



VANUATU NATIONAL CYBER SECURITY STRATEGY



“To Secure and Protect, Increase Resiliency,
Cyber-hygiene and Security-aware in Vanuatu

Published 09th March 2021 Port Vila, Vanuatu

The Office of the Government Chief Information Officer (OGCIO) – Vanuatu Government claims the Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Government of Vanuatu.

Contact us

This publication is available in PDF format. All other rights are reserved. For enquiries regarding the license and any use of this publication, please contact: The PRIME MINISTER'S OFFICE – OGCIO

Rue Emmanuel Brunet, PMB 9108, PORT VILA T: +678 33380

The Vanuatu National Cyber Security Strategy has been drafted by Dr. Jeffery Garae with the help of the Deputy CIO – John Jack, CERT Vanuatu team, OGCIO Policy Team and key Stakeholders (TRBR, VBS, VPF, VanIGF).

It has been driven and lead under the direction of the Office of the Government Chief Information Officer (OGCIO) and the CERT Vanuatu Office, Prime Minister's Office.

The creation of this Strategy has been possible thanks to all stakeholders involved including our Donor Partners. Booklet Designed by Grind Designs and Printed by Sun Productions.

Table of Contents

Foreword	1
Acknowledgements	2
Executive Summary.....	3
2.0 Vanuatu’s National Cyber Security Strategy Outline	6
The Cyber Security Coherent Position and Ecosystem of Vanuatu	8
3.0 Background Information: Cyber Security in a Nutshell	9
3.1 Vanuatu’s Cyber-threat Environment	9
3.2 Understanding Vulnerabilities in Vanuatu’s Cyberspace	10
3.3 Reported and Recorded Cyber-threats in Vanuatu	11
3.4 Cyber Security Development in Vanuatu.....	12
3.5 The Ideal National Cyber Security Hierarchy at Glance	13
3.6 The National Cyber Security Maturity Model.....	14
The National Cyber Security Statement for Vanuatu	18
4.0 National Cyber Security Vision Statement	19
5.1 Vision.....	20
5.2 Our Mission	20
5.3 Cyber Security Goals.....	20
The National Cyber Security Strategy And The Strategy Direction	24
5.0 The Strategy Consultation Process	25
5.1 The Strategy Consultation Timeline	25
5.2 The Strategy Consultation Execution Methodology	26
5.3 The Strategy Consultation Coverage and Demography.....	26
a) One-to-one Consultation Method:.....	27
b) Nationwide Consultation Method:.....	27
c) The Targeted Consultation Method:.....	28
6.0 Cyber Security for National Critical Infrastructure in Vanuatu.....	29
6.1. Critical Infrastructure Sectors	30
7.0 National Cyber Security Priorities	31

7.1. Cyber Resilience	34
7.2. Cyber Security Awareness.....	35
7.3 Cyber Capacity and Literacy.....	36
7.4 Addressing Cybercrime.....	38
7.5 International Engagement	40
7.6 Cyber Security Standards and Legal Frameworks	40
8.0 The National Cyber Security Strategy Response Deliverables	43
8.1. The National Cyber Security Generalised Delivery Response Model	43
8.2. The Cyber Security Awareness Campaign Response	44
9.0 Conclusion.....	44
9.1 It does not End Here.....	45
10.0 References.....	46
11.0 Appendices	47
Appendix 1: The National Cyber Security Strategy Consultation Report	47
Appendix 2: Cyber-threats Recorded in Vanuatu Report.....	58

Definitions

CERT Vanuatu | CERTVU: Vanuatu's National Computer Emergency Response Team.

Coronavirus Disease (COVID-19): is an infectious disease caused by a newly discovered coronavirus.

Cyber-attack: is a deliberate exploitation of computer systems and networks launched by cybercriminals via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Border: is best defined as the Functional Equivalent of the Border (FEB) where the data arrives at the first practical point of inspection— a network router, computer server, PC, or other networked device.

Cyber Capacity: is a term coined to refer to adequate number of cyber experts and professionals across the entire cyber security spectrum i.e., cyber security experts in ICT and Telecommunications sector, legal sector, financial sector, health sector, academic sector and civil society sector.

Cybercrime: is defined as any crime that is committed using a computer or network or hardware device.

Cybercriminals: are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.

Cyber Literacy: is the ability to use computer technologies effectively and to simultaneously understand the implications of those actions.

Cyber-resilience: is the ability to effectively prepare for, adapt, withstand, respond to and recover from cyber-attacks.

Cyber Security: is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Cyber Security Bundles: refers to Government lead initiatives to support or assist organizations and communities with enhance security efforts.

Cyberspace: is the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

Cyber Sovereignty: is a phrase used in the field of Internet governance to describe governments' desire to exercise control over the Internet within their own borders, including political, economic, cultural and technological activities; that is, to extend the concept of sovereignty to include all aspect of the Internet.

Cyber-threat: any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Darknet: a network used for routing and/or content that all services and sites are accessible only through non-globally routable addresses or only through overlay networks such as Tor, **The Invisible Internet Project (I2P)**, or **FreeNet**.

Data Security: is the process of protecting your most critical business assets (your data) against unauthorized or unwanted use.

eSafety Commission: an entity/agency serves with the primary role to enhance the online safety of Internet users in a country, particularly the online safety of children and young people, primarily through a complaints service on cases experiencing serious online abuses such as cyberbullying, hate speech, shaming, adult cyber abuse, image-based abuse, and other technology-related concerns for people at risk of family or domestic violence.

Harmful Digital Communications: is a term used to refer to specific types of negative behaviour online, disclosing of sensitive personal facts, publishing or offensive materials and messages, spreading degrading rumour, and publishing online invasive photographs or videos of others that cause harm. Examples include cyber bullying, harassment and revenge porn.

Information Security (IS): often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.

Information Security Management Systems: an ISMS is a set of guidelines and processes created to help organizations in a data breach scenario. By having a formal set of guidelines, businesses can minimize risk and can ensure work continuity in case of a staff change. ISO 27001 is a well-known specification for a company ISMS.

ISO 27001 Standard: The ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

LAN: Local Area Network, is a group of computer and peripheral devices which are connected or linked together in a limited area such as home, school, laboratory, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application.

Legal Frameworks: comprise a set of documents that include the constitution, legislation, policies, regulations, and contracts.

Malware: is a catch-all term for any type of malicious software designed to harm or exploit any programmable device, service or network.

OGCIO: This Office will play a primary role in centralizing all information technology and data utilised by all government Agencies.

PaCSO: is the Pacific Cyber Security Operational Network, a key deliverable of Australia's International Cyber Engagement Strategy – under the Cyber Cooperation Program. PaCSO is a Cyber Security Platform established to enable cooperation and collaboration by empowering members to share cyber security threat information, tools, techniques and ideas between nations.

PILON: is a network of senior law offices from 19 Pacific Island countries, including Australia and New Zealand, who work together to contribute to a safe and secure Pacific by advancing key law and justice issues.

Ransomware: is an emerging form of malware that locks the user out of their files or their device, then demands an anonymous online payment to restore access.

Secure Sockets Layer (SSL): is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client (e.g., Outlook).

The CIA Triad: is a benchmark model in information security designed to govern and evaluate how an organization handles data when it is stored, transmitted, or processed.

Traffic Light Protocol: is a set of designations used to ensure that sensitive information is shared with the appropriate audience. TLP was created in order to facilitate greater sharing of information.

Type-Approval Regulation: is a process by which Information, and Communications Technology (ICT) equipment and devices, such as RTTE, is authorized for sale and use in a country (“approved”).

Vanuatu National Infrastructure: are those facilities, systems, sites, information, people, networks and processes, necessary for Vanuatu to function and upon which daily life depends.

YUMI40: is the Vanuatu 40th Independence Day Anniversary 2020 celebration theme which resembles the new stage of Vanuatu's struggle through to being independence. It symbolizes Vanuatu's Maturity.

Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
CAAV	Civil Aviation Authority Vanuatu
CERT	Computer Emergency Response Team
CERT Vanuatu CERTVU	Vanuatu's National Computer Emergency Response Team
CERTVU	Vanuatu's National Computer Emergency Response Team
CI	Critical Infrastructure
CIA	Confidentiality Integrity and Availability
CIO	Chief Information Officer
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
COM	Council of Ministers
COVID-19	Coronavirus disease
CSIRT	Computer Security Incident Response Team
CSP	Cyber Security Priority
CSRWG	Cyber Security Reference Working Group
CSTWG	Cyber Security Technical Working Group
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
ENV2	Environment Pillar-2
EOC2	Economic Pillar-2
GBN	Government Broadband Network
GCSCC	Global Cyber Capacity Centre
HDC	Harmful Digital Communication
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IETF-RFC 2828	Internet Security Glossary
IoT	Internet of Things
IR	Incident Response
IS	Information Security
ISMS	Information Security Management Systems Standard
ISO	International Organization for Standards
ISO 27001	Information Security Management Systems (ISMS) Standard.

ISP	Internet Service Provider
IT	Information Technology
ITS	Information Technology Services
ITU	International Telecommunications Union
MoC	Memorandum of Cooperation
MOU	Memorandum of Understanding
NCSA	National Cyber Security Agency
NCSC	National Cybersecurity Steering Committee
NCSS	National Cyber Security Strategy
NGO	Non-government Organization
NIST	National Institute of Standards and Technology
NSDP	National Sustainable Development Plan (The Peoples Plan)
NSS	National Security Strategy
OCSC	Oceania Cyber Security Centre
OGCIO	Office of the Government Chief Information Officer
OS	Operating System
PaCSO	Pacific Cyber Security Operational Network
PII	Personally Identifiable Information
PILON	Pacific Islands Law Officers' Network
RFC	Request for Comments
RTI	Right to Information
RTTE	Radiocommunications and Telecommunications Terminal Equipment
SLO	State Law Office
SSL	Secure Sockets Layer
SOC	Security Operations Centre
SOC2	Society Pillar-2
SQL	Structured Query Language
The CIA Triad	Information Confidentiality Integrity and Availability
TLP	Traffic Light Protocol
TRBR	Telecommunications Radiocommunications and Broadcasting Regulator
URL	Uniform Resource Locator
VPF	Vanuatu Police Force
VBS	Vanuatu Bureau of Standards
VanIGF Vanuatu IGF	Vanuatu Internet Governance Forum

Foreword

I have the pleasure to present to you Vanuatu's National Cyber Security Strategy 2030. This Strategy complements and strengthens our efforts towards the National Security of our nation and is a firm step to accomplish a standard National Security framework for Vanuatu. The National Cyber Security Strategy (NCSS) outlines our national aspiration, set out in the National Security Strategy (NSS) 'Pillar-5: Cyber Security', which was founded on the National Sustainable Development Plan (NSDP) 2030, for a safe, secured, resilient, stable, sustainable and prosperous Vanuatu.

The Cyberspace is an intrinsic part of the development of Vanuatu. The Cyberspace has by far paved new alternatives for the current predictive global business challenges to ensure operations are sustainable and communications in this 'new-normal' environment do not hinder day-to-day operations, particularly during the COVID-19 pandemic.

In the practical world of technology, Vanuatu has leveraged on ICT to enable and enhance its daily business operations and by far shown positive impacts and economic benefits.

These benefits are visible because of the establishment of the ICN1 Submarine Fibre Cable into Vanuatu, connecting Port Vila and Suva (Fiji) on the 15th of January 2014. However, technologies, processes and people in Vanuatu are becoming more and more an important priority of Cyber Security in Vanuatu as we continue with our efforts towards nation building and in particular our National Security efforts. We need to secure and protect our Personally Identifiable Information (PII), sensitive information/data and most importantly organizational sensitive data which are highly valuable.

A crucial and practical way forward to secure Vanuatu is to create an environment that encompasses a strong cyber capacity with the intellect of being security-aware as we strive to progressively improve cyber literacy in Vanuatu. Such environment will effectively enable us to identify potential risks and cyber-threats. It is also critical to integrate cyber capacity building, cyber operations within our development policies to ensure proper mechanisms are strategized for, and implemented.

As commonly quoted by security experts: "we cannot protect you from your own mother if she takes your unlocked phone without a passcode." These are some of the challenges we face in Vanuatu and across the globe. Therefore, it is very important to address Cyber Security efforts and combat Cybercrime issues in Vanuatu.

I am calling on all stakeholders to prioritise and effectively collaborate with the Government on this national Strategy to secure, protect and develop our country and harness the power of secure ICTs in these efforts to uphold our National Security as we progress in our development journey.



Hon. Bob Loughman WEIBUR (MP)

Hon. Bob Loughman WEIBUR (MP)

Prime Minister

Acknowledgements

The development of the National Cyber Security Strategy of 2030 would not have been completed without the determined efforts and contributions of individuals, and the financial and technical support from various stakeholders and institutions.

Tankio tumas to the Government through the Prime Minister and the Director-General, the Chief Information Officer (CIO) and Deputy CIO of the Prime Minister's Office for their support and motivation in leading the development of this significant National Strategy.

Tankio tumas to the various institutions who have provided technical and financial support towards the development of the Strategy; particularly the Australian High Commission in Vanuatu, the New Zealand High Commission in Vanuatu, the Vanuatu Police Force (VPF), the Vanuatu Bureau of Standards (VBS), the Telecommunications Radiocommunications and Broadcasting Regulator (TRBR) office, the Vanuatu Internet Governance Forum (Vanuatu IGF), the Office of the Government Chief Information Officer (OGCIO), CERT Vanuatu and all technical units within various Government agencies that provided financial and technical support during the development and consultation phase of this National Cyber Security Strategy (NCSS).

Tankio tumas to the dedicated agencies and their representatives who formed the National Cyber Security Strategy Review Committee. We humbly appreciated your time and knowledge in reviewing the national Strategy document to ensure it meets all requirements. These review committee members are: OGCIO representatives, CERT Vanuatu representative, Vanuatu Financial Service Commission (VFSC) representative, Vanuatu Bureau of Standards (VBS) representative, PHAMA Plus representative and the Right to Information (RTI) Unit representative.

Finally, **bigfala tankio** to all the government agencies, state owned enterprises, private sector organizations, schools, communities and the Internet users who have accepted and responded to our consultation invitation. Your contribution has made this strategy robust, practical, valuable and user-centric.

Executive Summary

Traditionally, the concept that “security is everyone’s business” has been an essential part of any normal security best practices, education and awareness campaigns against phishing and, or other cyber-related attacks. Technically, these cyber-attacks are often the very first step for cybercriminals to work their way to their ultimate target. For instance, the first cyber-attack, ‘Morris worm’ or the infamous ‘ILOVEYOU’ worm which 20 years ago contributed to revolutionizing the way cyber-attacks are deliberately executed. These cyber-attacks brought about new knowledge on how countries and organizations respond to cyber-threats. ‘Lesson learnt’ shows that awareness and diligence are important at all levels and often referred by security experts as one of the best ways to combat cybercrime. Moreover, the implementation of national cyber security frameworks including policies, strategies and standard operating procedures, are key guides and plans to enhance cyber security efforts in any country.

As more traditional services such as sending of handwritten mails or norms of doing business transactions are transforming into online or e-services, there are increasing cyber risks associated with the way technology is evolving. Moreover, the current COVID-19 pandemic reaffirms cyber security as a top concern for governments and businesses around the world.

The prioritization and enforcement of cyber security is a challenge and does not come easy or cheap for an organization, and even for someone whose job does not involve sensitive data, systems or Vanuatu as a whole. That cyber security mindset must change or evolve over time when employees or Internet users realize they do hold the missing piece that enable attackers to infiltrate key systems. Therefore, cyber security education and awareness are essential steps in creating a ‘security-literate’ and a ‘security-aware’ society that ensures employees and Internet users understand that any data or credentials they expose, regardless of how insignificant they seem, can become a foothold for attackers to pivot toward bigger cyber-attacks or prizes of much greater value. Being security-literate and security-aware can help organizations and users develop concrete Incident Response (IR) plans which clearly define all stages:

- ❖ *Preparation;*
- ❖ *Detection & Analysis;*
- ❖ *Containment, Eradication & Recovery; and*
- ❖ *Post-Incident Activities.*

This National Cyber Security Strategy delivers six national priorities to strengthen National Security and address cyber-threats and issues in Vanuatu. The Strategy priorities include:

- ❖ *Cyber Resilience;*
- ❖ *Cyber Security Awareness;*
- ❖ *Cyber Capability and Literacy;*
- ❖ *Addressing Cybercrime;*
- ❖ *International Engagement; and*
- ❖ *Cyber Security Standards and Legal Frameworks.*

It is also important to address these national priorities with critical national responses to ensure the Government, Businesses and Internet users are secured and protected from cyber-attacks. These responses are classified under a multi-stakeholder approach which are categorized into three groups:

- ❖ *Government Responses;*
- ❖ *Private Sector Responses; and*
- ❖ *Civil Society Responses.*

Furthermore, the strategy emphasises on the importance of ‘Cyber Security Education’ and the urgent need to unify efforts through the multi-stakeholder framework. It is a cornerstone for building effective unified cyber security awareness campaigns. Organizations and cyber security stakeholders must develop and contribute in helping employees and other Internet users learn how to identify security risks and threats such as phishing attacks. Hence, awareness has to reach a more personal level to be truly effective for everyone who utilize the Internet and technology on a daily basis. Once at the personal level, the sense of ‘trust’ and ‘ownership’ evolves therefore Internet users to make better choices and decisions while being online.

The bottom line is that security or cyber security is not only about tools or technology nor a business problem, it is about establishing a broad, fundamental awareness and sense of responsibility and ownership among the society at large. Building this cyber security fundamental knowledge creates a society that is security-literate and security-aware regardless of circumstances.

Overall, this National Cyber Security Strategy (NCSS) is a plan of action designed to improve '*Security and Resilience*' of Vanuatu's National Critical Infrastructure and services. It is a mixture of a high-level top-down and bottom-up approach to cyber security that establishes a range of national objectives and priorities that is achievable for Vanuatu within the next ten years - 2030.

VISION

- To create a secure, self-taught and security-aware capability environment for Vanuatu citizens, Government, business organizations by creating a better protected mindset for all citizens while being online; and
- To improve cyber security resilience, cyber hygiene and ensure cyber-threat preparedness of our borders and cyberspace are effectively active for a better National Security.

MISSION

We strive to create a proactive Cyber Security framework to secure and protect business operations by ensuring an improved two-way information sharing channel for a better Information Security management.

- Adjusting to other National Frameworks.
- Unify Awareness Campaigns.
- Build Cyber Capabilities and Talents.
- Increase International Cooperation.

Strategic Priorities

Cyber Resilience

Cyber Security Awareness

Cyber Capabilities and Literacy

Addressing Cybercrime

International Engagement

Cyber Security Standards and Legal Frameworks

2030 Action Plan

- » Improve Cyber Resilience to proactively protect and defend our critical infrastructure in Vanuatu.
- » Increase Cyber Security Awareness Raising nationwide.
- » Build effective Capacity Building Programs for all sectors in Vanuatu.
- » Work towards the establishment of the National Cyber Security Agency.
- » Enhance our Law Enforcement operations.
- » Build on Standards and Legal Frameworks including Regulations and Policies.
- » Increase our International Engagement.
- » Create more Cyber Security Bundles for all sectors in Vanuatu.
- » Promote and encourage establishment of CSIRTs and SOCs.
- » A better 'Information Sharing Platforms' for Internet and technology users.

