isif asia

Project factsheet information

Project title	Developing *cert*Tonga
Grant recipient	2nd Floor O.G.Sanft Building Corner of Wellington and Taufaáhau Roads Nukuálofa Kingdom of Tonga Tel: +676 7729000- Fax: +676 24861 Website: www.cert.to
Dates covered by this report	01 – 10 – 2016 / 23 – 11 - 2017
Report submission date	24 – 11 – 2017
Country where project was implemented	Tonga
Project leader name	Sosaia Vaipuna svaipuna@mic.gov.to
Team members (list)	Andrew Toimoana atoimoana@mic.gov.to (Initial Interim Project Leader) Paula Latapu platapu@mic.gov.to Abner Tokai ‘Otukolo atokai@mic.gov.to
Partner organizations	• International Partnerships APNIC, Australia DFAT, CERT Australia, CERT NZ, Council of Europe through the GLACY and GLACY+ Project, Mauritius CERT, Sri Lanka CERT, ShadowServer Foundation, Thailand CERT, Waikato University (NZ) • Local Partnerships Attorney General’s Office, Digicel, Tonga Police, Tonga Cable Ltd., Tonga Communications Corporation (TCC)
Total budget approved	AUD 56,000.00
Project summary	On 16th July 2016, the Tonga Government Cabinet established the Tonga’s National Computer Emergency Response Team (*cert.to*) The mandate of *cert.to* includes: • Serve as the Kingdom of Tonga’s national point of contact for cyber security issues • Collaborate with the regional and international CERTs • Issuance of security warnings and alerts • Provide security awareness campaigns • Conduct an annual cyber security threat survey • Digital evidence handling The project is primarily to assist in the setting up of Tonga CERT’s capacity and capability to undertake its mandated function.

Table of Contents

Background and Justification

In August 2013, the submarine cable connecting Tonga to the Internet was commissioned. Prior to the submarine cable, satellite communication was used.

In light of the new faster and foreseeable cheaper Internet connectivity, the Government of Tonga anticipated that alongside the social and economic benefit this will bring there will be some challenges. As such, in December of the same year the Government Cabinet established the Cyber Challenges Task Force to provide a coordinated approach to technology issues in Tonga.

The Task Force is a multi-stakeholder committee chaired by the Minister responsible for Communications (currently the Deputy Prime Minister, Hon. Siaosi Sovaleni) and membership are from Government Ministries, Public Enterprises, Private Sector and NGOs. The Task Force's terms of reference included establishing a national CERT to protect the government, private businesses, and the public.

In the same year, Tonga was invited so sign the Budapest Convention on Cyber Crime. Tonga took part in various capacity building initiatives provided by the Council of Europe aimed at building capacity and capability in order to meet the requirements to be a party to the Convention. This included study tours to National CERTs from various countries including Sri Lanka CERT and Mauritius CERT.

In May 2016, APNIC conducted two thematic workshops in Tonga:

1. High level officials (Board Members, CEOs of Telcos and Stakeholders chaired by the Deputy Prime Minister) on CERT Governance; and
2. ICT practitioners on Operations.

The outcome of the workshops was that both high level officials and technical team had a certain degree of confidence on how a Tonga CERT might look like.

In July 2016, Tonga's CERT (the first national CERT in the Pacific Islands) was officially established. The CERT Board was also established with memberships from the following organisations:

- Ministry responsible for Communication
- Attorney General's Office
- Tonga Cable Ltd
- Tonga's only two (2) ISPs
- Tonga Chamber of Commerce
- National Reserve Bank of Tonga
- Tonga Civil Society
- Tonga Police

The Government of Tonga and CERT Stakeholders contributed to the setting up of the CERT by providing office space, equipment and staffing.

The Government of Tonga further applied for the ISIF Asia Cybersecurity Grant to assist in the development of *certTonga*.

Project Narrative

As mentioned above, Tonga commissioned its submarine fiber optic cable in August 2013. This connected the main island of the isolated group of islands to the super information highway via Fiji. This was a major improvement from using satellite connection.

