COOK ISLANDS

CYBER SECURITY POLICY 2024

SOURCE: KIERAN SCOTT

CONTENTS

Page 4

MESSAGE FROM THE PRIME MINISTER

Page 6

INTRODUCTION

Page 8

CYBER SECURITY THREATSCAPE

Who is targeting the Cook Islands? 9

Who is targeted in the Cook Islands? 10

What global trends does the Cook Islands need to plan for? 11

Page 12

THE POLICY OUR CYBER SECURITY PILLARS

PILLAR 1 ONLINE HARM AND CYBERCRIME 13

PILLAR 2 OUR GOVERNMENT 14

PILLAR 3 OUR PEOPLE 15

PILLAR 4 CRITICAL NATIONAL INFRASTRUCTURE 16

Page 18

HOW WE WILL DELIVER OUR POLICY

Glossary 20

MESSAGE FROM THE PRIME MINISTER

Cyber security threats affect all Cook Islanders. This policy is about improving our cyber security resilience so we can better protect the Cook Islands now and into the future.

In developing this policy, we have heard about the impact of cybercrimes on Cook Islanders, their communities and Government. Cyber security risks are real, they are affecting us now, and we all have a part to play in strengthening cyber security.

We know our Government networks need to be more resilient to cyber threats. This policy channels several initiatives undertaken by the Cook Islands Government in 2024, which kick start our resilience planning. We have been engaging with international partners and making use of private sector expertise to determine the level of risk we face and the actions we need to take to mitigate these risks.

The policy upholds commitments made in the *Boe Declaration on Regional Security* by highlighting the priority we place on cyber security resilience domestically.

The objective of this policy is to improve cyber security resilience, capacity, and response within the Cook Islands.

Hon. Mark Brown
Prime Minister

INTRODUCTION

This policy is for everyone. Cyber security threats affect us all: children, the elderly, businesses, community groups, as well as the three pillars of Cook Islands society – traditional leaders, church, and Government. Building cyber resilience is also a shared responsibility. It cannot be achieved by one group alone.

What is cyber security?

Cyber security is about protecting Cook Islanders. It protects our people's personal information, our country's reputation, our Government's sensitive information, the infrastructure we rely on, our businesses, and our connections to the world. All information in the Cook Islands, including that online, has value and should be protected.

Why we have a cyber security policy

Having a cyber security policy:

- gives us an ongoing plan for protecting our cyber security needs
- communicates the intent of Government across domestic, regional, and wider international audiences
- forms part of the ongoing cooperation and consultation on national security-related issues with New Zealand and other partner countries
- aligns our cyber security work with the goals in *Te Ara Akapapa'anga Niu – National Sustainable Development Agenda (NSDA)* and related policies and strategies, including pillar 8 of our *National Security Policy 2023–2026*.

We are basing our cyber security policy in ka'a

The policy draws on research methodology of the *NSDA* ka'a, the braided sennit cord of the coconut. Braiding and knotting the ka'a require a careful selection of coconut husks and strands.

- Our policy must be braided into existing Cook Islands policies, including the *NSDA*.
- Our policy's fibres will be woven with knowledge, wisdom and guidance provided by Cook Islanders.

What we have heard in making this policy

People that contributed to this policy shared examples of a wide range of cyber and cyber-enabled harms to Cook Islanders. Cyber threats are real and are already impacting our communities and our businesses. This policy provides a pathway to help prepare, protect, and respond to the full range of anticipated cyber threats.

These include:

- online scams
- banking risks
- cyber bullying
- transnational crime links
- online extortion
- technology facilitated gender-based violence
- targeting of the Government computer networks.

How this fits in with existing national strategies

As we use information and communications technology (ICT) and new technologies to strengthen our connectedness with the world, increase efficiencies online, and enable economic prosperity, we must ensure we are managing any resulting risks as much as possible.

Our *National ICT Policy 2023–2027* and *National Digital Strategy 2024–2030* lay the foundations for these goals. This policy builds on this work, helping us to balance opportunities with risks and threats that come with a more digitally open position.