2.0 Vanuatu's National Cyber Security Strategy Outline

The National Cyber Security Strategy provides the Government's plan on Vanuatu's various national cyber security goals, objectives, priorities, the level of cyber-readiness and resilience. This strategy is structured in three parts which covered the following areas:

Part 1: The Cyber Security Coherent Position and Ecosystem of Vanuatu

- ❖ *Background Information: Cyber Security in a Nutshell*
 1. *Vanuatu's Cyber-threat Environment*
 2. *Understanding Vulnerabilities in Vanuatu's Cyberspace*
 3. *Reported and Recorded Cyber-threats in Vanuatu*
 4. *Cyber Security Development in Vanuatu*
 5. *The Ideal National Cyber Security Hierarchy at Glance*
 6. *The National Cyber Security Maturity Model*

Part 2: National Cyber Security Statement for Vanuatu

- ❖ *National Cyber Security Vision Statement*
 1. *Vision*
 2. *Our Mission*
 3. *Cyber Security Goals*

Part 3: The National Cyber Security Strategy and the Strategy Direction

- ❖ *The Strategy Consultation Process*
 1. *Cyber Security for National Critical Infrastructures in Vanuatu*
 2. *National Cyber Security Priorities*
 3. *The National Cyber Security Strategy Response Deliverables*
 4. *Conclusion*

PART 01



The Cyber Security Coherent Position and Ecosystem of Vanuatu



3.0 Background Information: Cyber Security in a Nutshell

Cyberspace is both essential to the existence of the governments and those who governed, and dangerous in its relative anonymity and connectivity to virtually all corners of the world. Every day, governments, enterprises and organizations wrestle with cybersecurity compromises of all sizes and types, ranging from simple viruses to complex, stealth targeted online attacks. To successfully defend their data and the organization's reputation, Information Technology (IT) and security firms are developing teams, tools, processes, policies, strategies and even introducing or amending legislations to quickly respond to new cyber-threats and compromises, but not all of them are succeeding. Many security leaders and decision makers appear to be overestimating or under prioritizing their ability to detect and respond to security incidents. This can be due to many organizations lacking dedicated staff to handle incident response tasks. It is cautionary that heightened awareness around cyber incident response and some organizations' definition of a "security incident" may overlook significant events which are often critical for successfully mitigating cyber-threats.

The openness of the Internet is integral because the prosperity of all nations are now strongly linked by many forms as well as through bilateral and diplomatic partnerships. With the current COVID-19 pandemic crippling almost all economies, the use of Information and Communication Technology (ICT) and the Internet is paramount to enabling business continuity. Conversely, as new threats spread across the borders due to the increase of users going online, the need to identify a cyber-border is as important as the physical borders. The notion of establishing Cyber-borders provides an avenue and desire for governments to exercise and implement proper security controls over the Internet within their own borders, including economic, political, cultural and technological activities; that is, to an extend the concept of Cyber Sovereignty. This whole concept requires a new era of cooperation to ensure the growth and stability of the national and global economy.

3.1 Vanuatu's Cyber-threat Environment

'Cyber Security' is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as the process of protecting sensitive data, networks, and software applications from cyber-attacks. Consequently, 'Security' isn't only about tools or technology; it is about establishing a broad, fundamental awareness and sense of responsibility among all Internet and technology users.

The ever-changing cyber-attacks and techniques occur daily, posing major threats to organization applications and networks. The execution of cyber-attacks and techniques have become incredibly dynamic and stealth in nature. Users need flexible solutions and the ability to make frequent adjustments aligning with the changes in the technology landscape in order to appropriately protect systems and networks. This is how complex cyber-attacks are evolving, bringing challenges for cybersecurity professionals in Vanuatu and abroad.

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused situation created by COVID-19."by the unstable social and economic

- Jurgen Stock, INTERPOL Secretary General.

Vanuatu is no different to other countries where decision makers and security professionals are struggling to keep up with the pace of the ever-changing threats and threat behaviours. The likes of phishing attacks, online scams, Ransomware, the rise of IoT bots, botnets, Malware attacks and defacing of websites are also threatening Vanuatu's Internet environment. Consequently, Vanuatu needs to be proactive in cyber security. The establishment of the Computer Emergency Response Team (CERT Vanuatu) of Vanuatu is a key step to implementing its cyber security framework and mechanisms.

Since the establishment of CERT Vanuatu, the cyber-attack trends indicated that threats will increase due to the rapid evolution in the technological world which is economically driven by various global technology power enterprises and firms. This phenomena is observed globally based on the technology and cyber-attack trends and also the increase in consumer demands for technology and online services.

This Strategy provides a brief two brief subsections on the on major reported cyber-threat cases identified in Vanuatu in 2018, 2019 and 2020. These data were recorded by CERT Vanuatu.

It is also crucial to understand why Cybercriminals develop malware or cause cyber-attacks. Cyber-threats occur for a reason and the attackers responsible for these cyber-threats have specific motives. Motives are usually for financial gains and reputation. Cybercriminals or attackers leverage on vulnerabilities in systems, networks or from exploits and loopholes found in systems. Vulnerabilities exist not only in networks, but also within the user's computer systems and mobile platforms.

3.2 Understanding Vulnerabilities in Vanuatu's Cyberspace

The technical perspective based on the IETF-RFC 2828 definition classifies vulnerabilities to common software, system and network security vulnerabilities. Over the years the common vulnerabilities identified in Vanuatu include some of the following [4], [5]:

- ❖ *Missing data encryption; flaws*
- ❖ *OS command injection;*
- ❖ *SQL injection;*
- ❖ *Missing authorization;*
- ❖ *Unrestricted upload of dangerous file types;*
- ❖ *Reliance on untrusted inputs in a security decision;*
- ❖ *Cross-site scripting and forgery;*
- ❖ *URL redirection to untrusted sites;*
- ❖ *Bugs; and*
- ❖ *Weak passwords;*

The list of vulnerabilities increases every year as new ways of stealing and corrupting data, systems and networks are discovered.

Based on known past assessments with utilised resources, it is known that the systems and networks in Vanuatu are highly susceptible to cyber-threats.

“Vulnerabilities’ in cyber security is defined as flaws or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy”

- IETF-RFC-2828

Over the years identified vulnerabilities range from unsecure default ports, open ports, unsecured websites, and easy passwords and are extremely vulnerable to social engineering, phishing and spams.

In addition, lack of security awareness across the Internet and computer users in Vanuatu adds to the impact of how vulnerable Vanuatu is, in terms of Cyber-threats/attacks. Other vulnerabilities or threats include spams, DDoS attacks, SSL Poodle and SSL Freak vulnerabilities, DNS vulnerabilities and other minor vulnerabilities.

These vulnerabilities expose Vanuatu in terms of computer security. Exposure leads to threats and critical errors in software, systems and networks can leave data in the entire network vulnerable to malicious threats. Some of these threats include:

- ❖ *Malware;*
- ❖ *Phishing;*
- ❖ *Proxies;*
- ❖ *Spyware and adware;*
- ❖ *Botnets;*
- ❖ *Spams; and*
- ❖ *Darknet services.*

Most Vulnerabilities that are frequently identified and reported locally, often has global connections, especially when using cloud services, hosts and other international services. The vulnerabilities have given CERT Vanuatu a better understanding of what types of cyber-threats Vanuatu could be facing or expecting in the years to come. Thus, necessary security measures are continuously introduced, developed and taken to address these vulnerabilities from escalating into severe cyber-attacks.

Furthermore, there are other forms of vulnerabilities and threats seen in Vanuatu that involves online abuse and harmful digital communications (HDC) over the Internet and online platforms. The known online social threats are often caused by Internet users and are targeted towards both the government of Vanuatu and private sector organizations which automatically targeting Internet users who are caught up in between social issues in Vanuatu. This is a rising cyber safety issue and concern for the government and communities which must be addressed through policies, strategies and security best practices and mechanisms such as through the establishment of an ‘eSafety commission.’

3.3 Reported and Recorded Cyber-threats in Vanuatu

Given there are vulnerabilities identified in the networks and the cyberspace in Vanuatu, there has been a number of cyber-threats reported and recorded by CERT Vanuatu and its joint partners. The cyber-threats in Vanuatu are observed or detected across all domains and constituents of CERT Vanuatu, i.e. in both the government systems and networks, the private sector organization systems and civil society.

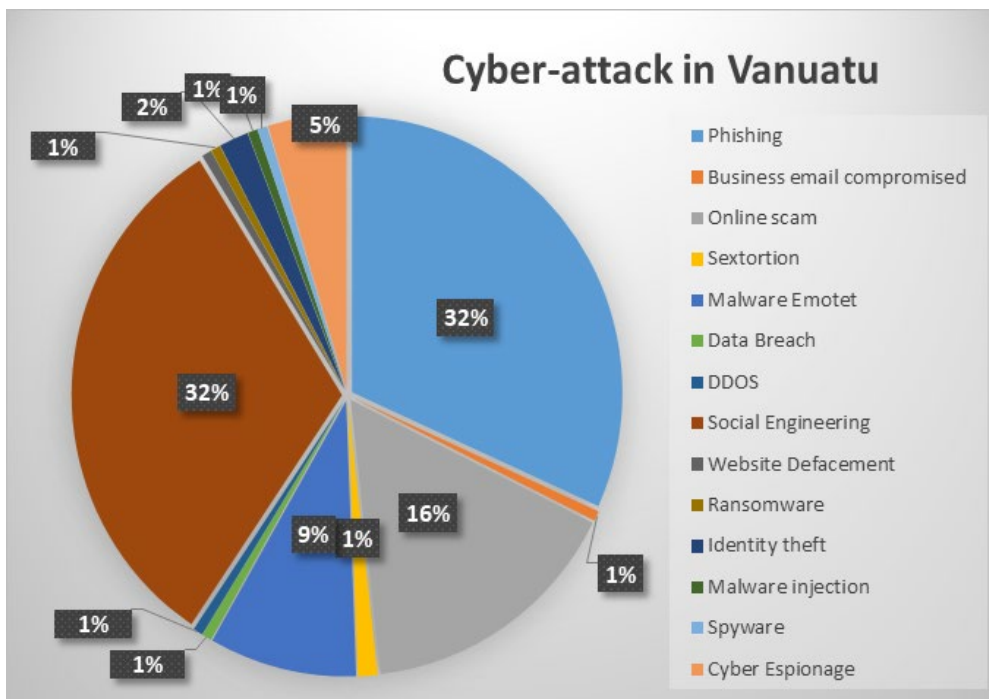


Figure 1: Reported Cyber-threats in Q1, Q2, and Q3 of 2020

Figure 1 provides an account of the reported and recorded cases by the CERT Vanuatu office this year - 2020. This analysis is based on Quarter 1 (Q1), Quarter 2 (Q2) and Quarter 3 (Q3) of 2020. As observed in Figure 1, Phishing attacks (it accounts for 32% of the reported threats.) and Business Email Compromises (BEC) (32%) are the current common threats to Vanuatu’s Internet and cyberspace.

However, compared to 2018 and 2019, the reported incidents cyber-threats/attacks collected and mitigated by CERT Vanuatu are of a smaller recorded volume which are summarized in Figure 2. Appendix 2 in the Appendices section of this strategy provides thorough details of the types of cyber incidents reported to the CERT Vanuatu office. These treats were reported using either emails, phone call, website portal and, or walking into the office and reporting the incident. The 2018 and 2019 incident reports were mainly from Government agencies and not as much from the private sector or communities.

Abuse of Social Media and Violation of Online Privacy:

Another prominent cyber-threat or issue faced in Vanuatu and globally is the 'abuse of Social Media and violation of Online Privacy.' The previously mentioned reported cyber-threats and attacks are not the only threats to Vanuatu's national security.



Figure 2: Types of Reported Cyber-threats in 2018 and 2019

The use of social media in Vanuatu to infiltrate and abuse peoples' personal privacy is also a critical issue. For example, posting pieces of information (images, snapshots of text messages, etc.) of a person without getting consents or approval do cause issues in communities, societies and even in organizations. Although the information posted can either be legitimate or not, it is a breach of one's privacy. Other cases involve sharing of pornographic materials in closed and secret social media groups which is a recurring issue in Vanuatu. In summary, social media in Vanuatu brings about the following issues and social media-enabled crimes such as:

- ❖ *Cyberbullying or Cyberstalking;*
- ❖ *Social Engineering;*
- ❖ *Infiltrating online personal privacy;*
- ❖ *Shaming and spreading hate speech to entertain bigger issues;*
- ❖ *Having possession and/or sharing of pornographic materials;*
- ❖ *Sextortion and online abuse;*
- ❖ *Encouraging and spreading of fake news; and*
- ❖ *Data Leakage (Leaking sensitive information to the public)*

The above social media issues are based on reported cases. They are not directly associated with cyber-threats to Vanuatu but has an impact on the societies and communities in Vanuatu.

3.4 Cyber Security Development in Vanuatu

Vanuatu's liberty, prosperity and security depend upon an open and reliable access to information and Internet. Hence, it is crucial that information security (Confidentiality, Integrity and Availability | The CIA Triad) and its application, forms the bases to proper information sharing and all processes associated with facilitating the act of sharing information.

The Internet empowers technology users and improves lives by providing greater access to new knowledge, essential services and businesses in Vanuatu and globally. While, the Internet and

technologies enhance daily living, the need to secure and protect citizens must be the core of business models, policies and strategies. High-level dialogues are encouraged whereby top-level management must lead as well as take ownership of the cyber security affairs in Vanuatu. Over the years Vanuatu has transitioned progressively and effectively through the ICT and Cyberspace development, and these efforts are summarized in Figure 3. It is also crucial that Vanuatu must identify and strive to strengthen National Security by protecting its cyber-border at all times. Therefore, to leap forward in terms of cyber security or national security, Vanuatu must portray and envision a practical, yet robust national security hierarchy system. This will ensure a holistic development approach is entailed and executed to achieve Vanuatu's 2030 cyber security Priorities.

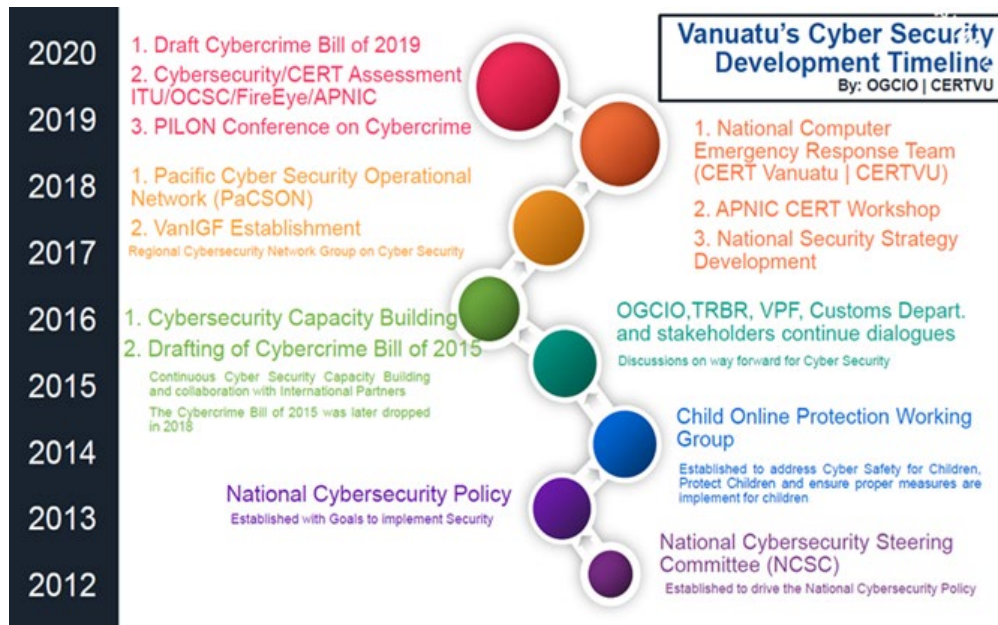


Figure 3: Cyber Security Development over the past 10 years

3.5 The Ideal National Cyber Security Hierarchy at Glance

The National Cyber Security Strategy (NCSS) of Vanuatu is summarised in numerous ways. Figure 4 depicts a proposed future National Cyber Security framework that provides the ideal security hierarchy at a glance. It portrays the expected National Cyber Security framework with respect to the needs of Vanuatu on how National Security is designed with the need of including various leading agencies.

The purpose of the National Cyber Security hierarchy in this strategy is to help pave the way for Vanuatu's Cyber Security priorities. It is a visionary and ideal holistic security perception displayed in this strategy to help decision makers, technical experts and readers. Such holistic view provides an overview of how various entities or components of the Cyber Security hierarchy interact with each other. For example, various agencies established under this ideal framework have a purpose which directly links to Vanuatu's National Security, the Cyber Security layer and finally the Information Security and Governance layer as shown in Figure 4.

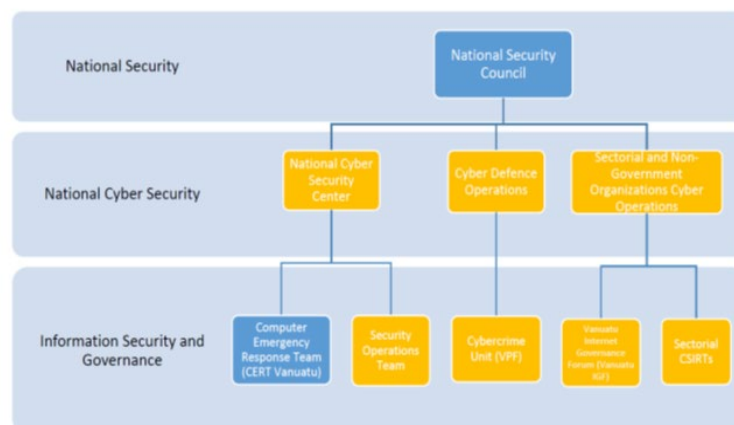


Figure 4: The National CyberSecurity Hierarchy Overview

Overall, the hierarchy must be designed and developed in a thoughtful philosophical manner to cover all levels of Cyber and Information Security (IS). It is only through such development that proper incident response operations are able to address cyber-threats, attacks and issues. This is made easy by establishing a clear incident response mitigation plan and an incident response recovery plan. Furthermore it also provides the ability to further understand and identify cyber-threats that can aid effective decisions based on the structure established through the hierarchy.

3.6 The National Cyber Security Maturity Model

A national economy values critical assessment mechanisms to stay healthy and in moving forward to building a stronger vibrant economy as well as a strong cyber security framework. In cyber security, maturity model assessments and certifications are a form of assessing the National Security status of a country. An ideal cyber security maturity model offers an accelerative pathway which enables Vanuatu to periodically assess where it is within the term of this cyber security strategy plan. The maturity model has been a valuable tool for improving cyber security efforts that are outlined in this strategy, as well as communicating and obtaining the necessary support from upper management, boards, and Council of Ministers (COM). As part of the Vanuatu National Sustainable Development Plan (NSDP) goals and objectives which is echoed in 'Pillar 5' of the National Security Strategy of Vanuatu states that 'Cyber Security' is a priority. Thus, the maturity model helps maintain efforts in aligning and achieving the broader National Security goals.

The Capability Maturity Model Integration (CMMI) framework is an example of a well-known process measuring and improvement meta-framework that helps organizations measure their processes' effectiveness [9]. It also helps identify how to improve these processes over-time.