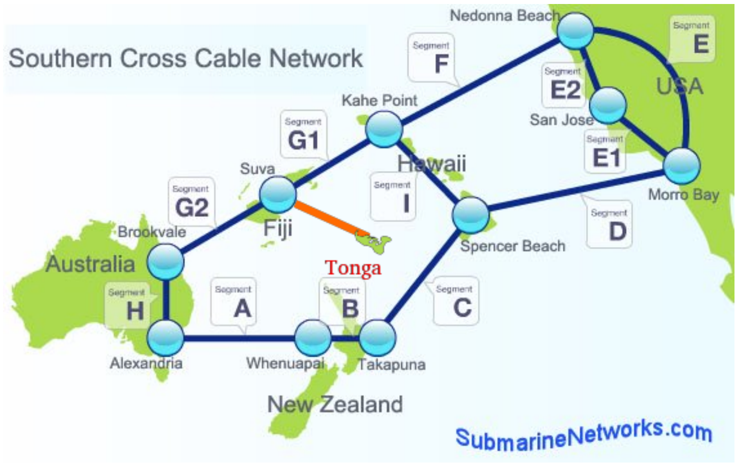


Figure 1 Cable Network

The Government realised that along with the opportunities for social and economic development, there would be challenges that the people of Tonga will face. As such, Government established the Cyber Challenges Taskforce and one of its mandates was to establish a CERT.

In July 2016, the Government of Tonga established Tonga's National CERT including a Board to provide oversight and a Terms of Reference with the vision:

"A safe and secure digital environment for the Kingdom of Tonga and its citizens"

The Government of Tonga as well as the organisations who sits on the board provided various resources including, staffing, office space and equipment. However, there were gaps in equipment and resources for capacity building in which the ISIF Asia Cybersecurity grant was sought to fill.

Project Objectives

The objective of the project was to assist *certTonga* build capacity and capability to undertake its mandated functions. The original objectives in accordance with the grant application were as follows:

- To be a national focal point to coordinating incident handling activities
- Analyzing and synthesizing incident and vulnerability information disseminated by other national CERT, vendors and technology experts to provide an assessment for Tonga.
- Facilitating communications across a diverse constituency – bringing together multiple local sectors to share information and address computer security problem.
- Developing mechanism for trusted communication

As the project progressed it was realized that the above objectives did not fully reflect the mandated scope of activities that *certTonga* was mandated with. Four (4) months into the project *CertTonga*'s strategic plan and activities were reviewed to be more aligned with its vision and mission. The below depicts the results map that *certTonga* was to operate under:

