Cybersecurity maturity in the Pacific Islands | Integrating CERT services in a regional framework

Anthony Adams (Monash University, Australia)
Tony Adams

PhD Candidate
Department of Software Systems and Cybersecurity, Faculty of Information Technology
Monash University
Melbourne, Australia

anthony.adams@monash.edu.au
Twitter @tony_adams1969
LinkedIn https://www.linkedin.com/in/tonyadams1
Phone +614 0786 3600 (WhatsApp, Signal)
Contents

The Problem
Pacific Islands region
Research Scope
Conceptual Model (Initial)
Study One
Conceptual Model (Updated)
Implementation Approach
The Problem

What is the Problem to be addressed?
Who is impacted?
Why should it be addressed?
How does this research contribute to a solution?
What is the problem to be addressed?

Pacific Island nations do not use a coordinated regional approach to manage their cybersecurity threat responses.
Who is impacted?

- Pacific Islands nations
  - Governments
  - Residents
  - Communities
  - Companies
  - Universities
- Visitors to the region
  - Neighbouring governments
  - Visitors, tourists
  - Companies, partners
Why should it be addressed?

The lack of regional CERT framework creates two significant problems for the Pacific Islands region.
How does this research contribute to a solution?

Two key contributions to our understanding of how national CERT services can be delivered in the Pacific Islands region
Pacific Islands region

18 member nations of the Pacific Islands Forum

3 ethnic and cultural sub-regions (excluding Australia)
Research Scope

Research Aim
Research Questions
Research Objectives
Research Aims

Understand how nations prioritize and align cyber threat capabilities, within a multi-stakeholder regional CERT framework.
To meet these aims, this research addresses three questions:

1. How do Pacific Island national CERTs select cybersecurity threat response capabilities, within a regional framework?
2. How are these choices impacted by national drivers?
3. How are these choices impacted by regional approaches?
To address these questions, the research has four objectives.
Conceptual Model (Initial)

- Conceptual Foundation
- Initial Conceptual Model
- Theoretical Framework (CHAT)
- Updated Conceptual Model
The foundation for a regional CERT model has three pillars (Adams, 2020)

1. Form and function are determined by the participating national governments' domestic policy priorities.
2. National governments will place their domestic priorities above those of the regional framework.
3. National governments will work within a regional framework on issues of shared interest.
Three pillars

1. Form and function are determined by the participating national governments' domestic policy priorities.
2. National governments will place their domestic priorities above those of the regional framework.
3. National governments will work within a regional framework on issues of shared interest.

The foundation is enacted by four action-based drivers (Adams, 2020):

- **Network**: Affiliated, independent national CERTs
- **Capabilities**: Align to national interests; Collaborate on shared interest
- **Partners**: Provide support that targets national priorities
- **Support**: Internal governance, sound planning
Initial Conceptual Model

The initial Conceptual Model is built on the Conceptual Foundation.

It contains three key themes.

Global | Centralised CERT capability
- International behavioural norms
- Regional cooperation
- Institutional frameworks

Regional | Regional Framework
- Integration with regional bodies
- Decision making
- Remediation approach

National | National Drivers
- Architecture
- Internal governance
- Critical infrastructure
- Capability maturity
Initial Conceptual Model

The three themes are linked by enablers.

National Governance
- Determines how a national government will choose to engage with a global “best practice” approach to CERT delivery

CERT services
- Connects the national government’s policy approach and priorities with a regional community

Aligned CERTs
- National CERTs present their interests through a regional framework, using global institutions and practices
Initial Conceptual Model

**Limited research**
How do affiliated CERTs choose which functions to share, retain and ignore?

[Research Question 1]
CERT services

Regional Engagement
- Integration with regional bodies
- Remediation approach
- Decision making

[Research Question 3]
Relationship > Regional Framework, CERT services

[Research Question 2]
Relationship > National Drivers, CERT services

National Drivers
- Architecture
- Internal Governance
- Critical infrastructure
- Capability Maturity

Global CERT capability
- International norms
- Regional cooperation
- Institutional framework

Aligned CERTs

National Governance

Dependent concept - KNOWN

Relationship - UNKNOWN
Theoretical Framework

CHAT – 2\textsuperscript{nd} generation
Object 1 – the services that a national CERT will provide