CMMI has five maturity levels, which follow the original guidelines of Capability Maturity Model (CMM) [9]. These levels are:

1. **Initial:** *Processes are somewhat ad hoc and undefined aside from localised documentation.*
2. **Managed:** *Processes are managed in accordance with agreed metrics, but there is no focus on assessing efficacy or gathering feedback and while processes are followed there is no notion of their success. Processes are not consistent across the business.*
3. **Defined:** *Processes are well-defined and acknowledged as standard business processes, and are broken down into more detailed procedures, work instructions and registers (artefacts) used to record process outputs.*
4. **Quantitatively Managed:** *Metrics are gathered from each process and are fed back to a process governance committee who analyze and report on process efficacy.*
5. **Optimizing:** *Process management includes a focus on disciplined optimization and continual process improvement, and a full team of business analysts who measure and assess every aspect of the business for possible issues and improvement opportunities.*

Based on the CMMI 5 levels of maturity, a similar approach was adopted and executed by Vanuatu in 2019. This CMM assessment was conducted by the Oceania Cyber Security Centre (OCSC) [10] and the International Telecommunication Union (ITU) [11] in partnership with the Government of Vanuatu through CERT Vanuatu and the Office of the Government Chief Information Officer (OGCIO). The maturity assessment has paved a pathway to prioritize cyber security as a national objective for Vanuatu.

The CMM assessment utilized the Global Cyber Security Capacity Centre's (GCSCC) cybersecurity Capacity Maturity Model (CMM), which defined the five (5) dimensions of cybersecurity capacity:

1. *Cybersecurity Policy and Strategy;*
2. *Cyber Culture and Society;*
3. *Cybersecurity Education, Training and Skills;*
4. *Legal and Regulatory Frameworks; and*
5. *Standards, Organizations and Technologies.*

These maturity model dimensions are seen as reasonable essential cyber security indicators required to address Vanuatu's current cyber security status whereby, the Vanuatu's National Security and sovereignty is improved, strengthened, secured and protected. These indicators are the basis of the

National Cyber Security Strategy approach 2030 that provide recommendations and pathways for further development, studies, and implementation of security frameworks.

The CMM assessment report presented to the Government of Vanuatu outlines Vanuatu's cybersecurity maturity status with the 5 established dimensions of cybersecurity capacity as shown in Figure 5:

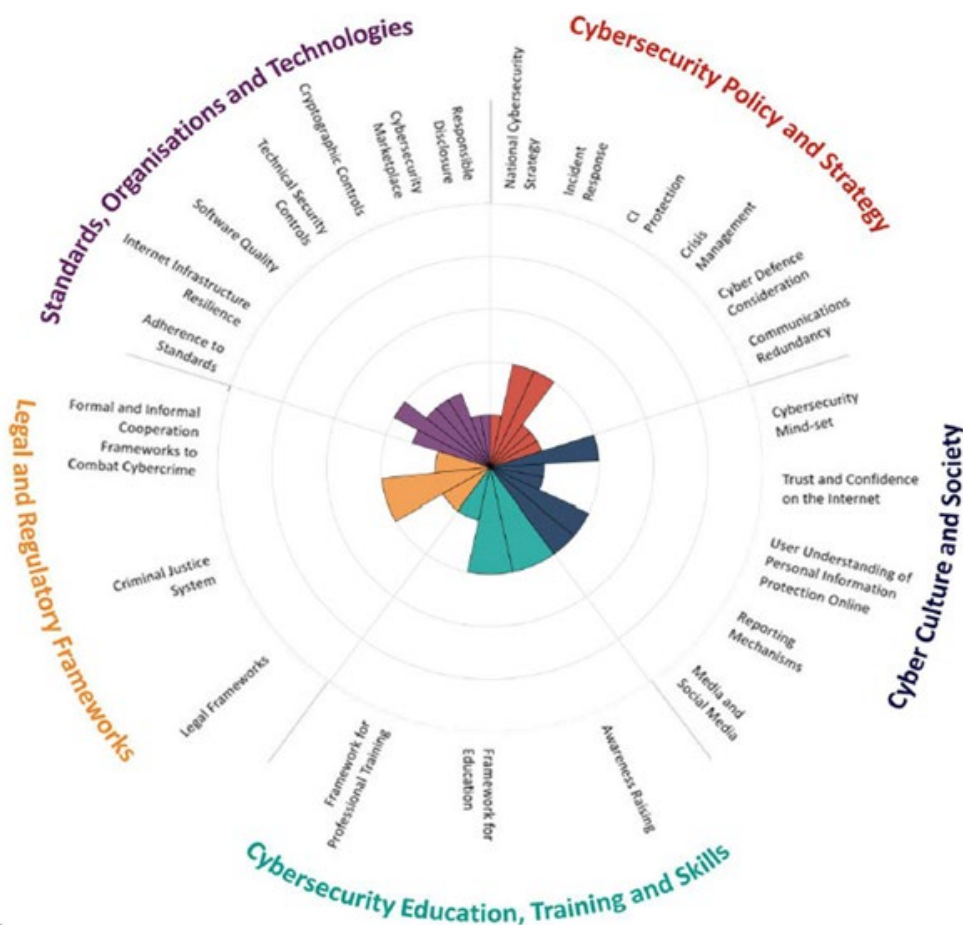


Figure 5: The Overall representation of the Cybersecurity capacity in Vanuatu – 2018

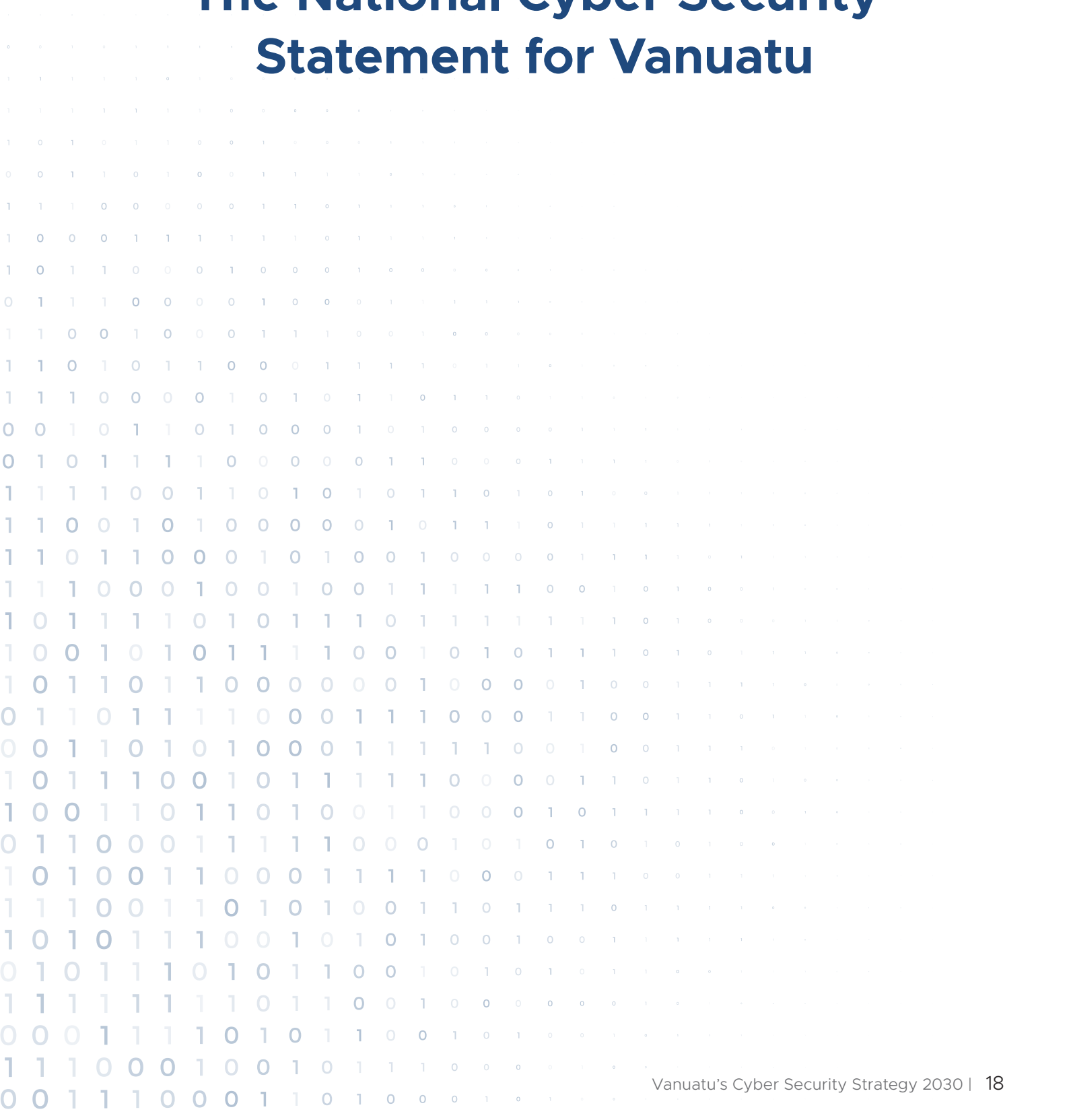
In summary, Figure 5 shows an overall representation of Vanuatu's CMM cybersecurity capacity using the maturity model that illustrates the maturity estimates in each of the five dimensions. Given the fact that this cybersecurity capacity maturity assessment was executed in 2018, this National Cyber Security Strategy will not dwell on the outcome and recommendations but acknowledge all indicators and recommendations identified. To conclude, these CMM dimensions and recommendations including the execution of the National Cybersecurity policy of 2013 goals and objectives help contribute to the development of this strategy.

¹ The CMM Cybersecurity capacity maturity report for Vanuatu can be accessed using the following link: Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition> (accessed 25 February 2018).

PART 02



The National Cyber Security Statement for Vanuatu



4.0 National Cyber Security Vision Statement

Security is about securing and protecting technologies, processes and most importantly about protecting people. It has been famously quoted “Security is everyone’s business” and therefore, it needs a holistic effective approach with robust solutions to address the ever increasing frequency and sophistication of cyber-attacks.

“National Cyber Security Strategies can take many forms and can go into varying levels of detail, depending on the particular country’s objectives and levels of cyber-readiness. Therefore, there is no established and commonly agreed definition of what constitutes a National Cybersecurity Strategy.”

The National Cyber Security vision is supported, guided and echoed through numerous goals of the National Sustainable Development Plan – 2030, the National Security Strategy and through the National Cybersecurity Policy of 2013. To be precise, it is stated in the Vanuatu National Sustainable Development Plan (NSDP) 2030 in 3 pillars namely the Society Pillar-5 (SOC5): Security, Peace and Justice; the Environment Pillar-2 (ENV2): Blue-green Economic Growth; and in the Economic Pillar-2 (EOC2): Improve Infrastructure in Vanuatu usually require the national critical infrastructure to be secured, protected and well managed. These NSDP Goals and objectives endorses the implementation of the National Security Strategy of 2019 in which Pillar-5 of the National Security Strategy pledges the need of the National Cyber Security Vision.



The National Cyber Security Vision of the Republic of Vanuatu recognizes an open, secure and protected Internet or cyberspace, where all citizens of Vanuatu and tourists who visit Vanuatu ought to enjoy the luxury of a fast Broadband service. This vision is also shared among all critical infrastructure and businesses whereby an enhanced interoperability capability is encouraged in all business continuity services and processes. In addition, the utilization of the essential services by all sectors such as in ICT services and, or the use of Internet of Things (IoT) for information sharing, access and data collection. The National Cyber Security vision strives to establish security mechanisms to enable organizations and users to access a secure and safe Internet with no fear of being a victim of an organized or an unintentional cyber-attack, cybercrime and, or cyber-enable crimes.

As a nation, both National Security and Cyber Security frameworks outlining approaches require a broader vision with sets of goals and objectives to support action plans. This means the entire National Cyber Security framework should co-exist as a process at all levels of government, organizations, communities and schools. These processes will provide assurance to all cyber security personnel, stakeholders and organizations with an effective sustainable level of security. From a broader national

Our Vision



Vision

Our Vision for the Republic of Vanuatu in 2030 is:

1. To create a secure, self-taught and cyber security-aware capability environment for Vanuatu citizens and business organizations by creating a better protected mindset for all citizens while being online; and
2. To improve cyber security resilience, cyber hygiene and ensure cyber-threats preparedness of our borders and cyberspace are effectively active for a better National Security.

Mission

We strive to create a proactive Cyber Security framework to secure and protect business operations by ensuring an increased and improved two-way information sharing channels whereby information security must be adhere to at all times.

Goals

In order to achieve this national vision for cyber security by 2030, the Republic of Vanuatu aims to:
To be Resilient, Strengthened, Secured, Protected and be Cyber Security-aware in Vanuatu.

Figure 6: The National Cyber Security Vision, Mission Goals of Vanuatu.

vision, a secure, cultivated and protected cyber security mindset is crucial and a defensive mechanism for every citizens in Vanuatu to ensure that they equip themselves to embrace the concept of resilience (cyber resilience). To be resilient means all citizens of Vanuatu will have the ability to identify cyber-threats and are able to efficiently adapt to change especially when users are less exposed to risks and in situations where citizens are able to leap from disasters.

5.1 Vision

Our National Cyber Security vision for the Republic of Vanuatu is:

1. *To create a secure, self-taught and cyber security-aware capability environment for Vanuatu citizens and business organizations by creating a better protected mindset for all citizens while being online; and*
2. *To improve cyber security resilience, cyber hygiene and ensure cyber-threat preparedness of our borders and cyberspace are effectively active for a better National Security.*

5.2 Our Mission

We strive to create a proactive Cyber Security framework to secure and protect business operations by ensuring an increased and improved two-way information sharing channels whereby Information Security (IS) must be adhere to at all times.

5.3 Cyber Security Goals

In order to achieve this vision by 2030, the Republic of Vanuatu aims to achieve the following broader Goals (Figure 6):

Goal 1: To secure and protect our critical infrastructure and cyberspace thus, create and enforce proactive security mechanisms against cyber-threats and cybercrime in Vanuatu.

Goal 2: To enhance resilience aimed at robust Incident Response (IR), information security, business continuity and overall organizational resilience from cyber-attacks and have the ability to defend against the full range of threats.

Goal 3: To increase cyber security awareness through a multi-stakeholder unified approach that will ensure all critical infrastructure users and Internet users understand cyber security and cybercrime.

Goal 4: To develop effective communications and collaborative security frameworks between all levels of authorities, stakeholders, private sector organizations and communities for the purpose of

effective Information Sharing.

Goal 5: To cultivate cyber talents and increase cyber capability in order to boost and improve our National Security and cyber defense environment.

Goal 7: To improve and expand International Engagement on National Security and Cyber Security.

Goal 8: To increase cyber education, literacy and cultivate cyber experts in order to build a cyber-security culture that will safeguard Vanuatu's assets, data and critical infrastructures.

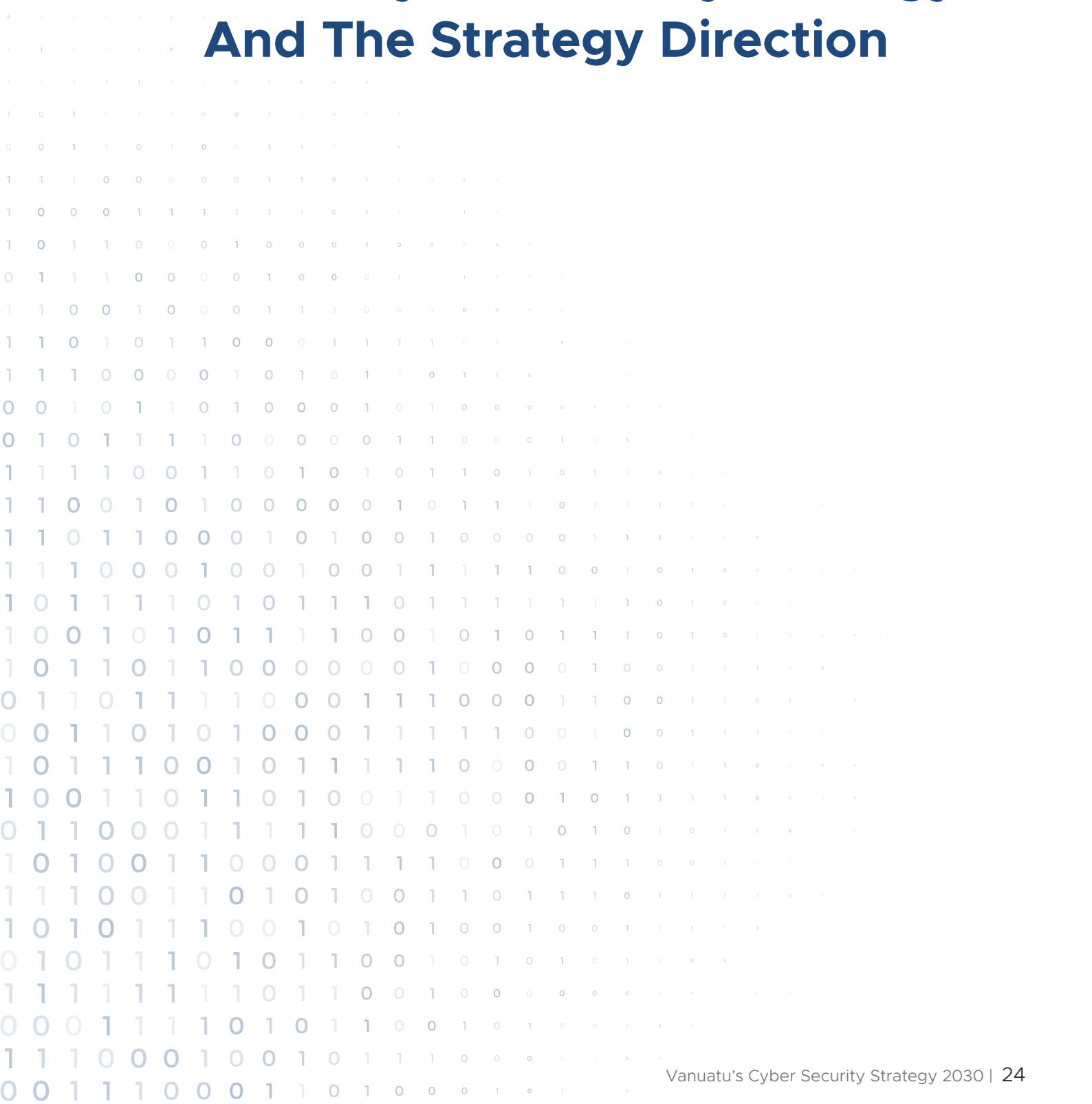
Goal 9: To design, develop and implement various cyber security guidelines, standards, regulations and legal frameworks in order to enable business continuity and better trading of goods and services in Vanuatu.

These national strategy goals are further communicated and expanded in Section 7.0 of the Strategy in the 'Action Plan'. The action plans are outlined in each of the six priorities detailing various objectives required to ensure Vanuatu continues its efforts in Cyber Security.