Most recently, the action plan for pillar 8 of the *National Security Policy 2023–2026* set out the need for a cyber security policy to protect individuals, Government and the private sector against cybercrime and other malicious cyber activities. The development and implementation of this cyber security policy is a key part of strengthening the Cook Islands' overall national resilience.

Informing this policy is a cyber security investment plan, which has helped us understand high priority actions that can make the most difference to our cyber security resilience.

How to use this policy

The threatscape (page 8) outlines the core risks and threats we need to consider.

The rest of the policy is focused around 4 pillars (page 12), which outline our objectives for building cyber resilience in relation to:

1. online harm and cybercrime
2. our Government
3. our people
4. critical national infrastructure.

Finally, our plans for delivery (page 18) brings together the most relevant actions identified in the above documents and the cyber security investment plan and outlines what should be done now, next year, and into the future.

CYBER SECURITY THREATSCAPE

The Cook Islands' online connections to the world brings cyber threats into our homes, workplaces, and community in a way that has no regard for the protection that our remoteness otherwise provides. Even within the nation, satellite broadband has brought modern internet, with all of its risks and benefits, to the Pa Enua.

Cyber security threats come from a wide range of malicious actors targeting an equally wide range of individuals and organisations. The unique factors that define our economy, our people, and our connections to the wider world help us identify how malicious actors may target us and why.

The similarities to our neighbours in the wider Pacific community help us understand, through their experiences, the threats we face.

Who is targeting the Cook Islands?

CYBER ATTACKS ON PACIFIC ISLANDS

In November 2022, Vanuatu's Government networks and significant services were disrupted for weeks. By December, a financially motivated ransomware gang claimed to have stolen a large number of files.

The extent of major cyber attacks in the Pacific continues to grow. For example, in February 2023, Tonga's state-owned telecommunication operator was struck by a ransomware attack, and in March 2024 the Government of Palau suffered a significant attack on its computer networks disrupting its Government payroll system.

There are many motivations for undertaking cyber attacks and cybercrimes. The attackers and criminals can be based anywhere in the world.

Financially motivated cybercriminals are often indiscriminate and see little distinction between potential victims beyond opportunity and potential returns. As a nation with a significant financial sector and modern telecommunications, the Cook Islands has not escaped the notice of cybercriminals. Those targeting the Cook Islands will be the same as those targeting other nations in the Pacific and wider online community. In the Cook Islands we will face threats that range from relatively unsophisticated scammers operating through social media, through to sophisticated transnational cybercrime syndicates that may seek to hold critical infrastructure to ransom.

The threat to the nation's cyber security from state actors must also not be ignored. All nations have sensitive information that others may want to access. Internal decision making, economic data and details of nations' foreign relations will continue to be of interest to other nations. We cannot assume our small size means we do not possess information that others seek.

It is also important not to overlook homegrown cybercriminals. Threats that may affect businesses and Government agencies can include 'insider threats', those seeking to cause disruption or commit fraud within organisations.

Who is targeted in the Cook Islands?

CYBERCRIME IN THE COOK ISLANDS

In 2022, customers of a local bank found illegitimate transactions made on their credit and debit cards after fraudsters undertook a bank identification number (BIN) attack. The fraudsters effectively guessed the account details of their victims by exploiting the way banks assign card numbers. BIN attacks are a global problem – the fraudsters behind these attacks constantly search for new targets and novel ways to avoid bank defences.

The threats from malicious actors faced by the Cook Islands are largely the same as those faced by the rest of the world. Simply put, every individual and organisation that is connected to the internet is a potential target for malicious actors.

International reporting of malicious cyber activity shows a growing level of harm affecting the wider Pacific community. A number of our Pacific neighbours have suffered significant disruption to their critical services as a result of ransomware. Ransomware attacks are often opportunistic with victims largely selected on the basis of vulnerabilities within their systems. In this way critical infrastructure in the Cook Islands is as much a target as infrastructure in other nations.

Any organisations that holds sensitive and private data can be a target for malicious actors. Data and information can be valuable in many ways. Criminal groups and state actors may illegally harvest data to gain information to help them commit financial fraud, extort data owners with the threat of disclosure or to support espionage.

