG ICTS' Five-year ICT Strategic Plan.

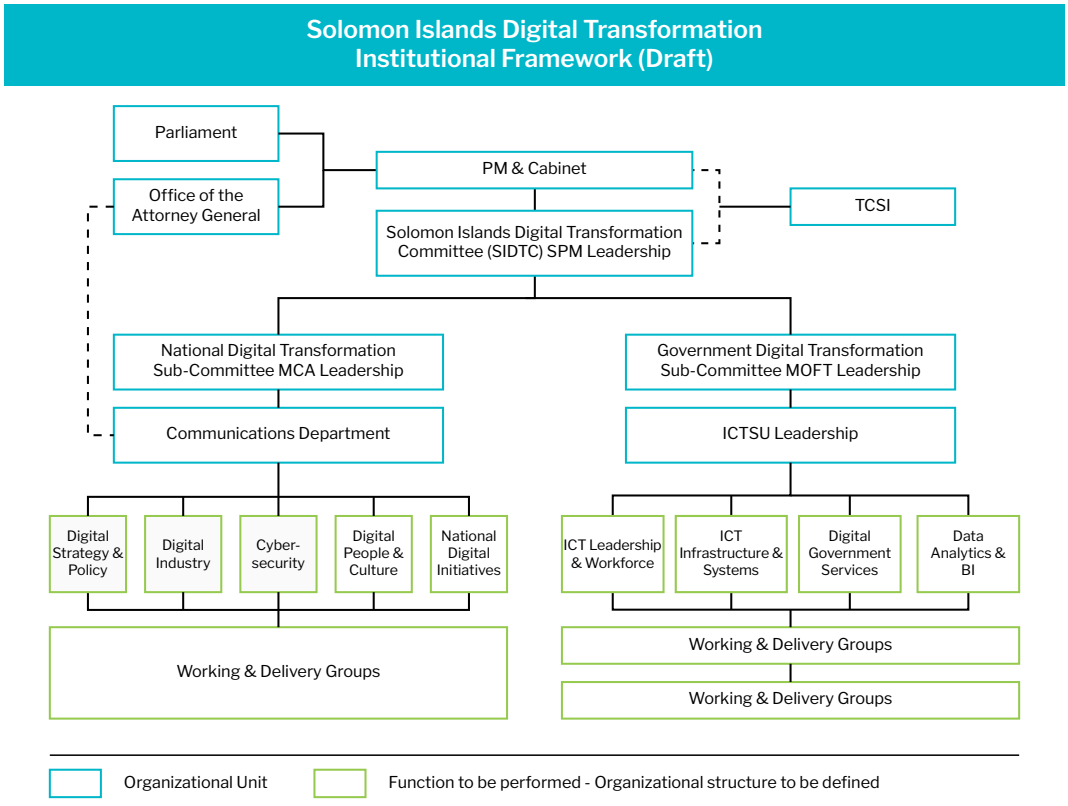


Figure 12: Solomon Islands – Digital Transformation Institutional Framework

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

Threat landscape

There is no fully-functional mechanism in place specifically for cyber incident management and reporting as this is currently being developed through the implementation of a security operations centre within SIG ICTS, which is still at an infant stage.

Reporting is; however, done via our helpdesk support system through:

- emails
- phone calls
- direct engagement with stakeholders
- monitoring and addressing incidents through our Security information and event management (SIEM).

For the Solomon Islands, common types of incidents we respond to include:

- phishing:
  - identify scams
  - analyse links and report to portals, such as virusTotal
  - block domain and emails through our email security gateway
  - provide awareness to end users
- malware:
  - identify
  - patch and upgrade or update system
  - provide awareness to end users
  - information leakage, data spills and insider threats:
  - log analysis and email audit
  - identify and report
- ransomware:
  - analyse files infected with the maql file extension
  - identify the infected machines and take them offline for further analysis
  - send sample files for further analysis by the antivirus team vendor (Eset).

During the 2021 reporting period, SIG ICTS responded to, and provided assistance or advice regarding, several cyber events. This included addressing phishing emails via an email security gateway by blocking inbound malicious emails, analysing the phishing links through virusTotal, and patching servers and client computers with updates in a timely manner.

Offline machines were taken from the network for further investigation when affected by ransomware (maql file extension). A sample of infected files were sent to Eset for further analysis.

Awareness raising

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

In 2021, SIG ICTS participated in the PaCSON Cyber Smart Pacific Campaign. This effort allowed SIG ICTS to facilitate assistance via direct constituent engagement and has helped to improve the Solomon Islands cyber smart capacity.

Figure 13: Solomon Islands – Cyber Up Campaign

New articles and security advice is released via email, and plans are in place to have a dedicated page via the Solomon Islands Government portal.

Tokelau

Overview

Telecommunication Tokelau Corporation, also known as TELETOK.

Resourcing and constituency

Teletok currently consists of 18 staff.

Prior to 1996, telecommunications were administered by a government department. The 1996 TELETOK Rules corporatised this service and, since 1997, TELETOK has remained a monopoly.

TELETOK has been confronted with the formidable problem of a deteriorating network over the years. The signaling protocol used in the past is no longer practical and, as a legacy system, there has been great difficulties in getting technical support services and spare parts in the market. Therefore, TELETOK worked hard to upgrade its network system from the old PABX to a soft switch in 2014.

Then, in 2015, TELETOK upgraded its public switched telephone network (PSTN) multi-service access node (MSAN) equipment to ensure the provision of reliable services and ongoing outside support by Challenge Networks Australia. The upgrade was initiated by local demand due to plain old telephone service (POTS) on landlines and an asymmetric digital subscriber line (ADSL) on the fixed network. The upgrade was fully completed in late April 2016. Around the same time, TELETOK's voice emergency system was also upgraded.

TELETOK has had outages at times which completely disconnected sites from national and international links. This reaffirms that we are always vulnerable without full power and voice emergency systems on all island sites.

In 2017, TELETOK completed major capital projects on a 4G long-term evolution (LTE) mobile network (a new ICT broadband platform), solar upgrades, HF and VHF emergency voice systems, and multicast. With the new broadband 4G LTE mobile network, digital bridges have been constructed between islands to international destinations. The Government supported the 4G LTE project with $1.05 million from its financial year budgets of 2015–16 and 2016–17. Other capital developments on domestic cable, submarine cable, national radio, online charging system (OCS), equipment rooms, and offices are not factored into financial plan but are, nevertheless, ongoing projects.

TELETOK is now over 20 years old. It has shared difficulties and obstacles, and so lessons learned have helped in engineering this ongoing plan based on demand.

Corporate governance

At present, the Board of Directors is TELETOK's governing body. The committee comprises six members of the Council for the Ongoing Government of Tokelau. The Board's role as the principal decision-maker is to make sure proper direction and control of practices and processes are in place and followed accordingly. Management functions are enunciated under the requirements of TELETOK legislation, Rules 2016.

