Government of Samoa

Ministry of Communication
and Information Technology

SAMOA NATIONAL CYBERSECURITY STRATEGY

2016 - 2021

Ministry of Communications and Information Technology,
Private Bag,
Level 6,
Tui Atua Tupua Tamasese Efi Building,
Apia,
SAMOA.
Telephone: (685) 26117
Facsimile: (685) 24671
Email: www.mcit.gov.ws

Minister's Foreword

Samoans are embracing the many advantages cyberspace offers and our economy and quality of life are the better for it. However, as we enjoy the benefits of cyberspace, we also recognize that it threatens us in a variety of ways. The increasing use of Information Communications Technology (ICT) has raised issues of security and privacy. The exploitation of computers and telecommunications technology for criminal activities has increased. Incident of hacking, virus attacks, access and dissemination of pornographic materials misuse of information and network security can no longer be ignored. Cyber security has become a critical issue especially now with the rise of cyber-terrorism and its impact on national and global security.

The National Cybersecurity Strategy outlines the Government's intention of harnessing resources to protect the public and private sectors. The goals set out in the strategy aims to strengthen existing cyber systems and critical infrastructure sectors, support economic growth and protect the public in terms of connectivity to each other and to the rest of the world.

Cyber Security is a shared responsibility and this Strategy calls upon all Internet users, to be vigilant and informed about online threats, and how their own actions can be the first line of defense.

Honorable Afamasaga Lepuia'i Rico Tupa'i
MINISTER OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

Contents

Executive Summary

The National Cybersecurity Strategy 2016-2021 (the strategy) sets out areas for development in Samoa's cybersecurity.

The Ministry anticipates within the next five (5) years:

- Individuals become aware of cybersecurity threats and are empowered to exist safely in this digital era;
- Businesses become responsive to cybersecurity issue and establish a working relationship with Government, trade associations and other business partners to tackle cyber threats so the world will see that Samoa is a safe place to do business in cyberspace;
- Government has:
    - ✓ Sharpened law enforcement response to cybercrime;
    - ✓ Secure funding's to provide cyber security services;
    - ✓ Encouraged business to operate securely in cyberspace;
    - ✓ Bolstered defences in our critical national infrastructure against cyber attack;
    - ✓ Strengthened our capabilities to detect and defeat attacks in cyberspace;
    - ✓ Enhanced education and skills; and
    - ✓ Established and strengthened working relationships with other countries, business and organisations around the world to help positively shape an open and vibrant cyberspace that supports strong and better societies here and across the globe.

Introduction

"As Samoa enters into the new paradigm of globalized Information and Communications Technology (ICT) services and telecommunications convergence, attention is needed towards developing an enhanced cyber or Internet security framework."[1]

Samoa's connectivity through Internet, access to mobile phones, and broadcast technologies continues to increase, warranting the need to promote and establish Cybersecurity measures to ensure that the economic, social, environmental and infrastructure sectors are secure and equipped to address challenges and cyber threats including but not limited to infrastructure impairment and criminal activities; to ensure continuity of operations, development and the well being of digital citizens.

It is expected that the implementation of this Strategy will ensure a secure cyberspace; Ensure a secure cyberspace; that will contribute to improving Samoa's socio-economic development. To achieve this objective, the Strategy is a platform for the common understanding and action of all relevant stakeholders.

[1] Samoa National Broadband Policy 2012 Pg 13

Vision

For all citizens of Samoa, tourists, businesses and Government to enjoy the full benefits of a secure and resilient cyber space

To achieve this vision, five (5) goals are identified:

i. Develop necessary organizational structures with a focus on utilizing existing structures in Samoa as well as in the region;

ii. Establish relevant technical measures (Entities and Standards) to eliminate Cyber Threats and Attacks, enhance Cybersecurity and promote Cyber Safety.

iii. Strengthen the legal framework to meet the highest regional and international standards with regard to protection of fundamental rights as well as criminalization, investigation, electronic evidence and international cooperation relative to computer and electronic crimes;

iv. Capacity Building – Build digital citizens capacity, raising awareness and attaining resources to enhance Cybersecurity, combat Cybercrime activities and promote Cyber Safety to the highest levels; and

v. Strengthen and establish cooperation to respond to the Global nature of Cyber.