Even where the Cook Islands are not a direct target, we may still be affected. In an interconnected world the devices and networks that we use can be harnessed by cybercriminals and state actors for their own purposes. Some of the simplest internet connected devices, such as security cameras, have been used to power global cyberattacks. Other compromised computer and networked systems have been used as proxies for sophisticated actors to undertake cybercrime and espionage and hide their true locations.

At an individual level, people's information, data and devices are of high interest to malicious actors. While everyone who is online may be a target of scams and financial fraud, people's offline problems may also follow them online. Family harm and abusive relationships can often be made worse by offenders using the internet to harass or stalk their victims. Personal information that has been carelessly shared on social media can also be used by offenders to enable physical, emotional or financial abuse. As more of our lives become intertwined with the digital world, our domestic and community life become reliant on people staying safe and secure online.

What global trends does the Cook Islands need to plan for?

As part of the global internet, the Cook Islands is experiencing similar changes in the cyber security threat landscape as other nations. The global threat landscape changes constantly and there are many drivers of change. While some changes relate to technology, such as developments in artificial intelligence and quantum computing, others relate to malicious actors seeking new ways to exploit vulnerabilities.

Four major global trends have been observed during the development of this policy.

THE INCREASING PROFESSIONALISATION OF CYBERCRIME

Major cybercrime campaigns often occur through multiple criminal groups collaborating and sharing services. More groups can access high-end skills, and scams are being undertaken on an industrial scale. In the Cook Islands, these scams impact the vulnerable in our communities the most, in particular through the use of social media.

MORE FREQUENT ATTACKS ON SOFTWARE SUPPLY CHAINS

Cybercriminals and state espionage groups are using and sometimes creating vulnerabilities in critical software. Managing computer networks will require not only protecting networks against direct attacks, but preparing for attacks on hardware and software suppliers.

FASTER EXPLOITATION OF VULNERABILITIES

The time taken between discovery of a vulnerability and its mass exploitation has shortened. This places further burden on those administering computer networks as there is less time to respond.

CYBER ATTACKS ARE INCREASINGLY PART OF WIDER MALICIOUS CAMPAIGNS

Cyber attacks are a business-as-usual part of malicious campaigns such as disinformation and military aggression. The use of cyber attacks to support a wide range of malicious activity makes cyber security an increasingly important part of broader national security.

SOURCE: COOK ISLANDS TOURISM

THE POLICY OUR CYBER SECURITY PILLARS

4 key pillars work together to secure cyber resilience for all Cook Islanders

PILLAR 1 ONLINE HARM AND CYBERCRIME

Objectives

People will have access to the knowledge and skills to stay safe online and know where to go to report cybercrimes.

Legislation will allow for the effective investigation, prosecution and deterrence of cybercrime within the Cook Islands.

Current state

Cook Islanders are increasingly targeted by criminals online. As use of the internet continues to increase, more people are exposed to increasing amounts of harmful content online.

Current support for getting help, both to stay safe and respond to incidents, needs to evolve to match growing demand. Cook Islanders need access to reliable information and advice on how to prevent and respond to online harm.

Government agencies and institutions need to have the right tools and powers to protect the community and to help them recover when harm is caused. Legislation needs to be relevant and able to address the issues that are being faced by internet users. It must be robust enough to cope with the changing technological environment and able to be easily amended when required.

Targets and actions

- Improve cybersecurity and cybercrime legislation. (NSP PAF[1] 8.2)
- Upgrade law enforcement agencies' digital crime detection systems, including those relating to objectionable content. (NSP PAF 8.2)
- Establish a Cook Islands Computer Emergency Response Team. (NSP PAF 8.4)
- Explore opportunities for gaining access to additional support from international partners for addressing cybercrime. (NSP PAF 8.5)
- Explore opportunities to become a party to the Budapest Convention on Cybercrime and other treaties. (NSP PAF 8.5)

WHAT WE HEARD ABOUT SCAMS

During consultation on this policy, a story that was heard too many times was how people had suffered financial losses in the tens of thousands of dollars to online scams. Alongside the impact this had on people financially, the psychological impact of these scams, including shame and embarrassment, was extreme. Sharing these stories is important in raising awareness of scams, but also in helping victims understand support is available.