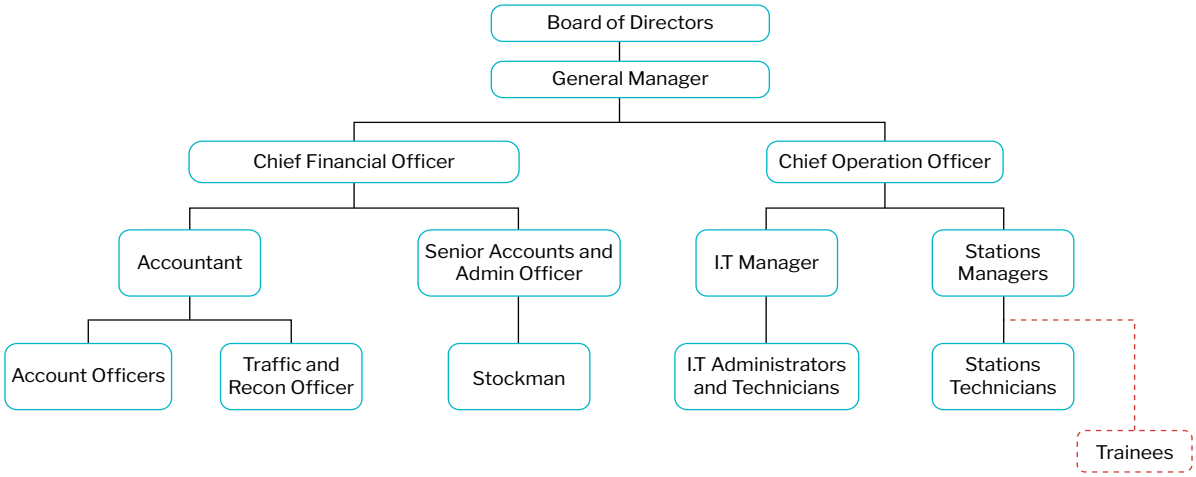


Figure 14: Tokelau – TELETOK organisation structure

Ownership

TELETOK is a state-owned enterprise, wholly owned by the Government of Tokelau as precisely spelled out and established under the requirements of the TELETOK Rules 1996.

Objectives

TELETOK, through the planning process of the Government National Strategic Plan 2016–20, adopted five broad objectives based on a Strengths, Weakness, Opportunities and Threat (SWOT) analysis:

1. Governance

   This objective ensures good practices of corporate governance are applied in TELETOK. Applicable laws, decisions reached on matters taken up to Board level, policies and procedures are followed to manage all risks surrounding the business environment and activities.

2. Human development

   To maintain and sustain these services, it is prudent that human capacity and technical skills are ongoing priorities and that training is available to staff through short and long-term attachments for the duration of the plan.

3. Infrastructure

   With the fast pace in technological advancement in the ICT industry, it is paramount that TELETOK should commit to keeping abreast with these changes. Therefore, TELETOK must comply with compatible standards in place to enable reliable delivery of services and, more importantly, with a suitable and effective ICT infrastructure for Tokelau.

4. Sustainability

   TELETOK, without doubt, struggles to sustain its economic status because of its market nature and small size. Corporate practices aim to ensure TELETOK operates in a financially sustainable manner. The Taupulega and the Government may wish to consider supporting TELETOK by subsidising its capital developments and operations to ensure achievement of key development priorities for the nation.

5. Climate change

   With the geographical nature of the islands and seasonal weather conditions experienced in the past, TELETOK is encouraged to undertake disaster recovery measures that ensure continuity of service delivery during unforeseen circumstances, and to consider disaster and climate risks when planning new or upgrades of existing infrastructure.

TELETOK is mandated to support Tokelau's three coral atolls. This supports all elements of Tokelau's society with matters of cyber security, internet access and telecommunications services. This includes provision of services to the public, government and business.

Reports to TELETOK can be submitted via our website and other official communication channels.

Threat landscape

Tokelau experiences cyber security threats that are unique to its small island structure compared to the broader Pacific region. Some common types of cyber threats to Tokelau include:

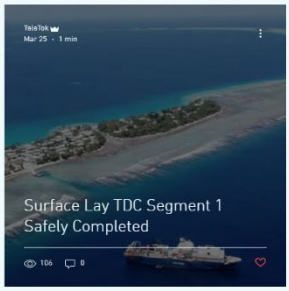
- securing and hardening networks, including firewall maintenance and resourcing
- election abuse and misinformation.

Other challenges to Tokelau include the hardships of creating repeatable processes and developing longstanding corporate knowledge.

Awareness raising

The TELETOK website is the primary means of awareness raising. In October 2021, TELETOK was fortunate to participate in the Cyber Smart Pacific 2021 and used their company website technician to support development of this initiative. TELETOK promoted the campaign on Facebook, via their website and on Twitter.

Other methods of awareness raising include the TELETOK Facebook and Twitter social media accounts. On our website, TELETOK shares news articles, public notices and cyber security advisories.



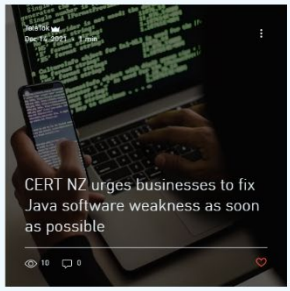
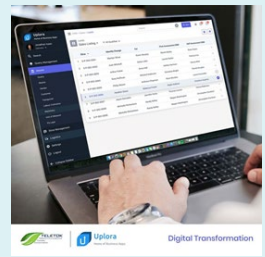


Figure 15: Tokelau – Online cyber awareness with 'Cyber Up with TELETOK'

Case Study 8: Tokelau – journey of digital transformation how TELETOK beat COVID-19

What is digital transformation?



Digital transformation is the rethinking of how organisations apply technology consistently with the fundamentals of how technology optimises spending, liberates people, improves processes and perhaps opens new revenue streams. "Transformation is not about buying and consuming point-solutions but about having a broad strategy and defining business's journeys with technology".

Why is it a journey?

It is a journey because it is not a one-time purchase but rethinking every business activity or flow, and applying technology to modernise them by leveraging new tools and processes. More specifically, in the current climate, use is made of cloud-based, secure services including digital signing, digital contracts, digital transactions and everything in between.

Why do we need digital transformation now?

It is unfortunate we are all affected directly or indirectly by COVID-19. Since COVID-19 hit, we know very well how retailers moved online, people transacted online and masses adopted remote tools like Zoom to stay connected. Some businesses rushed to use ad hoc solutions to survive. Those who did not, ended up off the map. While digital transformation started a few years ago, COVID-19 accelerated it to start now, if not before.

What is TELETOK's digital journey?

TELETOK's digital transformation journey started well before COVID-19 was here, as early as 2018. TELETOK's leadership made a very smart decision to hear the story of digital transformation, advancing into cloud adoption, doing business online, removing problems with overheads, and managing its own IT. So TELETOK actively engaged to build its business services with the Uplora team to become how TELETOK wanted to do business.

TELETOK has transformed all paper-based business activities to digital forms, including financial and people services, and this effort has liberated it from the COVID-19 lockdown pain. Since August 2021, TELETOK services have been running on the second generation Uplora platform and operating seamlessly. TELETOK staff have also been trained to use the new platform.

TELETOK pledges to serve the needs of the people of Tokelau and their customers at large with a view to further modernising all existing services in a way that they can leverage advantages of technology by reducing their IT and operational overheads, getting cloud reliability, and being a leading modern telecommunications enterprise. By embracing digital transformation, TELETOK is reducing its physical footprint, and doing its part in fighting against climate change.

Testimonial

Please listen to the audio cast with Taitai, product manager at TELETOK, covering the adoption of Uplora's digital platform.

About Uplora

Uplora is a 'cloud native no-code' platform helping businesses in their digital transformation journey. Uplora works with their clients from problem to concept to solution, using the secure digital platform. The platform also offers pre-built solutions and uses cases via their hub (aka app store). Please visit uplora.com to learn more.