PART 03



The National Cyber Security Strategy And The Strategy Direction

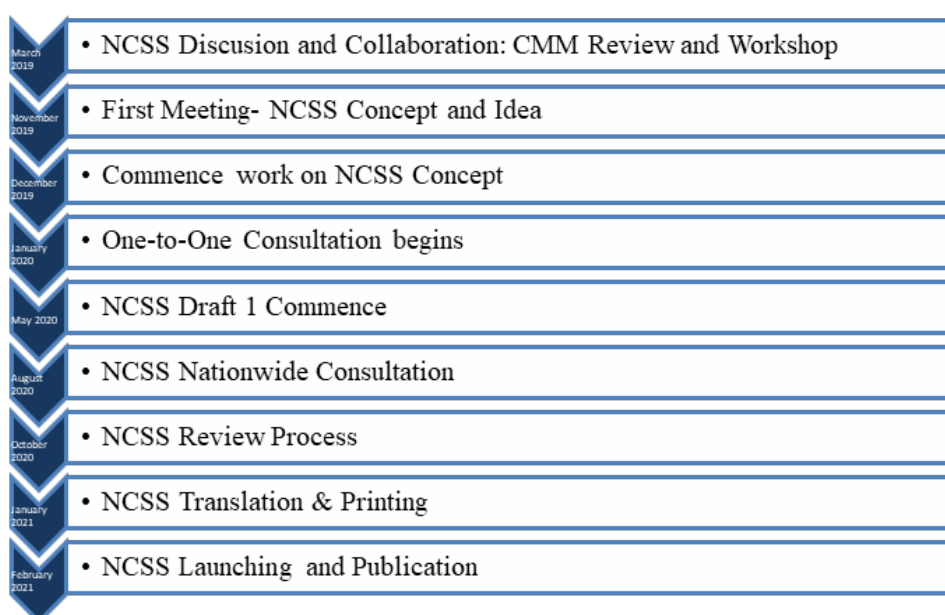


5.0 The Strategy Consultation Process

The vision, mission and goals of the cyber security strategy has provided a visible interpretation where issues are well analysed, cyber security barriers are removed, and 6 critical priorities are identified as the core elements of the national cyber security action plan for the next ten years. Prior to providing the National Cyber Security priorities of Vanuatu, the national cyber security consultation approach is discussed to provide the implementers and viewers of this strategy with a clear understanding on the efforts, integrity and the depth of the strategy development.

5.1 The Strategy Consultation Timeline

The National Cyber Security Strategy (NCSS) is designed and developed according to numerous national security requirements and needs to ensure Vanuatu's National Security is robust. The summary of the strategy development timeline is shown in the flow diagram and in Figure 7. This timeline outlines all NCSS phases and the milestone dates.



In addition, the aim of the NCSS development timeline is to show various key development phases. These covers assessments, consultations, reviews and the translation processes. The phases are categorised into three main groups:

- ❖ *Information Gathering Phase;*
- ❖ *Information Processing Phase; and*
- ❖ *Information Reporting Phase.*

Within the three development phases, there are four critical stages required for the successful development of the National Cyber Security Strategy (NCSS):

- ❖ *Design;*
- ❖ *Development;*
- ❖ *Review; and*
- ❖ *Launching of the strategy.*

These development phases outlined in Figure 7 remain valuable in warranting all cyber security priorities and action plans are identified and included for the benefit of this National Cyber Security Strategy.

5.2 The Strategy Consultation Execution Methodology

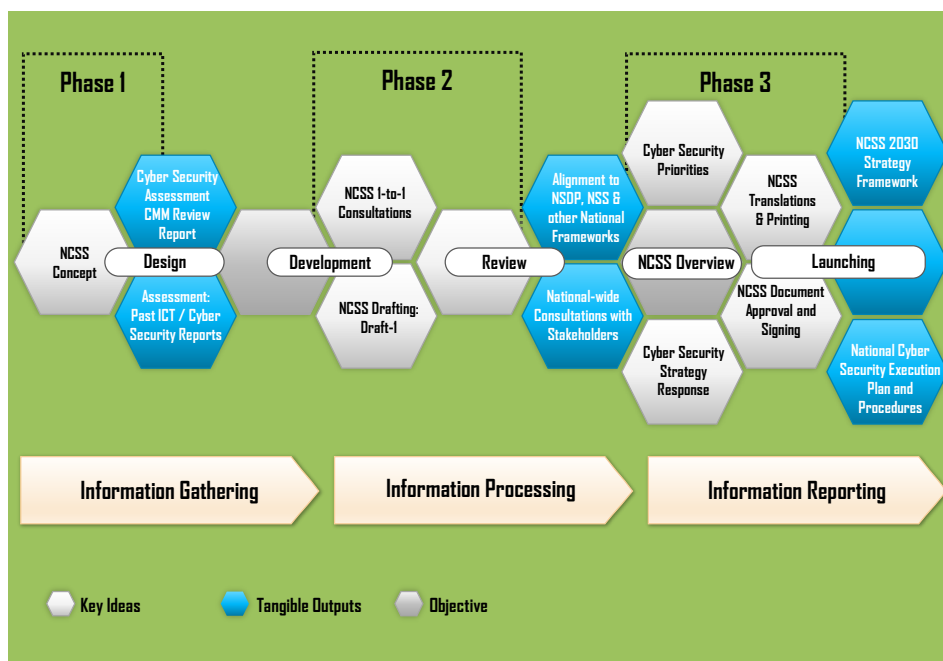


Figure 7: Cyber Security Development Timeline with critical phases

The development of the Strategy required numerous methodologies to ensure all cyber security components are captured. This meant that a careful assessment on existing cyber security infrastructure, capacity capability, the cyber-threat landscape and the broader government policies and strategies are carried out. It also meant that including crucial security components for this strategy will cater for, and provide top-level priority needs that will go in line with both the National Security Strategy and the National Sustainable Development Plan of 2030. As a result, it will achieve various important national goals and objectives in the cyberspace and Information and Communications Technology (ICT) realm.

The strategy pathway requires that all cyber security and critical infrastructure stakeholders were consulted to capture and determine current cyber security needs, risks, issues and challenges that hinder business continuity and processes. Addressing the challenges and issues aids the implementation of this strategy in achieving and maximising economic benefits.

The National Cyber Security Strategy is designed to enable all government agencies, statutory bodies, non-government organizations (NGOs), private sector and the civil society to execute various plans as well as identify and follow a relevant effective strategical cyber security framework for Vanuatu.

Hence, the strategy consultation outcomes are aimed at achieving the following:

- ❖ *Provide primary guidelines for all cyber security infrastructure implementation in Vanuatu;*
- ❖ *Build on the National Cybersecurity Policy and the National Security strategy to formulate key government policies and essential services with cyber security requirements – i.e., build government or business operations around cyber security and by developing a cyber-security culture;*
- ❖ *Implement proper cyber security frameworks to secure and protect all citizens and international visitors accessing Internet, technology services and other essential services in Vanuatu; and*
- ❖ *Provide for, and guide the sharing, access and dissemination of information in Vanuatu and across international borders. This requires the adoption and enforcement of various information security best practises such as the ‘Information Sharing’ and ‘Traffic Light Protocol (TLP)’.*

5.3 The Strategy Consultation Coverage and Demography

The National Cyber Security Strategy consultation procedure has utilized two primary methods and covers in total an approximately 10,946 attendees who are from all sectors. These 3 consultation methods are:

a) One-to-one Consultation Method:

The approach with the “One-to-one” consultation (Figure 8) refers to specific consultation meetings with certain stakeholders who are involved with cyber security and information communication technology in Vanuatu. Basically, this include all critical infrastructure in Vanuatu. The one-to-one consultations serve the purpose of identifying current cyber security mechanisms that are implemented by organizations in Vanuatu. These consultations include government ministries, departments, agencies, regulatory institutions, private sector organizations, academics, international partners and non-government organizations.

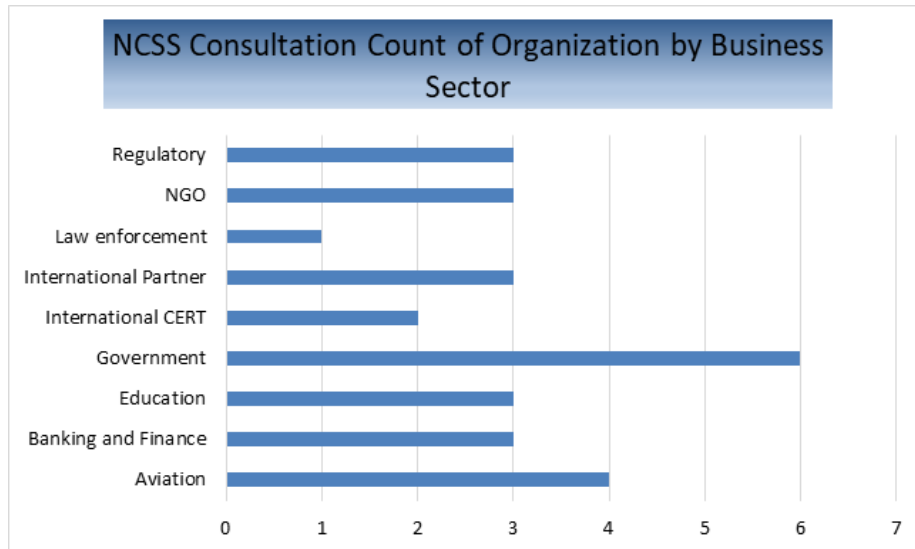


Figure 8: Cyber Security Strategy One-to-One Consultation Sectors

b) Nationwide Consultation Method:

The Nationwide consultation throughout all 6 provinces of Vanuatu was based on a strategic consultation delivery approach that utilized existing Information sharing and communication platforms throughout Vanuatu. This was made possible through the existence of the Ministry of Internal Affairs - Area Council contacts who are known as “Area Administrators” and “Area Secretaries”. These roles are permanent positions with the department of Local Authorities and their roles were established as a part of Vanuatu’s decentralization plan into the rural areas of Vanuatu.

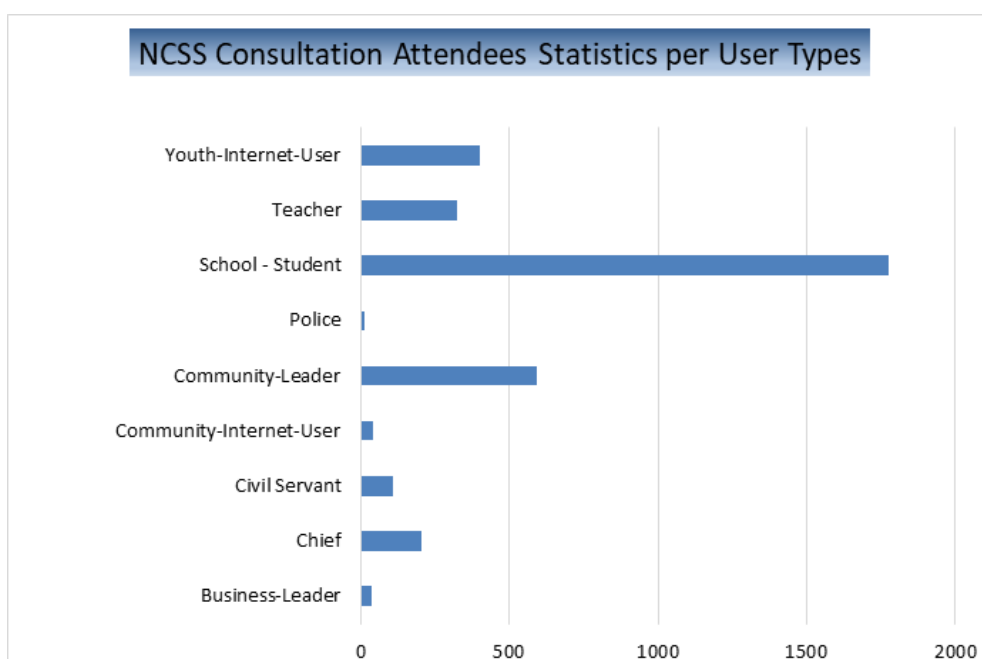


Figure 9: Cyber Security Strategy Nationwide Consultation Attendees Statistics by User Types

Figure 9 shows the statistics of different types of users who attended the consultations in various locations of Vanuatu. Users that attended the consultations were selected and invited based on their potential contribution as leaders and decision makers in businesses, communities and societies in Vanuatu.

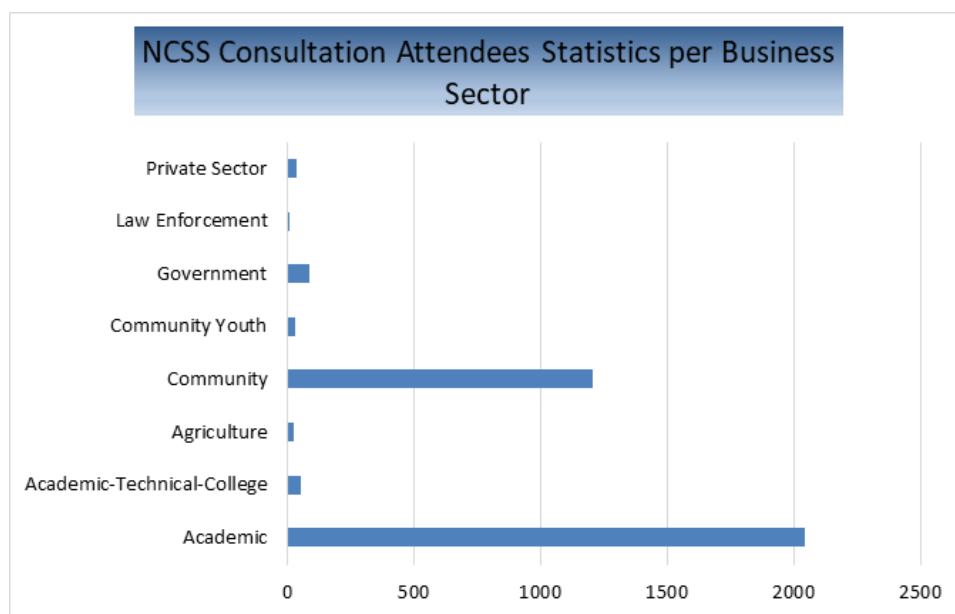


Figure 10: Cyber Security Strategy Nationwide Consultation Counts by Business Sectors

Based on the statistics collected the relatively high number of attendees for these consultations were school students (primary & secondary schools and university students) and community leaders. Community leaders include religious and cultural leaders, chairpersons, women leaders,

People living With Disability (special needs) representatives and the area secretaries and administrators of the various area council in Vanuatu. School students and youths are vital for this consultation as they make up around 70% of the population that uses the Internet and technologies in Vanuatu. Interestingly, village chiefs have positively acknowledged the urgency and importance of these consultations and have voiced their concerns, needs and proposed thoughts for the National Cyber Security Strategy.

Figure 10 portrays a different view of the types of organizations present during the consultation session throughout Vanuatu. The graph clearly shows that most users who attended are from the academic followed by the communities. The consultation data highlighted the number of Internet or technology users in the communities who have issues are victims of cyber-threats, and it also displayed the most vulnerable group in Vanuatu.

The nationwide consultation findings evidently supports the need to further reach out to the wider communities with vital cyber security services and awareness programs to help secure and protect businesses and citizens from cyber-attacks. Various comments and feedback from these consultations have outlined critical issues in both the urban and rural communities of Vanuatu. These issues include the increase of cyber-threats and online social abuses which are causing harm to Internet users throughout Vanuatu.

c) The Targeted Consultation Method:

The final consultation method utilized for this strategy is the 'Targeted' Consultation method which targeted our development partners, working-partners, academics, and other technical experts in the field of Cyber Security and Government Diplomatic Partners.

The Development Partners played a vital role in this consultation and strategy as Vanuatu must align its strategy with the bigger regional and global Cyber Security strategies to combat cybercrime. Similarly, working-partners are our core partners in ensuring this strategy must be in line with all yearly work plans as well as their respective roles and tasks to addressing cyber security issues and cyber safety issues. Academic consultation representatives also played an important role in providing research

theories and critiques which will test the capability and response action plans on whether they are achievable or not.

The 'One-to-one' consultations, the 'Nationwide' consultations and the 'Targeted consultations have great benefits for development of this Strategy and the future cyber security agenda. The consultations have brought out the following key findings:

- ❖ *The identification of Cyber-threat statistics in throughout Vanuatu;*
- ❖ *The need to increase Cyber resiliency and International engagement;*
- ❖ *The need for the establishment of a National Cyber Security Agency;*
- ❖ *The need to increase Cyber Security Awareness programs;*
- ❖ *The need to increase in cyber capabilities which will help combat cybercrime;*

- ❖ *There is critical need for an Information Sharing Platform or Resource Centre; and*
- ❖ *Recommendation to design and develop community ICT and Cyber Security Standards, Regulations and community bylaws to enhance community policing.*

The consultations has highlighted the urgent need for cyber security and ICT standards, regulations, and legal framework development. Consultation attendees have emphasized the need for legislations, standards, regulations and community bylaws to be developed and enforced on the use of technologies and age restrictions in communities and villages.

6.0 Cyber Security for National Critical Infrastructure in Vanuatu

The Government of the Republic of Vanuatu is committed to its economic independence and self-reliance through cross-sector trade efforts. This commitment and determination has by far proven maturity to-date through major developments. Some of these developments in the Information and Communication Technology (ICT) and Telecommunications sector include the establishment of the Government Broadband Network (GBN) infrastructure, the National Cybersecurity Policy, the National Security Council, the National Security Strategy and the establishment of the Vanuatu National Computer Emergency Response Team (CERT Vanuatu | CERTVU). The developments highlighted above are part of the entire Vanuatu National Infrastructure.

“National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organizations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public.”

- UK CPNI.

In the Critical Infrastructure (CI) context, Cyber Security is usually a missing piece that poses an increasingly urgent risk to any nation or organization. The risks associated with critical infrastructure relate to either national disasters or Cyber-attacks. These risks and Cyber-attacks present unique sophisticated challenges [8] such as:

- ❖ *Cyber-threat or attacks lack distinct borders;*
- ❖ *Threat or attack tactics and technologies are constantly evolving and increasing in frequency;*
- ❖ *Public and private sector entities that manage critical infrastructure lack the following best practices; coordinated efforts, information-sharing processes, and effective standard operating procedures.*

Evolving technologies have also contributed to the increased risks in organizations but at the same time provides a greater level of protection against threats. The use of integrated robust Cyber Security methods can defend against malicious activities and anomalies in systems and networks. In addition, evolving technologies allow interconnectivity and interoperability between online essential services, processes and the security systems implemented to protect Vanuatu's critical infrastructures. Interconnectivity and interoperability platforms and services bring in efficient service delivery and as

well as broaden the scope and target for cybercriminals. Hence, it is crucial for organizations to defend against risks associated with evolving technologies.

However, the use of technology alone is not the only solution to successfully manage risks associated with sophisticated cyber-attacks. It is important that organizations in Vanuatu be more strategic about their ICT and Cyber Security approaches, and must continuously assess existing defences. Executing plans such as investing in ongoing Cyber Security capacity building programs, policies, regular incident response drills, and providing Cyber Security awareness campaigns are ways to achieving National Security. Furthermore, working effectively with collaborative partners that strengthen cyber security capabilities is an essential tool that can help Vanuatu and businesses to increase and improve cyber resiliency and literacy. Increased Cyber literacy will help combat the rise in cyber-attacks and cybercrime activities in Vanuatu, and across the globe.

The National Cyber Security Strategy (NCSS) values and highlights the importance of Cyber Security for National Critical Infrastructure. It is important that all National Critical Infrastructures are identified and associated formally to lead agencies to ensure they take full responsibility and have that sense of 'ownership.' Such ownership encourages and motivates commitment that will drive appropriate security efforts to secure and protect Vanuatu.

6.1. Critical Infrastructure Sectors

The urgency of protecting Vanuatu's critical infrastructure and ensures this strategy identifies all lead agencies, organizations, and recognize the types of critical infrastructure and their impacts on Cyber Security. Figure 11 outlines all Critical Infrastructure and their respective lead agencies and organizations.