Goals

GOAL 1: Develop necessary organizational structures with a focus on utilizing existing structures in Samoa as well as in the region.

Strategy Statement:
Organizational and Procedural Measures are necessary for the proper implementation of any type of national initiative to combat Cybercrime and strengthen Cybersecurity.

Strategy Guidelines:

1. Strengthen and redefine the National ICT Steering Committee ("NICT") and its members and prioritize Cybersecurity in its mandate. The NICT is to lead the coordination and the implementation of the Cybersecurity strategy and the process of carrying out the necessary tasks.

2. Establish a Roadmap for Governance of Cybersecurity in Samoa;
   - 2.1. Identify key stakeholders to develop a culture for Cybersecurity;
   - 2.2. Identify needs of national critical information infrastructure protection;
   - 2.3. Foster information sharing within the public sector and between the public private sector;
   - 2.4. Establish process for addressing ICT security breaches and incident handling (reporting, information sharing, alert management, justice and police collaboration);
   - 2.5. Ensure effective of the implementation of the national Policy;
   - 2.6. Ensure Cybersecurity program control, evaluation validation and optimization

3. Implementation of National Benchmarking scheme to;
   - 3.1. Ensure Cybersecurity is continuously developed in accordance within internationally accepted standards;
   - 3.2. Analyze the effect of Cybersecurity breaches on citizen businesses and Government

4. The Office of the Attorney General ("OAG"), Samoa Law Reform Commission ("SLRC"); National Prosecution Office ("NPO"), Judiciary and other law enforcement agencies must develop a National Crime Prevention Strategy related to Cybercrime; this initiative is to be coordinated by NICT to ensure that measures discussed are in line with measures to the implemented.

5. Development of Child Online Protection ("COP") or Strategy to promote the use of ICT and to implementation precaution and protection of children users; in addition Child Sexual Abuse Material ("CSAM") Filtering Policy.

GOAL 2: Establish relevant Technical Measure (Entities and Standards) to eliminate Cyber Threats and Attacks enhance Cybersecurity and promote Cybersecurity.

Strategy Statement: *Defining and controlling technical measures to ensure security standards are implemented with the required expertise and in accordance with international trends.*

Strategy Guidelines:

1. Establishment of a National Computer Incident Response Team (“CIRT”) that is capable of dealing with relevant Cybersecurity Threats and Attack on citizens, tourist, businesses and government in Samoa. The CIRT must have the capability to identify combat, respond and manage Cyberspace Threats or Attacks; as well as enhance Cyberspace security in Samoa. Furthermore CIRT must be responsible for the computer forensic component of criminal investigations relative to computer technology or electronic evidence.

   The National CIRT must also gather its own intelligence instead of relying on secondary reporting incidents.

2. Development of a unit within Police Services (Ministry of Police) that serves as a single point of contact for Cybercrime with the ancillary purpose of data collection and increasing available information.

3. Establishment of a Child Online Protection Working Group (“COPWG”) consisting of but not limited to the Ministry of Police, (“MOP”); OAG; Ministry of Education Sports and Culture (“MESC”), Ministry of Women, Community and Social Development (“MWCSD”), Ministry of Justice and Courts Administrations (MJCA), Ministry of Communications and Information Technology (MCIT), Office of the Regulator (OOTR), Social Welfare Services such as Samoa Victim Support Group (SVSG), and other child protection NGOs; Internet Service Providers (ISP), Electronic Service Providers (ESP); Telecommunications Mobile and Fixed Network Providers; other Hi-Tech Companies; Owners of Internet Cafes and other public access providers e.g. libraries and telecentres.

4. Develop or Identify Standards to be implemented to ensure that the rest of the Cybersecurity related attacks are minimized.