Tonga

Overview

Tonga's National Computer Emergency Response Team (CERT Tonga)

Resourcing and constituency

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

CERT Tonga consists of three full-time staff, as well as volunteers to assist the team throughout our daily operations. However, one of our full-time staff, Mr Siosaia Vaipuna, who was the Director for CERT Tonga, has resigned.

Our constituents are government ministries, private sector, public enterprises, and NGOs.

Threat landscape

Cyber reporting to CERT Tonga can be made by:

- calling our Hotline number 2378
- sending a report about any cyber incident via email report@cert.gov.to or through our website https://www.cert.gov.to/

In Tonga, common types of cyber security threats include:

- phishing email and scams
- botnets
- web defacement
- Microsoft exchange vulnerabilities.

We respond mostly to:

- botnet activities
- Darknet activities
- business email compromise (BEC)
- phishing and scams.

Awareness raising

Awareness program to the outer islands, February 2021
(government, schools and district officers)

Government

Awareness program by CERT team to the Ministry of Public Enterprises

CERT Tonga's awareness program to the Ministry of MEIDECC

CERT Tonga's awareness program for the Ministry of Lands and Natural Resources

Attorney General Office staff joining the CERT Tonga Awareness program

Private Sector



CERT Tonga providing awareness program with Nishi Trading

Public Enterprise


CERT team continued its journey by providing awareness program to
Tonga Airports Limited staff

Exhibitions

CERT Tonga also joined exhibitions as part of the awareness campaign for MEIDECC.

Exhibition hosted by the Environment Department 2021

Exhibition hosted by Climate Change Department 2021

Exhibition hosted by NEMO Department 2021

Exhibition during Law Week 2021

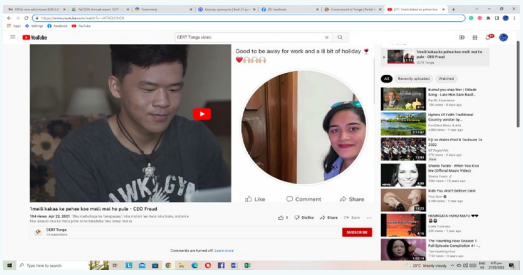
Engagement in these exhibition events strengthened our relationships with these organisations and our domestic stakeholders. We supported them, and at the same time, we made the public aware of CERT Tonga and our services.

CERT Tonga continued engagement with its stakeholders effectively and efficiently to ensure all sides achieved their purpose of overcoming the impact of malicious activities.

Having the *Electronic Communication Abuse Offence Act 2020* in place highlights the core role of CERT Tonga, especially in performing digital forensic services, and in coordinating and collaborating with the Attorney-General's Office and Tonga Police in their implementation to combat breaches of the Act.

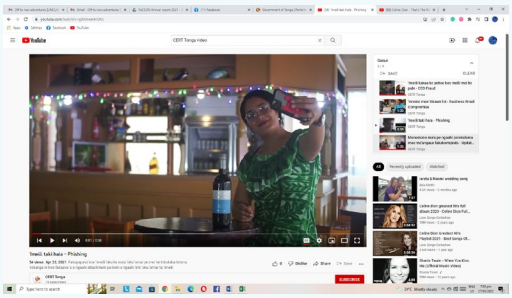
We use social media platforms such as Facebook and Twitter to share our advisories, monthly security bulletins and cyber security tips, and link them to our website. We also disseminate news on the government portal.

Four short video clips

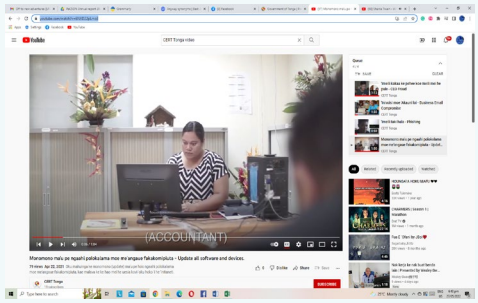


https://www.youtube.com/watch?v=vK74CUJ3tC4

https://www.youtube.com/watch?v=ffk5nr24LU4



https://www.youtube.com/watch?v=gXANwh4nUXc



https://www.youtube.com/watch?v=6NXD22pLmqE

Online resources

Monthly Security Bulletins, can be found through Facebook and Twitter both in English and local language.

- Facebook – https://www.facebook.com/CERTTonga
- Twitter – https://twitter.com/CertTonga

Advisory on Facebook and Twitter and in local language and in English

- Facebook – https://www.facebook.com/CERTTonga
- Twitter – https://twitter.com/CertTonga

Cyber security tips and in local language and in English

- Facebook – https://www.facebook.com/CERTTonga
- Twitter – https://twitter.com/CertTonga

Case Study 9: Tonga – BEC, phishing and Botnet

CERT Tonga has not seen much of an increase in cyber attacks in-country, as most of incidents have been BEC, phishing and botnet activities. CERT Tonga has issued advisories for our people and organisations to be aware of such misinformation and cyber attacks.

Tuvalu

Overview

Department of Information and Communications Technology (ICT)

Resourcing and constituency

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

The current organisational structure for the Ministry of Justice, Communications, and Foreign Affairs includes:

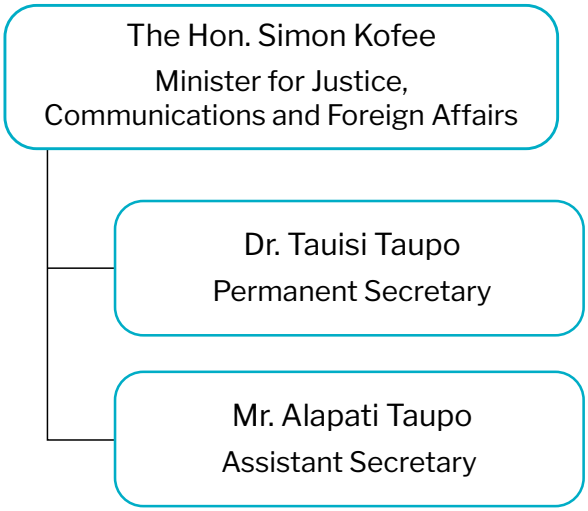


Figure 16: Tuvalu – Ministry of Justice, Communications, and Foreign Affairs organisation structure

The Department of ICT supports the Tuvalu Government's IT services. As its primary constituency, the Department of ICT provides support to all government departments and offers support to the private sector in capacity building, and cyber safety for schools and the general public. In Tuvalu, cyber incidents can be reported to the police, the Department of ICT or even the Office of the Peoples' Lawyer, who is the major legal aid service for the general public.

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. The newly launched GetSafeOnline website in Tuvalu is a huge boost for Tuvaluans, especially with translations in the local language.

The Department of ICT uses its social media accounts as a platform to share cyber security and cyber safety updates.

The Department of ICT shares Security Advisories from PaCSON partners, like Tonga CERT, Vanuatu CERT, NZ CERT and CISA, on various social media outlets like government Facebook pages and Tuvalu news pages.

Case Study 10: Tuvalu – Cybersecurity Capacity Review

Our efforts to improve and increase our cyber resilience and capacities are continual. In 2021, the Department of ICT had the privilege of working with the Oceanic Cyber Security Centre (OCSC) on a Cybersecurity Capacity Review.