Cyber Security Critical Infrastructure Sectors

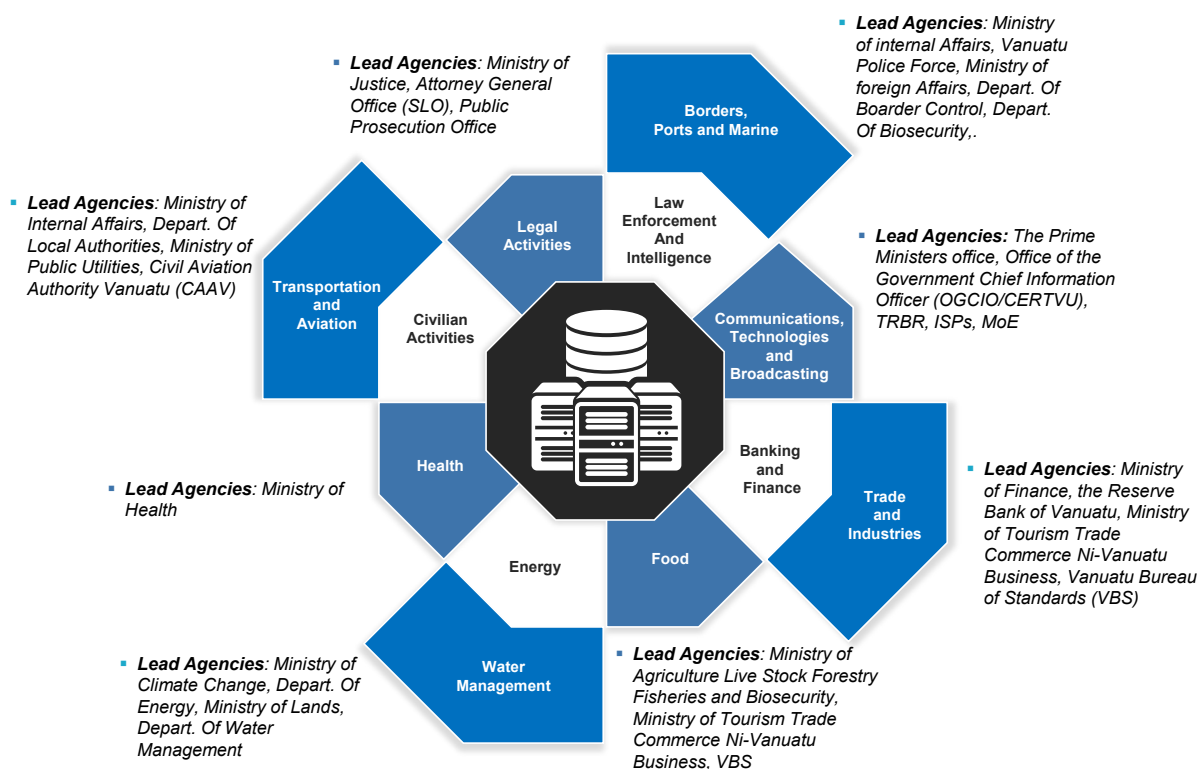


Figure 11: Critical Infrastructure Sectors for Cyber Security in Vanuatu

Figure 11 also emphasize the importance of protecting all critical infrastructure and not just the core Cyber Security infrastructure. Currently the CIs that are involved in Cyber Security development are:

- ❖ Communications, Technologies and Broadcasting;
- ❖ Law Enforcement and Intelligence;
- ❖ Legal Activities;
- ❖ Civilian Activities;

- ❖ *Banking and Finance; and*
- ❖ *Borders, Port and Marine.*

However, this approach needs to change. As illustrated in Figure 11, all other CIs in Vanuatu must be identified, protected and continuously monitored for Cyber Security development and efforts. Protecting all CIs will ensure all assets, technologies and people of Vanuatu are protected from Cyber-attacks.

The identified 'Lead Agencies' are institutions who will bear the responsibility and ensure up-to-date systems, technologies, Policies, Strategies and frameworks exist throughout all Critical Infrastructure organizations. The lead agencies must also capitalise on the existing 'Multi-stakeholder' collaboration, partnerships and information sharing channels to strengthen Vanuatu's Cyber Security framework and National Security.

7.0 National Cyber Security Priorities

Cyber-attacks knows no boundary and has no limitations to causing harm to a person or disrupting business operations from any location regardless of its origin. Past surveys and assessments have statistically indicated that cyber-attacks affect one in every five Internet users. This is a concerning issue that requires not only the cyber security experts attention but everyone's attention. It is of utmost importance that countries, institutions and individuals prioritize to invest in Cyber Security. However, prioritizing and investing in Cyber Security is not an easy exercise. It needs a shared vision between the Government, businesses and individuals on the importance of Security. This shared vision will maximize economic benefits, protect and secure Critical Infrastructures and citizens from Cyber-attacks.

Cyber security recapitulates measures involving the Confidentiality, Integrity and Availability (The CIA Triad) of information provenance. These measures require numerous cyber security approaches to be designed, implemented and enforced to safeguard the information of interest. While the need for effective cyber security frameworks are yet to be established, taking simple effective solution to tackle and address cyber security issues and cybercrime require a multi-stakeholder approach. This multi-stakeholder approach is the key to successfully implementing and enforcing Vanuatu's National Cyber Security priorities detailed in this Strategy of 2030.

NCSS VISION Approach

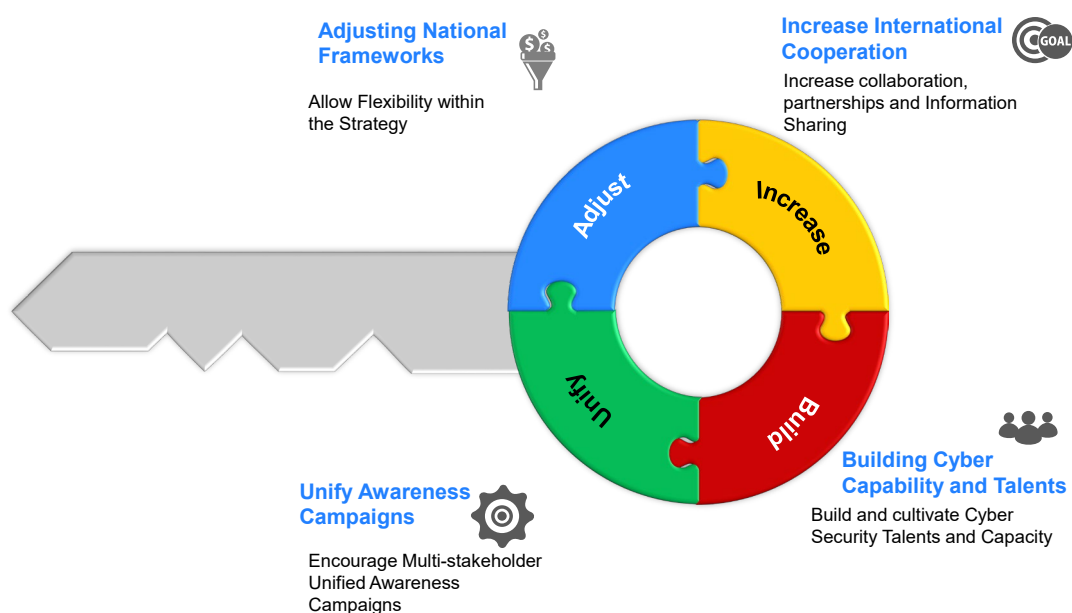


Figure 12: The National Cyber Security Strategy Vision Approach for Vanuatu.

In order to successfully achieve the goals, priorities as well as executing all responses or action plans outlined in this Strategy, Vanuatu must understand the entire critical infrastructure operations, user needs, trade and economic development that rely on technologies and the Internet. This strategy is designed and developed in a specific way to easily integrate itself into other National Frameworks without causing any hiccups or delaying various frameworks to not achieving their respective goals and objectives within the required timeframe.

The core of this Strategy provides the 'Ideal Vision' with its components which will enable the six National Cyber Security Priorities to be addressed in the next ten years. This vision entails the broader enforcement concept of the robust National Cyber Security Strategy which successfully relies on identifying, executing and enforcing a holistic approach of Vanuatu's Cyber Security Priorities as seen in Figure 12. The vision approach is greatly entrusted on the execution of the following specific actions:

- 1. Adjusting National Frameworks:** *This strategy understands and acknowledges the existence of other national strategies, policies, plans and frameworks which may have an impact or effect on the Cyber Security strategy development outcome. The strategy action plans and responses in Subsections 7.1 to 7.6 are ascribed to adjust, support and deliver all the National Cyber Security Priorities successfully.*

The recent graduation from a 'Least Developed Country' to a 'Developing Country' status, Vanuatu must develop robust yet flexible National frameworks to cater for the rapid rate at which technologies are invented and manufactured. Vanuatu must adapt and become more active, be responsive in developing and updating our National Cyber Security policies and strategies. These efforts contribute to the overall security frameworks which must include the technical, legal, regulatory and civil societies and will enhance cyber security mechanisms in Vanuatu.

- 2. Increase International Cooperation:** *Increasing International Cooperation as part of Vanuatu's Cyber Security vision approach is paramount and has strategical benefits to our National Cyber Security efforts.*

The International cooperation benefits are primarily for smart cyber incident response and the ability to increase a two-way information sharing capability and channel. 'Information Sharing' is crucial across all sectors in Vanuatu and foreign borders. It is important to maintain, increase momentum of the information flow and to formalize all cyber-related issues whereby international partnerships can contribute towards Vanuatu's Cyber Security operations. This process requires proper 'Information or Data Security' mechanisms. For example, 'Ransomware' cyber-attacks are lethal weapons used by organized cyber-gangs in the cyberspace; hence collaboration at the technical, law enforcement and policy levels will be vital to protect Vanuatu allowing relevant institutions to find solutions. Cyber Security needs International Cooperation through the establishment of formal and 'trusted' relationships. Overall, the establishment of trust between countries and businesses that have direct security impacts on Vanuatu's economy and welfare is paramount.

- 3. Unify Awareness Campaigns:** *Unifying Cyber Security Awareness Campaigns is the innovative vision approach that Vanuatu is embarking on to effectively deliver comprehensive security awareness throughout Vanuatu.*

Cyber Security awareness campaigns and capacity building programs are proven effective to improve cyber literacy, build technical experts and contribute to the overall building of a cyber-culture with a probable realization of a cyber-boundary and cyber sovereignty. It comes with the saying "No one is immune to a cyber-incident or one 'bad click'."

There is an urgent need to increase awareness for all age groups and levels in all sectors. In the era of rapid technological advancement and an increase of interoperability services, children and youths need to immerse themselves into technologies at a very young age in order to communicate efficiently and learn new skills that are vital to their livelihood. This brings in the concept of 'empowering' everyone to make the most out of such opportunity, while staying connected, protected and aware of the risks that the Internet and cyberspace can bring.

The Government of Vanuatu and the private sector institutions must utilize existing 'Multi-stakeholder' cooperation partnerships to unify awareness campaigns on cyber security, cybercrime, cyber safety and on harmful digital communications. For example, the annual joint

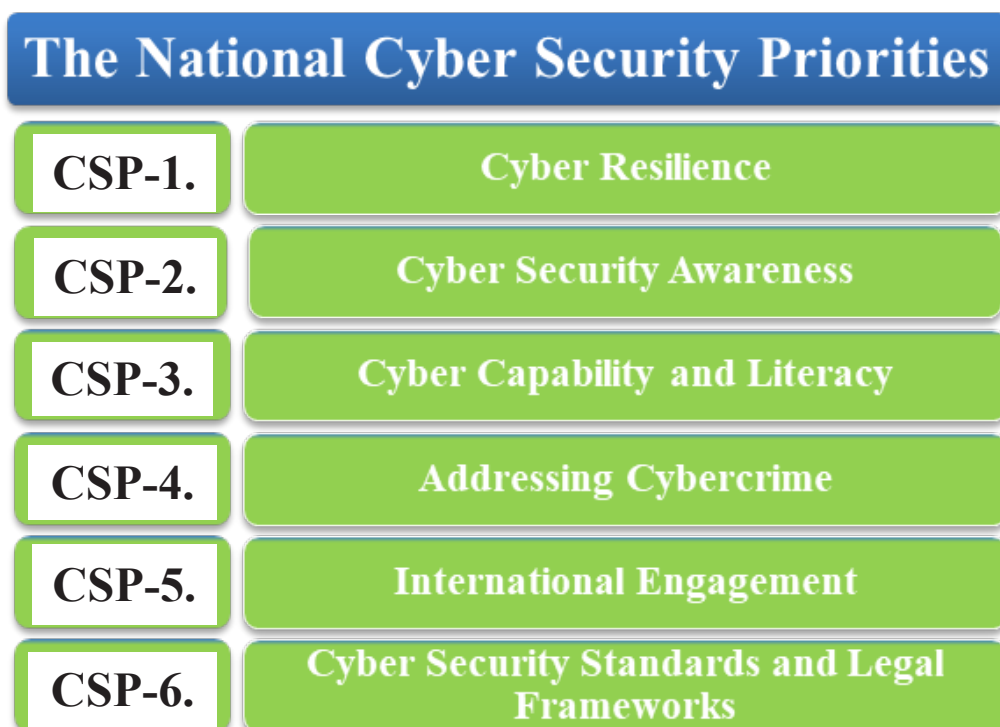
initiative by CERT Vanuatu and the ‘Pacific Cyber Security Operations Network (PaCSON)³ community’, - [Cyber Smart Pacific Month Awareness campaign⁴](#) and the “[Stop.Think.Connect.⁵”](#) are popular platform rallying on unified awareness campaigns on Cyber Security.

- 4. Building Cyber Capability and Talents:** *Building Cyber capabilities and talents is the backbone to Vanuatu’s Cyber Security vision approach and to a robust National Security. It is vital that Vanuatu must prioritize security by taking significant steps to build our cyber capabilities and talents with the aim of improving and creating a pool of knowledgeable resources which will be the first to respond to cyber security incidents and issues when identified.*

Current lack of cyber security experts across all cyber related professions calls for the need to establish capacity building mechanisms that will ensure Vanuatu has the capacity to Protect, Detect, Identify, Respond and Recover from incidents across all sectors. Vanuatu must formulate appropriate capacity building and training program plans. The program plans must be implemented from the National Bodies responsible for education, human resource development, policies and strategies, standards, legal, Information and Communications Technology (ICT) and security. It is also important to manage human resources effectively in order to accomplish bigger strategy goals and objectives.

The above specific actions perceive the need to collaborate in an environment involving critical partners and agencies to ensure our cyber security priorities are effectively developed and implemented. These collaborative environment capitalizing on multi-stakeholder frameworks motivates and enables the Government of the Republic of Vanuatu not only to see and use these formal collaboration channels but a need-to-establish connection and to work together in an organized manner for the advancement of securing and protecting our National Security. Therefore, executing multi-stakeholder operations permit better information sharing, sectoral analysis and assessments to help identify critical issues, risks and prospective solutions.

To date, cyber security issues, work plans and prospective solutions are derived and delivered through the following key National Cyber Security Priorities (CSPs) (Figure 13) for Vanuatu:



3 PaCSON is the Pacific Cyber Security Operations Network, a Cyber Security platform where all countries in the Pacific could collaborate together to share information, address cyber security issues, matters and cybercrime. An initiative by the Australian Government to support efforts in the Pacific region.

4 CERT Vanuatu’s Cyber Smart Pacific Awareness Campaign: <https://cert.gov.vu/cybersmart/>

5 STOP. THINK. CONNECT. is the global online safety awareness campaign to help all digital citizens stay safer and more secure online. URL: <https://www.stopthinkconnect.org>

Vanuatu's National Cyber Security Priorities



Figure 13: Vanuatu's National Cyber Security Priorities

7.1. Cyber Resilience

'Resilience' is generally defined as the capacity to recover rapidly from difficulties or problems. In the context of the National Cyber Security Strategy (NCSS) of Vanuatu, 'Cyber resilience (CSP-1)' is distinctive and defined as the ability to effectively prepare for, adapt, withstand, respond to and recover from cyber-attacks.

"Cyber-resilience is the ability to anticipate, withstand, recover and adapt to adverse conditions, stresses, attacks or compromises on systems that include cyber resources."
- NIST

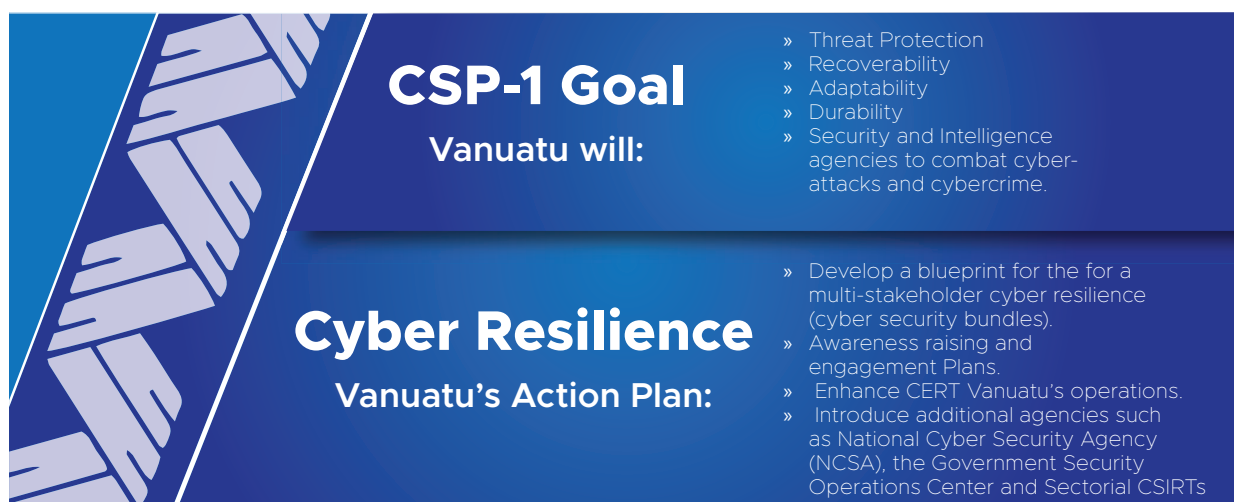
It is also defined as having the ability to be security-aware, be vigilant and have the ability to detect and identify cyber-threats. Thus, the national priority of cyber resilience is to help Vanuatu protect itself from cyber risks, defend against attacks by means of having the ability to limit the severity of attacks and ensure Vanuatu has a healthy and proactive cyber-resilience culture. The aim is to ensure Vanuatu continuously improves its Cyber Security efforts to strengthen National Security.

The recently launched 'National Security Strategy of 2019' stated that Cyber Security is a key priority that will help Vanuatu increase its strategic plans to further invest in improving Vanuatu's National Security by securing and protecting itself against cyber risks and attacks.

The ability to effectively identify and manage risks permits better prioritization of threat mitigation and reporting. As such, Vanuatu's emphasis is on implementing active and real-time measures to protect businesses, communities and citizens from a series of persistent attacks. These measures include establishing relevant policies and processes to help cyber resiliency in Vanuatu. The measures will also help organizations sustain operations, develop cyber resilience plans, cyber-preparedness plans, invest in tools and technologies, increase capability and execute long-term strategies with implementation plans.

The Cyber resilience priority will help protect Vanuatu's critical infrastructure and assets, improve incident responses and enable the development of a holistic risk management approach that forms part of our Cyber Security strategy.

These measures are set out through the following national goals and action plans shown below:



The infographic is a blue-themed graphic with a white diagonal line. On the left, there is a stylized illustration of hands clasped together. The text is organized into two main sections: 'CSP-1 Goal' and 'Cyber Resilience'. The 'CSP-1 Goal' section includes the text 'Vanuatu will:' followed by a list of five bullet points. The 'Cyber Resilience' section includes the text 'Vanuatu's Action Plan:' followed by a list of four bullet points.