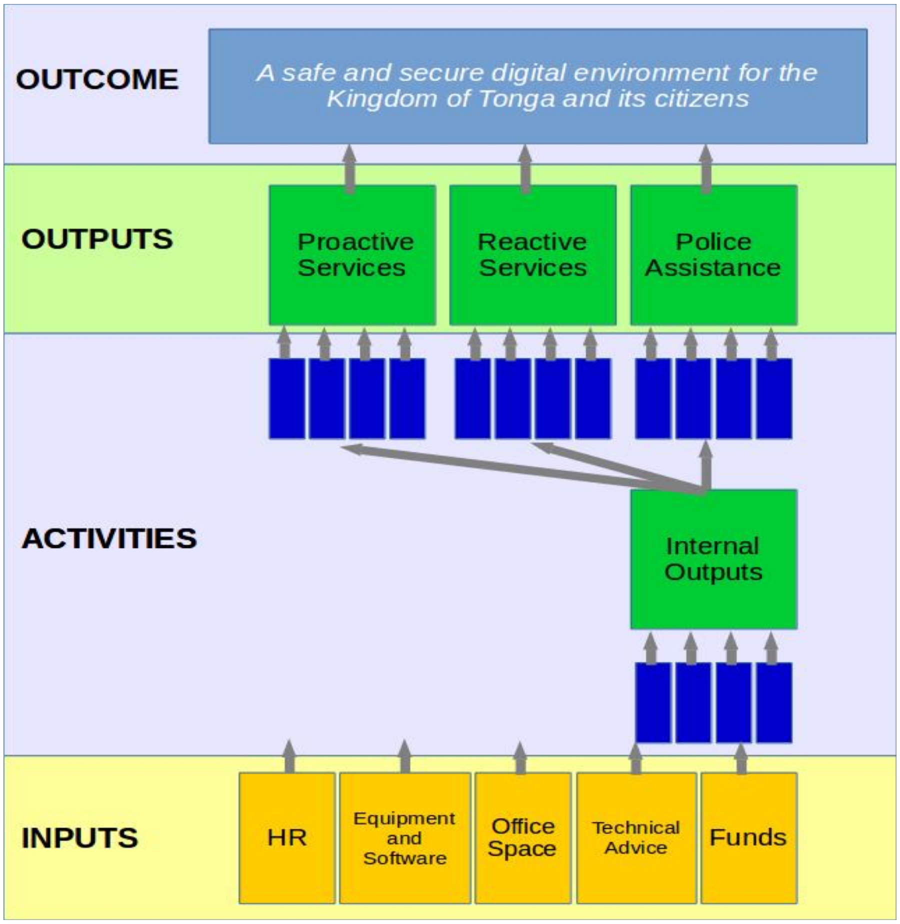


Figure 2 certTonga Results Map certTonga Results Map

As from above the vision or the outcome that *certTonga* wishes to achieve is:

"A safe and secure digital environment for the Kingdom of Tonga and its citizens"

and to achieve that vision was the mission:

"To coordinate and collaborate amongst stakeholders to prevent through public awareness, detect and manage cyber threats in the Kingdom of Tonga"

The mission can be captured in three (3) high level outputs and one (1) internal output to categories the activities tasked with the team. These outputs (depicted in green from the illustration) are:

1. That proactive initiatives and services are provided to the constituents of *certTonga* to minimize the chances a cyber incident will occur.

2. That reactive services are provided to the constituents to respond to cyber incidents in order to minimize the impact of cyber incidents and in the best way possible restore the services of the affected systems.

3. That computer forensic and ICT related advice is provided to the Ministry of Police to assist with their relevant function under the law.

4. That management and administrative activities are carried out to build the capacity and capability of the team to be able to deliver services to its customers.

Inputs from several sources and organisations including the ISIF grant were also received to facilitate the activities to deliver the outputs to support the Mission and Vision. These were:

Organisations	**Inputs**
APNIC	Technical Advice, Financial (through ISIF), Capacity Building, resource information
Attorney General's Office	Legal Advice
Australia DFAT	Financial
CERT Australia	Intelligence and Information
CERT NZ	Intelligence and Information
Council of Europe through the GLACY and GLACY+ Project	HR (Capacity Building and Workshops)
Government of Tonga	Salaries for Staff, Office Space, Administrative Support & Corporate Services
Mauritius CERT	Information, advisories
ShadowServer Foundation	Intelligence and Information
Thailand CERT	Information
Tonga Cable	Office Space, Website & Email Server
Waikato University, NZ	Technical Advice and Information

The funds from the ISIF grant were used for Equipment and Furniture (Call Centre Equipment & Software; Computers and Laptops for staff; Computers and equipment for Forensic Laboratory; Desks and Filing Cabinet) as well as Capacity Building (Certified Training; Study Tours; participation at Conferences).

Partnerships

To carry out its mandated activities, *certTonga* and the Government of Tonga could not have done it without the assistance of the following partners both formal and informal and are listed in alphabetical order within each category. It does not reflect whether a partner was more important or did more than others:

- International Partnerships

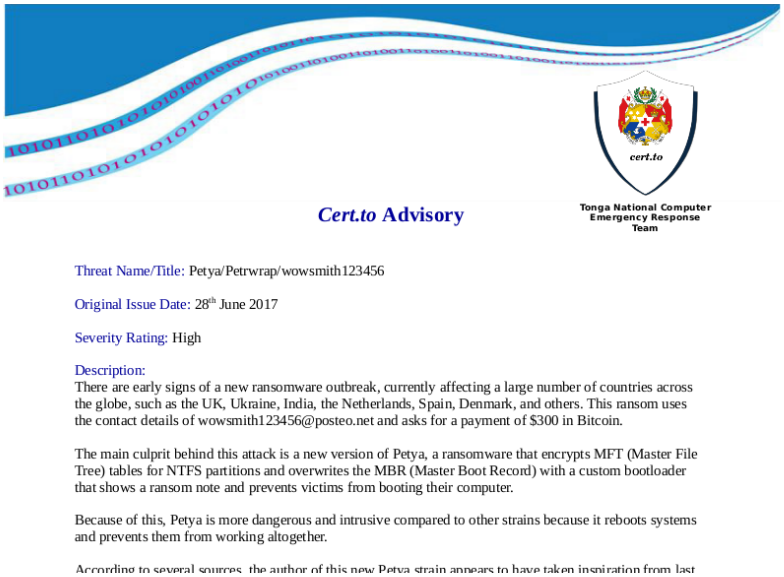
    - APNIC
    - Australia DFAT
    - CERT Australia
    - CERT NZ
    - Council of Europe through the GLACY and GLACY+ Project
    - Mauritius CERT
    - Sri Lanka CERT
    - ShadowServer Foundation
    - Thailand CERT
    - Waikato University, NZ
- Local Partnerships
    - Attorney General's Office
    - Digicel
    - Tonga Police
    - Tonga Cable Ltd.
    - Tonga Communications Corporation (TCC)
- Internal Partnerships
    - Department of Communication
    - Department of Information
    - Corporate Services Department