Similar to many countries in the world, due to COVID-19, Tuvalu experienced an ever-increasing need for equitable access to technologies within a safer and more secure digital environment that protected citizens' rights, their information, and the national infrastructure.

In Tuvalu, the Ministry of Justice, Communications, and Foreign Affairs has a vision for Tuvalu to actively participate in the global digital economy, not just consuming content but also creating it in the form of digital goods and services. Demonstrating the commitment to this vision, the Ministry has joined more than 80 countries across the world to prioritise understanding of where they are now on the digital resilience journey by undertaking the first ever remote Cyber Security Capacity Maturity Model for Nations (CMM) Review in the Pacific. Due to travel restrictions relating to COVID-19, this was the first time that OCSC conducted a review remotely.

The CMM review was conducted by OCSC over four days, involving discussions with more than 30 decision-makers and technical personnel from the emergency response, criminal justice and law enforcement, education and civil society, critical infrastructure, government, and parliamentarians.

Temporary technical issues with the Australian internet connection aside, the review went smoothly. The unique approach for the review enabled Tuvalu to conduct the assessment at least 12 months earlier than expected, while continuing to experience the benefits of informal face-to-face discussions with friends and colleagues away from the office.

Vanuatu

Overview

Cyber Security Response Team Vanuatu (CERTVU)

Resourcing and Constituency

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

Being the national cyber security and IR responder, CERTVU's constituency covers the government sector, private sector, NGOs and civil society.

People can report cyber incidents to us through the following methods:

- phone: +678 33380
- email: incident@cert.gov.vu
- web portal – https://cert.gov.vu/index.php/services/incident-resolution
- social media platform – https://www.facebook.com/CERTVU/
- through our assisting partners.

Threat landscape

- phishing
- business email compromise
- malware attack
- ransomware attack
- disinformation and misinformation issues.

CERTVU responded to all cyber-related incidents that are reported by our constituents using the reporting means provided above. We responded to all forms of cyber threats and attacks, including phishing attacks, malware attacks, ransomware attacks, and misinformation and disinformation incidents.

During the reporting period, we responded to 360 reported incidents.

Awareness raising

Our yearly awareness raising program involves the following:

- radio talkback shows
- social media platform awareness programs
- open air awareness talks
- flyers and brochures dissemination
- one-to-one awareness sessions with organisations
- video clips awareness
- music (cyber security songs)
- quizzes and games awareness programs through an open, outdoor mobile lab platform
- regular rural community awareness initiatives
- schools educational awareness talks
- published press releases on the mass defacement of the Vanuatu Government websites
- republished Cyber Smart Pacific Week 2021 news
- published advisories on different cyber threats.

Case Study 11: Vanuatu – ELBIE ransomware

In the week leading up to Christmas Eve of 2021 and early January 2022, we received a report of a cyber incident from a business house in town, which involved a ransomware attack.

The CERTVU team mobilised and activated its IR plan and procedure and reached out to the organisation for further investigation to confirm the type of attack. It was related to ELBIE ransomware, which at that time was also affecting other parts of the world.

The CERTVU team identified the point of compromise from the RDP port which was allowed from the host server. This was the loophole for the attacker to launch its attack, encrypting the main Point of Sale data system and its backups.

As a result of the investigation, the CERTVU IR team helped the organisation recover most, but not all, of its sales data from its other alternative backups. Further advice was given to the organisation IT team to recover other data from its old offline data backups stored offsite.

Such attacks have greater impact on organisations and are associated with financial setbacks; hence, doing regular backups and ensuring a backup of backups, is best practice cyber hygiene, otherwise there is not always a 100 per cent guarantee of recovering data from any ransomware attacks.

We require various security measures to protect critical company or organisation data.

Partner Updates

Cybersecurity and Infrastructure Security Agency

Overview

Cybersecurity and Infrastructure Security Agency (CISA), within the US Department of Homeland Security

Resourcing and constituency

CISA is organised into six divisions.

Cybersecurity Division (CSD)

CSD is responsible for CISA's cyber security mission to defend and secure domestic cyberspace, lead efforts to protect the federal '.gov' domain of civilian government networks, and collaborate with the private sector to increase the security of critical networks. CSD executes its mission through collaborative, proactive risk reduction and by working with partners to continually prioritise the most significant risks and address them before harm occurs. CSD conducts operations to actively defend cyberspace and help the nation respond to significant incidents, build resilience by addressing systemic risk, help organisations operate safely and reliably even when being targeted by adversary activity, and set the conditions that contribute to the vitality and health of the cyber ecosystem. CSD also provides a wealth of cyber security resources to help stakeholders identify and protect their critical assets, detect threats and vulnerabilities, and, when necessary, respond to and recover from cyber events.

Emergency Communications Division (ECD)

The ECD was established in 2007 in response to communications challenges faced during the attacks on September 11, 2001, and Hurricane Katrina in 2005. ECD supports and promotes communications used by emergency responders and federal, state, local, tribal, and territorial (FSLTT) government officials to keep America safe, secure, and resilient. ECD leads the nation's operable and interoperable communications efforts used for public safety, as well as national security and emergency preparedness (NS/EP). It also provides training, coordination, tools, and guidance to help FSLTT and industry partners develop their emergency communications capabilities. ECD's programs and services coordinate emergency communications planning, preparation, and evaluation to ensure safer, better-prepared communities nationwide.

Infrastructure Security Division (ISD)

The ISD leads CISA's infrastructure security mission. ISD conducts cyber and physical exercises with FSLTT, private sector, and international partners to enhance the security and resilience of critical infrastructure. These exercises provide partners with effective and practical mechanisms to examine plans and procedures, identify areas for improvement, and share best practices. These exercises also inform future planning, technical assistance, training, and education efforts. CISA offers a suite of free exercise services, resources, and materials. ISD also conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and FSLTT partners understand and address risks to critical infrastructure. ISD also provides information on emerging threats and hazards, such as unmanned aircraft systems and cyber security and physical convergence, so that appropriate actions can be taken to reduce risks.

Among other critical infrastructure security and resilience programs and services, ISD also facilitates vulnerability and consequence assessments, and provides tools and training to help partners in government and industry manage the risks to their assets, systems, and networks.

Integrated Operations Division (IOD)

The IOD provides a national capability to deliver CISA services to stakeholders and partners across state and local governments and the critical infrastructure community. Via CISA's ten regional offices around the US, IOD delivers cyber and physical vulnerability assessments, architecture reviews and design, subject matter expertise, IR support, exercise planning and support, National Special Security Event planning and support, and chemical facility inspections and site security planning for Chemical Facility Anti-Terrorism Standards implementation.

Stakeholder Engagement Division (SED)

SED develops partnerships, facilitates dialogue, convenes stakeholders, and promotes awareness to help CISA achieve a secure and resilient infrastructure for the American people. SED coordinates stakeholder engagements and partnerships to support the agency's efforts to reduce national risk. SED focuses on three lines of effort: strategic partnerships, stakeholder engagement strategy, and stakeholder relationship management.

National Risk Management Center (NRMC)

The NRMC is a planning, analysis, and collaboration center within CISA, leading risk reduction efforts and working to identify and address the most significant risks to our nation's critical infrastructure. Guiding the NRMC's risk management efforts are the National Critical Functions (NCF)—the functions of government and the private sector that are so vital to the US that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety. NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to identify, analyse, prioritise, and manage these risks to help advance our nation's collective defense.