Object 2 – the individual interests of a national CERT, reflected in a regional CERT

Object 3 – the shared interests of different participants, reflected in a regional CERT
Study One
Study One

10 participants

- Australia
- Switzerland
- Lithuania
- Bosnia
- APNIC
- USA – commercial
- USA – CERT/CC
- New Zealand
- Kiribati
- Malaysia
- Samoa
- Tonga

Goals
- To set the scene.
- To understand the current distribution of CERT services and capabilities in the Asia-Pacific region

Key Services
- Threat Detection
- Incident Response
- Forensic Analysis
- Advisories
- Community awareness

Key Themes
- Trust as an enabler of success
- People, not technology
- National CERTs – their role in raising community awareness
- National CERTs – support national priorities, areas of shared regional interest
- Partners – promoting increased national cyber resilience

Nov 2021 – Mar 2022
Conceptual Model (Updated)
Updated Conceptual Model

Study One highlights key elements of the Conceptual Model

Themes
- **Global** | CERT capability
  - International behavioural norms
- **Regional** | Regional Framework
  - Integration with regional bodies
- **National** | National Drivers
  - Capability maturity

Enablers
- National Governance
- CERT services

Challenges
- Fluidity, lack of resources
Updated Conceptual Model

Global CERT capability
- International norms
- Regional cooperation
- Institutional framework

Challenges
- Fluidity
- Limited resources

Government alignment

Regional Engagement
- Integration with regional bodies
- Remediation approach
- Decision making

National Drivers
- Architecture
- Internal Governance
- Critical infrastructure
- Capability Maturity

[Research Question 1] CERT services
[Research Question 2] Relationship > National Drivers, CERT services
[Research Question 3] Relationship > Regional Framework, CERT services
Updated Conceptual Model

National Governance [Tools and signs]

- Aligned CERT [Subject]
  - Research Question 1: Contradiction
- National Drivers [Rules]
- Regional Framework [Community]
- Global CERT capability [Division of labour]

CERT services [Object]

Contradiction

Research Question 2: Contradiction

Unclear blend of services [Outcome]

Research Question 3

Global CERT capability [Division of labour]
Implementation Approach
Implementation Approach

Literature Review

Initial
Conceptual Model (initial)

Updated
Conceptual Model (updated)

Case Studies 1-3 Pacific Island CERTs
Case Studies 4-5 Regional partners

Comparative analysis
Conceptual Model (final)

Study 1
Implementation Approach

**Deliverable: Initial Conceptual Framework**

- Critical Literature Review: Contemporary (post-2005)
- Study 1: Current state — CERT service mapping
  - Case Study 1: Pacific Islands CERT #1 - Melanesia
  - Case Study 2: Pacific Islands CERT #2 - Polynesia
  - Case Study 3: Pacific Islands CERT #3 - Micronesia
  - Case Study 4: Pacific Islands - regional partner #1
  - Case Study 5: Pacific Islands - regional partner #2

**Deliverable: Iterative updates to the conceptual framework**

**Deliverable: Conceptual Framework**

- Comparative Analysis: Conceptual framework

**Participants**: (1.) Members of national and sectoral CERTs across the Asia-Pacific region, and USA; (2.) Members of global non-government/private partners

**Methodology**: Qualitative
- Multiple comparative case studies
- Deductive analysis

**Structure**: Semi-structured interview

**Analysis**: Inductive analysis of content and semantic themes

**Participants**: Members of Pacific Island national CERTs
- One nation from each of the 3 sub-regions
- One SIS nation will be selected from Polynesia, Micronesia

**Participants**: Members of Pacific Island cybersecurity partners

**Participants**: (1.) Members of national and sectoral CERTs across the Asia-Pacific region, and USA; (2.) Members of global non-government/private partners

**Key**
- In Progress
- Complete
- Not Started
Tony Adams

PhD Candidate
Department of Software Systems and Cybersecurity, Faculty of Information Technology
Monash University
Melbourne, Australia

anthony.adams@monash.edu.au
Twitter @tony_adams1969
LinkedIn https://www.linkedin.com/in/tonyadams1
Phone +614 0786 3600 (WhatsApp, Signal)