The services that *certTonga* provides are mainly aimed at organisations and businesses in Tonga that at least have: a network, shared computer service and has access to the Internet. As such, *certTonga*'s constituents are mainly government ministries, public enterprises and private businesses. The following describes how they benefit from the different outputs outlined above:

1. Proactive Activities
    - Advisories and Press Releases

      We send out advisories based on information we receive from our partners or other sources on the Internet. During the early days of the WannaCry and NotPetya outbreaks, *certTonga* sent out advisories on how to avoid falling victim to these ransomwares and also what to do if their computers fall victims to it.[1]

[1] Please see here for a list of advisories that *certTonga* has sent out. https://www.cert.to/?page_id=268



cert.to
Tonga National Computer Emergency Response Team

Cert.to Advisory

Threat Name/Title: Petya/Petrwrap/wowsmith123456

Original Issue Date: 28th June 2017

Severity Rating: High

Description:
There are early signs of a new ransomware outbreak, currently affecting a large number of countries across the globe, such as the UK, Ukraine, India, the Netherlands, Spain, Denmark, and others. This ransom uses the contact details of wowsmith123456@posteo.net and asks for a payment of $300 in Bitcoin.

The main culprit behind this attack is a new version of Petya, a ransomware that encrypts MFT (Master File Tree) tables for NTFS partitions and overwrites the MBR (Master Boot Record) with a custom bootloader that shows a ransom note and prevents victims from booting their computer.

Because of this, Petya is more dangerous and intrusive compared to other strains because it reboots systems and prevents them from working altogether.

According to several sources, the author of this new Petya strain appears to have taken inspiration from last

Figure 3 Advisory sent from CertTonga

There were also sector specific advisories that were sent out to specific sectors that would be affected by specific vulnerabilities

- External Vulnerability Assessments

  We subscribe onto and receive vulnerability feeds the ShadowServer Foundation. We use these reports to inform our constituents individually of vulnerabilities that are showing up for their specific IP addresses.

- Social Media Posts

  certTonga uses Twitter and Facebook to send out general cyber security and safety tips with links to specific information from all over web and some from the local website.[2]

2. Reactive activities

   Incidence Response

   Through the reactive services, *certTonga* was able to assist affected constituents in restoring and patching their systems to avoid a repetition of the same attack.

3. Police Advisory and Forensics

   certTonga were able to provide digital forensic services for the Tonga Police various types of cases including Toll Fraud, Defamation, Illegal Access and Interference with Data.

certTonga were able to handle and carry out the above activities, and while doing so, it became clear that it was very important to expand the team's knowledge around Digital Forensics and Computer Security, so registration for certified training for two team members in Offensive Security Certified Profession (OSCP) and Computer

[2] *certTonga* twitter page can be found here: https://twitter.com/tonga_cert. *certTonga* Facebook page can be found here: https://www.facebook.com/tonganationalcert/

Certified Examiner (CCE) was completed. The course certification will also give *certTonga* credibility among the community.

certTonga Staff also had opportunities to partake in other capacity building activities and opportunities to collaborate and form partnerships with relevant organisations.