CISA leads the US national effort in understanding, managing, and reducing risks to our cyber and physical infrastructure. We connect our stakeholders in industry and government with each other as well as with resources, analysis, and tools to help them build their own cyber, communications, and physical security and resilience. This in turn helps to ensure a secure and resilient infrastructure for the American people.

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

SED's CISA International is committed to collaborating with our international partners to strengthen the security of our global digital infrastructure. In recognition of the importance of international partnerships, we launched our first international strategy in 2020. CISA Global outlines how CISA will work with international partners to fulfill our responsibilities, execute our work, and create unity of effort within our mission areas. The strategy details CISA's international vision and commits the agency to four goals:

1. advancing operational cooperation
2. building partner capacity
3. strengthening collaboration through stakeholder engagement and outreach
4. shaping the global policy ecosystem.

CISA is committed to promoting an open, interoperable, reliable and secure interconnected world within a global, operational and policy environment where network defenders and risk managers can collectively prevent and mitigate threats to critical infrastructure.

Threat landscape

Common cyber threats include:

- ransomware
- supply chain compromises
- phishing.

Awareness raising

CISA provides robust, publicly-accessible communications daily, weekly, and as needed operationally, to keep stakeholders up to date with timely and actionable information. CISA products are tailored for network defenders, C-suite level executives, and the general public, as appropriate, to ensure all stakeholder sets have information relevant to them. Most recently, we have shared critical, technical guidance and protective measures related to Russian threat actors, ransomware threats, destructive malware, and DDoS attacks across the entire cyber security community and all critical infrastructure sectors. Key product types are summarised below.

Current Activities: short, real-time communications drafted and published immediately with high-level, actionable information on observed high-impact security activity affecting the community at large. Multiple notifications of patch releases for significant vulnerabilities may be published daily.

Cybersecurity Advisories (CSAs): in-depth analysis of new or evolving cyber threats that include cyber security threat information, best practices and actionable mitigation recommendations for network defenders. CSAs provide indicators of compromise and tactics, techniques, and procedures when available. Data and information reflect consolidated cyber data, insights, and analysis from CISA's public-private sector partners and international partners.

Industrial Control Systems (ICS): timely and relevant information on cyber security vulnerabilities and threats with the potential to impact ICS and critical infrastructure computing networks. ICS CSA's provide ICS security best practices and mitigations for cyber security network defenders to action. Data and information reflect consolidated cyber data, insights, and analysis to reduce risks within and across all critical infrastructure sectors, and provide control systems-related security mitigation recommendations from CISA's public-private sector, international partners, and vendors.

ICS Medical Advisories (ICSMAs): timely and relevant information on cyber security vulnerabilities and threats related to ICS healthcare IT systems and medical devices. This includes notification of patch releases and proposed mitigation strategies associated with vulnerabilities in the medical device ecosystem.

Vulnerability Bulletins: weekly summaries of new vulnerabilities that do not pose immediate risk to systems but are significant enough that non-compliance with suggested actions and mitigation guidance may pose risk to your network.

Alerts: timely information about current security issues, vulnerabilities, and exploits.

Tips: describe and offer advice about common security issues for non-technical computer users.

Analysis Reports: provide in-depth analysis on a new or evolving cyber threat.

CISA often creates dedicated web pages for critical, ongoing activity in order to establish easy-to-access, one-stop resources for all related information. CISA continues to update these web pages in real-time with CISA products and partner resources. Examples include:

- **CISA.gov/Shields-Up**

  To help stakeholders protect their most critical assets ahead of Russia's invasion of Ukraine, CISA launched the Shields Up campaign on CISA.gov with current and regularly updated guidance to help organisations of every size adopt a stronger cyber security posture. The webpage includes steps organisations can take, free cyber security resources available to critical infrastructure partners, and guidance on how organisations can prepare themselves to mitigate the impact of potential foreign influence operations and mis-, dis-, and mal-information. Shields Up provides concrete actions for CISA's broad range of stakeholders, to include guidance for all organisations, recommendations for corporate leaders and CEOs, steps individuals can take to protect themselves and their families, ransomware response, and additional resources. This information is intended to be a high-level roadmap to help stakeholders heighten their cyber security posture and prepare for disruptive cyber incidents.

- **StopRansomware.gov**

  A one-stop resource where public and private sector entities can find US government tools, information, and resources that can help site visitors reduce their risk of ransomware attacks and improve resilience. This website is a coordinated initiative across the federal government, pooling publicly available federal resources into one location to help organisations better find the information they want on ransomware. The website includes tools and resources from the Department of Homeland Security—CISA and Secret Service—as well as from the FBI, Department of Commerce's National Institute of Standards and Technology, the Department of the Treasury and the Department of Health and Human Services. CISA led the design, development, and launch of the new website and continues to work collaboratively with federal partners to add more resources to the website.

- **Known Exploited Vulnerabilities Catalogue**

  A living catalogue of exploited vulnerabilities that carry significant risk to the US federal enterprise. Though required remediation deadlines are for US federal executive civilian branch agencies only, CISA strongly recommends all organisations monitor and remediate newly listed vulnerabilities to increase resilience.

CISA also recommends reviewing the *National Emergency Communications Plan, Goal 6: Cybersecurity: Strengthen the cybersecurity posture of the Emergency Communications Ecosystem*, which provides guidance on the nation's strategy to strengthen the cyber security posture of the emergency communications ecosystem. SAFECOM provides technology tools for practitioners that support communications and cyber resilience that can be referenced as a great public resource. These resources can be found at: https://www.cisa.gov/safecom/technology

Our first international strategy, CISA Global, published in February 2021, describes CISA's international vision and outlines our approach for working with international partners to fulfill our responsibilities, execute our work, and create unity of effort within our mission areas. If you are interested in learning more, please email us at CISAInternationalAffairs@hq.dhs.gov

About the agency:

- https://www.cisa.gov/
- https://www.cisa.gov/about-cisa

Mailing lists:

- https://www.cisa.gov/subscribe-updates-cisa
- https://www.cisa.gov/uscert/mailing-lists-and-feeds
- https://www.cisa.gov/social-media-directory
- https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RED

Reserve Bank of Fiji

Overview

The Reserve Bank of Fiji (RBF)