CSP-1 Goal
Vanuatu will:

- » Threat Protection
- » Recoverability
- » Adaptability
- » Durability
- » Security and Intelligence agencies to combat cyber-attacks and cybercrime.

Cyber Resilience
Vanuatu's Action Plan:

- » Develop a blueprint for the for a multi-stakeholder cyber resilience (cyber security bundles).
- » Awareness raising and engagement Plans.
- » Enhance CERT Vanuatu's operations.
- » Introduce additional agencies such as National Cyber Security Agency (NCSA), the Government Security Operations Center and Sectorial CSIRTs

Vanuatu's Cyber Resilience Priority Goals:

Build a strong and robust Cyber Security posture and culture for Vanuatu, its businesses, communities and citizens including tourists.

Increase and improve core cyber security mechanisms to equip Government Cyber experts and other experts to have the ability to actively respond to cyber-attacks at near real-time.

To achieve this goal Vanuatu is empowered to:

- ❖ *Establish proper mechanisms to strengthen Cyber Security and enable better Cyber resilience progress.*
- ❖ *Increase CERT Vanuatu's capability and ability to respond to cyber-attacks at near real-time.*
- ❖ *Encourage and introduce Security Operation Centres (SOC) in the Government ICT and Security structure and in the private sector organizations.*
- ❖ *Work towards the development of the National Cyber Security Agency (NCSA) of Vanuatu.*
- ❖ *Increase people's cyber resilience through Awareness Raising, increasing Capability, and Engagement.*
- ❖ *Increase people's cyber resilience at work and in societies.*
- ❖ *Establish and improve our whole cyber security workforce and framework to ensure that skills supply meets demand and early threat detection mechanisms are proactive throughout all Vanuatu.*
- ❖ *Establish sustainability and cyber-preparedness programs for organizations in Vanuatu.*
- ❖ *Establish the Cyber Emergency Communications Strategy.*

7.2. Cyber Security Awareness

It is commonly echoed across the cyber security domain that Cyber security is everyone's business and not the government or an agency alone. Cyber security is a shared responsibility and it is attracting the attention of the broader range of stakeholders in Vanuatu. It values the need for an operational Government-private sector partnership that incorporates institutions of all sizes along with state-owned enterprises, local, and regional agencies to execute effective Cyber-threat Incident Response.

For example, the current cyber security and cyber safety landscape in Vanuatu shows two popular distinctive cyber risk trends:

1. *An increase of online social issues rising from incorrect use or abuse of technologies and social media platforms. These abuse incidents include cyberbullying, cyber-stalking, online shaming, hate speeches, and misinformation or disinformation.*
2. *An increase of Internet users and organizations are victims of malware attacks, phishing and online scams relating to rewards (money and lottery prizes). These cyber-threats are equally common across all government, business and the civil society sectors.*

Therefore, tackling cyber security risks, threats and issues require an effective Cyber Security Awareness Raising approach. This approach will utilize the existing multi-stakeholder unified collaboration and cooperation awareness methodology to successfully disseminate proper and correct cyber security information to equip organizations and Internet users on cyber-attacks.

Cyber Security Awareness is a vibrant component for our Strategy. Cyber Security Awareness programs ensure all critical infrastructure users, Internet and technology users have a fair knowledge on how to identify a cyber-threat and report the incident to the appropriate authorities. Effective Awareness should contain relevant information with best practices that help users to work with authorities to mitigate the incident, collect digital evidences, create and deliver evidence in the court of law where such evidences are admissible to the courts.

The Vanuatu National 'Cyber Security Awareness (CSP-2)' Priority aims to address the lack of cyber knowledge in Vanuatu. CSP-2 aims to extend basic reliable cyber security knowledge to all Internet and technology users in Vanuatu. With these knowledge, Cyber-threats and risks are well mitigated and reported.

The CSP-2 priority will be achieved through the following national goals and action plans shown below:

CSP-2 Goal
Vanuatu will:

- » Create and provide a continuous and effective cross-sectored awareness program.
- » Increase Cyber Security knowledge across the all of Vanuatu.
- » Make Vanuatu's population cyber security-aware

Cyber Security Awareness
Vanuatu's Action Plan:

- » Design and develop a Multi-stakeholder Awareness framework for Vanuatu.
- » Design, develop and roll out nationwide awareness campaigns in Vanuatu.
- » Develop Cyber Security Champions, Influencers and advocates Programs.

Vanuatu's Cyber Security Awareness Priority Goals:

Increase Cyber Security Awareness throughout Vanuatu, business institutions and civil societies.

Design and develop a holistic approach for a continuous Cyber Security awareness program which will target all sectors and audiences including people with special needs, elderly and children who have access to the Internet in Vanuatu.

To achieve this goal Vanuatu is empowered to:

- ❖ *Design and develop a set of unified multi-stakeholder awareness programs visible for Vanuatu and its businesses, and citizens.*
- ❖ *Assess and identify all critical stakeholders who are vital for information sharing and dissemination.*
- ❖ *Design and develop cyber security awareness needs, demands and technologies into the cyber security capacity building programs.*
- ❖ *Design, develop and implement effective Awareness Raising campaigns.*
- ❖ *Secure financial support for ongoing Cyber Security awareness programs.*

7.3 Cyber Capacity and Literacy

The Cyberspace is an intrinsic part of the development of any country including Vanuatu. It requires progressive investment capitalizing on existing infrastructure to maximize economic benefits, enhance communications and most importantly ensure online services are always secured. Such assurance require resources and technical skills.

“YUMI40 AND BEYOND – An improved Cyber Capability and Cyber Literacy are intrinsic individual, community and corporate tools which needs to leverage on thus, Secure and Protect Vanuatu’s Border, increase National Security and Sovereignty.”

- By Dr. Jeff G Liu



It is important to invest in cultivating capabilities and talents across all sectors. ‘Cyber capacity’ is a term coined to refer to adequate number of cyber experts and professionals across the entire cyber security spectrum i.e., cyber security experts in Critical Infrastructure sectors. Vanuatu realizes the urgency to build and invest in developing its cyber capacity to boost economic and development benefits.

A strong Cyber capacity is fundamental for Vanuatu to progress and develop in economic, political and also social domains. There is an urgent need to integrate cyber capacity building and development policies for Vanuatu to maximise benefits and increase resilience. It will involve all cyber communities, academia, policy and decision makers to collaborate and develop effective Cyber Capacity Building programs for Vanuatu. Investing in Cyber Capacity Building Programs is a specific way to secure our cyberspace and contribute to the success rate of other policy initiatives.


However, profound dialogues must exist between all development stakeholders, organizations and communities in order to understand how to practically increase and implement Cyber capacities to achieve the development goals outlined in the National Sustainable Development Plan 2030 and the National Security Strategy of Vanuatu.

The aim of meeting the acceptable number of cyber capacity for Vanuatu would be feasible through the development of a national Capacity Building Plan and Program (CBPP) as the core priority for this CSP-3 priority. The CBPP will determine all critical resources required to address operations and issues across all business sectors and civil societies. Vanuatu’s cyber capacity building requirements are based on all critical infrastructure needs, business demands, customer/consumer demands and the key pillars, goals and objectives identified in the Vanuatu National Security Strategy of 2019 and the National Sustainable Development Plan 2030.

Therefore, the National Cyber Security Strategy prioritizes the need for ‘Cyber Capacity and Literacy (CSP-3)’ as a core priority to improving and strengthening Vanuatu’s Cyberspace and National Security.

Thus, integrating the Cyber Resilience (CSP-1), Cyber Security Awareness (CSP-2) priorities and CSP-3 affirms the increase in Cyber Security knowledge, which is vital for all users. Acquiring and equipping citizens of Vanuatu with relevant cyber knowledge as a Government led multi-stakeholder initiative must be prioritized in order to increase cyber literacy. It also requires the presence of effective mechanisms to offer Internet and technology users with the motivation and ambition to acquire valuable Cyber Security knowledge. ‘Self-taught methodological’ best practices that are simple enough for beginners to know and use allow users to make a choice to identify cyber-threats and report the cyber incident at any given time.

The CSP-3 priority will be achieved through the following national goals and action plans shown below:



CSP-3 Goal	<ul style="list-style-type: none">» promote cyber capacity through educational schemes.» develop a blueprint for multi-stakeholder framework to build cyber capacity in Vanuatu.» improve cyber literacy.» develop a cybersecurity mindset and cyber security culture
Vanuatu will:	
Cyber Capacity & Literacy	<ul style="list-style-type: none">» Implement various cyber security bundles to improve cyber security knowledge across all sectors.» Develop cross-sector capacity building plans and programs.
Vanuatu’s Action Plan:	

Vanuatu's Cyber Capacity & Literacy Priority Goals:

Design and develop a holistic Cyber Security education and capacity building framework, where all stakeholders need to combine and play a role instead of operating in silos.

Increase and improve Cyber Capacity, Talents and Literacy in Vanuatu, especially for the Government, private sector organizations, communities, churches and individuals who either do businesses and, or access the Internet and technologies in Vanuatu.

To achieve this goal Vanuatu is empowered to:

- ❖ *Assess Vanuatu's current Cyber Security Capacity capability.*
- ❖ *Assess Vanuatu's current capacity building programs (trainings, workshops and formal education) for Cyber Security and National Security.*
- ❖ *Design and implement capacity building programs that were outlined as 'recommendations' in the Vanuatu CMM Assessment Report of 2019.*
- ❖ *Design and develop various Cyber Security bundles to improve cyber security knowledge across all sectors thus increase cyber literacy.*
- ❖ *Design and develop a National Capacity Building Plan and Program (CBPP)*
- ❖ *Design, develop and enforce effective Awareness Raising campaigns.*
- ❖ *Facilitate, design and develop a Cyber Security Research and Development Hub for Vanuatu.*
- ❖ *Secure financial Support for ongoing capacity building programs.*

"CYBERCRIME is defined as any crime that is committed using a computer or network or hardware device."

- By Symantec Corporation



7.4 Addressing Cybercrime

The fear and challenges of Cybercrime and cybercriminal activities continue to impact nations, industries and communities as the steady advancement of electronic information technology systems enabling more online businesses and online transactions. Cybercrime is a global problem which needs a coordinated national and international response. It creates uncertainty within the business environment thus, pushing nations and governments to act swiftly to secure and protect critical infrastructure from cybercriminals.

Rapidly combating cybercrime activities require a fair understanding of all forms of crime: the physical crime, cybercrime and cyber-enabled crimes. This knowledge can help organizations and Internet users understand all types of crimes associated with ICT as well as understand cybercrime motives. It is also important that all stakeholders involved must understand our legal frameworks, have established communications strategies and plans, and must set out clear Standard Operating Procedures (SOPs) to enhance investigation and mitigation processes.

For Vanuatu to positively address cyber-attacks and combat cybercrime activities, there must be concrete basis and backing from all stakeholders, especially the law enforcement – Vanuatu Police Force, the Legal and Standards bodies, ICT, Security agencies, Internet Services Providers (ISPs) and other critical infrastructure agencies. Over the years, digital stakeholders are genuinely concerned about:

- ❖ *the frequency of information security breaches and malware incursions;*
- ❖ *the need for e-security awareness and education;*
- ❖ *the roles played by the law and law enforcement; and*
- ❖ *the installation of current security applications and systems.*

While not necessarily criminal in nature, some stakeholders also expressed deep concerns over the use of computers for cyberbullying and harmful digital communications such as online abuse, particularly involving younger and school aged users.

Therefore, addressing cybercrime as the national Cyber Security Priority (CSP-4) is an essential Government objective to increase efforts and enhance our National Security and sovereignty. Cybercrime efforts must be spearheaded by the Vanuatu Police Force, the Legal and Intelligence agencies and other cyber security agencies such as CERT Vanuatu. There must be robust multiple systems and frameworks that require joint-efforts to combat cybercrime such as setting up cybercrime and digital forensics capabilities and agencies. Cybercrime agencies and digital forensic laboratories are initiatives to boost Vanuatu's fight against cybercrime. Equipped with proper investigative and digital forensics capabilities also increase the chances of collecting viable evidences that are admissible to the court of law.

Overall, an increased capability for Vanuatu will pave a way forward for better incident response, intelligence gathering and effective decision making.

The CSP-4 priority will be achieved through the following national goals and action plans shown below:

The infographic is a blue-themed graphic with a stylized image of hands shaking on the left. It is divided into two main sections. The top section, titled 'CSP-4 Goal', lists three bullet points: 'Combat Cybercrime effectively through a multi-stakeholder framework.', 'Develop specialized agencies to address cyber security threats.', and 'Develop and enforce the cybercrime Act, Harmful Digital Communications Act and Data Privacy and Protection Act.' The bottom section, titled 'Addressing Cybercrime Vanuatu's Action Plan', lists three bullet points: 'Vanuatu Police Force (VPF) to work with OGCI to establish a Cybercrime department and Digital Forensic Lab under VPF.', 'Develop international collaboration partnership to combat cybercrime.', and 'Establish Cyber Intelligence and Digital Forensics Capabilities'.

Vanuatu's Addressing Cybercrime Priority Goals:

Effectively collaborate across national and international digital environment to combat Cybercrime through multiple frameworks and approaches.

Establish the Vanuatu Police Cybercrime Department, Cyber Defence and Intelligence Unit and Digital Forensics Lab.

Enforce the National Cybercrime Act of Vanuatu.

Enforce future Harmful Digital Communications Act of Vanuatu.

Enforce future Data Privacy and Protection Act of Vanuatu.

Develop and establish an eSafety Commissioner body to address cybercrime and cyber safety issues and incidents.

To achieve this goal Vanuatu is empowered to:

- ❖ *Design policies and strategies to guide the establishment of the Vanuatu Police Force Cybercrime department/unit, Cyber Defence and Intelligence Unit and Digital Forensics Lab.*
- ❖ *Develop a Cybercrime Prevention Policy and Strategy.*
- ❖ *Collaborate across all business and civil sectors to develop various Cybercrime and Cyber safety Awareness Raising Campaigns.*
- ❖ *Develop and establish national cyber security and cybercrime bundles for all stakeholders to improve National Security.*
- ❖ *Assess Vanuatu's current capacity building programs for Cybercrime, Cyber Security and National Security.*

7.5 International Engagement

The Vanuatu National Security Strategy Pillar 5 (Cyber Security), Pillar 7 (Political Stability and Good Governance), and Pillar 8 (Foreign Relations – External Engagement) provided emphasis on cyber security, political stability, good governance and foreign relations or International engagement. Thus, the purpose of Cyber Security International Engagement Priority (CSP-5) of this strategy is to improve and strengthen Vanuatu’s National Security and Cyber Security operations.

International engagement is paramount and is imperative that international engagement and partnerships are well established as part of Vanuatu’s National Cyber Security efforts against the warfare on Cybercrime.

In this strategy priority, Vanuatu through the Ministry of Foreign Affairs and the Ministry responsible for ICT must take lead and ownership to spearhead proper visible frameworks that will create multiple communication and information sharing channels with our international partners.

The CSP-5 priority will be achieved through the following national goals and action plans shown below:

The infographic is a blue-themed graphic with a background image of hands shaking. It is divided into two main sections. The top section is titled 'CSP-5 Goal' and 'Vanuatu will:', followed by three bullet points: 'Create, and strengthen International partnership to tackle security issues.', 'Provide better Information Sharing Platforms.', and 'Encourage and invest in International Cyber Security Engagement opportunities'. The bottom section is titled 'International Engagement' and 'Vanuatu's Action Plan:', followed by two bullet points: 'Develop policies for Involvement in International Bilateral treaties and Collaboration.' and 'Formulate attractive avenues to attract International Security frameworks and partnerships.'

Vanuatu’s International Engagement Priority Goals:

Create and establish formal Cyber Security International partnerships.

Establish Information Sharing and Communication Networks.

Develop International policies and frameworks to enhance global Cyber Security Collaboration, Research and Innovation.

To achieve this goal Vanuatu is empowered to:

- ❖ *Establish strong strategical Cyber Security relationships with international partners.*
- ❖ *Expand and maintain strong Cyber Security relationships with international partners.*
- ❖ *Encourage and collaborate on innovative Cyber Security and Intelligence solutions, frameworks and mechanisms.*
- ❖ *Develop and upskill national and regional Cyber Security Capability through Research and Development Partnership.*
- ❖ *Promote Cyber Security Awareness and Information Sharing avenues.*

7.6 Cyber Security Standards and Legal Frameworks

Vanuatu is currently progressing into the maturity stage and certain current national goals and objectives are unlocking future potentials and visions. One of this realization is the need to implement ‘Standards’ and ‘Legal frameworks’⁶ including regulations and policies which contribute significantly to improving Cyber Security.

6 Legal frameworks comprise a set of documents that include the constitution, legislation, policies, regulations, and contracts.

The recent Vanuatu Independence Anniversary 'YUMI40' theme of 'Prosperity for Self-Reliance and a Resilient Future,' allowed the Vanuatu Bureau of Standards (VBS) to introduce the theme of "Tingting Kwality, Tingting Standad". This has enabled Vanuatu to also prioritize the development and adoption of Standards. Such theme displayed the need to drive the usage, application and enforcement of Standards in Vanuatu purposely to improve and contribute to economic benefits. The Vanuatu Bureau of Standards is mandated to promote standardization in industry and commerce; act as a depository for all Standards; prepare draft Standards and to declare them as Vanuatu Standards.

Similarly, the Office of the Government Chief Information Officer (OGCIO) and the Telecommunications Radiocommunications Broadcasting Regulators (TRBR) office are also responsible for the development of ICT and Cyber Security Policies, Standards and Regulations.

These responsibility places the lead agencies to continually work on developing national standards and regulations that will contribute to the improvement of Telecommunications and ICT services in Vanuatu.

Other developments include the recent membership of Vanuatu to the International Organization for Standards (ISO). The Office of the Government Chief Information Officer (OGCIO) and its Cyber Security arm (CERT Vanuatu) in collaboration with the Vanuatu Bureau of Standards have taken the necessary preparatory steps to adopt the ISO 27000 Standards series and precisely the ISO 27001 Standard – Information Security Management Systems (ISMS) Standard. The adoption ISO 27001 Standard will enable OGCIO, CERT Vanuatu and the Vanuatu Bureau of Standards (VBS) to implement measures of the Standard in order to ensure Vanuatu's Information Security framework are certified and have met an adequate compliance.

Implementing a national Cyber Security Standard is crucial to establish a common avenue for all national and international sectors to effectively collaborate with the intention of improving business continuity and effectively sharing information. For example, the current work towards adopting the ISO 27001 Information Security Management System (ISO 27001 ISMS) which will keep information assets secure and protected. The ISO 27001 Information Security Management System Standard permit organizations to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

Moreover, Cyber Security legal frameworks comprising legislations and regulations are important and compliment Standards. The Strategy aims to allow our Cyber Security lead agencies to work with multiple stakeholders to develop appropriate Cyber Security and ICT regulations. These regulations will ensure the usage of technologies, online platforms, applications, and processes that exist over the Internet are used accordingly and legally and not for a malicious intent. An example is the newly developed 'Type-Approval' regulation that require all types of electronic hardware imported into Vanuatu must meet certain requirements. It has allowed better screening of hardware products imported into Vanuatu and it is a step forward to safeguard products imported into Vanuatu.