5. NICT must carry out assessment and identify the critical processes, standards for the introduction of the different security levels. Furthermore the CIRT and other relevant stakeholders must be responsible for the implementation and control of the developed standards.

6. MCIT, OOTR, Samoa Qualification Authority (SQA), shall develop a framework for the certification and accreditation of national agencies and public sector professions by internationally recognized Cybersecurity Standards.

GOAL 3: Strengthen the legal framework to meet highest regional and international standards with regard to protection of fundamental rights as well as criminalization, investigation, electronic evidence and international cooperation;

Strategy Statement: *In order to promote openness and a safe cyberspace environment. Samoa should have a reliable legal framework that reflects its uniqueness as well as international best practices.*

Strategy Guideline

1. The MCIT and OOTR will coordinate a diagnostic of Convention and other International Instruments appropriate for Government endorsement, ratification and accession.

2. MCIT and the OOTR will coordinate a legislative compliance review in collaboration with Cybersecurity stakeholder to determine all necessary powers exist including:

   2.1. enabling law enforcement and other relevant agencies to protection digital citizens material and intellectual aspects as well vital infrastructure;

   2.2. establish or improving definitions, penal legislation, investigation instruments of law enforcement, admissibility of electronic evidence, liability of Internet Service Providers (ISPs), and specific provision children online and international cooperation.

   The review shall include that identification of existing provision that could be utilize in relation to Cybersecurity, a comparison with international best practices, a gap analysis suggestion for amendments and the related drafting instructions. This activity shall be carried out in close collaboration with the OAG and built upon existing work carried out in the region (e.g. the assessment of the legislation within the ICB4PAC Project).

GOAL 4: Build digital citizens capacity, raising awareness and attaining resources to enhance Cybersecurity, combat Cybercrime activities and promote Cyber safety to the highest levels.

Strategy Statement: *Ensuring that all relevant stakeholders including citizens, students, businesses, judiciary, and law enforcement receive sustainable trainings.*

Strategy Guidelines

1. The Ministry and NICT to inform all stakeholders involved of the functions and roles of NICT and other proposed working groups.

2. Identify Cybersecurity stakeholder to coordinate training and awareness on Cyber related issues, it may include;
   - 2.1. the establishment and fostering of links with village council about recent ICT developments;
   - 2.2. the distribution of Cybersecurity information to community through the MWCSD through the usage of Feso'ota'i Centre Outlets;
   - 2.3. use of Government media outlet to publicize Cybersecurity information;
   - 2.4. creation of Internet Safety Messages and material which reflect cultural norms and law for postage online and to air on Television;
   - 2.5. development of Tertiary level Computer Science Curriculum to include Cybersecurity measures;
   - 2.6. Development of School Curriculums concerning Computer Studies in the primary and secondary levels; which include a model on Cybersecurity and Cyber safety.

3. Development of sustainable training program for law enforcement officers (police, customs), Finance, Prosecutors, Service Providers; OOTR and Judiciary.

4. Development of sustainable training programs for Communication and IT engineers to support and assist managing Cybersecurity programs.

5. MCIT and OOTR shall provide a list of capacity building programs related to Cybersecurity that Samoa should benefit from to avoid an overlapping both entities shall develop a roadmap that list the difference capacity activities that Samoa requires.

6. MCIT, OOTR, SQA shall develop for the certification and accreditation of national agencies and public sector professions by internationally recognize Cybersecurity standards

GOAL 5: Cooperation; Responding to the global nature of Cybersecurity threats and attacks through a multi-stakeholders approach and strengthening local and global partnerships.

Strategy Statement: *To be part of the transnational dimension of cybersecurity incidents and benefit from the support of different organizations for developing countries by utilizing means of local and international cooperation and support.*

Strategy Guidelines

Intra-State Cooperation:

1. MCIT to coordinate data collection on Intra-State Cooperation and recommend further required partnership stakeholders[2]
2. MCIT and OOTR will make recommendations with regard to a potential access to international or regional agreements, current processes of developing binding standards where Samoa should participate, as well as 24/7 networks (such as the G8 or Interpol Network).