[1] National Security Policy Performance Assessment Framework (NSP PAF)

PILLAR 2 OUR GOVERNMENT

Objectives

Government defences will be strengthened to keep our sensitive information safe and secure.

The people of the Cook Islands and their institutions will have the capability to protect themselves from online harms and cybercrime.

Current state

The Government's computer networks and systems are critical for maintaining and delivering the services that the people of the Cook Islands depend on to go about their daily lives.

The Government faces many of the same cyber security risks and barriers faced by nations across the globe and by domestic organisations.

Issues include:

- recruiting, upskilling and retaining the right people and having the right skills to manage cyber security risks
- managing the risks of legacy ICT systems and challenges of modernising infrastructure
- preparing to respond to cyber security incidents, including establishing the right relationships with those who can assist in times of need
- improving the efficiency and effectiveness of the procurement of Government ICT while managing cyber risks related to Government ICT.

Targets and actions

- Develop guidelines for assessing cyber security risks in Government procurement and acquisition of technology and hardware.
- Enable Government-wide purchasing decisions on secure and resilience technology.
- Integrate assessment of cyber security risks into security and disaster planning.
- Develop a cyber security emergency response plan.
- Establish methods for reporting and data collection on cyber security risks and incidents within Government.
- Advocate for increased caucusing on regional cyber issues.
- Explore the use of the National Security Committee to take strategic decisions on cyber issues.
- Protect access to our security related information through the protective security requirements framework. (NSP PAF 1.6)
- Develop a cybersecurity prevention plan leveraging support of regional partnerships, such as the Cyber Safety Pacifica program and Get Safe Online Cook Islands.

PILLAR 3
OUR PEOPLE

Objectives

All our working professionals, whether in Government, private companies and businesses, non-governmental organisations (NGOs), and the ICT sector, will be empowered to protect themselves online. Likewise, people in all parts of society need the skills and knowledge to keep themselves and their families safe.

We must work to retain cyber professionals in the Cook Islands and train people. We must also ensure that the next generation of cyber warriors are ready for the cyber challenges that will come with advances in technologies. We must actively identify these people and encourage cyber security tertiary qualifications and remunerate them well.

Current state

- Training exists but is limited and often oversubscribed. There are limited training providers in the Cook Islands. Repetition of training is required but resource limitations prevent this from occurring regularly.
- Building local capacity is a priority, but it can be difficult to enable.
- Limited regional ICT fora or perspective.
- Limited regional research into cyber issues, meaning it can be difficult to understand the extent of cyber challenges in the region and the specific effects these have on Pacific countries.

Targets and actions

- Build on existing cybercrime prevention initiatives through strengthening awareness campaigns to upskill communities, including Cook Islands cyber security stories.
- Establish strong regional and international connections so we can access expertise when required.
- Encourage cyber security tertiary qualifications and establish study and career pathways in cyber. (*National ICT Policy* 9.3.4)
- Upskill our Government workers through secondments and training for Government staff, including partnering with the New Zealand Government in the first instance.
- Develop interventions to encourage retention of ICT professionals. (*National ICT Policy* 9.3.4)

PILLAR 4 CRITICAL NATIONAL INFRASTRUCTURE

Objective

Our most important infrastructure will be protected from cyber harms to ensure the services the nation relies on are not disrupted.

Current state

We are concerned about the potential effects of a large-scale cyber compromise on core infrastructure including our connections to the wider world, and flow-on impacts on the economy and critical services.

Critical infrastructure providers often do not bear the full risk of their decisions – which can sometimes be borne by their customers and Government. We need to balance the cost of doing business with the costs that disruptions can impose on the nation as a whole.

An increasing number of systems in the Cook Islands are monitored or supported by offshore providers. This can deliver efficiencies and resilience but can introduce new risks and vulnerabilities. We need to ensure we are properly managing these efficiencies and risks.