The development and enforcement of necessary legislation, regulations, policies and contracts are important as they provide guiding principles and controls to govern the actions of people and organizations in both the private and public sectors. The proposed Cybercrime Act No. of 2020 and other relevant laws and regulations will help address issues that affect order and good governance. Thus, through the implementation of proper Cybercrime, Data Privacy and Protection laws, and Harmful Digital Communications legislation that allows Vanuatu to:

- ❖ *understand and manage geographical borders and cyber sovereignty, i.e. the issue of no geographical borders in the digital world;*
- ❖ *understand and manage the bond that the Internet and connected devices bring to users;*
- ❖ *enable the transnational world and realm; and*
- ❖ *manage, guide and understand issues and the reach which devices enable communication capabilities.*

Therefore, in the National Cyber Security Strategy, various legal and policy institutions such as the Ministry of Justice, the office of the State Law (SLO), Prosecution agencies and OGCIO play a vital role in ensuring our laws uphold National Security and ensure offenders or culprits are held accountable for their crimes committed.

It is equally important that the application and enforcement of Cyber Security Standards and Legal frameworks provide guidelines, remove barriers and offer opportunities with a Cyber-boundary to secure and protect Vanuatu's cyberspace, industries, technologies, processes and people (citizens). It also helps build trust and confidence for consumers and businesses when using digital services. For example, applying Standards can help keep user private data and information secure and protected.

The CSP-6 priority will be achieved through the following national goals and action plans shown below:

CSP-6 Goal
Vanuatu will:

- » Implement and enforce Cyber Security Standards, and relevant standards and regulations.
- » Create an avenue for suitable Security, ICT and Trade standards, regulations and legislation.

Cyber Standards and Legal Frameworks
Vanuatu's Action Plan:

- » Create relevant national policies, strategies, & procedures to accommodate and guide national standards.
- » Implement & enforce Cyber Standards and Legal Frameworks. e.g. Data Protection & Online Privacy Act.
- » Collaborate with stakeholders on adopting, & enforcing sectorial Standards, regulations and compliance to various standards and Legal acts

Vanuatu's Standards and Legal Frameworks Priority Goals:

- ❖ *Develop and implement national policies and strategies to accommodate Cyber Security Standards, regulatory frameworks and other relevant non-Cyber Standards.*
- ❖ *Stimulate avenues to encourage the adoption of international Standards, and regulations such as the 27000 Family Series of Standards and specifically the ISO 27001 Information Security Management Systems, ISO 31000 Risk Management Standards,⁷ and ISO 9001 – Quality Management Systems (QMS) Standards⁸*
- ❖ *Encourage dialogues on the need to develop appropriate laws aimed at the cyberspace and relevant areas.*
- ❖ *Encourage development of new national Standards, Regulations, and laws in Cyber Security, ICT and the trade and commerce environment.*

To achieve this goal Vanuatu is empowered to:

- ❖ *Collaborate with stakeholders on adopting, and enforcing sectorial Standards, regulations and compliance to various standards and Legal acts.*
- ❖ *Develop and upskill national and regional Cyber Security Capability within Standards and Legal frameworks.*
- ❖ *Promote Cyber Security Standards and Regulations Awareness Raising programs and campaigns.*
- ❖ *Encourage an increased and improved Quality and Risks Management frameworks to comply with various national and international Standards enforced.*
- ❖ *Implement and enforce the Cybercrime Act of Vanuatu.*
- ❖ *Develop and implement a Harmful Digital Communications Act of Vanuatu.*
- ❖ *Develop and implement a Data Privacy and Protection Act of Vanuatu.*

⁷ ISO 31000 Risk Management Standards provides principles, a framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

⁸ ISO 9001 Quality Management Systems Standards is the international standard that specifies requirements for a quality management system (QMS). Organizations use the standard to demonstrate the ability to consistently provide products and services that meet customer and regulatory requirements.

8.0 The National Cyber Security Strategy Response Deliverables

The National Cyber Security Strategy (NCSS) priorities have provided six priority goals with action plans. The Analysis from the data collected from cyber-threat trends, current government policies and strategies, and the nationwide consultations have contributed to developing various practical national response deliverables as part of the six priority goals and action plans.

Therefore, these national goals and action plans are further expressed through the ‘Cyber Security Strategy Response Deliverables’ that are categorised into three main approach clusters:

- ❖ *Government Responses;*
- ❖ *Private Sector Responses; and*
- ❖ *Civil Society Responses.*

These three response categories have expected deliverables that are designed to be developed and implemented through a ‘Multi-stakeholder’ approach. Utilizing the multi-stakeholder partnership between all critical stakeholders in Vanuatu, will allow Vanuatu to address the Response deliverables through numerous development programs and implementation within the next ten year period. These deliverables will encourage yearly or three yearly strategic plans developed by the stakeholders to ensure the six priorities stated in this strategy are successfully implemented.

These efforts will also support the introduction of new Cyber Security working groups, namely; the ‘Cyber Security Technical Working Group’ and the ‘Cyber Security Reference Working Group.’ These working groups consist of experts from all critical infrastructure agencies and organizations. Their primary roles include providing expert insights and managing various tasks assigned or developed through business plans. The working group roles also include being the point-of-contact for lead agencies whom are responsible and would guarantee that the Response deliverables are accurately executed within the next ten years.

8.1. The National Cyber Security Generalised Delivery Response Model

The Multi-stakeholder Response Approach



Figure 14: The Multi-stakeholder Response Approach for Vanuatu

Figure 14 displays the three distinctive Response approach categories outlined as key Response deliverables that Vanuatu will execute. The outlined key Response deliverables in this strategy is not exhaustive. Other Response deliverables can be added later due to the fact that technologies rapidly evolve over time, Cyber-threats are increasing in frequency and becoming more sophisticated and also Governments can change their plan of actions overtime.

8.2. The Cyber Security Awareness Campaign Response

TIPS FOR STRONG PASSWORD PROTECTION



- » The longer the better – use at least 8 characters.
- » Include symbols, numbers, & uppercase letters.
- » Don't reuse passwords across multiple sites.
- » Don't use personal identifying information like dates.
- » Change your passwords regularly.

HOW TO FIGHT CYBERCRIME

- » Become vigilant when browsing websites.
- » Flag and report suspicious emails.
- » Never click on unfamiliar links or ads.
- » Use a VPN whenever possible
- » Ensure websites are safe before entering credentials.
- » Keep antivirus/application systems up to date.
- » User strong passwords with 14+ characters.

9.0 Conclusion

The future and strength of our National Security relies on our strategies and yearly implementation matrix, our cyber security knowledge, our decision makers and most importantly the Internet and technology users. Being security-aware allows our Internet users to identify a luring phishing link or a malicious email attachment. This could avoid that 'one bad-click' on a malicious link that could result in the loss of reputation and or financial implications.

Our culture, values, behaviours and geographical identity could be and may remain the basis and strength of Vanuatu to ensure Information Security, Cyber Security and daily business operations, where processes and people are safe from Cyber-attacks and Cybercrime activities.

9.1 It does not End Here

Following on from the launching of this National Cyber Security Strategy 2030, continuous efforts on addressing Cyber Security, Cybercrime and Cyber Safety matters remain an ongoing exercise for Vanuatu to ensure National Security and the security of citizens and business operations are secured and protected effectively.

It is important to note that this strategy greatly relies on a multi-stakeholder collaborative platform where all Critical Infrastructure lead agencies will work together to ensure the six National Cyber Security Priorities and respective Response Action Plans are successfully implemented and enforced. It is understandable that due to the fact that this strategy is a ten year strategy plan, the lead agencies and various stakeholders have been working to establish two critical working groups which include the 'Cyber Security Technical Working Group (CSTWG)' and the 'Cyber Security Reference Working Group (CSRWG).' These working groups will work with all Cyber Security experts in Vanuatu and abroad to manage and ensure yearly work plans are developed and executed accordingly to address Cyber Security efforts for Vanuatu. These working groups will also work closely with all lead agencies to develop Vanuatu's National Cyber Security Strategy Implementation Matrix, a matrix that will be the implementation guideline for our national Cyber Security efforts. The implementation matrix will acknowledge all other existing policies, strategies and plans that the Government of Vanuatu is embarking on, and those that will be developed in the near future.

10.0 References

1. NIST Framework: <https://medium.com/@musttrn/nist-cybersecurity-framework-process-structure-e847e7a45829>
2. Cyber Security Maturity Models: <https://innovationatwork.ieee.org/what-is-a-cyber-security-maturity-model/>
3. CMMI Cybersecurity Maturity Models: <https://www.huntsmansecurity.com/blog/understanding-cyber-security-maturity-models/>
4. Cyber Security talent shortage: <https://www.issa.org/cybersecurity-skills-crisis-worsens-for-fourth-year-in-a-row-impacting-70-of-organizations/>
5. Cyber Security Definition: <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>
6. Misinformation: <https://www.cfr.org/blog/misinformation-threat-democracy-developing-world>
7. Disinformation: <https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation>
8. Critical Infrastructure: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-public-sector-cybersecurity-critical-infrastructure.pdf>
9. U. Global Cyber Security Capacity Centre - University of Oxford, "The CMM," Global Cyber Security Capacity Centre, Mar. 31, 2016. <https://gcsc.web.ox.ac.uk/the-cmm> (accessed Oct. 26, 2020)
10. OCSC, "The CMM," Oceania Cyber Security Centre. <https://ocsc.com.au/capacity-initiatives/the-cmm/> (accessed Oct. 26, 2020).
11. "GCSCC University Of Oxford." <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/GCSCC-university-oxford.aspx> (accessed Oct. 26, 2020).
12. [What is a Malware? https://www.mcafee.com/en-us/antivirus/malware.html](https://www.mcafee.com/en-us/antivirus/malware.html)
13. ISO 27001 Standard: <https://www.iso.org/standard/54534.html>
14. Ransomware: <https://www.malwarebytes.com/ransomware/>
15. NIST – Cyberspace definition - <https://csrc.nist.gov/glossary/term/cyberspace>
16. TrendMicro – Cybercriminals definition - <https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals>
17. NIST – Cyber-attack definition - https://csrc.nist.gov/glossary/term/Cyber_Attack
18. TLP - <https://www.first.org/ttp/>

11.0 Appendices

Appendix 1: The National Cyber Security Strategy Consultation Report

The National Cyber Security Strategy Consultation report provides a brief summary of the various organizations, agencies, and communities which were involved during the process of developing the strategy. These organizations, agencies and communities are:

Consultation Agency, Organization, Community Name	Participant Categories	Feedback Summary
Government Ministries – Port Vila, Efate	Director Generals, Directors, Managers, CEOs, Civil Servants,	<p>One-to-one Consultation:</p> <p>The importance of ensuring ICT and Cyber Security enhance business operations, protect and secure critical infrastructure, sensitive information and assets.</p> <p>There is a critical need for Cyber Security Awareness to all provinces, communities especially when cyber security tools, technologies can be an asset at the same time a weapon.</p> <p>Harmful Digital Communications and Data protection and Privacy Legal framework are critically needed for Vanuatu going forward.</p>
Aviation Sector	Directors, Managers, organization representatives	<p>One-to-one Consultation:</p> <p>The application of Cyber Security Standards in compliance to Aviation regulations and operations are mandatory for our aviation sector and operations. The government must work with our aviation sector to address this gap.</p>

Banking and Finance Sector	Directors, General Managers, CEOs, organization representatives	One-to-one Consultation: The privacy of user personally identifiable information is very important and the government must address Data Protection and Privacy for better security in organizations and in Vanuatu
Health Sector	Directors, CEOs, Managers, Civil Servants,	One-to-one Consultation: The privacy of user personally identifiable information is very important and the government must address Data Protection and Privacy for better security in organizations and in Vanuatu
ICT, Telecommunication and ISP Sector	Directors, General Managers, CEOs, organization representatives	One-to-one Consultation: Cyber-attacks are daily issues which can be a nightmare for the ICT, Telecommunications and ISP sector. A multi-stakeholder approach to tackling cyber-attacks and cybercrime is critical for Vanuatu.
Energy Sector	Directors, CEOs, Managers, Civil Servants,	One-to-one Consultation: Technologies, critical infrastructure are important and requires proper security framework to protect and safeguard our energy sector.
Legal Sector	Directors, Public Prosecutor, CEOs, Managers, Civil Servants,	One-to-one Consultation: There is an urgent call for Cyber Security Legal frameworks, procedures, policies and strategies to combat cybercrime. We need capacity Building programs for lawyers and legal teams.
Education and Academic Sector	Directors, CEOs, Managers, Civil Servants,	One-to-one Consultation: There are critical needs for Cyber Security curriculum in Schools. There are needs for Awareness programs to address cyberbullying, hate speech, online shaming, and misinformation.

Civil Sector and Local Authorities	Directors, CEOs, Managers, Civil Servants,	<p>One-to-one Consultation:</p> <p>There is a great need for a proper cyber security communications strategy to allow information dissemination throughout Vanuatu.</p> <p>There are needs for Awareness programs to address cyberbullying, hate speech, online shaming, and misinformation.</p>
Trade, Tourism and Industry Sector	Directors, CEOs, Managers, Civil Servants,	<p>One-to-one Consultation:</p> <p>Cyber Security is a novel term and area where this sector still needs more awareness and dialogues to enhance Vanuatu's Tourism and Trade sector.</p>
Telecommunications, Radiocommunications Broadcasting Regulator	Regulator, Managers, Organization representatives	<p>One-to-one Consultation:</p> <p>Cyber Security is very important for our telecommunication sector and addressing it through our current multi-stakeholder framework is key to achieving effective solutions to cybersecurity issues.</p>
Civil Aviation Authority Vanuatu	Director, Managers, Organization representatives	<p>One-to-one Consultation:</p> <p>Cyber Security or Security is critical for our Aviation sector and we must work with relevant cyber security agencies in Vanuatu an internationally to ensure we secure our aviation sector and comply with aviation regulations and standards.</p>
National Standards Body	CEO, Organization representatives	<p>One-to-one Consultation:</p> <p>Developing and adopting core cyber security standards, risk management standards and other relevant standards are key to establishing better guidelines for businesses, operations, trade and procedures. These guidelines can enhance, facilitate and set standards for improved service delivery thus maximise benefits for Vanuatu.</p>

Vanuatu Police Force	Commissioner, Sensor Commanders, Organization representatives	<p>One-to-one Consultation:</p> <p>We are the most critical agency who has the law in our hands and must take cybercrime seriously to ensure we protect, secure and uphold our national security and sovereignty.</p> <p>It is critical we collaborate with other security agencies for intelligence sharing, combating cybercrime and ensuring we improve cyber capabilities.</p>
Non-Government Organizations	Director, Organization representatives	<p>One-to-one Consultation:</p> <p>Lack of proper Information sharing and integrity. Social Media abuse, pornography, cyberbullying, cyber/online-shaming, Hate speech, Misinformation and Disinformation are real issues.</p>
Reserve Bank of Vanuatu	Managers, Organization representatives	<p>One-to-one Consultation:</p> <p>Information Security and cyber legal frameworks and relevant mechanisms are very important and must be implemented urgently.</p>
Border Control Sector	Directors, Managers, Organization representatives	<p>One-to-one Consultation:</p> <p>Cyber Security contributes to border control mechanisms to uphold our National Security of Vanuatu.</p>
Enaro Council Area – South Tanna	Area Secretary and Administrator, Community Leaders, Chiefs, Youths, Teachers,	<p>Cyber Security is a totally new topic for the community. Issues include Money scams, fake news, Phishing. Appreciated the consultation.</p>
Iarkei Community – Whitesands Area Council of Chiefs	Area Secretary and Administrator, Community Leaders, Chiefs, Youths, Teachers	<p>Cyber Security is new and timely topic of discussion. Appreciated the consultation.</p>
Lamnatu Village – Middle bush Area Council of Chiefs	Area Secretary and Administrator, Community Leaders, Chiefs, Youths, Teachers	<p>There were many awareness in the past, however this is very new and appreciate the government for coming out to the communities. Appreciated the consultation.</p>

Napraentata Area Council of Chiefs	Area Secretary and Administrator, Community Leaders, Chiefs, Youths, and community representatives	This is a very new topic of discussion and very important. Appreciated the consultation.
Tafea Provincial Head Quarter – West Tanna (2 sessions)	Area Secretary and Administrator, Civil Servants, Law Enforcement, Island Court Judges, Community Leaders, Chiefs, Youths, and community representatives	A critical topic for discussion and awareness. Appreciated the consultation.
North Tanna Area council of Chiefs	Area Secretary and Administrator, Community Leaders, Chiefs, Youths, and community representatives	Cyber Security is new and timely topic of discussion. Appreciated the consultation.
Annelcauhat – West Aneityum	Community Leaders, Chiefs, Youths, and community representatives	The need for Cyber Security Response and Preparedness Plans.
Umeg – South Aneityum	Community Leaders, Chiefs, Youths, and community representatives	The need for Cyber Resiliency.
Port Patrick - North Aneityum	Community Leaders, Chiefs, Youths, and community representatives	Lack of proper Information sharing and integrity. Misinformation and Disinformation issues.
Ipota, North Area Council – East Erromango	Community Leaders, Chiefs, Youths, and community representatives	Need to Address Cybercrime effectively such as programs to help train youths, special needs and elderly people in society.
Port Narvin - North East Erromango	Community Leaders, Chiefs, Youths, and community representatives	Need to Address Cybercrime effectively such as programs to help train youths, special needs and elderly people in society.
Bongil, South Area Council – South West Erromango	Community Leaders, Chiefs, Youths, and community representatives	Need to Address Cybercrime effectively such as programs to help train youths, special needs and elderly people in society.
Dillons Bay, South Area Council – West Erromango	Community Leaders, Chiefs, Youths, and community representatives	Need to Address Cybercrime effectively such as programs to help train youths, special needs and elderly people in society.
Luganville, Malo, Aore, Big Bay Area, North West Santo, West Coast, – Santo	Civil Servants, Law Enforcement, Community Leaders, Area Secretary and Administrator, Chiefs, Youths, teachers and community representatives	There is a big need for Cyber Security Awareness in towns, schools, and rural areas.
Hog Harbour Village - East Santo	Community Leaders, Area Secretary and Administrator, Chiefs, Youths, and community representatives	There is a need for more awareness, regulations in schools, and bylaws for communities to address cyber threats, abuse, and social media issues.

Nakere Village – South Santo	Community Leaders, Area Secretary and Administrator, Chiefs, Youths, Students, Teachers, and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Port Olry – North East Santo	Community Leaders, Area Secretary and Administrator, Chiefs, Youths, Students, Teachers, and community representatives	Technologies, Social Media and Pornography are concerning issues in schools, villages and communities.
Sara Village – East Santo	Community Leaders, Chiefs, Youths, and community representatives	No reception coverage, and lack of awareness in that area contribute to the rise in money scams, and social media issues in communities.
Matevulu College – Luganville, Santo	Teachers and Students	Concerns around Social Media abuse, cyberbullying, hate speech, and regulations in Schools.
Santo East School – Luganville, Santo	Teachers and Students	Concerns around Social Media abuse, cyberbullying, hate speech, and regulations in Schools.
Walaha and Ambore area – West Ambae	Civil Servants, Community Leaders, Area Administrator, Chiefs, Youths, Teachers and community representatives	Cyber Security is new and needs further Awareness. The continuous lack of cyber bylaws to address cyber activities in communities.
Lolopuepue – North Ambae	Community Leaders Chiefs, Youths and community representatives	Cyber Security is new and needs further Awareness. The continuous lack of cyber bylaws to address cyber activities in communities.
Sakau Village – South Ambae	Community Leaders Chiefs, Youths and community representatives	Cyber Security is new and needs further Awareness. The continuous lack of cyber bylaws to address cyber activities in communities.
Penama Provincial Council HQ – Saratamata, East Ambae	Civil Servants, Law Enforcement, Community Leaders, Area Secretary and Administrator, Chiefs, Youths, Teachers and community representatives	Cyber Security is new and needs further Awareness. The continuous lack of cyber bylaws to address cyber activities in communities. Threats include harmful contents, lack of regulating online contents and the Internet.