Events	**Details**
Internet Governance Forum (IGF) 2016, Mexico, *Sponsored by APNIC*	Member of *certTonga* was able to participate this forum where he was exposed to Internet Governance and various workshops as well as networking with vendors
Training Course on Cyber Security Technologies, Japan *Sponsored by APT*	• *certTonga* staff was able to participate on this workshop in 2016 and 2017 • They were exposed to Security Operation Centers of large corporation and also hands on exercises in one of Japan's leading security organisations
Study Visit to APNIC and CERT Australia, Brisbane, Australia sponsored *from the ISIF Grant*	Two members of *certTonga* were able to undertake a study visit to APNIC Head office in Brisbane
Study Visit to Waikato University, NetSafe Inc., **Meeting with NZ Government Cyber Security Agencies**, New Zealand *sponsored by New Zealand MFAT*	• Meeting with NetSafe Inc. and sign MOU around information sharing and collaboration. • Toured University of Waikato Cyber Security Lab (CROW) and signed MOU for collaboration and information sharing • Meeting with New Zealand organizations that deal with Cyber Security including CERTNZ
FIRST Network Conference 2016, Puerto Rico *sponsored from the ISIF Grant*	Representative from *certTonga* participated in the security workshops and was able to network with representatives from the industry including ShadowServer Foundation, Global Cyber Alliance and other CERTs in the region.
Asia Pacific Region Internet Governance Forum (AprIGF) 2017, Thailand, *Fellowship from APrIGF Secretaria*	*CertTonga* staff participated in the Forum attending the security workshops including assisting in the facilitation on one security role play workshop and being on a panel discussion with regional CERT on one workshop.
Global Action on Cybercrime Extended, Cybercrime Investigation Training for Pacific Region, Fiji, *sponsored by Council of Europe through GLACY+ Project*	Training offered a customized training addressed to police officials (Note: *certTonga* does digital forensics for Tonga Police) involved in cybercrime investigations, equipping them with the methods and techniques to conduct more effective online investigations and forensic examination of Digital Evidence.
Global Action on Cybercrime Extended, INTERPOL Instructor Development Course (IDC), Singapore, *sponsored by Council of Europe through GLACY+ Project*	Provided the participant the fundamentals in adult instruction and curriculum design. Participants will learn and practice a variety of instructional strategies to deliver effective instruction through in-person training, blended training and/or on-line training.
Asia Pacific Computer Emergency Response Teams (APCERT) Annual General Meeting and Conference 2017, India, *sponsored by APCERT Secretariat*	Participants were able to take part in presentations from experts in the industry, network with other CERT teams in the region and also presented on the Cyber Security situation in the Pacific alongside CERT Australia

CertTonga appreciates all the assistance provided by the above partners which allowed to develop its cyber security and digital forensics capacities which are two of our most important services to our constituents. The travel also allows the team to build relationships and network with various organisations that can further support the team in different areas. *CertTonga* appreciates and would like to acknowledge the assistance provided by the APNIC Foundation for finding various sources of fellowships that allows the *CertTonga* team to attend these events.

Indicators

Indicators	**Baseline**	**Progress assessment**	**Course of action**
Constituents of *certTonga* are aware of potential digital threats that can hinder the Confidentiality, Integrity and Availability of their Systems and are informed how to avoid and recover from them	Most organisations in Tonga were not aware of cyber threats and there was no authority that could provide advisories on global attacks or new-found vulnerabilities. A few organisations that are part of international organisations may have had advice from their head offices. Others who had International counterparts may have received advice from their overseas partners.	80% Completed. *certTonga* started receiving ShadowServer reports at the beginning of March 2017. Vulnerabilities regarding specific IPs were forwarded to the IP owners and also provided advice on how they may mitigate the risks associated with those vulnerabilities. Prior to the establishment of *certTonga* no organisation was tasked with providing advice regarding global attacks etc. *certTonga* provide these services to its' constituents. *certTonga* also uses Social Media namely Twitter and Facebook to provide general advice to constituents on how to be digitally safe and secure. There are still other vulnerability feeds that *certTonga* would like to subscribe to and use for this purpose and currently taking actions to achieve this.	This general indicator was defined to be able to measure the effectiveness of the first objective of the project i.e. *"That proactive initiatives and services are provided to the constituents of CertTonga to minimize the chances a cyber incident will occur"* We recognize that this indicator is very general but we are hoping that in the future we are able to provide some statistical data to measure how effective the activities under this objective/output are. These indicators will include statistical data informed by various vulnerability feeds from ShadowServer, Team Cymru and Microsoft.
Systems that has been compromised are promptly addressed in a timely manner through collaborating with the organization's technical team if any.	When organisations encountered incidents, they would deal with it internally if they were aware there has been an incident. In some cases, they would request assistance from the local suppliers.	80% COMPLETED. *certTonga* is now the focal point when organisations encounter cyber incidents. The team collaborates with the affected organization in restoring of their system and also patching to ensure that it does not reoccur. *certTonga* continuously seeks to build its capacity and capability to be able to respond to incidents better and faster.	This general indicator was defined to be able to measure the effectiveness of the second objective of the project i.e. *"That reactive services are provided to the constituents to respond to cyber incidents in order to minimize the impact of cyber incidents and in the best way possible restore the services of the affected systems."* We recognize that this indicator is very general but we are hoping that in the future we are able to provide some statistical data to measure how effective the activities under this objective/output are. These indicators will mostly be compiled from data from the ticketing system.

