Cyber Security Operations in an Island State

TLP: CLEAR

CERTVU Operations

By: Dr. Jeff G Liu
OGCIO & CERTVU Team
Outline

- Background
- The Problem
- The Strengths
- The Mandate
- The Incident Response Governance
- The Incident Response Structure
- Mechanism
- CERTVU Operations
- Setbacks
- Concluding Remarks
Acknowledgement
2016 / 2017 - Cybersecurity Policy Mandate to establish a CERT
Prior to CERTVU - Information Security Officer under OGCIO
Systems & Network Security tasks
SOC discussion
CERTVU - 19th June 2018
GBN Infrastructure spread across Vanuatu:
  - 6 Provinces
  - Submarine Cable & Towers
  - ISPs
  - 5000 + Users
Services to all
The Problem

- Geographic Disadvantages
- Lack of Resources
- Financial Constraints
- Absence of Legislation
- Lack of Political Will or Buy-in
- Time
- Infrastructure
- Vulnerabilities
- Low Cyber-literacy
The Problem

- Bulleted
- Lack of Resources
- Financial Constraints
- Absence of Legislation
- Lack of Political Will or Buy-in
- Time
- Infrastructure
- Vulnerabilities
- Low Cyber-literacy

Strengths

- Bulleted list
- Entity: CERTVU
- National ICT Policy 2013
- National Cyber Security Policy 2013
- Cybercrime Act No.22 of 2021
- National Cyber Security Strategy 2030
- GBN Infrastructure
- Political Will or Buy-in
The Mandate

- Incident Response

INCIDENT RESPONSE PLAN

Triage
- a) Assess impact
- b) Categorize incident
- c) Assign incident manager
- d) Check for false positive

Core Response
- Analyze
  - Capture and analyze data/information

Contain
- Stop or lower the impact, prevent spread of the problems
  - Consider the potential impact

Eradicate
- Fully remove/stop the incident, Conduct successful remediation

Recover
- Recover data and systems if needed. Resume ‘Business as usual’

Preparation
Detection & Analysis
Containment & Recovery
Post-Incident Activity
The Mandates

- Incident Response
- Provide Capacity Building and Awareness
**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
The Incident Response Governance Mechanism

Critical infrastructure:
- What?
- What is working, & What not working

Incident Response Team:
- Capabilities
- Willing to work
- Collaboration

Workflow:
- How tasks are done
- SOPs, Best Practices
- Communication

TLP: CLEAR
The Incident Response Structure

Planning & Preparation
- Notify NSO/PCIS
- Notify & Work with critical stakeholders

Detection
- Notify NCIC/IM
d

Triage
- Work with Vanuatu Police Force (VPF)

Respond
- Update TLP

Recovery
- Execute Incident Response Plan
- It is Business or Individual Incident
- Does it have Criminal Component?
CERTVU Operations

SANMA PROVINCE

TLP:CLEAR

Security Policies Handbook

The Office of the Government Chief Information Officer (OGCIO)

"A set of Security Policies, Guidelines and Requirements"
Setbacks

1. Time & Financial Constraints
2. Sophisticated Cyber-attacks
Concluding Remarks

TLP: CLEAR

Know Your Infrastructure & Threat Landscape

Communication is Key

"Logs are Gold"

Visibility: Systems and Network

Trust & Verify: Team Work

Standards, Regulations and Legislations