Nasawa Village – South Maewo	Civil Servants, Community Leaders, Area Secretary and Administrator, Chiefs, Youths, Teachers and community representatives	Cyber Security is new and needs further Awareness. The continuous lack of cyber bylaws to address cyber activities in communities.
Pangi Area, South Pentecost Area Council	Community Leaders, Area Secretary, Chiefs, Youths, Teachers and community representatives	Facebook provides a lot of benefits but also changes traditions, loss of custom values and principles, and contributes to misinformation, fake IDs, scams, pornography and online abuse.
Bwatnapni Area, Central Pentecost 1 Area Council	Community Leaders, Area Secretary, Chiefs, Youths, Teachers and community representatives	The analogy that Facebook is the Internet provides a perception that everything is done via Facebook, both positive and negative uses of Facebook.
Sara Area, North Pentecost Area Council	Community Leaders, Chiefs, Youths and community representatives	The National Government needs cyber bylaws to address cyber activities in communities.
North West A & North West B Malekula	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Lakatoro – Central Malekula Area Council	Civil Servants, Law Enforcement, Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Urupiv Island	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Wintua – South West Bay	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Tisman – South East Malekula Area Council	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Lamap – South Malekula Area Council	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Okai Village – South Malekula	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Maskylne Island	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.

Akam Island	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Varum Village – South Malekula	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Penapo – South East Ambrym Area Council	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Maat Community – South East Ambrym	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Mota Lava Area Council	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Sola Island	Civil Servants, Law Enforcement, Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
West Vanua Lava Area Council	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Mota Island Area council	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
West Gaua Area Council	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
East Gaua Area Council	Community Leaders, Chiefs, Youths and community representatives	Technologies, Social Media and Pornography are concerning issues in villages and communities.
Shefa Province Area Council - Efate	Shefa Province President and representatives, Shefa Province Secretary General, Provincial Staff	There is a critical need for Cyber Security Awareness to all provinces, communities especially when cyber security tools, technologies can be an asset at the same time a weapon.
Pango Area Council - Efate	Community Leaders, Chiefs, Youths and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.
Erakor Area Council - Efate	Community Leaders, Chiefs, Youths and community representatives	Social Media abuse and Money Scams are very serious issues in rural areas of Vanuatu and needs urgent attention.

Eratap Area Council - Efate	Community Leaders, Chiefs, Youths and community representatives	Social Media abuse and Money Scams are very serious issues in rural areas of Vanuatu and needs urgent attention.
Meleamat Village and Primary School - Efate	Community Leaders, Chiefs, Youths, Teachers and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.
Mele Area Council - Efate	Community Leaders, Chiefs, Youths and community representatives	There is a big need for cyber security and cybercrime awareness in villages and throughout Vanuatu.
Suango Bilingual School and Community - Efate	Teachers and Students	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Central School – Port Vila	Teachers and Students	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Manua School – North Efate	Teachers and Students	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Ulei Junior Secondary School – North Efate	Teachers and Students	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Onesua Prysbetrian College North Efate	Teachers and Students	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Ifira island and School – Port Vila	Teachers, Students and community representatives	Need more awareness programs to reach rural areas and the islands of Vanuatu.
Sara and Fotlo Villages – Vermol Area Council, South Epi Island	Community Leaders, Chiefs, Youths and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.
Burumba Bilingual School – Epi Island	Teachers and Students	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Burumba Community – Epi Island	Community Leaders, Chiefs, Youths and community representatives	There is a big need for cyber security and cybercrime awareness in villages and throughout Vanuatu.

Rovo Bay (East and West Epi Coverage)	Community Leaders, Chiefs, Youths and community representatives from both East and West Epi Island	Social Media abuse and Money Scams are very serious issues in rural areas of Vanuatu and needs urgent attention.
Laman Bay Community – Epi Island	Community Leaders, Chiefs, Youths and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.
Epi High School – Epi Island	Community Leaders, Chiefs, Youths, Teachers and community representatives	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Akama Centre School – Epi Island	Community Leaders, Chiefs, Youths, Teachers and community representatives	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Finongo Market house and community – Emae Island	Community Leaders, Chiefs, Youths and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.
Nofo Centre School – Emae Island	Community Leaders, Chiefs, Youths, Teachers and community representatives	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Finonge Market House – Emae Island	Community Leaders, Chiefs, Youths and community representatives	Social Media abuse and Money Scams are very serious issues in rural areas of Vanuatu and needs urgent attention.
Tebakor Community – Emae Island	Community Leaders, Chiefs, Youths and community representatives	There is a big need for cyber security and cybercrime awareness in villages and throughout Vanuatu.
Morua Court Room – Tongariki Island	Community Leaders, Chiefs, Youths and community representatives	Social Media abuse and Money Scams are very serious issues in rural areas of Vanuatu and needs urgent attention.
Buninga Island	Community Leaders, Chiefs, Youths and community representatives	Social Media abuse and Money Scams are very serious issues in rural areas of Vanuatu and needs urgent attention.
Noworaone School – Tongoa Island	Community Leaders, Chiefs, Youths, Teachers and community representatives	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Purau Village – Tongoa Island	Community Leaders, Chiefs, Youths and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.

Kurumambe Village – Tongoa Island	Community Leaders, Chiefs, Youths and community representatives	Social Media abuse and Money Scams are very serious issues in rural areas of Vanuatu and needs urgent attention.
Lupalea Village – Tongoa Island	Community Leaders, Chiefs, Youths and community representatives	Social Media abuse and Money Scams are very serious issues in rural areas of Vanuatu and needs urgent attention.
Woraviu Village – Tongoa Island	Community Leaders, Chiefs, Youths and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.
Pele Village – Tongoa Island	Community Leaders, Chiefs, Youths and community representatives	There is a big need for cyber security and cybercrime awareness in villages and throughout Vanuatu.
Lekanon School – Tongoa Island	Teachers and Students	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.
Matangi Village – Tongoa Island	Community Leaders, Chiefs, Youths and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.
Morua Area (Euta / Magarisu / Meriu / Bongaponga / Ravenga villages) – Tongoa Island	Community Leaders, Chiefs, Youths and community representatives	There is a critical need for Cyber Security Awareness to all provinces, communities to address cyber-threats and online abuse issues.
Nambangasale Junior Secondary School – Tongoa Island	Teachers and Students	There are critical needs for Cyber Security curriculum in Schools and Awareness programs.

Appendix 2: Cyber-threats Recorded in Vanuatu Report

APP-2.1 Phishing Attacks:

A Phishing attack is when attackers attempt to trick users into doing ‘the wrong thing’, such as clicking a bad website link that will download malware, or direct them to a malicious or dodgy website.

Phishing is usually conducted via a text message, social media, or by phone, but the term ‘phishing’ is mainly used to describe attacks that arrive by email. Phishing emails can reach millions of users directly, and hide amongst the huge number of benign emails that busy users receive. Attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money.

Phishing emails can hit an organization of any size and type. An Internet or email user might get caught up in a mass campaign (where the attacker is just looking to collect some new passwords or make some easy money), or it could be the first step in a targeted attack against your company, where the aim could be something much more specific, like the theft of sensitive data (data theft). In a targeted campaign, the attacker may use information about employees or company to make their messages even more persuasive and realistic. This is usually referred to as ‘spear phishing.’

In 2018 to 2019, more than 70% of the reported incidents in Vanuatu reported to CERT Vanuatu are Phishing related attacks. These phishing incidents are often not the only mode of attack but a beginning of bigger cyber-attacks that fall into the category of Social engineering. Most phishing cases reported are those targeted towards the Government Internet and technology users. This is because most of the government network provide around 40% of the entire attack landscape for malicious actors. This is critical and a concerning matter which current collaboration from all stakeholders are working together to combat phishing attacks as well as cybercrime as a whole.

APP-2.2 Online Scams:

Humans can become an easy target for malicious actors who want to steal our most valuable personal data. Some examples of online scams include: *email scams, the Nigerian scam, the Samsung lottery scam, greetings card scam, bank loan or credit card scam, lottery scam, romance scam, fake antivirus scam, Facebook impersonation scam (or hijacked profile scam), SMS scamming (Smshing), make money fast scams, and Tech support online scams.* These examples and variants of online scams that were seen and recorded in Vanuatu by users of the internet, often over their mobile platforms and computers.

More than 50% of the online scams reported have a phishing component to it, with potential malicious attachments sent to various organization employees. The common means of phishing scams are via emails and social media platforms. Bank loan or credit card scam and make money fast scams are also popular in Vanuatu with several cases reported to CERT Vanuatu (CERT VU).

APP-2.3 Spams:

A spam is an electronic junk mail, junk newsgroup postings or unsolicited email. However, real spam is an email advertising for some products sent to a mailing list or newsgroup. Spams are very common globally and also in Vanuatu. “Where and when Internet is present, there is spam.” Spams are less harmful considering there are other critical threats that threaten to cripple an organization’s or country’s economy. Hence, while Vanuatu records a higher magnitude of spam cases through email servers, they are well managed or controlled due to effective mail spam filters and through other anti-spam tools.

APP-2.4 Cyberbullying/Cyberstalking:

Cyberbullying and cyberstalking are often viewed as one common online practice by offenders. However, they are both different. “*Cyberbullying is the use of technology to harass, threaten, embarrass, shame, or target another person.*” “*Cyberstalking on the other hand, is a crime in which an attacker harasses a victim using electronic communication, such as emails and instant messaging (IM) or messages posted to a web site or a discussion group.*” When an adult is involved in cyberbullying, it could be seen as a cyber-harassment or cyberstalking, a crime that can have legal consequences and involve a jail term.

CERT Vanuatu has received cases involving cyberbullying or cyber-shaming and cyberstalking. However, with current challenges within the technical and legal space in Vanuatu, addressing Cyberbullying or Cyberstalking is currently a difficult task to tackle or mitigate. The heavily use of online social media platforms such as Facebook and Instagram makes it difficult to address these issues. A way forward to capturing these culprits involved in cyberbullying and cyberstalking requires external parties such as the Facebook team to help address these cases effectively. The cases reported were found mainly in schools and among youths who affiliate themselves in social activities.

APP-2.5 Ransomware Attacks:

“*Ransomware is regarded as one of the lethal type of malicious software, often quite simple that locks and encrypts a victim’s computer data, then demands a ransom to restore access.*” Ransomware attacks come in many shapes and sizes to encrypt and hold your personal files (data) hostage such as documents, photos, and financial information. In all cases of a ransomware attack, all personal files are right in front of you on your computer, but are in an encrypted form. Thus the attacker (s) will request a ransom or demand in a form of digital currency or financial transfer via bank transfers.

In 2018, CERT Vanuatu (CERTVU) has received 2 reported cases involving ransomware attacks on both personal systems and organization systems. The executed analysis indicated the attacks were variants of lockers. *Lockers is a kind of ransomware known for infecting your operating system to completely lock you out of your computer, making it impossible to access your files or applications.* The victim had to reinstall the operating system with the last known backup of the system. Chances of recovering files from the attacker is very minimal. It is common that such attack often has a phishing / back door component to gain access to your system before locking the user out from his/her system. The second case of ransomware involved a Scareware ransomware. *Scareware is a fake software that acts like an antivirus or a cleaning tool.* With a claim to have found issues on your computer, scareware demand money to resolve the issue. Some types of scareware lock your computer while others flood your screen with annoying alerts and pop-up messages. The reported ransomware case involves pop-up messages. Again, to recover from this attack, the technical team had to reinstall the operating system (OS) and restore all files to the last known backup stored. Ransomware are still very common and are now used for targeted organized attacks for financial and reputational damage reasons. Common trends indicated that ransomware attacks are associated to state-sponsored and, or targeted cyber-attacks on organizations and government for specific reasons which involves ‘money’ and ‘reputation.’

APP-2.6 Malware Attacks:

Malware attacks are common and is a traditional method of attacking systems. It covers a wide range of types of cyber-attacks and it is still the very basis of cyber-threats and attacks for most hacking incident. A malware is a software designed to covertly operate on a compromised system without the consent of the user. In an event of cyber-attack, a malware of malicious software, scripts perform activities on the victim’s computer system, usually without his or her (user) knowledge. In most cyber-attacks, there is a malware vector to it which is the base of the attack payload. In computer security, the payload is a component of a computer virus that executes a malicious activity, which contains malware such as worms or viruses. Malicious actions performed by the payload includes deleting data, stealing data, sending spam or encrypting data. All malware attacks identified and report to CERT Vanuatu were treated as random attacks at this stage.

APP-2.7 Data Breach and Data Leakage:

Data Breach and Data Leakage are associated however two different threats. Data breach is the act of unauthorised access and/or compromising a computer system or systems by attackers and gaining access to sensitive data due to existing identified bugs, vulnerabilities, loopholes or exploits found in a system (s). Data leakage is the act of unauthorised transmission of data from within an organization to an external destination or recipient. It is also the act of publicly disclosing sensitive data of companies, organization to shame them and/or destroy their reputations.

CERT Vanuatu has recorded various cases involved in both data breach and data leakage. The indication from data leakage cases analysed show that users involved in leaking sensitive information are not really aware of the impact and damage it can do to the victims (government, organizations and/or users). Whereas, data breach or accounts compromised in Vanuatu are due to not using computers and the Internet in a safe manner, i.e. carelessness can contribute to data breach cases.

Like any other types of cyber-attacks, the increase of data breach and leakage are due to lack of awareness in the areas of information security issues. Users not being aware of such threats poses a huge role as to why users do not stop to think and act while online browsing or surfing the Internet. The absence of ICT, security policies (Access control, etc.), information sharing/dissemination and regulations in organizations also contribute to the high cases of data/information leakage. This is a concerning issue and threat towards state secrets, intelligence and National Security in Vanuatu.

APP-2.8 Extortion Cases:

Extortion cases are common in Vanuatu however, time and again cases are not recognised due to lack of awareness of such act. Mobile users and social media users have become a victim to extortion without their understanding yet follow on and take part in the act of extortion. Lack of understanding extortion threats has placed users to pay their way out from such cases.

The common extortion cases identified in Vanuatu have both a technology component as well as a human (victim) contribution. The attacker leverages on persuasive and convincing methods to lure the victim into the act which is then recorded then demands a ransom before releasing recorded videos and messages. Victims are convinced to have to pay up the ransom in digital currencies and/or bank transfers to overseas accounts.

Again, the need to understand online extortion attacks as severe and damaging as any other online attacks. Users in Vanuatu like other pacific island countries and abroad are vulnerable to extortion cases thus, require proper security best practices on how to surf the Internet and be secure online. This is paramount to staying secure and not be a victim of extortion attacks. Avoiding phishing baits in emails and on social media is critically important to minimize chances of being a victim of an extortion attack.

APP-2.9 Website Defacement:

Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. It is similar to drawing graffiti on a wall, but only it happens virtually as a kind of electronic graffiti and is a form of vandalism. Websites' appearance change – pictures and/or words are scrawled across the defaced website. These are typically the work of defacers (Security hackers), who break into a web server and replace the hosted website with one of their own. Attackers may have different motivations when they deface a website. Political motivation is one, which is often used to spread messages by “cyber protesters” or hacktivists.

Other attackers may choose to deface a website for fun – to mock site owners by finding website vulnerabilities and exploiting these to deface a website. The most common method of defacement is using SQL Injections to log on to administrator accounts. Although website defacement is harmless, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware or deleting essential files from the server. In both cases, website owners face damages to their business and reputation once their sites are defaced.

The website defacement case in Vanuatu indicated that the web servers have been compromised due to lack of proper security implementation at the hosted platform thus, all website hosted on this platform were defaced. In this case, the website defacers call themselves as “Phenix-TN & Mr. Anderson.” Thus as mentioned above, analysing the threat identified indicated that it potentially linked to random cyber protesters.

APP-2.10 Misinformation and Disinformation:

Misinformation is a concerning threat to Vanuatu’s cyberspace and communities. It is defined by the inadvertent spread of misleading and false information, whereas disinformation reflects the deliberate and coordinated spread of misleading and false information. Misinformation proliferates partly because people are more likely to accept advice and information from friends, family, and people they feel their community trusts.

The problem of ‘misinformation’ online is bedevilling governments around the world including Vanuatu. Misinformation becomes more and more of a threat to governments or nations as deceiving technologies improve such as Deepfake – a synthetic media in which a person in an existing image or video is replaced with someone else’s likeness.

Similarly, ‘Disinformation’ is “verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public.” Due to the COVID-19 Pandemic and recently the Tropical Cyclone Harold ‘State of Emergency,’ disinformation may have far-reaching consequences, does cause public harm, remains a threat to the democratic political and policy-making processes, and may even put the protection of Vanuatu citizens’ health, security and their environment at risk.

APP-2.11 Abuse of Social Media and Violation of Online Privacy:

Another prominent cyber-threat or issue faced in Vanuatu and globally is the very own ‘abuse of Social Media and violation of Online Privacy.’ The previously mentioned reported cyber-threats and attacks are not the only threats to Vanuatu’s national security or individuals in organizations, society and communities.

The unregulated nature of social media platforms contributes to ‘*social media-enabled*’ crimes or ‘*cyber-enabled*’ crimes and the increased use to violate online privacy, shame or hate people and, or threaten people is now an on-going common threat in Vanuatu and across the Pacific. It is also not different around the world due to the easy global connectivity at reach to any users on the Internet. Social media-enabled crimes are entertained through social exploitation tactics where cybercriminals are effortlessly gaining data which are in a form used in various cyber-attacks.

Lack of social media account creation restrictions, security checks, fake account checks or filtering, and checks against legitimate databases, encourages the use of ‘*fake Identities.*’ Restricted and closed social media groups entertain fake identities which are promoting or facilitating the sharing of pornographic contents and abusive languages entertained to encourage or initiate hate speeches among Internet users.

Another despicable factor contributing to the abuse and exploiting online personal privacy cases in Vanuatu is due to the lack of information verification and validation on social media platforms as well as within organizations. The fact that users do not know and understand where the boundaries of freedom of speech versus privacy, does cause users to post sensitive information online without knowing or executing facts-checking if such information published would cause bigger issues online and in societies. Again, the unregulated nature of social media contributes to no proper information validation process executed before information are published online via social media platforms. Hence, the absence of verifying the information source in social media entertains the ability of creating fake news, rumours and can destroy organization or individual’s reputation.

The use of social media in Vanuatu to infiltrate and abuse peoples’ personal privacy is also a critical issue. For example, posting pieces of information (images, snapshots of text messages, etc.) of a person without getting consents or approval do cause issues in communities, societies and even in organizations. Although the information posted can either be legitimate or not, it is a breach of one’s privacy. Other cases involve sharing of pornographic materials in closed and secret social media

groups and pages. It is becoming a trending issue in Vanuatu. In summary, social media in Vanuatu brings about the following issues and social media-enabled crimes such as:

- ❖ *Cyberbullying or Cyberstalking;*
- ❖ *Infiltrating online personal privacy;*
- ❖ *Shaming and spreading hate speech to entertain bigger issues;*
- ❖ *Having possession and/or sharing of pornographic materials;*
- ❖ *Sextortion and online abuse;*
- ❖ *Encouraging and spreading of fake news; and*
- ❖ *Data Leakage (Leaking sensitive information to the public)*

The above social media issues are based on reported cases. They are not directly associated with cyber-threats to Vanuatu but has an impact on the societies and communities in Vanuatu.