Indicators	Baseline	Progress assessment	Course of action
Tonga Police receive digital forensic advice and services on a timely manner	Tonga Police would refer their digital forensics overseas to New Zealand Police or Australia Federal Police, sometime using local private companies. The cost for these usually are very expensive.	75% Most cases handled by the Police that involves digital forensics is referred to *certTonga*. Even though *certTonga* has commenced handling these cases. We are still proactively building our capacity to better respond to these requests.	This general indicator was defined to be able to measure the effectiveness of the third objective of the project i.e. "*That computer forensic and ICT related advice is provided to the Ministry of Police to assist with their relevant function under the law.*"
CertTonga is well resourced and managed to undertake its core functions	Prior to the project, *CertTonga* only had Office Space and salary for staff	Ongoing *certTonga* has a new office (currently used as a forensic lab only) with Internet connection and power. Through the various conferences and study tours *certTonga* has a fair idea and confident in carrying out its mandated functions.	This general indicator was defined to be able to measure the effectiveness of the third objective of the project i.e. "*That management and administrative activities are carried out to build the capacity and capability of the team to be able to deliver services to its customers.*"

Project implementation

Project activities	Input	Outputs	Timeline	Status
Identify of the key technical role that needs for the initial launch of the CERT team	Hire 2 CERT staff to develop the technical team. Form a structure that is sustainable for the CERT Operation	Establish posts with align to the organizational chart with clear line of reporting for each role	August – December 2016	Completed
Install, test and launch of a communication system for the CERT team	Installation the Hardware and software for the Unify communication system. Communicate concept and vision	Establishing of a Call Centre with 2 agents. Execute of the communication features of the system that added value to the services.	November 2016 – January 2017	Completed
Install, test and Launch of the *certTonga* website	Staff Time, Hosting Service	www.cert.to website with secured access.	August 2016	Completed
Identify support roles to assist with CERT operation.	Hire support team for the CERT. Provide TOR and framework for the call agents	Established 2 support personnel to work with the CERT team.	November 2016 - March 2017	Completed
Equip the CERT team with computer equipment to provide services with.	Laptops and server with Software needed for the CERT team.	Enable better service platform	November 2016 – November 2017	Completed
Establish a closed computer network for the CERT operation	Network routers and firewall	Secured closed network for CERT operation	January – November 2017	Completed

Project Management and Sustainability

The administration and management of the project has been done by existing senior administrator that is currently attached to the Ministry of MEIDECC and within the ICT department workforce. This approach was strategically used so that senior level personnel can be utilized to administer and manage the operation since its launching date. With this approach, the Government of Tonga has agreed to increase the number of staff to this Unit based on its annual management plans that ties into the overall corporate plans of the Information Department of the Ministry of MEIDECC.

Since the launching of this project in 2016, there has been a lot of activities that strengthen management ability of the team due to the establishing of a proper Standard Operating Procedures (SOP) for the *certTonga* team to follow, engaged in different workshops and short training from APNIC as well as other CERTs study visits to the some of the established CERT in the region to learn of their best practice. The ISIF funding has instrumental in building of a well-managed communication system for the CERT as well as equipped the operation with computers and capacity building opportunities for the team. This also ensures the delivering of the desired results according to the CERT different goals and mandates.

The goal for this project is to be self-sustain at one stage in the future, but with the attachment to the Government Ministry from the start benefits the CERT project from drawing resources from the limited pool of resources of government when there is a need. The Government has shown strong support for this project and they are committed to continue support this project in anyways they can see fit.

Project Outcomes and Impact

The project has delivered the expected outputs as especially outlined in stages 1 and 2.