Resourcing and Constituency

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

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

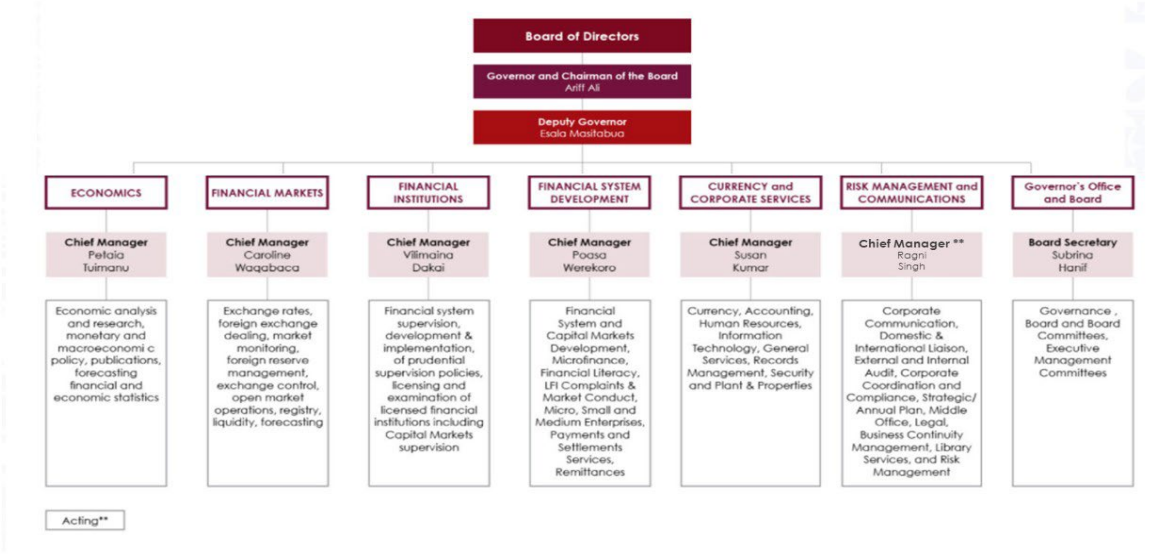


Figure 17 – The Reserve Bank of Fiji organisation structure

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

Threat landscape

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

- business email compromise attacks
- whaling attacks
- spear phishing attacks
- port scanning attacks
- malware
- ransomware threats
- Emotet malware attacks.

Awareness raising

The RBF contributes awareness raising efforts to:

- financial institutions
- prudential standards
- cyber security.

Working Groups

Awareness Raising

Since the establishment of PaCSON in 2017, the PaCSON ARWG serves the primary objective of acting on behalf of the PaCSON Community and taking the lead on the following key initiatives:

- increasing cyber security awareness in all PaCSON member nationalities
- increasing regional collaboration among Pacific Island Countries for the purpose of security information-sharing
- increasing awareness and collaboration with international partners with the aim to combating cross-border and transnational cybercrime activities
- working effectively with the PaCSON Secretariat, PaCSON CBWG and the PaCSON Communication Working Group on PaCSON operations.

The aims translated through the above initiatives are also supported by the outlined Working Group Terms of Reference.

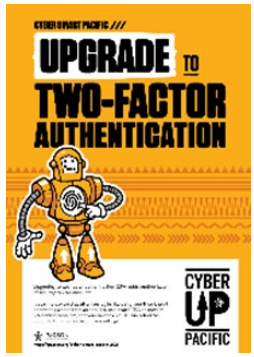
The ARWG is responsible for raising awareness on behalf of the PaCSON Community. The purpose of the ARWG is to advocate the PaCSON Vision and Mission on behalf of the Community.

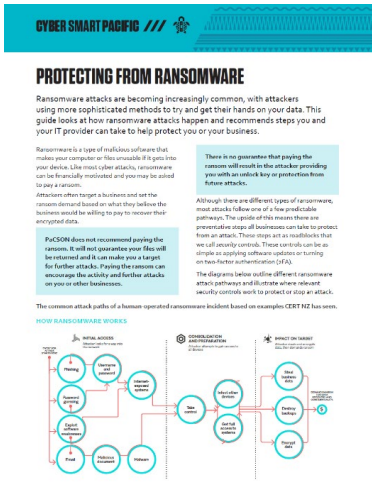
2021 Awareness Raising Working Group activities

During the reporting period, the ARWG successfully launched the second PaCSON awareness raising campaign – the Cyber Smart Pacific campaign (https://pacson.org/cyber-smart-pacific). Held throughout October 2021, as part of National Cyber Security Awareness Month, the Cyber Smart Pacific Campaign centred on four simple, yet impactful actions, which were designed to improve the individual user's cyber security. These actions capitalised on visual infographics due to their ability to translate critical and useful knowledge, and thus relate to all targeted audiences regardless of their level of cyber literacy and capability. The campaigns four key messages were:

1. Upsize your passwords
2. Upgrade to two-factor authentication
3. Update your apps and devices
4. Uphold your privacy.

In 2021, the campaign centred on the theme 'Cyber Up with PaCSON', with the campaign tag line being 'Cyber security threats are on the rise, so let's Up our digital safety and security'. Continuing the support from CERT NZ, the 2021 campaign developed mascots and promotional material that assisted PaCSON members to educate and raise the awareness in their local community.




CYBER SMART PACIFIC ///

PROTECTING FROM RANSOMWARE

Ransomware attacks are becoming increasingly common, with attackers using more sophisticated methods to try and get their hands on your data. This guide looks at how ransomware attacks happen and recommends steps you and your IT provider can take to help protect you or your business.

Ransomware is a type of malicious software that makes your computer or files unusable if it gets into your device. Like most cyber attacks, ransomware can be financially motivated and you may be asked to pay a ransom.

Attackers often target a business and set the ransom demand based on what they believe the business would be willing to pay to recover their encrypted data.

PaCSON does not recommend paying the ransom. It will not guarantee your files will be returned and it can make you a target for further attacks. Paying the ransom can encourage the activity and further attacks on you or other businesses.

There is no guarantee that paying the ransom will result in the attacker providing you with an unlock key or protection from future attacks.

Although there are different types of ransomware, most attacks follow one of a few predictable pathways. The upside of this means there are preventative steps all businesses can take to protect from an attack. These steps act as roadblocks that we call security controls. These controls can be as simple as applying software updates or turning on two-factor authentication (2FA).

The diagrams below outline different ransomware attack pathways and illustrate where relevant security controls work to protect or stop an attack.

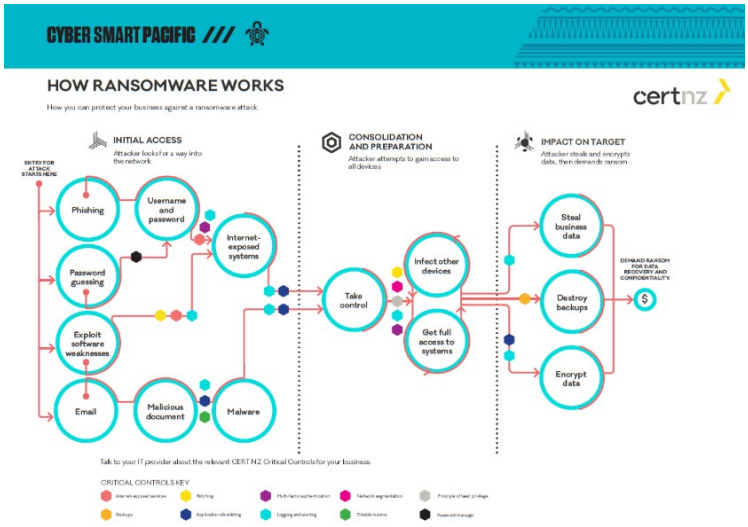
The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.

HOW RANSOMWARE WORKS

Accompanying the 2021 Cyber Smart Pacific Campaign, the ARWG published the first ever PaCSON Guide. Covering the challenge of ransomware, this guide outlined different ransomware attack pathways and illustrated where relevant security controls work to protect or stop an attack. Paired with advice and tips on how to manage and prevent ransomware attacks, this first guide aims to set up a tradition of releasing informative and actionable cyber security advice to the Pacific community.

We are now preparing and looking forward to another successful 'Cyber Smart Pacific Campaign – 2022'.

#PACSON #PaCSONARWG #CYBERSMARTPACIFIC



Capacity Building

The goal of the 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.

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

2021 Capacity Building Working Group activities

In 2021, the CBWG focused on better understanding members' local needs and contexts, strengthening operational partnerships, and delivering the flagship Remote Session Series.