Targets and actions

- Develop guidelines and tools for assessing cyber security risks in critical infrastructure.
- Conduct a comprehensive cyber risk assessment for the port, airport, and other critical infrastructure to proactively reveal cyber gaps and issues.
- Consider minimum standards and guidelines for critical infrastructure providers (such as reporting criteria for cyber security incidents).
- Include cyber resilience requirements in service-level agreements with critical infrastructure providers and their key suppliers.
- Assess risks, benefits, and mitigations of offshore data storage and control of automated systems.

SOURCE: MINISTRY OF FOREIGN AFFAIRS AND IMMIGRATION

SOURCE: DANIEL FISHER

HOW WE WILL DELIVER OUR POLICY

This section brings together key documents and actions on cyber security and explores a prioritised pathway to cyber resilience.

The actions identified in this policy's 4 pillars make up the wider action plan for improving national cyber security and resilience.

A *Cyber Investment Plan Roadmap* was developed for the Cook Islands by a private contractor earlier in 2024. This plan will help guide initial investment by the Cook Islands Government to build capability and resilience within national institutions and critical national infrastructure.

Further information on existing priorities for improving cyber security in the Cook Islands are detailed in pillar 8 of the *Cook Islands National Security Policy Performance Assessment Framework.*

Short-term priorities

In the first two years of this policy, we will focus on areas where rapid action is required to address critical risks or enable further work.

- Implement the *Cyber Investment Plan Roadmap.* (Enables this cyber security policy)
- Improve cyber security and cybercrime legislation. (NSP PAF 8.2)
- Establish a national cyber emergency response team (CERT) for implementation in 2025–2026. (NSP PAF 8.2)
- Explore opportunities for gaining access to additional support from international partners for addressing cybercrime. (NSP PAF 8.5)
- Develop a cyber security emergency response plan.

Medium-term priorities

We will focus on strengthening resilience.

- Build on existing cybercrime prevention initiatives through strengthening awareness campaigns to upskill communities, including Cook Islands cyber security stories.
- Explore opportunities for the Cook Islands to become a party to the Budapest Convention on Cybercrime and other treaties. (NSP PAF 8.2)
- Complete actions identified in pillar 4, critical national infrastructure.

Long-term priorities

We will focus on actions that depend on completion of the short-term and medium-term priorities.

- Complete actions identified in pillar 3, our people, to upskill and retain ICT capacity.

Glossary

Critical infrastructure, critical national infrastructure

Physical and digital assets, services, and supply chains, where disruption would severely impact the maintenance of national security, law and order, economic activity and public safety.

Cyber attack

A malicious act that attempts to collect, disrupt, deny, degrade, or destroy an ICT system or its data.

Cyber incident, cyber security incident

An event, whether intentional or not, that causes adverse consequences to an ICT system or its data.

Cyber resilience

The ability to anticipate, withstand, recover from, and adapt to cyber incidents and attacks.

Cyber security

Protecting people and their computers, networks, programs and data from cyber attacks.

Cybercrime

Crimes that are committed through the use of computer systems and are directed at computer systems. Examples include producing malicious software, denial of service attacks, and phishing.

Cyber-enabled crime

Crimes that are assisted, facilitated or escalated in scale by the use of technology. Examples are online scams and fraud and the online distribution of child exploitation material.

Cyberspace

The internet and everything connected to it – the global network of interdependent information systems, telecommunications networks and systems with embedded ICT.

Ransomware

A type of malicious software that locks up the files on an information system until a ransom is paid.

Acronyms

BIN – bank identification number

ICT – information and communications technology

Technologies and equipment that handle (for example access, create, collect, store, transmit, receive, disseminate) information and communication, associated devices, services and applications and their governance.

NGO – non-governmental organisation

NSDA – National Sustainable Development Agenda

Te Ara Akapapa'anga Niu – National Sustainable Development Agenda (NSDA)

NSP – National Security Policy

Cook Islands National Security Policy 2023–2026

NSP PAF – National Security Policy Performance Assessment Framework

SOURCE: OFFICE OF THE PRIME MINISTER