Intra-Agency Cooperation:

3. National Cybersecurity Stakeholders are encouraged to enter into partnerships and programs for sharing Cybersecurity assets (people, process, tools) within the public sector (i.e. official partnerships for the cooperation or exchange of information, expertise technology and/or resources between departments ministries and agencies)[3]

Public and Private Partnerships

4. Promote Public and Private Partnership to share Cybersecurity assets (people, process, tools) between the public sectors (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and resources)[4]
5. Furthermore identify cooperation partners (such as Matai and Fa'afeagaiga) in rural areas that can support the capacity building initiatives by providing information about security within their daily work and provide them with necessary background information and training materials for the community.

[2] Intra-State Cooperation refers to any officially recognised national or sector-specific partnership for sharing cybersecurity assets across borders with other nation state (i.e. signed bi-lateral or multi-lateral partnership for the cooperation or exchange of information, expertise, technology and/or resources)

http://www.itu.int/en/ITU-D/Cybersecurity/Document/GCI_conceptual_Framework .pdf. Pg.9.

[3] Ibid……………………………………………………………………………………..

[4] Ibid……………………………………………………………………………………..

International Cooperation

6. MCIT and OOTR to conduct appraisal and make recommendation with regards to potential International or Regional Agreements, current process of developing binding standards where Samoa should participates, as well as 24/7 networks (such as the G8 or Interpol Network).

Strategic Priorities

Activity	Lead Agency	Proposed Timeframe
NICT redefined roles and responsibilities	MCIT	2016 - 2019
Establishment of Roadmap for Governance of Cybersecurity in Samoa	MCIT	2016 - 2019
National Benchmarking scheme	MCIT/OOTR	2017 - 2019
National Crime Prevention Strategy	MOP	2017 - 2020
Development of Child Online Protection Policy or Strategy	MCIT/OOTR/MWCSD/MOP	2018 - 2020
Establishment of CIRT	MCIT	2016 - 2019
Development of Cybersecurity Unit with a Law Enforcement	MCIT/MOP	2017 – 2020
Establishment of COPWG	MCIT/MESC/MWCSD	2016 - 2019
Assessment for standards	MCIT/OOTR	2016 - 2019
Development of standards	MCIT/OOTR	2016 - 2019
Framework for certification and accreditation of National Agencies and Public Sector Professions by Internationally Recognized Cybersecurity Standards	MCIT/SQA/OOTR	2017 - 2020
Convention and International Instruments Diagnostic	MCIT/OOTR	2018 - 2020
Legislative Compliance Review	OAG/MCIT/OOTR	2018 - 2020

Inform Stakeholders involved in the policy or functions and roles of NICT and other proposed working groups	MCIT	2019 - 2020
Coordination of trainings and awareness	MCIT/MESC/OOTR/ MWCSD/MOP	Ongoing
Development of tertiary level Computer Science Curriculum to include Cybersecurity measures	MCIT/OOTR/MESC/SQA	Ongoing
Development of a sustainable training program for law enforcement officers (Police, Customs), Finance, Prosecutors, Service Providers; Office of the Regulator and the Judiciary.	MCIT/OOTR/MOP/OAG	Ongoing
Development sustainable training programs for communication and IT engineers to support and assist in managing Cybersecurity programs.	MCIT	Ongoing
Data Collection and Intra-State Cooperation and Partnerships Recommendations	MCIT	Ongoing
Mobilization/Strengthening of National Cybersecurity Stakeholders (Government Ministries, Authorities, Offices) partnerships	MCIT	Ongoing
Mobilization/Strengthening of Public and Private Partnerships	MCIT	2020
Identify contact point at the community level/village level	`MWCSD	2017 - 2019
Identification and Establishment of International Relationships	MCIT/OOTR/OAG	Ongoing