The **Remote Session Series** was established in June 2020 as a way for the community to stay engaged in the face of COVID-19 challenges. It has since developed into a regular monthly opportunity for the community to connect. The series, organised by CERT NZ, covers a wide range of topics, including technical workshops, awareness raising sessions, as well as sharing case studies and good practice. In 2021, the CBWG hosted nine workshops for 218 participants from 18 economies.

Operational Partnerships remain a mainstay of the working group's efforts. The success of the program has come from the willingness of PaCSON members and partners to share insights and operational experiences directly. In 2021, the CBWG continued to grow its informal collaboration with **Cyber Safety Pasifika** (CSP) and **Pacific Islands Law Officer's Network** (PILON) to invite members of each their networks to relevant remote sessions and share their expertise, promote better coordination, and bring more communities together.

CBWG Membership

- Australia
- Cook Islands
- Fiji
- Nauru
- New Zealand
  Working Group Convener
- PNG
- Solomon Islands
- Tonga
- Vanuatu

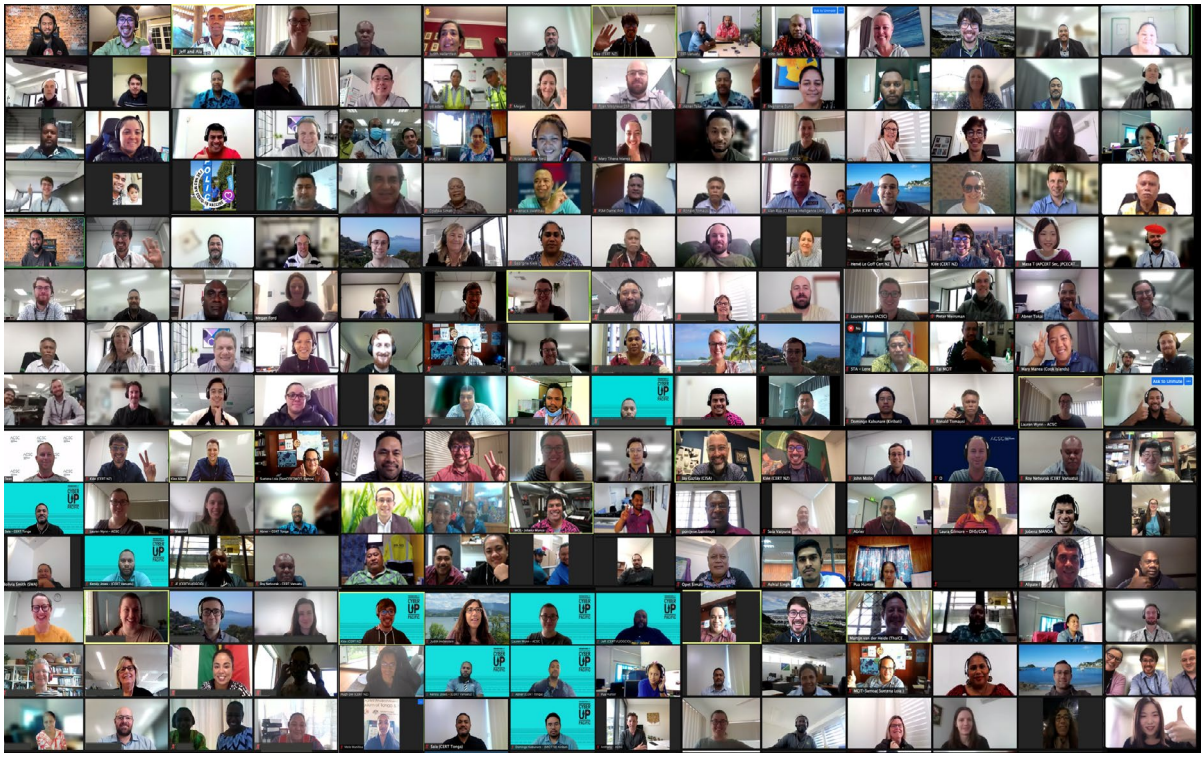


Figure 18: PaCSON Remote Session Series participant's group photo collage

The CBWG also enhanced its partnership with the **ASIA Pacific Computer Emergency Response Team** (APCERT), building connections between the wider Asia-Pacific and PaCSON incident response communities. This included a remote session featuring ThaiCERT in April 2021.

For the CBWG to better serve the needs of PaCSON and the Pacific cyber community, an understanding of members' **local needs and contexts** is critical. The CBWG has worked to build this understanding through regular formal and informal engagements, as well as through regular one-on-one member updates delivered through the PaCSON Secretariat.

In 2021, PaCSON and individual members closely collaborated with the **Global Forum on Cyber Expertise** (GFCE), resulting in PaCSON accessing GFCE capacity building engagements and gaining the opportunity to feed into the development of the upcoming GFCE Pacific Hub.

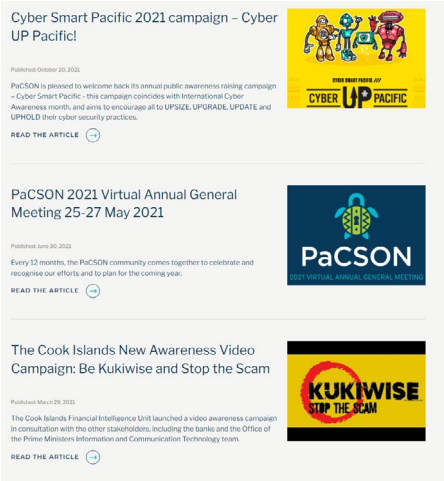
The CBWG appreciates the support and engagement from the whole PaCSON membership and our regional and global partners. We are excited to deliver another ambitious year of work together in 2022.

Communications

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

2021 Communications Working Group activities

During 2021, the major deliverable for the Communications Working Group was the publication of the first ever PaCSON Annual Report. The PaCSON 2020 Annual Report is a unique firsthand account from our PaCSON members and partners detailing how cyber security is managed in their home countries and how it affects the businesses and lives of their communities.



The Working Group continued to sustain pacson.org and is pleased to have published four new news articles throughout 2021. The function of these news articles is to publicise the work of PaCSON, and they double as a method of amplification of key cyber security initiatives by our members and partners.

During 2021, pacson.org 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. Viewership during the reporting period was steady with a high number of visitors discovering pacson.org through organic searches.

The Working Group was pleased to be able to continue supporting the ARWG and CBWG throughout 2021, and looks forward to continuing our collaboration in 2022.

Partners

The PaCSON Partners Working Group (PPWG) is the newest PaCSON working group. The PPWG has been established with the aim of providing opportunities to support and collaborate with the PaCSON primary working groups (ARWG, CBWG and Communications WG) on their planned activities.

The PPWG looks forward to supporting the PaCSON Community to deliver against its mission of working together across the Pacific to cooperatively 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.

2021 PaCSON Partners Working Group activities

Our major contribution to PaCSON in 2021 was the delivery of a session at the PaCSON 2021 Virtual Annual General Meeting, which explored cloud-based solutions and provided PaCSON members with an understanding of common challenges as well as practical hints and tips to help overcome common barriers.

The PPWG looks forward to expanding our partnerships and continuing to support PaCSON in 2022 with more capacity building opportunities, and through face-to-face engagements.

Future Plans – 2022

In 2022, PaCSON will remain flexible and responsive to the needs and wants of our PaCSON Community. As we continue to manage the unprecedented impact of COVID-19, PaCSON looks forward to returning to in-person engagements – albeit socially distanced.