Stage 1 – Educating stakeholders about the development of a national team

- Awareness stage

- Identify Participation

- Identify Role that National CERT play

- Identify Key Issues that a likely to be faced

Stage 2 – Planning the CERT

(This stage building on the knowledge and information that is gained during stage 1)

- Identify need for having team and benefits it will provide

- Identify its constituency, the services and support that National CERT will have

- Outline Requirement and need for National CERT

- Outline a Vision of how National CERT will operate

Stage 3 – Operating the CERT

Stage 4 – Collaboration

There has been a lot of awareness and Educational initiatives in relation to the functions of the CERT and through the better understanding of its security role in the Government and society, participation and involvement is being increased from time to time.

The capacity building of the CERT team has been increased tremendously with in the specific scope of the Cert area. The knowledge gained has contributed to the improved services provided to the current clients served by the CERT team.

Despite the lack of resources and local expertise in the arena of the CERT service, this project has pierce through most of the challenges and stumbling blocks on the way, and made an accomplishment on establishing a standard procedure which enhance the process of preserving data for evidence and other purposes as well as securely protect the integrity and privacy of the client's data.

Relevant stake holders, such as Tonga Communication Corporation and Digicel are now getting involved with some of the activities and cooperate more in providing data and information that are requested by the CERT team a specific cases and incidences. The Tonga Police is now starting to refer cased as part of their SOP get the views of the CERT team as part of their ongoing investigation of any cyber related cases.

In May 2017, *certTonga* were successful in obtaining funds from the Australia Department of Foreign Affairs and Trade under the Cyber Cooperation Program. The AUD$200,000 grant will build on the activities supported by the ISIF grant and allow *certTonga* to carry further awareness programs, continue to build the capacity of the *certTonga* staff and also ICT practitioners within Tonga.

Overall Assessment

This project has been successful so far in achieving of the outlined objectives and goals for this project and organizations and members of society are better aware of the role of CERT and they are starting to get CERT involvement in activities that are related to the cyber security and cyber safety.

The Tonga CERT is now playing a vital role in the Tonga Police investigation process which has placed the Tonga CERT in a position to be actively planned to grow in all areas to be able to cope with the demand. There is a particular focus on building capacity of the team as it now essential to the continuous operation of the CERT as well as obtaining a reliable information obtained from a verified sources and undisturbed evidences.

Considering the size of the Tonga population, we are now realizing the crucial role of the CERT in providing security alerts and forensic services for our law enforcement agencies that they currently don't have capacity and procedures in place within their own respective organizations.

Recommendations and Use of Findings

Recommendations for this project:

1. Continue developing in the area of capacity building
2. Continue enhancing the SOP and policies to align with the National priorities
3. Develop the different technical capabilities of the team

Bibliography

FIRST Site Visit Document - https://www.first.org/membership/site-visit-v2.5.pdf

RFC2350 - https://www.rfc-editor.org/info/rfc2350

CERT efforts accelerate in Tonga https://blog.apnic.net/2016/06/01/cert-efforts-rev-tonga/

Tonga CERT study trip comes to APNIC https://blog.apnic.net/2017/04/17/tonga-cert-study-trip-comes-apnic/

Event Wrap: APrIGF 2017, Bangkok https://blog.apnic.net/2017/08/04/event-wrap-aprigf-2017-bangkok/

MEIDECC hosts workshop for Computer Emergency Response Team (CERT) - http://www.mic.gov.to/news-today/press-releases/6025-meidecc-hosts-workshop-for-computer-emergency-response-team-cert

PM launched Tonga National CERT - http://www.mic.gov.to/news-today/press-releases/6159-pm-launched-tonga-national-cert

Tonga CERT urges computer users to stay alert as a new ransomware attack struck Europe - http://www.mic.gov.to/news-today/press-releases/6782-tonga-cert-urges-computer-users-to-stay-alert-as-a-new-ransomware-attack-struck-europe

Tonga National CERT Signs a Framework of Operational Corporation (FOC) with the CERT Australia to manage Cyber Security - http://www.mic.gov.to/news-today/press-releases/6725-tonga-national-cert-signs-a-framework-of-operation-coorperation-foc-with-the-cert-australia-to-manage-cyber-security

Tonga's National Computer Emergency Response Team marks one year in operation - http://www.mic.gov.to/news-today/press-releases/6867-tongas-national-computer-emergency-response-team-marks-one-year-in-operation

Official Opening of Tonga's National CERT Awareness Workshop - http://www.mic.gov.to/news-today/press-releases/6869-official-opening-of-tongas-national-cert-awareness-workshop

Phishing Email Warning - http://www.mic.gov.to/news-today/press-releases/6798-phishing-email-warning