Our PaCSON Community may continue to experience an increasing pace and frequency of cyber security events, but will continue to support each other and improve our regional cyber security capabilities and readiness through cooperation and collaboration.

More than ever, cyber security continues to be a shared responsibility, a responsibility which PaCSON is answering through our committed and coordinating activities which benefit the Pacific regions' cyber security posture. Maintaining an awareness of the risks and threats which impact the Pacific region, PaCSON is assisting our governments, businesses and constituents to remain safe and prepared against cyber events.

Success in 2022 looks like it will consist of:

- building the PaCSON brand as a trusted partner and source of truth among cyber security IR professionals
- deepening our existing stakeholder relationships and discovering new relationships
- strengthening the resilience of the Pacific region's cyber security posture by welcoming new members and partners
- delivering a contextualised and tailored 2022 Cyber Smart Pacific Campaign that addresses the needs and wants of our PaCSON Community and their constituents
- continuing to build relationships, conduct engagements and offer training opportunities which reflect the small-island context of the Pacific
- continuing to deliver specialist and tailored activities that help boost the cyber security posture of the Pacific region.

Acnkowledgements

PaCSON acknowledges the valuable contributions made by all of our supporting partners. The PaCSON Community is very grateful for the advice, contributions and support of all the government organisations, not-for-profit organisations, private enterprises and academic bodies who work with our network.This report and the activities of PaCSON are made possible thanks to the support and advice of many individuals and organisations. The PaCSON Executive Committee, on behalf of the entire PaCSON Community, would like to thank everyone who contributed to PaCSON in 2020, with special thanks to the following:

ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM (APCERT)

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

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

To learn more, please visit APCERT.

ASIA PACIFIC NETWORK INFORMATION CENTRE (APNIC)

APNIC is an open, member-based, not-for-profit 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 for the internet to operate and grow. As part of this service, APNIC is responsible for maintaining the public APNIC Whois Database and managing reverse DNS zone delegations. APNIC also provides forums for internet policy development that are bottom-up and open to everyone.

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

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

To learn more, please visit APNIC.

CYBER SAFETY PASIFIKA (CSP)

CSP is a program led by the Australian Federal Police and is aimed at increasing the cyber safety awareness and education of vulnerable communities in the Pacific region. It is also aimed at upskilling Pacific police officers in cybercrime investigations.

To learn more, please visit Cyber Safety Pasifika.

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE (DFAT)

Australia's Cyber and Critical Tech Cooperation Program (CCTCP) works in partnership with countries in Southeast Asia and the Pacific to enhance cyber resilience. Established in 2016, the CCTCP plays an important role in supporting Australia's international cyber engagement, championing 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 delivering on the United Nations 2030 Agenda for Sustainable Development, which recognises the vital role of digital technologies to achieving a better and more sustainable future for all.

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

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

PACIFIC ISLANDS LAW OFFICERS NETWORK (PILON)

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

To learn more, please visit PILON.

Glossary

ACSC	Australian Cyber Security Centre (AUS)
ADSL	asymmetric digital subscriber line
APCERT	Asia Pacific Computer Emergency Response Team
APNIC	Asia Pacific Network Information Centre
ASD	Australian Signals Directorate (AUS)
AWRG	Awareness Raising Working Group (PaCSON)
BEC	business email compromise
CALD	culturally and linguistically diverse
CBWG	Capacity Building Working Group (PaCSON)
CCTCP	Cyber and Critical Tech Cooperation Program (AUS)
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERT NZ	Computer Emergency Response Team New Zealand (NZL)
CERT Tonga	Tonga's Computer Emergency Response Team (TON)
CERTVU	Computer Emergency Response Team Vanuatu (VUT)
CISA	Cybersecurity Infrastructure & Security Agency (USA)
CMM	Cyber Security Capacity Maturity Model for Nations
CSA	Cybersecurity Advisories (USA)
CSD	Corporate Services Department (PNG)
CSD	Cyber Security Division (USA)
CSIRT	Computer Security Incident Response Team
CSP	Cyber Safety Pasifika
DDoS	Distributed Denial-of-Service
DFAT	Department of Foreign Affairs and Trade (AUS)
DGTO	Digital Government Transformation Office (FJI)

DICT	Department of Information and Communications Technology (PNG)
DTO	Digital Transformation Office (KIR)
EC	Executive Committee
ECD	Emergency Communications Division (CISA, USA)
ECIA	Economics, Consumer and International Affairs (PNG)
ERPD	Engineering & Resource Planning Department (PNG)
FICAC	Fiji Independent Commission Against Corruption (FJI)
FIU	Fiji Financial Intelligence Unit (FJI)
FSC	Financial Supervisory Commission (COK)
FSLTT	federal, state, local, tribal, and territorial
FTA	file transfer appliance
GFCE	Global Forum on Cyber Expertise
ICS	industrial control systems
ICSMAs	ICS Medical Advisories (USA)
ICT	information and communications technology
ICT-TWG	ICT Technical Working Group for Government (WSM)
IOD	Integrated Operations Division (USA)
IR	incidence response
ISD	Infrastructure Security Division (USA)
IT	information technology
ITCS	Department of Information Technology and Computing Services (FJI)
LED	Licensing & Enforcement Department (PNG)
LTE	long-term evolution
MCIT	Ministry of Communications and Information Technology (WSM)
MEIDECC	Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Communications and Climate Change (TON)
MICT	Ministry of Information, Communications and Transport (KIR)
MIPD	Marshall Islands Police Department (MHL)
MSAN	multi-service access node
NCF	National Critical Functions (USA)
NCSC	National Cyber Security Centre (PNG)

NGO	non-government organisation
NICTA	National Information and Communications Technology Authority (PNG)
NRMC	National Risk Management Center (USA)
NS/EP	national security and emergency preparedness
OCS	Online Charging System (TKL)
OCSC	Oceanic Cyber Security Centre
OGCIO	Office of the Government Chief Information Officer (VUT)
OPM ICT	ICT Division within the Office of the Prime Minister (COK)
OSC	Online Safety Commission (FJI)
PaCSON	Pacific Cyber Security Operational Network
PANGTEL	Papua New Guinea Telecommunication Authority (PNG)
PILON	Pacific Islands Law Officer's Network
PMU	Project Management Unit (COK)
PNGCERT	Papua New Guinea Computer Emergency Response Team (PNG)
POTS	plain old telephone service
PPWG	Partners Working Group (PaCSON)
PSTN	public switched telephone network
RBF	The Reserve Bank of Fiji (FJI)
Sam CERT	Samoa Computer Emergency Response Team (WSM)
SED	Stakeholder Engagement Division (USA)
SIEM	Security Information and Event Management
SIG	Solomon Islands Government
SIG ICTS	Solomon Islands Government Information Communication Technology Services (SLB)
SITA	Samoa Information Technology Association (WSM)
SMMD	Social Media Management Desk (PNG)
SMPP	Samoa Ministry of Police and Prisons (WSM)
SQL	Samoa Qualification Agencies (WSM)
SWOT	Strengths, Weaknesses, Opportunities, and Threats analysis
Teletok	Telecommunication Tokelau Corporation (TKL)
UAS	Universal Access Scheme Secretariat (PNG)

Disclaimer

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


PaCSON
PACIFIC CYBER SECURITY OPERATIONAL NETWORK
pacson.org